DECRETO N. 944 DEL 25/10/2022
DEL DIRETTORE GENERALE

OGGETTO: ATTUAZIONE DELLE REGOLE PREVISTE DAL "CODICE DELL'AMMINISTRAZIONE DIGITALE" E DALLE LINEE GUIDA AGID: AGGIORNAMENTO DEL MANUALE DI GESTIONE DOCUMENTALE E ADOZIONE DEL MANUALE DI CONSERVAZIONE .

copia informatica per consultazione

IL DIRETTORE GENERALE

RICHIAMATI:

- il Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, recante "*Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa*" (TUDA) e successive modificazioni e integrazioni;
- in particolare l'art 1 del citato D.P.R.n.445/2000 che definisce la "gestione dei documenti" come "*l'insieme delle attività finalizzate alla registrazione di protocollo e alla classificazione, organizzazione, assegnazione e reperimento dei documenti amministrativi formati o acquisiti dalle amministrazioni, nell'ambito del sistema di classificazione d'archivio adottato*";
- il Decreto Legislativo 7 marzo 2005, n. 82, recante "*Codice dell'amministrazione digitale*" e successive modificazioni ed integrazioni;
- le *Linee Guida sulla formazione, gestione e conservazione dei documenti informatici*, adottate dall'Agenzia per l'Italia Digitale con Determinazione 9 settembre 2020, n. 407 e successivamente modificate con Determinazione 17 maggio 2021, n. 371, che realizzano un unicum normativo per la formazione, gestione e conservazione dei documenti informatici, identificandone ruoli e responsabilità;

CONSIDERATO che, ai sensi dei paragrafi 3 e 4 delle suddette Linee Guida, l'Amministrazione è tenuta ad adottare, per ogni area organizzativa omogenea, un manuale di gestione documentale redatto su proposta del responsabile della gestione documentale ed un manuale di conservazione predisposto dal responsabile della conservazione, che ne cura l'aggiornamento periodico in presenza di cambiamenti normativi, organizzativi, procedurali o tecnologici rilevanti;

DATO ATTO che l'ASST di Mantova ha ritenuto di individuare al proprio interno un'unica Area Organizzativa Omogenea (AOO), ai sensi dell'art.50, comma 4 del TUDA;

PRESA VISIONE dell'assetto del sistema di gestione documentale in atto in Azienda:
- con Decreto n. 549 del 23.06.2022 è stato nominato il responsabile della conservazione dei documenti informatici dell'ASST di Mantova;
- con Decreto n. 1496 del 28.12.2021 è stato nominato il responsabile della gestione documentale dell'ASST di Mantova;
- con Decreto n. 213 del 19.02.2021 è stato nominato il responsabile della Transizione Digitale dell'ASST di Mantova;
- con Deliberazione dell'ex A.O. "C. Poma" n.1081 del 6.10.2015 è stato approvato il manuale di gestione documentale aziendale;
- Regione Lombardia ha fornito un sistema unico di conservazione digitale a norma a favore degli enti sanitari e amministrativi dislocati sul territorio e, a seguito di specifica gara, ha affidato il relativo servizio alla società ARUBA, gara a cui questa Azienda ha aderito, e sottoscritto con ARUBA il contratto;

RAVVISATA la necessità di aggiornare il vigente manuale di gestione documentale aziendale adottato con Deliberazione n.1081/2015, vista l'evoluzione della legislazione in materia di gestione documentale e di digitalizzazione della Pubblica Amministrazione;

copia informatica per consultazione

RITENUTO opportuno procedere all'emissione di un nuovo manuale di gestione documentale in sostituzione del precedente e all'adozione del manuale di conservazione, in ottemperanza a quanto previsto dalle nuove linee Agid, entrate in vigore dal 01.01.2022;

VISTI gli schemi di manuale di gestione documentale e di manuale di conservazione redatti, rispettivamente, ai sensi del paragrafo 3.4, secondo capoverso e del paragrafo 4.5, sesto capoverso, lettera *m*), delle *Linee Guida sulla formazione, gestione e conservazione dei documenti informatici*;

EVIDENZIATO, altresì, che il Manuale della gestione documentale è completato dai seguenti documenti:

- Nomina del responsabile della gestione documentale, del responsabile della conservazione, del responsabile per la transizione digitale e del responsabile dei sistemi informativi;
- Titolario di classificazione e massimario di scarto della documentazione del Sistema Sociosanitario Lombardo;
- Piano per la sicurezza informatica;
- Regolamento di accesso agli atti;
- Manuale di conservazione dell'ASST;
- Manuale di conservazione del conservatore;

PRESO ATTO dell'attestazione di regolarità e di legittimità del presente provvedimento espressa da CANINO PIERO Dirigente della Struttura AFFARI GENERALI E CONTROLLI INTERNI, e da CANINO PIERO, responsabile del procedimento;

DATO ATTO che il presente provvedimento non comporta oneri o proventi a carico dell'Azienda;

ACQUISITI i pareri del Direttore Amministrativo, del Direttore Sanitario e del Direttore Socio Sanitario;

DECRETA

1. di adottare il *Manuale di Gestione Documentale dell'ASST di Mantova*, allegato al presente provvedimento per farne parte integrante e sostanziale, completato dai seguenti documenti:

- Nomina del responsabile della gestione documentale, del responsabile della conservazione, del responsabile per la transizione digitale e del responsabile dei sistemi informativi;
- Titolario di classificazione e massimario di scarto della documentazione del Sistema Sociosanitario Lombardo;
- Piano per la sicurezza informatica;
- Regolamento di accesso agli atti;
- Manuale di conservazione dell'ASST;

copia informatica per consultazione

- Manuale di conservazione del conservatore;

2. di precisare che il *Manuale di Gestione Documentale* che qui si approva sostituisce integralmente il precedente Manuale adottato con deliberazione dell'ex A.O. "C. Poma" n.1081 del 6.10.2015;

3. di adottare il *Manuale di Conservazione dell'ASST di Mantova*, che si allega al presente provvedimento quale parte integrante e sostanziale;

4. di precisare che il Manuale di Gestione Documentale e il Manuale di Conservazione sono stati redatti in conformità a quanto previsto dalle " *Linee Guida sulla formazione, gestione e conservazione dei documenti informatici"*, adottate dall'Agenzia per l'Italia Digitale con Determinazione 9 settembre 2020, n. 407 e s.m.i. ed entrate in vigore dal 01.01.2022;

5. di disporre la pubblicazione dei Manuali di cui ai punti 1 e 3 sul sito istituzionale dell'ASST di Mantova nella sezione "Amministrazione Trasparente";

6. di pubblicare il presente provvedimento all'Albo on line sul sito istituzionale aziendale, ai sensi dell'art. 32 della L. n. 69/2009 e dell'art. 17 della L.R. 33/2009, nel rispetto del Regolamento UE 2016/679.

PRESO ATTO dei pareri di

DIRETTORE AMMINISTRATIVO	FERRARI GIUSEPPE
DIRETTORE SANITARIO	MALINGHER ALESSANDRO
DIRETTORE SOCIOSANITARIO	BOSCAINI RENZO

DIRETTORE GENERALE
AZZI MARA
(atto firmato digitalmente ai sensi
delle vigenti disposizioni di legge)

copia informatica per consultazione

ASST Mantova

Manuale di Gestione Documentale

Redatto dal Responsabile della Gestione Documentale dell'Azienda Socio Sanitaria Territoriale di Mantova

Azione	Data	Nominativo	Funzione
Redazione		Piero Canino	Responsabile della gestione documentale
Verifica		Paolo Garbossa	Responsabile della conservazione Responsabile della transizione digitale
Approvazione		Mara Azzi	Direttore Generale

Registro delle versioni

N°Ver/Rev/Bozza	Data emissione	Modifiche apportate	Osservazioni
Rev.1	06/10/2022	Adeguamento LLGG AgiD	

copia informatica per consultazione

Indice

copia informatica per consultazione

copia informatica per consultazione

copia informatica per consultazione

1 Principi Generali

1.1 Premessa

Il manuale di gestione documentale descrive il sistema di gestione informatica dei documenti e fornisce le istruzioni per il corretto funzionamento del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi. In coerenza con quanto indicato da AgID nelle Linee Guida sulla formazione, gestione e conservazione dei documenti informatici "nel manuale di gestione documentale sono riportati, in particolare:

1. relativamente agli aspetti organizzativi:
    a. le modalità di utilizzo degli strumenti informatici per la formazione dei documenti informatici e per lo scambio degli stessi all'interno ed all'esterno dell'Area Organizzativa Omogenea (AOO), applicando le modalità di trasmissione indicate nell'allegato 6 delle Linee Guida sulla formazione, gestione e conservazione dei documenti informatici "Comunicazione tra AOO di Documenti Amministrativi Protocollati";
    b. l'indicazione delle unità organizzative responsabili (UOR) delle attività di registrazione di protocollo e di archiviazione dei documenti all'interno dell'AOO;
    c. l'indicazione delle regole di assegnazione dei documenti ricevuti con la specifica dei criteri per l'ulteriore eventuale inoltro dei documenti verso AOO della stessa amministrazione o verso altre amministrazioni;
    d. i criteri e le modalità per il rilascio delle abilitazioni di accesso, interno ed esterno all'Amministrazione, al sistema di gestione informatica dei documenti;
2. relativamente ai formati dei documenti:
    a. l'individuazione dei formati utilizzati per la formazione del documento informatico, tra quelli indicati nell'Allegato 2 delle Linee Guida sulla formazione, gestione e conservazione dei documenti informatici "Formati di file e riversamento";
    b. la descrizione di eventuali ulteriori formati utilizzati per la formazione di documenti in relazione a specifici contesti operativi che non sono individuati nell'Allegato 2 delle Linee Guida sulla formazione, gestione e conservazione dei documenti informatici "Formati di file e riversamento";
    c. le procedure per la valutazione periodica di interoperabilità dei formati e per le procedure di riversamento previste nell'Allegato 2 delle Linee Guida sulla formazione, gestione e conservazione dei documenti informatici "Formati di file e riversamento";
3. relativamente al protocollo informatico e alle registrazioni particolari:
    a. le modalità di registrazione delle informazioni annullate o modificate nell'ambito delle attività di registrazione;
    b. la descrizione completa e puntuale delle modalità di utilizzo della componente «sistema di protocollo informatico» del sistema di gestione informatica dei documenti;
    c. le modalità di utilizzo del registro di emergenza ai sensi dell'art. 63 del TUDA, inclusa la funzione di recupero dei dati protocollati manualmente;
    d. l'elenco dei documenti esclusi dalla registrazione di protocollo, per cui è prevista registrazione particolare ai sensi dell'art. 53, comma 5, del TUDA;

copia informatica per consultazione

   e. determinazione dei metadati da associare ai documenti soggetti a registrazione particolare individuati, assicurando almeno quelli obbligatori previsti per il documento informatico dall'Allegato 5 alle Linee Guida;
   f. i registri particolari individuati per la gestione del trattamento delle registrazioni particolari informatiche anche associati ad aree organizzative omogenee definite dall'amministrazione sull'intera struttura organizzativa e gli albi, gli elenchi e ogni raccolta di dati concernente stati, qualità personali e fatti, riconosciuti da una norma;
4. relativamente alle azioni di classificazione e selezione:
   a. il piano di classificazione adottato dall'Amministrazione, con l'indicazione delle modalità di aggiornamento, integrato con le informazioni relative ai tempi, ai criteri e alle regole di selezione e conservazione, con riferimento alle procedure di scarto;
5. relativamente alla formazione delle aggregazioni documentali
   a. le modalità di formazione, gestione e archiviazione dei fascicoli informatici e delle aggregazioni documentali informatiche con l'insieme minimo dei metadati ad essi associati;
6. relativamente ai flussi di lavorazione dei documenti in uso:
   a. la descrizione dei flussi di lavorazione interni all'Amministrazione, anche mediante la rappresentazione formale dei processi attraverso l'uso dei linguaggi indicati da AgID, applicati per la gestione dei documenti ricevuti, inviati o ad uso interno;
7. relativamente alla organizzazione dei documenti informatici, dei fascicoli informatici e delle serie informatiche:
   a. la definizione della struttura dell'archivio all'interno del sistema di gestione informatica dei documenti. L'archivio informatico - formato ai sensi del capo IV "Sistema di gestione informatica dei documenti" del DPR 445/2000 - deve essere progettato in modo da assicurare certezza e trasparenza all'attività giuridico amministrativa;
8. relativamente alle misure di sicurezza e protezione dei dati personali adottate:
   a. le opportune misure tecniche e organizzative per garantire un livello di sicurezza adeguato al rischio anche in materia di protezione dei dati personali;
9. relativamente alla conservazione:
   a. per le Pubbliche Amministrazioni il piano di conservazione è allegato al manuale di gestione documentale, con l'indicazione dei tempi entro i quali le diverse tipologie di oggetti digitali devono essere trasferite in conservazione ed eventualmente scartate; "

Ad integrazione delle informazioni contenute nel presente Manuale, sono allegati i seguenti documenti:

- Delibera di approvazione del Manuale
- Delibere di nomina dei Responsabili di cui al paragrafo 2.3
- Piano di classificazione/Titolario
- Piano per la sicurezza informatica
- Regolamento per accesso agli atti
- Manuale di conservazione dell'ASST
- Manuale di conservazione del conservatore

copia informatica per consultazione

Il Manuale del sistema di protocollo informatico è disponibile per gli utenti dell'Azienda, esclusivamente per uso interno.

La Pubblica Amministrazione è tenuta a redigere, adottare con provvedimento formale e pubblicare sul proprio sito istituzionale il Manuale di gestione documentale. La pubblicazione è realizzata in una parte chiaramente identificabile dell'area "Amministrazione trasparente" prevista dall'art. 9 del d.lgs. 33/2013.

Torna al sommario

1.2 Ambito di applicazione del manuale

Il presente Manuale di Gestione Documentale è adottato secondo le Linee Guida AgID sulla formazione, gestione e conservazione dei documenti informatici.

Esso descrive:

- La formazione, registrazione, classificazione, fascicolazione ed archiviazione dei documenti amministrativi, oltre alla gestione dei flussi documentali ed archivistici in relazione ai procedimenti amministrativi della AOO.
- La formazione e gestione dei documenti clinici generati dalla ASST.

Torna al sommario

1.3 Terminologia (Glossario dei termini e degli Acronimi)

Di seguito si riporta la tabella contenente in ordine alfabetico il Glossario dei termini e degli Acronimi ritenuti di particolare importanza.

Glossario dei Termini	
Accesso	Operazione che consente di prendere visione dei documenti informatici.
Affidabilità	Caratteristica che, con riferimento a un sistema di gestione documentale o conservazione, esprime il livello di fiducia che l'utente ripone nel sistema stesso, mentre con riferimento al documento informatico esprime la credibilità e l'accuratezza della rappresentazione di atti e fatti in esso contenuta.
Aggregazione documentale informatica	Insieme di documenti informatici o insieme di fascicoli informatici riuniti per caratteristiche omogenee, in relazione alla natura e alla forma dei documenti o in relazione all'oggetto e alla materia o in relazione alle funzioni dell'ente.
Archivio	Complesso dei documenti prodotti o acquisiti da un soggetto pubblico o privato durante lo svolgimento della propria attività.
Archivio informatico	Archivio costituito da documenti informatici, organizzati in aggregazioni documentali informatiche.
Area Organizzativa Omogenea	Un insieme di funzioni e di uffici individuati dall'ente al fine di gestire i documenti in modo unitario e coordinato, secondo quanto disposto dall'art. 50 comma 4 del D.P.R. 28 dicembre 2000, n. 445. Essa rappresenta il canale ufficiale per l'invio di istanze e l'avvio di procedimenti amministrativi.
Attestazione di conformità delle copie per immagine su supporto informatico di un documento analogico	Dichiarazione rilasciata da notaio o altro pubblico ufficiale a ciò autorizzato allegata o asseverata al documento informatico.
Autenticità	Caratteristica in virtù della quale un oggetto deve considerarsi come corrispondente a ciò che era nel momento originario della sua produzione. Pertanto un oggetto è

copia informatica per consultazione

	autentico se nel contempo è integro e completo, non avendo subito nel corso del tempo o dello spazio alcuna modifica non autorizzata. L'autenticità è valutata sulla base di precise evidenze.
Certificazione	Attestazione di terza parte relativa alla conformità ai requisiti specificati di prodotti, processi, persone e sistemi.
Classificazione	Attività di organizzazione di tutti i documenti secondo uno schema costituito da un insieme di voci articolate in modo gerarchico e che individuano, in astratto, le funzioni, competenze, attività e/o materie del soggetto produttore.
Codec	Algoritmo di codifica e decodifica che consente di generare flussi binari, eventualmente imbustarli in un file o in un wrapper (codifica), così come di estrarli da esso (decodifica).
Conservatore	Soggetto pubblico o privato che svolge attività di conservazione dei documenti informatici.
Conservazione	Insieme delle attività finalizzate a definire ed attuare le politiche complessive del sistema di conservazione e a governarne la gestione in relazione al modello organizzativo adottato, garantendo nel tempo le caratteristiche di autenticità, integrità, leggibilità, reperibilità dei documenti
Coordinatore della Gestione Documentale	Soggetto responsabile della definizione di criteri uniformi di classificazione ed archiviazione nonché di comunicazione interna tra le AOO ai sensi di quanto disposto dall'articolo 50 comma 4 del DPR 445/2000 nei casi di amministrazioni che abbiano istituito più AOO.
Documento amministrativo informatico	Ogni rappresentazione, grafica, fotocinematografica, elettromagnetica o di qualunque altra specie, del contenuto di atti, anche interni, formati dalle pubbliche amministrazioni, o, comunque, da queste ultime utilizzati ai fini dell'attività amministrativa
Documento elettronico	Qualsiasi contenuto conservato in forma elettronica, in particolare testo o registrazione sonora, visiva o audiovisiva
Documento informatico	Documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti
Esibizione	operazione che consente di visualizzare un documento conservato
Estrazione statica dei dati	Estrazione di informazioni utili da grandi quantità di dati (es. database, datawarehouse ecc...), attraverso metodi automatici o semi-automatici
Evidenza informatica	Sequenza finita di bit che può essere elaborata da una procedura informatica.
Fascicolo informatico	Aggregazione documentale informatica strutturata e univocamente identificata contenente atti, documenti o dati informatici prodotti e funzionali all'esercizio di una attività o allo svolgimento di uno specifico procedimento.
File	Insieme di informazioni, dati o comandi logicamente correlati, raccolti sotto un unico nome e registrati, per mezzo di un programma di elaborazione o di scrittura, nella memoria di un computer.
Filesystem	Sistema di gestione dei file, strutturato mediante una o più gerarchie ad albero, che determina le modalità di assegnazione dei nomi, memorizzazione e organizzazione all'interno di uno storage.
Firma elettronica	Vedi articolo 3 del Regolamento eIDAS.
Firma elettronica avanzata	Vedi articoli 3 e 26 del Regolamento eIDAS.
Firma elettronica qualificata	Vedi articolo 3 del Regolamento eIDAS.
Formato contenitore	Formato di file progettato per consentire l'inclusione ("imbustamento" o wrapping), in uno stesso file, di una o più evidenze informatiche soggette a differenti tipi di codifica e al quale possono essere associati specifici metadati.
Formato del documento informatico	Modalità di rappresentazione della sequenza di bit che costituiscono il documento informatico; comunemente è identificato attraverso l'estensione del file.
Formato "deprecato"	Formato in passato considerato ufficiale il cui uso è attualmente sconsigliato a favore di una versione più recente.
Funzioni aggiuntive del protocollo informatico	Nel sistema di protocollo informatico, componenti supplementari rispetto a quelle minime, necessarie alla gestione dei flussi documentali, alla conservazione dei documenti nonché alla accessibilità delle informazioni.
Funzioni minime del	Componenti del sistema di protocollo informatico che rispettano i requisiti di

copia informatica per consultazione

protocollo informatico	operazioni ed informazioni minime di cui all'articolo 56 del D.P.R. 28 dicembre 2000, n. 445.
Funzione di hash crittografica	Funzione matematica che genera, a partire da una evidenza informatica, una impronta crittografica o digest (vedi) in modo tale che risulti computazionalmente difficile (di fatto impossibile), a partire da questa, ricostruire l'evidenza informatica originaria e generare impronte uguali a partire da evidenze informatiche differenti.
Gestione Documentale	Processo finalizzato al controllo efficiente e sistematico della produzione, ricezione, tenuta, uso, selezione e conservazione dei documenti.
hash	Termine inglese usato, impropriamente, come sinonimo d'uso di "impronta crittografica" o "digest" (vedi).
Identificativo univoco	Sequenza di numeri o caratteri alfanumerici associata in modo univoco e persistente ad un'entità all'interno di uno specifico ambito di applicazione.
Impronta crittografica	Sequenza di bit di lunghezza predefinita, risultato dell'applicazione di una funzione di hash crittografica a un'evidenza informatica.
Integrità	Caratteristica di un documento informatico o di un'aggregazione documentale in virtù della quale risulta che essi non hanno subito nel tempo e nello spazio alcuna alterazione non autorizzata. La caratteristica dell'integrità, insieme a quella della completezza, concorre a determinare la caratteristica dell'autenticità.
Interoperabilità	Caratteristica di un sistema informativo, le cui interfacce sono pubbliche e aperte, e capaci di interagire in maniera automatica con altri sistemi informativi per lo scambio di informazioni e l'erogazione di servizi.
Leggibilità	Caratteristica di un documento informatico che garantisce la qualità di poter essere decodificato e interpretato da un'applicazione informatica.
Manuale di conservazione	Documento informatico che descrive il sistema di conservazione e illustra dettagliatamente l'organizzazione, i soggetti coinvolti e i ruoli svolti dagli stessi, il modello di funzionamento, la descrizione del processo, la descrizione delle architetture e delle infrastrutture.
Manuale di gestione	Documento informatico che descrive il sistema di gestione, anche ai fini della conservazione, dei documenti informatici e fornisce le istruzioni per il corretto funzionamento del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi.
Metadati	Dati associati a un o documento informatico, a un fascicolo informatico o a un'aggregazione documentale per identificarli, descrivendone il contesto, il contenuto e la struttura - così da permetterne la gestione del tempo - in conformità a quanto definito nella norma ISO 15489-1:2016 e più nello specifico dalla norma ISO 23081-1:2017.
Oggetto di conservazione	Oggetto digitale versato in un sistema di conservazione.
Oggetto digitale	Oggetto informativo digitale, che può assumere varie forme tra le quali quelle di documento informatico, fascicolo informatico, aggregazione documentale informatica o archivio informatico.
Pacchetto di archiviazione	Pacchetto informativo generato dalla trasformazione di uno o più pacchetti di versamento coerentemente con le modalità riportate nel manuale di conservazione.
Pacchetto di distribuzione	Pacchetto informativo inviato dal sistema di conservazione all'utente in risposta ad una sua richiesta di accesso a oggetti di conservazione.
Pacchetto di file (file package)	Insieme finito di più file (possibilmente organizzati in una struttura di sottoalbero all'interno di un filesystem) che costituiscono, collettivamente oltre che individualmente, un contenuto informativo unitario e auto-consistente.
Pacchetto di versamento	Pacchetto informativo inviato dal produttore al sistema di conservazione secondo il formato descritto nel manuale di conservazione.
Pacchetto informativo	Contenitore logico che racchiude uno o più oggetti di conservazione con i relativi metadati, oppure anche i soli metadati riferiti agli oggetti di conservazione.
Pathname	Concatenazione ordinata del percorso di un file e del suo nome.
Percorso	Informazioni relative alla localizzazione virtuale del file all'interno del filesystem espressa come concatenazione ordinata del nome dei nodi del percorso.
Piano della sicurezza del sistema di conservazione	Documento che, nel contesto del piano generale di sicurezza, descrive e pianifica le attività volte a proteggere il sistema di conservazione dei documenti informatici da possibili rischi.
Piano della sicurezza del	Documento che, nel contesto del piano generale di sicurezza, descrive e pianifica le

copia informatica per consultazione

sistema di gestione Informatica dei documenti	attività volte a proteggere il sistema di gestione informatica dei documenti da possibili rischi.
Piano di classificazione (Titolario)	Struttura logica che permette di organizzare documenti e oggetti digitali secondo uno schema desunto dalle funzioni e dalle attività dell'amministrazione interessata.
Piano di conservazione	Documento, allegato al manuale di gestione e integrato con il sistema di classificazione, in cui sono definiti i criteri di organizzazione dell'archivio, di selezione periodica e di conservazione ai sensi dell'articolo 68 del D.P.R. 28 dicembre 2000, n. 445.
Piano di organizzazione delle aggregazioni documentali	Strumento integrato con il sistema di classificazione a partire dai livelli gerarchici inferiori di quest'ultimo e finalizzato a individuare le tipologie di aggregazioni documentali (tipologie di serie e tipologie di fascicoli) che devono essere prodotte e gestite in rapporto ai procedimenti e attività in cui si declinano le funzioni svolte dall'ente
Piano generale della sicurezza	Documento che pianifica le attività volte alla realizzazione del sistema di protezione e di tutte le possibili azioni indicate dalla gestione del rischio nell'ambito dell'organizzazione di appartenenza.
Presa in carico	Accettazione da parte del sistema di conservazione di un pacchetto di versamento in quanto conforme alle modalità previste dal manuale di conservazione e, in caso di affidamento del servizio all'esterno, dagli accordi stipulati tra il titolare dell'oggetto di conservazione e il responsabile del servizio di conservazione.
Processo	Insieme di attività correlate o interagenti che trasformano elementi in ingresso in elementi in uscita.
Produttore dei PdV	Persona fisica, di norma diversa dal soggetto che ha formato il documento, che produce il pacchetto di versamento ed è responsabile del trasferimento del suo contenuto nel sistema di conservazione. Nelle pubbliche amministrazioni, tale figura si identifica con il responsabile della gestione documentale.
Rapporto di versamento	Documento informatico che attesta l'avvenuta presa in carico da parte del sistema di conservazione dei pacchetti di versamento inviati dal produttore.
Registro di protocollo	Registro informatico ove sono memorizzate le informazioni prescritte dalla normativa per tutti i documenti ricevuti e spediti da un ente e per tutti i documenti informatici dell'ente stesso.
Registro particolare	Registro informatico individuato da una pubblica amministrazione per la memorizzazione delle informazioni relative a documenti soggetti a registrazione particolare.
Regolamento eIDAS	electronic IDentification Authentication and Signature, Regolamento (UE) № 910/2014 del Parlamento Europeo e del Consiglio, del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE.
Repertorio	Registro su cui vengono annotati con un numero progressivo i fascicoli secondo l'ordine cronologico in cui si costituiscono all'interno delle suddivisioni del piano di classificazione.
Responsabile dei sistemi informativi per la conservazione	Soggetto che coordina i sistemi informativi all'interno del conservatore, in possesso dei requisiti professionali individuati da AGID.
Responsabile del servizio di conservazione	soggetto che coordina il processo di conservazione all'interno del conservatore, in possesso dei requisiti professionali individuati da AGID
Responsabile della conservazione	Soggetto che definisce e attua le politiche complessive del sistema di conservazione e ne governa la gestione con piena responsabilità ed autonomia.
Responsabile della funzione archivistica di conservazione	soggetto che coordina il processo di conservazione dal punto di vista archivistico all'interno del conservatore, in possesso dei requisiti professionali individuati da AGID
Responsabile della gestione documentale	Soggetto responsabile della gestione del sistema documentale o responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi, ai sensi dell'articolo 61 del D.P.R. 28 dicembre 2000, n. 445.
Responsabile della	Persona con conoscenza specialistica della normativa e delle prassi in materia di

copia informatica per consultazione

protezione dei dati	protezione dei dati, in grado di assolvere i compiti di cui all'articolo 39 del Regolamento (UE) 2016/679.
Responsabile della sicurezza dei sistemi di conservazione	soggetto che assicura il rispetto dei requisiti di sicurezza all'interno del conservatore, in possesso dei requisiti professionali individuati da AGID
Responsabile dello sviluppo e della manutenzione del sistema di conservazione	soggetto che assicura lo sviluppo e la manutenzione del sistema all'interno del conservatore, in possesso dei requisiti professionali individuati da AGID
Riferimento temporale	Insieme di dati che rappresenta una data e un'ora con riferimento al Tempo Universale Coordinato (UTC).
Riversamento	Procedura mediante la quale uno o più documenti informatici sono convertiti da un formato di file (ovvero di busta, ovvero di pacchetto di file) ad un altro, lasciandone invariato il contenuto per quanto possibilmente permesso dalle caratteristiche tecniche del formato (ovvero dei formati) dei file e delle codifiche di destinazione.
Scarto	Operazione con cui si eliminano definitivamente, secondo quanto previsto dalla normativa vigente, i documenti ritenuti non più rilevanti ai fini giuridico-amministrativo e storico-culturale.
Serie	Raggruppamento di documenti con caratteristiche omogenee (vedi anche aggregazione documentale informatica).
Sigillo elettronico	Dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati in forma elettronica, per garantire l'origine e l'integrità di questi ultimi.
Sistema di conservazione	Insieme di regole, procedure e tecnologie che assicurano la conservazione dei documenti informatici in attuazione a quanto previsto dall'art. 44, comma 1, del CAD.
Sistema di gestione informatica dei documenti	Insieme delle risorse di calcolo, degli apparati, delle reti di comunicazione e delle procedure informatiche utilizzati dalle organizzazioni per la gestione dei documenti. Nell'ambito della pubblica amministrazione è il sistema di cui all'articolo 52 del D.P.R. 28 dicembre 2000, n. 445
Titolare dell'oggetto di conservazione	Soggetto produttore degli oggetti di conservazione.
Trasferimento	Passaggio di custodia dei documenti da una persona o un ente ad un'altra persona o un altro ente.
TUDA	Testo Unico della Documentazione Amministrativa, Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, e successive modificazioni e integrazioni.
Ufficio	Riferito ad un'area organizzativa omogenea, un ufficio dell'area stessa che utilizza i servizi messi a disposizione dal sistema di protocollo informatico.
Utente abilitato	Persona, ente o sistema che interagisce con i servizi di un sistema di gestione informatica dei documenti e/o di un sistema per la conservazione dei documenti informatici, al fine di fruire delle informazioni di interesse.
Versamento	Passaggio di custodia, di proprietà e/o di responsabilità dei documenti. Nel caso di un organo giudiziario e amministrativo dello Stato operazione con la quale il responsabile della conservazione trasferisce agli Archivi di Stato o all'Archivio Centrale dello Stato della documentazione destinata ad essere ivi conservata ai sensi della normativa vigente in materia di beni culturali.

Glossario degli Acronimi	
AGID	Agenzia per l'Italia digitale
AOO	Area Organizzativa Omogenea
CAD	Codice dell'Amministrazione Digitale - Decreto legislativo 7 marzo 2005, n. 82 e successive modificazioni e integrazioni.
eIDAS	Regolamento (UE) № 910/2014 del Parlamento Europeo e del Consiglio, del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE.
FEA	Vedi firma elettronica avanzata.
FEQ	Vedi firma elettronica qualifica.
GDPR	Regolamento (UE) № 679/2016 del Parlamento Europeo e del Consiglio, del 27 aprile 2016 ("General Data Protection Regulation"), relativo alla protezione delle

copia informatica per consultazione

	persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE.
PdA (AiP)	Pacchetto di Archiviazione.
PdD (DiP)	Pacchetto di Distribuzione.
PdV (SiP)	Pacchetto di Versamento.
UOR	Unità Organizzativa Responsabile

Torna al sommario

1.4 Normativa di riferimento

Alla data odierna l'elenco dei principali riferimenti normativi italiani in materia è costituito da:

- **Legge del 7 agosto 1990, n. 241 e successivi aggiornamenti-** Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi
- **Decreto del Presidente della Repubblica del 28 dicembre 2000, n. 445 e s.m.i. (TUDA)** – Testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa.
- **Decreto legislativo del 30 giugno 2003, n. 196 -** Codice in materia di protezione dei dati personali
- **Decreto legislativo del 22 gennaio 2004, n. 42 -** Codice dei beni culturali e del paesaggio, ai sensi dell'articolo 10 della legge 6 luglio 2002, n.137
- Decreto legislativo del 7 marzo 2005, n. 82 e successivi aggiornamenti - Codice dell'Amministrazione digitale
- **Decreto del Presidente del Consiglio dei Ministri del 22 febbraio 2013 -** Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali, ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma 3, lettera b), 35, comma 2, 36, comma 2, e 71;
- **Decreto legislativo del 14 marzo 2013, n.33 e successivi aggiornamenti** - Riordino della disciplina riguardante il diritto di accesso civico e gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni;
- **Decreto del Presidente del Consiglio dei Ministri del 21 marzo 2013 -** Individuazione di particolari tipologie di documenti analogici originali unici per le quali, in ragione di esigenze di natura pubblicistica, permane l'obbligo della conservazione dell'originale analogico oppure, in caso di conservazione sostitutiva, la loro conformità all'originale deve essere autenticata da un notaio o da altro pubblico ufficiale a ciò autorizzato con dichiarazione da questi firmata digitalmente ed allegata al documento informatico, ai sensi dell'art. 22, comma 5, del Codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82 e successive modificazioni
- **Decreto del Presidente del Consiglio dei Ministri del 3 dicembre 2013 -** Regole tecniche per il protocollo informatico: art. 2 comma 1, Oggetto e ambito di applicazione; art. 6, Funzionalità; art. 9, Formato della segnatura di protocollo; art. 18 commi 1 e 5, Modalità di registrazione dei documenti informatici; art. 20, Segnatura di protocollo dei documenti trasmessi; art. 21, Informazioni da includere nella segnatura

copia informatica per consultazione

- **Reg. UE 910/2014**, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE - Regolamento eIDAS
- **Reg. UE 679/2016** (GDPR), relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE;
- **Circolare AgID del 18 aprile 2017, n. 2 -** recante le misure minime di sicurezza ICT per le pubbliche amministrazioni
- **Circolare AgID del 9 aprile 2018, n. 2 –** Criteri per la qualificazione dei Cloud Service Provider per la PA
- **Circolare AgID del 9 aprile 2018, n. 3 –** Criteri per la qualificazione di servizi SaaS per il Cloud della PA
- **Decreto del Presidente del Consiglio dei Ministri del 19 giugno 2019, n. 76 -** Regolamento di organizzazione del Ministero per i beni e le attività culturali, degli uffici di diretta collaborazione del Ministro e dell'Organismo indipendente di valutazione della performance.
- **Linee guida del 15 aprile 2019** dell'indice dei domicili digitali delle pubbliche amministrazioni e dei gestori di pubblici servizi;
- **Linee guida del 6 giugno 2019** contenenti le Regole Tecniche e Raccomandazioni afferenti la generazione di certificati elettronici qualificati, firme e sigilli elettronici qualificati e validazioni temporali elettroniche qualificate.
- **Linee guida del 9 gennaio 2020** sull'Accessibilità degli strumenti informatici.
- **Linee Guida AgID del 9 settembre 2020** sulla formazione, gestione e conservazione dei documenti informatici e relativi allegati
- **Circolare AgID n. 2/2021 del 29 marzo 2021,** recante integrazioni alla circolare AgID n. 2 del 9 aprile 2018 «Criteri per la qualificazione dei Cloud Service Provider per la PA» e alla circolare AgID n. 3 del 9 aprile 2018 «Criteri per la qualificazione di servizi SaaS per il Cloud della PA».

Torna al sommario

1.5 Standard di riferimento

Di seguito sono riportati i principali standard e specifiche tecniche di riferimento nell'ambito della gestione documentale dei documenti informatici e documenti amministrativi informatici, l'affidabilità e la sicurezza informatica.
Dove non sono indicate una versione e/o una data specifica, si intende fare riferimento alla più recente versione disponibile del documento citato:

- **UNI ISO 15489-1** - Informazione e documentazione - Gestione dei documenti di archivio - Principi generali sul record management.
- **UNI ISO 15489-2** -Informazione e documentazione - Gestione dei documenti di archivio – Linee Guida sul record management.
- **ISO/TS 23081-1** - Information and documentation - Records management processes – Metadata for records – Part 1 – Principles, Quadro di riferimento per lo sviluppo di un sistema di metadati per la gestione documentale.
- **ISO/TS 23081-2** - Information and documentation - Records management processes – Metadata for records – Part 2 – Conceptual and implementation issues, Guida pratica per l'implementazione.

copia informatica per consultazione

- **ISO 16175-1** - (ICA) Information and documentation -- Principles and functional requirements for records in electronic office environments -- Part 1: Overview and statement of principles.
- **ISO 16175-2** - (ICA) Information and documentation -- Principles and functional requirements for records in electronic office environments -- Part 2: Guidelines and functional requirements for digital records management systems.
- **ISO 16175-3** - (ICA) Information and documentation -- Principles and functional requirements for records in electronic office environments -- Part 3: Guidelines and functional requirements for records in business system.
- **ISO 15836** - Information and documentation - The Dublin Core metadata element set, Sistema di metadata del Dublin Core.
- **ISO 9001** – Sistemi di gestione per la qualità – Requisiti.
- **ISO 30300:2011** Information and documentation - Management systems for records - Fundamentals and vocabulary;
- **ISO 30301:2011** Information and documentation - Management systems for records – Requirements.
- **ISO 30302:2015** Information and documentation - Management systems for records - Guidelines for implementation.
- **ISO/TR 23081-3** - Information and documentation — Managing metadata for records — Part 3: Self-assessment method MoReq 2001 Model requirements for the management of electronic records. MoReq 2 Specification 2008 Model requirements for the management of electronic records – che individua i requisiti funzionali della gestione documentale. MoReq2010 Modular requirements for records systems.
- **ISO 16363** - Space data and information transfer systems -- Audit and certification of trustworthy digital repositories
- **ISO 16919** - Space data and information trans:fer systems -- Requirements for bodies providing audit and certification of candidate trustworthy digital repositories
- **ISO 17068** - Information and documentation -- Trusted third party repository for digital records
- **ISO/IEC 27001** - Information technology - Security techniques - Information security management systems – Requirements, Requisiti di un ISMS (Information Security Management System);
- **ISO/IEC 27017** - Information technology -- Security techniques -- Code of practice for information security controls based on ISO/IEC 27002 for cloud services;
- **ISO/IEC 27018** - Information technology -- Security techniques -- Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors;
- **ETSI TS 101 533-1 V1.2.1** - Technical Specification, Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part 1: Requirements for Implementation and Management, Requisiti per realizzare e gestire sistemi sicuri e affidabili per la conservazione elettronica delle informazioni;
- **ETSI TR 101 533-2 V1.2.1** - Technical Report, Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part 2: Guidelines for Assessors, Linee guida per valutare sistemi sicuri e affidabili per la conservazione elettronica delle informazioni.

Torna al sommario

copia informatica per consultazione

2 Aspetti Organizzativi

2.1 Area Organizzativa Omogenea

Il Testo Unico delle disposizioni in materia di documentazione amministrativa (D.P.R. n.445/2000 e s.m.i.) prescrive, all'art. 50 comma 4 che ciascuna pubblica amministrazione individui, nell'ambito del proprio ordinamento, gli uffici da considerare ai fini della gestione unica e coordinata dei documenti per grandi aree organizzative omogenee, assicurando criteri uniformi di classificazione e archiviazione.
In tale contesto la ASST Mantova (nel seguito, "ASST") ha individuato le seguenti strutture che afferiscono alle AOO per la gestione coordinata dei documenti.

Codice	AOO	PEC
A23285C	Struttura Complessa Affari Generali e Controlli Interni	protocollogenerale@pec.asst-mantova.it
A85808E	Area amministrativa fabbisogni di personale	reclutamento@pec.asst-mantova.it
A34F9EE	Protocollo Fatture elettroniche in ingresso	ragioneria@pec.asst-mantova.it
A514405	Protocollo Fatture elettroniche in uscita	fatture@pec.asst-mantova.it
A3219D2	Sistemi Informativi Aziendali	sia@pec.asst-mantova.it

L'ASST ha accreditato le strutture sopra indicate; tuttavia viene utilizzato un unico sistema di protocollazione e un unico titolario di classificazione, producendo un unico archivio, gestito dalla Struttura Complessa Affari Generali e Controlli Interni.

Torna al sommario

2.2 Accreditamento dell'AOO all'IPA

Per la gestione dei documenti, la ASST, ai sensi della normativa vigente, individua individua le AOO indicate nel paragrafo precedente; tuttavia, viene utilizzato un unico sistema di protocollazione e un unico titolario di classificazione, producendo un unico archivio, gestito dalla Struttura Complessa Affari Generali e Controlli Interni.
Il codice identificativo dell'AOO presso l'Indice delle Pubbliche Amministrazioni (Codice IPA) è "asstm".
La ASST ha effettuato l'iscrizione delle proprie caselle di posta elettronica certificata istituzionale presso l'IPA, indicate nel paragrafo precedente.

Torna al sommario

2.3 Ruoli e responsabilità

Per le/la AOO sono individuati i seguenti ruoli con responsabilità sui processi in essere.

copia informatica per consultazione

L'ASST, tramite specifica delibera, provvede alla nomina del Responsabile della gestione documentale, del Responsabile della transizione digitale, del Responsabile della conservazione e del Responsabile dei sistemi informativi.

Di seguito sono elencati i compiti dei **responsabili della gestione documentale** (che assumono anche il ruolo di **soggetto produttore del pdv**):

- attribuisce il livello di autorizzazione per l'accesso alle funzioni della procedura di protocollazione, distinguendo tra abilitazioni alla consultazione e abilitazioni all'inserimento e alla modifica delle informazioni;
- garantisce che le operazioni di registrazione e di segnatura di protocollo si svolgano nel rispetto delle disposizioni del testo unico delle amministrazioni;
- garantisce la corretta produzione e la conservazione del registro giornaliero di protocollo;
- cura che le funzionalità del sistema in caso di guasti o anomalie siano ripristinate entro ventiquattro ore dal blocco delle attività e, comunque, nel più breve tempo possibile;
- conserva le copie, in luoghi sicuri differenti;
- assicura la trasmissione del pacchetto di versamento al sistema di conservazione, secondo le modalità operative definite nel manuale di conservazione;
- provvede a verificare il buon esito della operazione di trasferimento al sistema di conservazione tramite la presa visione del rapporto di versamento prodotto dal sistema di conservazione stesso;
- garantisce il buon funzionamento degli strumenti e dell'organizzazione delle attività di registrazione di protocollo, di gestione dei documenti e dei flussi documentali, incluse le funzionalità di accesso e le attività di gestione degli archivi;
- autorizza le operazioni di annullamento;
- vigila sull'osservanza delle disposizioni del testo unico delle amministrazioni (TUDA) da parte del personale autorizzato e degli incaricati.
- d'intesa con il responsabile della conservazione, il responsabile per la transizione digitale e acquisito il parere del responsabile della protezione dei dati personali, predispone il manuale di gestione documentale relativo alla formazione, alla gestione, alla trasmissione, all'interscambio, all'accesso ai documenti informatici nel rispetto della normativa in materia di trattamenti dei dati personali ed in coerenza con quanto previsto nel manuale di conservazione
- In accordo con il responsabile della conservazione, con il responsabile per la transizione digitale e acquisito il parere del responsabile della protezione dei dati personali, predispone il piano della sicurezza del sistema di gestione informatica dei documenti, prevedendo opportune misure tecniche e organizzative per garantire un livello di sicurezza adeguato al rischio in materia di protezione dei dati personali
- Verifica periodicamente la rispondenza del piano di classificazione dei documenti informatici ai procedimenti amministrativi e agli affari in essere e procede al suo aggiornamento
- Assicura l'adozione di criteri uniformi per la gestione informatica dei documenti
- Verifica l'avvenuta eliminazione dei protocolli di settore, dei protocolli multipli e, più in generale, dei protocolli diversi dal protocollo informatico previsto dal TUDA.

Di seguito sono elencati i compiti del **responsabile della transizione digitale:**

- coordina lo sviluppo dei sistemi informativi, di telecomunicazione e fonia, in modo da assicurare anche la coerenza con gli standard tecnici e organizzativi comuni;
- indirizza e coordina lo sviluppo dei servizi, sia interni che esterni, forniti dai sistemi informativi di telecomunicazione e fonia dell'amministrazione;
- indirizza, pianifica, coordina e monitora la sicurezza informatica relativamente ai dati, ai sistemi e alle infrastrutture anche in relazione al sistema pubblico di connettività
- garantisce l'accesso dei soggetti disabili agli strumenti informatici e promuove l'accessibilità anche in attuazione di quanto previsto dalla legge 9 gennaio 2004, n. 4;

copia informatica per consultazione

- analizza periodicamente la coerenza tra l'organizzazione dell'amministrazione e l'utilizzo delle tecnologie dell'informazione e della comunicazione, al fine di migliorare la soddisfazione dell'utenza e la qualità dei servizi nonché di ridurre i tempi e i costi dell'azione amministrativa;
- coopera alla revisione della riorganizzazione dell'amministrazione ai fini del punto precedente;
- indirizza, coordina e monitora la pianificazione prevista per lo sviluppo e la gestione dei sistemi informativi di telecomunicazione e fonia;
- progetta e coordina le iniziative rilevanti ai fini di una più efficace erogazione di servizi in rete a cittadini e imprese mediante gli strumenti della cooperazione applicativa tra pubbliche amministrazioni, ivi inclusa la predisposizione e l'attuazione di accordi di servizio tra amministrazioni per la realizzazione e compartecipazione dei sistemi informativi cooperativi;
- promuove le iniziative attinenti l'attuazione delle direttive impartite dal Presidente del Consiglio dei Ministri o dal Ministro delegato per l'innovazione e le tecnologie;
- pianifica e coordina il processo di diffusione, all'interno dell'amministrazione, dei sistemi di identità e domicilio digitale, posta elettronica, protocollo informatico, firma digitale o firma elettronica qualificata e mandato informatico, e delle norme in materia di accessibilità e fruibilità nonché del processo di integrazione e interoperabilità tra i sistemi e servizi dell'amministrazione
- pianifica e coordina gli acquisti di soluzioni e sistemi informatici, telematici e di telecomunicazione al fine di garantirne la compatibilità con gli obiettivi di attuazione dell'agenda digitale e, in particolare, con quelli stabiliti nel piano triennale di cui all'articolo 16, comma 1, lettera b) del CAD

I compiti del **Responsabile della conservazione** sono descritti nel Manuale di Conservazione allegato al documento.

Di seguito sono elencati i compiti del **Responsabile dei sistemi informativi:**

- Opera d'intesa con il responsabile della conservazione e può affidare, ai sensi dell'articolo 34, comma 1-bis, lettera b) del CAD, la conservazione dei documenti informatici ad altri soggetti, pubblici o privati, che offrono idonee garanzie organizzative, e tecnologiche e di protezione dei dati personali
- Gestisce l'esercizio delle componenti hardware e software;
- monitora il mantenimento dei livelli di servizio (SLA) concordati con il fornitore e segnala eventuali difformità degli SLA e individuazione e pianificazione delle necessarie azioni correttive;
- pianifica lo sviluppo delle infrastrutture tecnologiche;
- controlla e verifica i livelli di servizio erogati da terzi con segnalazione delle eventuali difformità.

Per le figure individuate per ciascun ruolo, fare riferimento alle delibere allegate.

Torna al sommario

2.4 Unità Organizzative coinvolte nei processi di formazione, gestione e conservazione delle classi documentali

Di seguito sono riportate le UO della ASST coinvolte nei processi di formazione, gestione e conservazione delle classi documentali prodotte:

- UOC Risorse Umane
- UOC Risorse Economico Finanziarie
- UOC Affari Generali e Direzione Amministrativa
- SS Direzione Medica

copia informatica per consultazione

Torna al sommario

2.5 Unità organizzative responsabili (UOR) delle attività di registrazione di protocollo e di archiviazione dei documenti all'interno dell'AOO.

L'UO responsabile delle attività di registrazione di protocollo in entrata, in uscita e interni è la UOC Affari Generali e Controlli Interni, e in particolare l'ufficio Protocollo.
Il sistema di protocollazione dell'ASST è centralizzato. Nello specifico, è l'Ufficio Protocollo che ha la facoltà di protocollazione della documentazione in entrata, uscita e interna, scambiata sia tramite posta elettronica certificata che tramite posta elettronica ordinaria.
Per la documentazione in uscita, sono i vari gli Uffici di competenza che provvedono ad inviare i documenti a seguito della protocollazione da parte dell'Ufficio Protocollo.

La casella di Posta Elettronica Certificata Istituzionale (protocollogenerale@pec.asst-mantova.it), pubblicata sull'Indice delle Pubbliche Amministrazioni (IPA), è accessibile:

- per la ricezione di documenti - solo all'Ufficio Protocollo;
- per la manutenzione e la gestione tecnica è accessibile agli Uffici Informatici dell'ASST.

Torna al sommario

2.5.1 Orari osservati dal Servizio Protocollo

Lo sportello al pubblico del Servizio Protocollo è aperto dal Lunedì al Venerdì dalle ore 8:30 alle ore 16:00 (salvo variazioni). Solamente l'Ufficio Protocollo è autorizzato al ritiro dei documenti, pertanto, la ricezione della corrispondenza su supporto cartaceo segue i relativi orari di apertura al pubblico.

Torna al sommario

copia informatica per consultazione

3 Modalità di utilizzo degli strumenti informatici per la formazione dei documenti informatici e per lo scambio degli stessi all'interno ed all'esterno dell'Area Organizzativa Omogenea (AOO)

Secondo quanto previsto dall'art. 40, comma 1 del CAD, le pubbliche amministrazioni formano gli originali dei propri documenti con mezzi informatici.

3.1 Documento Amministrativo

Ai sensi dell'articolo 22, comma 1, lettera d), della legge n. 241/1990, per documento amministrativo si intende "ogni rappresentazione grafica, foto cinematografica, elettromagnetica, informatica o di qualunque altra specie del contenuto di atti, anche interni o non relativi ad uno specifico procedimento, detenuti da una pubblica amministrazione e contenenti attività di pubblico interesse, indipendentemente dalla natura pubblicistica o privatistica della loro disciplina sostanziale".

Torna al sommario

3.1.1 Classificazione in termini tecnologici

3.1.1.1 Documento informatico

Il documento amministrativo informatico è la rappresentazione, mediante dati binari associati a un formato, del contenuto di atti, fatti, o dati giuridicamente rilevanti espressi mediante un testo, un'immagine, un filmato, una riproduzione sonora. Il documento informatico è memorizzato su un supporto fisico che può essere di vari tipi ed è leggibile solo mediante l'ausilio di strumenti tecnologici.

Torna al sommario

3.1.1.2 Documento Analogico

Il documento amministrativo analogico è la rappresentazione, mediante dati continui memorizzati su un supporto analogico, del contenuto di atti, fatti o dati giuridicamente rilevanti espressi mediante un testo, un'immagine, un filmato, una riproduzione sonora.
Il documento analogico è prodotto con strumenti analogici (es. a mano, macchina da scrivere, ecc.) o con strumenti informatici (es. lettera scritta con Word, ecc.). L'originale è cartaceo e dotato di firma autografa.

Torna al sommario

3.1.2 Classificazione in termini operativi

3.1.2.1 Documento ricevuto

I documenti in ingresso sono tutti gli atti aventi rilevanza giuridico probatoria, prodotti da soggetti esterni ed acquisiti dall'ASST nell'esercizio delle sue funzioni.

copia informatica per consultazione

I documenti informatici possono essere recapitati:

- a mezzo posta elettronica convenzionale o certificata,
- per telefax (attraverso fax server),
- su supporto rimovibile quale, ad esempio, pen drive, etc,
- consegnato direttamente all' UP

I documenti analogici trasmessi da soggetti esterni all'amministrazione possono essere recapitati:

- a mezzo posta convenzionale o corriere,
- a mezzo posta raccomandata,
- telegramma,
- con consegna diretta da parte dell'interessato o tramite una persona dallo stesso delegata all'UP.

Torna al sommario

3.1.2.2 Documento inviato

I documenti in uscita sono tutti gli atti aventi rilevanza giuridico probatori, prodotti dal personale dell'ASST nell'esercizio delle proprie funzioni e trasmessi a soggetti esterni.
I documenti informatici sono trasmessi ai destinatari normalmente per mezzo della posta certificata o mediante e-mail istituzionali.
I documenti su supporto cartaceo sono inviati:

- a mezzo posta convenzionale, posta raccomandata o corriere;
- a mezzo telegramma;
- a mezzo consegna diretta al destinatario.

I documenti informatici, compresi di eventuali allegati, sono inviati, di norma, per mezzo della sola posta elettronica certificata se la dimensione del documento e/o di eventuali allegati, non supera la dimensione prevista dal sistema di posta utilizzato dalla AOO. In caso contrario, il documento informatico viene trasmesso al destinatario con altri mezzi verificandone l'autenticità e l'integrità.
La corrispondenza in uscita tramite Pec o mail non è di esclusiva competenza dell'Ufficio Protocollo ma compete anche agli altri uffici e operatori.

Torna al sommario

3.1.2.3 Documento interno formale

I documenti interni formali sono documenti di rilevanza amministrativa giuridico-probatoria, redatti al fine di documentare fatti, stati o qualità inerenti alle attività svolte e alle azioni amministrative intraprese, ovvero qualsiasi documento dal quale possano nascere diritti, doveri o legittime aspettative di terzi. Sono formati, di norma, con tecnologie informatiche e sono soggetti a protocollazione.

Torna al sommario

copia informatica per consultazione

3.1.2.4 Documento interno informale

I documenti interni informali sono documenti di rilevanza esclusivamente interna a ciascuna UO della AOO e, di norma, scambiati attraverso lo strumento della posta elettronica. Le modalità di formazione e gestione sono demandate, nei limiti della propria autonomia organizzativa, a ciascuna UO. Per tali documenti non vige l'obbligatorietà di sottoscrizione e protocollazione.

Torna al sommario

3.2 Documento clinico

I documenti clinici sono i documenti prodotti dalla ASST nell'esercizio delle attività mediche e possono contenere informazioni su osservazioni cliniche dirette, quali rivelazioni di anamnesi, segni vitali o sintomi, o su osservazioni indirette derivanti, ad esempio, da diagnostica strumentale, esami di laboratorio o rappresentazione iconografica di resoconti radiologici, oppure opinioni mediche quali valutazioni di osservazioni cliniche, consulti e consulenze, obiettivi da raggiungere o piani diagnostico terapeutici, azioni di natura clinico-sanitaria atte a generare osservazioni cliniche ed opinioni mediche.
I documenti clinici non sono soggetti a protocollazione.

Torna al sommario

3.3 Requisiti degli strumenti informatici di scambio dei documenti con l'esterno

Scopo degli strumenti informatici di scambio e degli standard di composizione dei messaggi è garantire sia l'interoperabilità sia i requisiti minimi di sicurezza di seguito richiamati:

- Integrità del messaggio
- Riservatezza del messaggio
- Non ripudio del messaggio
- Automazione dei processi di protocollazione e smistamento dei messaggi all'interno della AOO
- Certificazione dell'avvenuto inoltro e ricezione
- Interoperabilità dei sistemi informativi pubblici.

Torna al sommario

3.4 Protocollo informatico

Il "Sistema di Gestione Informatica dei Documenti" è utilizzato dalle Pubbliche Amministrazioni per gestire il ciclo di vita dei "Documenti Amministrativi Informatici", a partire dalla loro formazione/ricezione fino alla loro archiviazione e/o trasmissione, nell'esercizio delle proprie funzioni istituzionali.
Il "Protocollo Informatico" è la componente software del sistema di "Sistema di Gestione Informatica dei Documenti" che assicura la gestione contemporanea della registrazione di protocollo e segnatura di protocollo:

copia informatica per consultazione

- registrazione di protocollo: attività di memorizzazione dei dati necessari a conservare le informazioni per ogni documento ricevuto o spedito o interno.
- segnatura di protocollo: apposizione o associazione all'originale del documento, in forma permanente non modificabile, dei metadati riguardanti il documento stesso funzionali alla ricezione o spedizione.

Torna al sommario

3.5 Firma digitale

La sottoscrizione dei documenti informatici, con valenza giuridico-probatoria, è ottenuta con un processo di firma digitale conforme alle disposizioni di legge dettate dalla normativa vigente. Lo strumento di firma digitale soddisfa i seguenti tre requisiti:

- Integrità del messaggio
- Riservatezza del messaggio
- Non ripudio del messaggio

Inoltre, i documenti informatici prodotti dall'AOO, indipendentemente dal software utilizzato per la loro redazione, prima della sottoscrizione con firma digitale, sono convertiti in uno dei formati standard previsti dalla normativa vigente in materia di archiviazione al fine di garantirne l'immodificabilità.
L'ASST firma i documenti clinici elettronici apponendo la firma tramite un software certificato (SISS) e i documenti amministrativi tramite l'utilizzo di Smart Card Operatore (SCO).

Torna al sommario

3.5.1 Verifica delle firme digitali per i documenti inviati e ricevuti

Per la verifica delle firme digitali apposte sui documenti informatici è possibile utilizzare uno dei software di verifica messi a disposizione dai prestatori di servizi fiduciari accreditati da AgID.
È inoltre possibile utilizzare uno dei seguenti servizi di verifica on-line:

- Consiglio Nazionale del Notariato: https://vol.ca.notariato.it
- Infocert: https://www.firma.infocert.it/utenti/verifica.php
- Poste Italiane – Postecert: https://postecert.poste.it/verificatore

In particolare il Responsabile del procedimento amministrativo effettua la seguente sequenza di operazioni:

- Apertura della busta "virtuale" contenente il documento firmato;
- Verifica della validità del certificato; questa attività è realizzata verificando on-line le Certificate Revocation List (CRL);
- Verifica della firma (o delle firme multiple); in particolare, il software calcola l'impronta del documento e la verifica con quella contenuta nella busta "logica";
- Verifica dell'utilizzo, nell'apposizione della firma, di un certificato emesso da una Certification Authority (CA).

La validità della firma è verificata dal destinatario del documento.

Torna al sommario

copia informatica per consultazione

3.6 Posta Elettronica

Ai sensi dell'art.47, comma 3 del CAD, le comunicazioni tra l'ASST e i dipendenti, nonché tra le varie strutture aziendali, avvengono di norma mediante l'utilizzo della casella di posta istituzionale (dominio @asst-mantova.it), nel rispetto delle norme in materia di protezione dei dati personali.
L'utilizzo della casella di posta istituzionale avviene anche per comunicazioni verso altre Amministrazioni o aziende.

Per la trasmissione ad altre Pubbliche Amministrazioni:

- dei documenti amministrativi protocollati,
- di comunicazioni che necessitano di una ricevuta di invio e/o di una ricevuta di consegna e
- in generale di documenti il cui contenuto impegna l'ASST verso terzi

l'ASST utilizza la posta elettronica certificata.

Il servizio di posta elettronica certificata è strettamente correlato all'indice della pubblica amministrazione (IPA), dove sono pubblicati gli indirizzi istituzionali di posta certificata associati alle AOO.

InoltreformA per permettere l'univocità della segnatura di protocollo è utilizzato l'XML Schema previsto dalle attuali regole tecniche per la generazione dei file da prevedersi come body part dei messaggi scambiati tramite posta elettronica. L'XML Schema è anche riportato nel repository github pubblico consultabile all'URL https://github.com/AgID/protocollo-comunicazione-aoo.
La data e l'ora di formazione, di trasmissione o di ricezione di un documento informatico, redatto in conformità alla normativa vigente e alle relative regole tecniche, sono opponibili ai terzi.

Torna al sommario

4 Regole di assegnazione dei documenti ricevuti con la specifica dei criteri per l'ulteriore eventuale inoltro dei documenti verso altre amministrazioni

4.1 Attività di assegnazione

4.1.1 Regole Generali

Dopo la registrazione, la corrispondenza indirizzata a destinatari interni esplicitamente indicati viene trasmessa dall'Ufficio Protocollo direttamente all'Ufficio competente attraverso apposita funzionalità del sistema informatico di gestione documentale.
Dunque, con l'assegnazione, si procede all'individuazione dell'UO competente e destinatario del documento, e quindi al conferimento della responsabilità del procedimento amministrativo.
Il sistema informatico di gestione documentale consente ad ogni Ufficio di rifiutare la trasmissione di un documento nel caso in cui esso valuti di avere ricevuto il documento per

copia informatica per consultazione

errore. In questo caso, il documento ritorna di competenza dell'Ufficio Protocollo che lo riassegna ad un'altra UO.
Tutta la corrispondenza non indirizzata esplicitamente ad un ufficio di competenza è smistata, dall'Ufficio Protocollo che provvede ad assegnare i documenti per competenza ed eventualmente per conoscenza ai destinatari presumibilmente coinvolti dal contenuto delle missive.
La data di protocollazione è corrispondente al giorno in cui il documento viene ricevuto dall'Ufficio Protocollo e sancisce l'inizio dei termini per la definizione del procedimento amministrativo secondo quanto disposto per legge.

Il sistema di gestione informatica dei documenti memorizza tutti i passaggi ed eventuali modifiche, conservando, per ciascuno di essi, l'identificativo dell'utente che effettua l'operazione, la data e l'ora di esecuzione.
La traccia risultante definisce, ai fini normativi e regolamentari, i tempi del procedimento amministrativo ed i conseguenti riflessi sotto il profilo della responsabilità.

L'eventuale documento cartaceo originale è successivamente consegnato al destinatario ritenuto "di competenza".

Torna al sommario

4.1.2 Modifica delle assegnazioni

Nel caso di assegnazione errata, il documento deve essere restituito dal Servizio/UO assegnatario all'Ufficio Protocollo, utilizzando l'apposita funzione del sistema di gestione documentale e inserendo la motivazione del rifiuto e, ove possibile, segnalando l'ufficio ritenuto competente.

L'Ufficio Protocollo provvederà a riassegnare lo stesso documento individuando l'Ufficio competente. Qualora il nuovo assegnatario non fosse chiaramente individuabile, l'UP provvederà ad inoltrare il documento alla Direzione Generale che fornirà le opportune indicazioni.

Torna al sommario

4.2 Criteri di inoltro dei documenti ricevuti verso altre AOO

I documenti ricevuti tramite PEC, di competenza di terzi (PA/altre strutture/AOO), vengono rifiutati dall' ASST comunicando al mittente l'errore di trasmissione.
La corrispondenza cartacea destinata a terzi viene respinta all'atto del ricevimento.
Nel caso non sia stato possibile verificare la competenza di terzi all'atto del ricevimento il documento è inoltrato al destinatario con lettera protocollata di accompagnamento. Nel caso in cui il destinatario non sia individuabile il documento deve essere rimandato al mittente. Se il documento è stato erroneamente protocollato il numero di protocollo deve essere annullato.

Torna al sommario

copia informatica per consultazione

5 Criteri e modalità per il rilascio delle abilitazioni di accesso, interno ed esterno all'amministrazione, al sistema di gestione informatica dei documenti

5.1 Criteri generali

Le abilitazioni all'accesso al sistema informatico di protocollo e gestione documentale Prisma vengono rilasciate dal responsabile della Gestione Documentale, in coordinamento con la Struttura Sistemi Informativi. L'accesso al sistema è consentito unicamente al personale dell'ASST: non vengono pertanto rilasciate abilitazioni a soggetti esterni all'Amministrazione.
I nuovi utenti vengono abilitati all'accesso al sistema previa richiesta formulata dal responsabile della U.O./Servizio presso la quale operano; ad essi viene assegnato un livello di abilitazione corrispondente al ruolo ricoperto. Ogni utente abilitato accede al sistema utilizzando le proprie credenziali di dominio, secondo una logica di "Single Sign On".
Per quanto riguarda le istruzioni operative relative alle funzionalità di profilazione degli utenti, si rimanda al manuale del sistema Prisma , pubblicato sul sito web aziendale.
Torna al sommario

5.2 Abilitazione alle funzioni di visualizzazione

Il sistema informatico garantisce la riservatezza delle informazioni, consentendo di limitare la visibilità dei documenti/registrazioni ai soli utenti che possiedono uno specifico livello di abilitazione. In particolare, gli utenti sono abilitati alla visione dei soli documenti/registrazioni da essi stessi caricati nel sistema, o di quelli che gli sono stati trasmessi da altri utenti.
Valgono inoltre le regole di trasmissione gerarchica delle abilitazioni, in base alle quali un utente B con livello gerarchicamente superiore ad un utente A, è abilitato automaticamente alla visione dei documenti caricati dall'utente A.
Una specifica funzionalità del sistema consente di ottenere in ogni momento l'elenco degli utenti che hanno visibilità su un determinato documento.

Torna al sommario

5.3 Gestione dei log di sistema

Il sistema Prisma è predisposto per tracciare eventi o azioni compiute dagli utenti e dagli amministratori durante l'uso del protocollo informatico e la gestione documentale (c.d. "Log").
Le funzionalità del sistema è contenuta nel manuale del sistema di protocollo informatico allegato al presente documento.

Torna al sommario

copia informatica per consultazione

6 Formati dei documenti

6.1 Formati utilizzati per la formazione del documento informatico previsti dalle Linee Guida AgID

La Tabella successiva riassume le classi documentali formate, gestite e trasmesse in conservazione dall'ASST e i relativi formati, rientranti tra quelli standard previsti dalla normativa vigente, al fine di garantire la loro inalterabilità durante le fasi di accesso e conservazione, nonché l'immutabilità nel tempo del contenuto e della struttura.

Classi documentali	Tipologia
Fatture PA Attive	XML (firmato P7M)
Fatture PA Passive	XML (firmato P7M)
Notifiche SDI Fatture PA Attive	XML (firmato P7M)
Notifiche SDI Fatture PA Passive	XML (firmato P7M)
Delibere	ODT, DOC, DOCX, PDF (firmato P7M)
Determine	ODT, DOC, DOCX, PDF (firmato P7M)
Repertori	DOCX, PDF (firmato P7M, marcato TSD)
Documenti Protocollati	CSV, DAT, WORD DOC, WORD DOCX, PNG, EML, GIF, HTM, HTML, JPEG, JPG, M7M, ODB, ODG, ODP, ODS, ODT, PDF, PPSX, PPT, PPTX, P7M, P7S, RAR, RTF, TIF, TIFF, TSD, TSR, XLS, XML, ZIP, 7Z
Cedolini, Cartellini e CU Risorse umane	PDF
LOG di trasmissione di Cedolini e CU Risorse umane	PDF
Ricevute Telematiche RT	XML
Richiesta Pagamento Telematico RPT	XML
SINTEL 5/10/20 anni e illimitati	PDF, P7M, M7M, XML
Ricette Dematerializzate Erogate	ZIP, XML
Ricette Dematerializzate Erogate Annullate	ZIP, XML
Ricette Dematerializzate Prescritte	ZIP, XML
Ricette Dematerializzate Prescritte Annullate	ZIP, XML
Lettere di Dimissione	PDF (firmate P7M, marcate M7M)
Referti Ambulatoriali	PDF (firmate P7M, marcate M7M)
Referti di Documenti Clinici Generici	PDF (firmate P7M, marcate M7M)
Referti Anatomia Patologica	PDF (firmate P7M, marcate M7M)
Referti di Laboratorio	PDF (firmate P7M, marcate M7M)
Referti di Radiologia	PDF (firmate P7M, marcate M7M)
Verbali di Pronto Soccorso	PDF (firmate P7M, marcate M7M)
Verbali Operatori	PDF (firmate P7M, marcate M7M)
DICOM	DICOM

I formati portati in conservazione sono riportati nelle specificità di contratto relative alla classe documentale interessata.

Torna al sommario

copia informatica per consultazione

6.2 Formati utilizzati per la formazione del documento informatico non previsti dalle LLGG e valutazione di interoperabilità

La Tabella successiva riassume le classi documentali formate, gestite e trasmesse in conservazione dall'ASST e i relativi formati, non rientranti tra quelli standard previsti dalla normativa vigente oppure non consigliati/raccomandati.

Classe Documentale	**Formato**
LOG di trasmissione di Cedolini e CU Risorse umane	TXT
Documenti Protocollati	DAT, EMZ, JPE, LDIF, LOG, OTT, MSG, OTT, PPS, PROPERTIES, WFM, XLSB, TXT

I formati portati in conservazione sono riportati nelle specificità di contratto relative alla classe documentale interessata.

Torna al sommario

6.3 Procedure per la valutazione periodica di interoperabilità

Come previsto dalla normativa vigente, la ASST effettua con cadenza annuale una ricognizione delle procedure, allo scopo di individuare le tipologie di documenti informatici trattati, ed il censimento dei formati di file e delle tipologie di storage attualmente utilizzati.
In presenza di formati diversi da quelli previsti dalle Linee Guida è effettuata la valutazione di interoperabilità.
La valutazione di interoperabilità consiste in un dettagliato rapporto circa le seguenti azioni:

a) Includere nell'attività di classificazione un censimento dei formati di file e delle tipologie di storage attualmente utilizzati.
b) Per ciascun formato di file adottato, elencare tutti i dettagli tecnici, quali:
   - nome dei formati e, laddove applicabile, dei dialetti, profili, codec, schemi operativi;
   - suddivisione tra formati generici e specifici;
   - versioni utilizzate nei documenti già esistenti, ovvero producibili dagli attuali applicativi;
   - altre caratteristiche tecniche non vincolate dalle specifiche di cui ai punti precedenti (e.g. lingue adottate nei testi, numero di canali audio, spazi-colore, risoluzione per immagini e video, bitrate massimo, algoritmi di cifratura, presenza di password, ecc.).
c) Effettuare, per ciascun formato, il calcolo dell'indice di interoperabilità tenendo conto delle caratteristiche elencate sotto, e assegnando il relativo valore. Il formato è considerato sufficientemente interoperabile se il valore dell'indice è superiore a 12. Nel caso di formati di pacchetti o contenitori, andrà fatta una valutazione per ogni componente e considerato come addendo il valore più basso per ciascuna delle sue componenti.

Caratteristica	**Dettaglio**	**Valore**
Standard de iure	normative che ne obblighino, o per lo meno ne raccomandino, l'uso in determinati contesti amministrativo-legali e settori di riferimento.	3

copia informatica per consultazione

Standard de facto	questioni contingenti (anche fa loro correlate), quali l'efficienza in casi d'uso reali, l'autoregolazione dei mercati di riferimento, l'efficacia tecnica, ne hanno determinano una larghissima e non trascurabile diffusione, per lo meno in settori di riferimento	2
Nessuno standard		0

Caratteristica	**Dettaglio**	**Valore**
Aperto	esista e sia resa pubblicamente disponibile, una "specifica tecnica" del medesimo: la documentazione che descrive dettagliatamente, come minimo, la procedura di formazione e di lettura di file in quel formato e, possibilmente, l'elaborazione e i suoi possibili scenari di utilizzo, spesso descritti organicamente mediante operational patterns	3
Chiuso		0

Caratteristica	**Dettaglio**	**Valore**
Non Proprietario	gestione delle sue specifiche non è controllata in tale ambito (quindi possibilmente rilasciata al pubblico dominio, o comunque gestita da un organismo di standardizzazione)	4
Proprietario libero	creato da un'organizzazione privata che detiene la proprietà intellettuale ma di libero utilizzo anche nella produzione di nuovi file	3
Proprietario limitato	limitazione potrebbe permettere soltanto l'utilizzo libero di file già codificati in tale formato ma non la produzione di nuovi file	2
Proprietario	limitare anche la lettura dei file formattati secondo tale formato	0

Caratteristica	**Dettaglio**	**Valore**
Estendibile	qualora esso sia stato concepito ab initio per ammettere revisioni che ne aumentino progressivamente le funzionalità.	2
Non estendibile	I formati non estendibili, quindi, possono comunque essere soggetti a revisioni, che però potrebbero, per tali formati, richiedere una re-ingegnerizzazione o un adattamento più difficoltoso rispetto a formati estendibili, probabilmente anche a scapito delle compatibilità di cui al punto precedente.	0

Caratteristica	**Dettaglio**	**Valore**
Livello del modello per i metadati	segue l'analoga classificazione emanata nelle Linee guida nazionali per la valorizzazione del patrimonio informativo pubblico, emanate dall'Agenzia per l'Italia Digitale, ove al livello 1 vengono attribuiti 0 punti e così via via fino al livello 4 cui sono attribuiti 3 punti. Tale valore è indicato, per i formati descritti al §1.2.3, nelle loro tabelle riassuntive.	0-3

Caratteristica	**Dettaglio**	**Valore**
Completamente robusto	il file comprenda meccanismi per verificare l'eventuale perdita di integrità di un file (o pacchetto di file) e consenta, inoltre, di leggere correttamente le parti integre del file.	2

copia informatica per consultazione

Parzialmente robusto	il file comprenda meccanismi per verificare l'eventuale perdita di integrità di un file (o pacchetto di file)	1
Non robusto		0

Caratteristica	Dettaglio	Valore
Indipendente dal dispositivo	Non richiede specifici componenti hardware, firmware o software per essere creato o letto.	4
Dipendente dal dispositivo		0

Caratteristica	Dettaglio	Valore
Retro compatibile	formati il cui standard prevede by design che un applicativo in grado di interpretare una data revisione possa anche leggere file formattati con revisioni precedenti (eventualmente entro un limite massimo)	0
Compatibile in avanti	Quelli per cui gli applicativi disegnati al momento in cui una data revisione sia corrente possano leggere anche file formattati in base a revisioni successive del medesimo standard	0

Caratteristica	Dettaglio	Valore
Testuale	se, rappresentando ogni word di un file come caratteri testuali, sia possibile estrapolarne il contenuto informativo tramite lettura manuale e non automatizzata di tali caratteri — a seguito di uno sforzo di interpretazione di entità variabile, ma comunque proporzionato alle capacità intellettive di un tecnico di settore.	0
Binario	il processo è generalmente possibile solo mediante interpretazione automatizzata, "bit a bit", del contenuto digitale del file da parte di un algoritmo di parsing	0

d) Elencare i processi di riversamento di formato, con particolare riferimento ai software applicativi impiegati e alle procedure tecniche (automatiche, semiautomatiche o completamente manuali) adottate per configurare tali riversamenti.
e) Elencare le motivazioni attuali che hanno portato alla scelta di ciascun formato di file per il trattamento dei documenti informatici. In particolar modo, se del caso, distinguere i formati di file tra quelli adottati per i documenti:
   - accettati "in entrata" dal pubblico ovvero da altre organizzazioni,
   - utilizzati ad uso esclusivamente interno,
   - pubblicati, ovvero prodotti "in uscita" verso altre organizzazioni,
   - archiviati ovvero mandati in conservazione.
f) Valutare l'esistenza di standard o di iniziative di standardizzazione a livello internazionale, europeo e nazionale, relativamente alle tipologie di documenti informatici trattati.
g) Quantificare l'eventuale necessità di operare sui medesimi documenti informatici nell'arco di una finestra temporale futura.
h) Valutare gli scenari ove successive modificazioni o revisioni dei documenti vengano prodotte in formati diversi da quello originale.

copia informatica per consultazione

i) Valutare la sussistenza di leggi o altri tipi di obblighi in merito alla conservazione delle evidenze informatiche nel formato originale di acquisizione o formazione.
j) Dipendenza dei formati di file da:
   - licenze d'uso, marche e brevetti o altra proprietà intellettuale,
   - sistemi e architetture proprietarie, o comunque,
   - sistemi e architetture che, pur senza i suddetti vincoli, sono comunque associati a costi di manutenzione ordinaria o straordinaria, senza la quale diviene a rischio o è fortemente ridotta la capacità di elaborare i suddetti documenti.
k) Inserimento dell'obsolescenza dei formati di file e delle tecnologie di archiviazione all'interno di una più ampia strategia di trasformazione digitale dell'organizzazione.

Torna al sommario

6.4 Procedure di riversamento previste

Allo stato attuale non sono previste procedure di riversamento tramite cui avviene la conversione del formato dei documenti informatici prodotti.

Torna al sommario

7 Protocollo informatico e registrazioni particolari

7.1 Annullamento delle registrazioni di protocollo

I dati obbligatori relativi alla registrazione di protocollo non sono modificabili. La necessità di eventuali modifiche, comporta l'obbligo di annullare l'intera registrazione di protocollo.
Ai sensi degli art. 54 e 61 del "Testo Unico", i dati annullati e/o modificati rimangono memorizzati nella procedura del protocollo informatico unitamente alle informazioni relative all'ora, alla data, al nominativo dell'operatore che effettua l'operazione.
Il responsabile dell'Ufficio Protocollo (o un suo delegato) è autorizzato ad annullare le registrazioni di protocollo per propria iniziativa o a seguito di motivata richiesta scritta.

Nel caso di documenti analogici, l'indicazione dell'annullamento va apposta anche sul documento. Il documento la cui registrazione è annullata, deve essere conservato fatto salvo il caso di restituzione ad altra persona fisica o giuridica per non afferenza a procedimenti amministrativi dell'Ente.

Il sistema di protocollo tiene traccia dei documenti di cui sono state annullate le registrazioni.

Torna al sommario

copia informatica per consultazione

7.2 Descrizione completa e puntuale delle modalità di utilizzo della componente «sistema di protocollo informatico» del sistema di gestione informatica dei documenti

Il sistema informatico utilizzato per la componente di protocollo informatico è Prisma della ditta Data Processing. Il sistema Prisma garantisce l'immodificabilità delle registrazioni di protocollo nonché la contemporaneità della stessa con l'operazione di segnatura.
La descrizione funzionale ed operativa del sistema informatico è contenuta nel manuale del sistema di protocollo informatico allegato al presente documento.

Torna al sommario

7.3 Registro di emergenza

Nelle situazioni di emergenza nelle quali non sia possibile utilizzare il protocollo informatico, ogni evento deve essere registrato su un supporto alternativo, denominato "registro di emergenza".
Il registro di emergenza viene attivato al verificarsi di una delle due condizioni seguenti:

1. indisponibilità del sistema centrale di protocollo informatico, per guasto o malfunzionamento di una delle sue componenti (server, software, collegamenti di rete);
2. indisponibilità dei sistemi locali.

In entrambi i casi, registro di emergenza viene attivato su supporto cartaceo. Il responsabile del AGL autorizza lo svolgimento delle operazioni di protocollo su un registro di emergenza a norma dell'art. 63 del DPR 455/2000.

Sul registro di emergenza devono essere riportate la causa, la data e l'ora di inizio dell'interruzione, nonché la data e l'ora del ripristino della piena funzionalità del sistema, nonché eventuali annotazioni ritenute rilevanti dal responsabile del protocollo informatico.

Il registro di emergenza include i seguenti campi:

1. Codice dell'Amministrazione
2. Codice del registro di emergenza
3. Numero progressivo di protocollo
4. Data e ora di protocollo
5. Tipo di protocollo (Entrata/Uscita)
6. Oggetto
7. Mittente
8. Destinatari
9. Destinatari cc
10. Assegnazione
11. Data di arrivo
12. Data e numero di protocollo del mittente (se disponibili)

La numerazione del registro di emergenza è unica per l'intero anno. Ricomincia dal numero successivo all'ultimo generato per ogni attivazione.
Al termine dell'emergenza il responsabile dell'Ufficio Protocollo revoca l'autorizzazione al protocollo di emergenza e provvede al riversamento delle registrazioni di emergenza nel

copia informatica per consultazione

protocollo informatico generale. Durante la fase di ripristino, a ciascun documento registrato in emergenza viene attribuito un numero di protocollo del sistema informatico ordinario, che provvede a mantenere stabilmente la correlazione con il numero utilizzato in emergenza.
Torna al sommario

7.4 Elenco dei documenti esclusi dalla registrazione di protocollo

Non sono soggette a protocollazione le seguenti tipologie documentali:

- le tipologie espressamente previste dall'art. 53, comma 5 del DPR 445/2000;
- i documenti soggetti a registrazione particolare;
- i documenti che costituiscono mera notizia di prevalente rilevanza informativa
- i documenti clinici.

L'art. 53, comma 5 del DPR 445/2000 prescrive l'esclusione dalla registrazione a protocollo delle seguenti tipologie:

- Bollettini ufficiali P.A.
- Notiziari P.A.
- Note di ricezione circolari
- Note di ricezione altre disposizioni
- Materiali statistici
- Atti preparatori interni
- Giornali
- Riviste
- Libri
- Materiali pubblicitari
- Inviti a manifestazioni che non attivino procedimenti amministrativi

I documenti soggetti a registrazione particolare - e che, quindi, non devono essere protocollati - sono i seguenti:

- Decreti
- Determine
- Fatture emesse
- Fatture ricevute (le fatture provenienti dall'estero possono essere protocollate a seguito di richiesta da parte del SEF).

Il software di produzione e conservazione di queste tipologie particolari di documenti deve consentire di eseguire su di essi tutte le operazioni previste per il protocollo informatico.
Gli altri documenti che non devono essere protocollati sono i seguenti:

- Mandati di pagamento
- Reversali di incasso
- Denunce di infortunio
- Contratti e convenzioni
- Documenti di trasporto
- Documenti di occasione (biglietti augurali, condoglianze, congratulazioni varie ecc.)
- Comunicazione, da parte di altri enti, di bandi di concorso
- Estratti conto bancari
- Lettere accompagnatorie di fatture
- Offerte/preventivi di terzi non richiesti o non inerenti a gare
- Ricevute di ritorno delle raccomandate
- Cedolini stipendiali

copia informatica per consultazione

- Modelli CU
- Cartellini delle presenze/assenze
- RT Mypay
- RPT Mypay
- SINTEL

I documenti clinici, non protocollati sono:

- Ricette Dematerializzate Erogate
- Ricette Dematerializzate Erogate Annullate
- Ricette Dematerializzate Prescritte
- Ricette Dematerializzate Prescritte Annullate
- Lettere di Dimissione
- Referti Ambulatoriali
- Referti Anatomia Patologica
- Referti di Laboratorio
- Referti di Radiologia
- Verbali di Pronto Soccorso
- DICOM

Torna al sommario

7.5 Metadati associati ai documenti soggetti a registrazione particolare

I metadati associati alle registrazioni dei documenti:

- Fatture emesse
- Fatture ricevute
- Determine
- Decreti

Sono indicati e descritti nelle specificità di contratto, allegate al presente manuale.

Torna al sommario

7.6 Registri particolari per la gestione del trattamento delle registrazioni particolari

Sono gestiti i registri particolari relativi alle registrazioni di:

- Decreti
- Determine

Per le Determine e i Decreti il progressivo riparte dal n. 1 all'inizio di ogni anno solare.

Torna al sommario

copia informatica per consultazione

8 Piano di classificazione

8.1 Titolario di classificazione

La ASST ha adottato come titolario di classificazione quello messo a disposizione dalla Regione Lombardia, allegato al presente documento.

Torna al sommario

9 Formazione dei fascicoli informatici e delle aggregazioni documentali

9.1 Fascicolazione dei documenti

Il fascicolo conserva i documenti, classificati in maniera omogenea, relativi ad un determinato procedimento amministrativo di competenza di una unità organizzativa.
Tutti i documenti, indipendentemente dal supporto sul quale vengono formati, sono riuniti in fascicoli o serie documentali (decreti e determine).
L'Ufficio protocollo provvede alla classificazione dei documenti in ingresso, attraverso l'applicativo Prisma, registrando per ciascun documento le informazioni relative al Titolo, classe e sottoclasse del Titolario di classificazione.
L'apertura di un nuovo fascicolo è effettuata dall'Ufficio Protocollo.
Il sistema di protocollo informatico assegna automaticamente il numero di fascicolo e la data di apertura, mentre l'unità organizzativa di afferenza e la classificazione vengono inerite dall'operatore.
Il sistema di protocollo informatico provvede ad aggiornare automaticamente l'elenco dei fascicoli.
In presenza di un documento da inserire in un fascicolo, gli operatori dell'Ufficio Protocollo stabiliscono, consultando le funzioni del sistema informatico e l'elenco dei fascicoli già esistenti, se esso si collochi nell'ambito di un fascicolo già aperto o se debba essere creato un nuovo fascicolo.

I documenti in uscita prodotti dall'ASST sono fascicolati in fase di protocollazione, a cura degli operatori protocollo o protocollatori decentrati, attraverso la registrazione, nell'applicativo Prisma, delle seguenti informazioni:

- Titolo, classe e sottoclasse del Titolario di classificazione
- Oggetto del fascicolo

In presenza di documenti cartacei da inserire in fascicoli informatici, dovrà essere prodotta copia per immagine degli stessi secondo la normativa vigente.
L'originale del cartaceo sarà conservato presso l'unità organizzativa che ha creato il fascicolo.
I codici alfanumerici di fascicolazione devono essere riportati su tutti i documenti sia in entrata che in uscita.

Torna al sommario

copia informatica per consultazione

9.2 Modifica delle assegnazioni

La riassegnazione di un fascicolo informatico è effettuata dagli operatori dell'Ufficio Protocollo che hanno in carico il fascicolo, che provvede a correggere le informazioni del sistema informatico e dell'elenco dei fascicoli ed inoltrando successivamente il fascicolo al Responsabile del procedimento di nuovo carico.
Delle operazioni di riassegnazione è lasciata traccia nel sistema informatico di gestione dei documenti.

Torna al sommario

9.3 Metadati associati

Metadati relativi alla fascicolazione:

- Classificazione: titolo, categoria e classe
- Data apertura
- Oggetto
- Unità competente
- Stato: corrente, deposito e archivio

Torna al sommario

10 Flussi di lavorazione dei documenti protocollati

10.1 Flusso dei documenti ricevuti dalla AOO

10.1.1 Provenienza esterna dei documenti

I documenti possono pervenire all'Amministrazione attraverso:

- servizio postale;
- consegna diretta da parte dei cittadini/utenti;
- a mezzo telefax;
- a mezzo E-mail (prodotte in conformità alla vigente normativa per i documenti informatici) o posta elettronica certificata.

I documenti che pervengono all'ente attraverso il Servizio Postale (sacchi postali, raccomandate, etc.) vengono consegnati esclusivamente all'Ufficio Protocollo dove vengono smistati e consegnati agli uffici destinatari attraverso il servizio interno di pedonaggio.
I documenti ricevuti sull'indirizzo PEC protocollogenerale@pec.asst-mantova.it, vengono acquisiti dal sistema Prisma in formato elettronico, grazie all'integrazione dello stesso alla PEC. Tali documenti vengono protocollati, previa verifica del contenuto da parte dell'operatore incaricato.

Il sistema di protocollo informatico acquisisce esclusivamente i documenti ricevuti sull'indirizzo PEC protocollogenerale@pec.asst-mantova.it
Le PEC ricevute da altri indirizzi (di altre UUOO o Direzioni), se soggetti a registrazione di protocollo devono essere inoltrate all'indirizzo PEC del protocollo

copia informatica per consultazione

protocollogenerale@pec.asst-mantova.it affinché possano essere acquisite in automatico dal sistema.

Torna al sommario

10.1.2 Provenienza di documenti interni formali

Come specificato all'art. 53, comma 3 del DPR 445/2000, gli atti preparatori interni non sono soggetti a registrazione obbligatoria, intendendo per "atto preparatorio interno" un documento che faccia parte di un procedimento ancora in divenire. Si ritiene tuttavia opportuno distinguere due fattispecie:

- i documenti interni di preminente carattere informativo;
- i documenti interni di preminente carattere giuridico-probatorio.

I documenti interni di preminente carattere informativo sono memorie informali, appunti, brevi comunicazioni di rilevanza meramente informativa scambiate tra Uffici: questi documenti non vanno protocollati.
I documenti interni di preminente carattere giuridico-probatorio sono, invece, quelli redatti dal personale nell'esercizio delle proprie funzioni al fine di documentare lo svolgimento e la regolarità delle azioni amministrative o qualsiasi altro documento dal quale possano nascere diritti, doveri o legittime aspettative di terzi: questi documenti vanno protocollati.

Torna al sommario

10.1.3 Ricezione di documenti informatici sulla casella di posta istituzionale (PEC)

Il sistema di protocollo informatico Prisma accede direttamente alla casella email PEC istituzionale *protocollogenerale@pec.asst-mantova.it* e scarica i messaggi ad essa pervenuti.
Le email ricevute direttamente dalle UO della ASST nelle proprie caselle PEC, alle quali sia necessario attribuire efficacia probatoria, vanno inoltrate (esclusivamente via PEC) al Servizio Protocollo, che provvederà alla loro registrazione.
Il personale dell'Ufficio Protocollo controlla quotidianamente i messaggi pervenuti nella casella di posta istituzionale e, previa verifica della bontà e dell'integrità del messaggio, procede alla registrazione di protocollo.
Nel caso in cui il messaggio pervenuto sia illeggibile o incompleto, l'UP deve segnalare la circostanza al mittente, indicando che lo stesso non verrà sottoposto a protocollazione.
Il sistema consente di ricevere documenti pervenuti via PEC da un'altra Pubblica Amministrazione acquisendo i dati necessari alla protocollazione direttamente dalla segnatura XML allegata ai documenti stessi.
I messaggi vengono posti dal sistema nello stato "predisposto" e per ognuno di essi il sistema provvede a compilare una prima maschera di registrazione utilizzando i dati ricavabili dalle intestazioni del messaggio digitale e dalla segnatura di protocollo ad esso associata (se disponibile). L'operatore di protocollo provvede quindi a correggere/integrare i campi necessari alla registrazione e procede quindi con la protocollazione del documento.

Torna al sommario

10.1.4 Ricezione di documenti informatici sulla casella di posta elettronica non istituzionale (PEO)

La posta elettronica ordinaria (PEO), al contrario della email PEC, non permette di identificare con certezza il mittente di una comunicazione, né ha data certa.

copia informatica per consultazione

La PEO, tuttavia, rappresenta un mezzo riconosciuto di trasmissione di documenti: l'art. 65 del CAD consente infatti al cittadino di presentare istanze e dichiarazioni per via telematica alle pubbliche amministrazioni qualora esse siano sottoscritte e presentate unitamente alla copia del documento d'identità. L'indirizzo *protocollogenerale@pec.asst-mantova.it* è abilitato alla ricezione sia di PEC che di PEO.
I documenti ricevuti via posta elettronica ordinaria dalle UU.OO./Servizi dell'ASST e ai quali sia necessario attribuire efficacia probatoria, vanno inoltrati (esclusivamente via PEC) all'Ufficio Protocollo , che provvederà alla loro registrazione.
In alternativa, le UU.OO./Servizi possono stampare il messaggio ricevuto apponendo l'indicazione "ricevuto via email" e farlo pervenire all' Ufficio Protocollo per la registrazione come se fosse un documento originale cartaceo.

Torna al sommario

10.1.5 Errata ricezione di documenti digitali

Nel caso in cui pervengano sulla casella di posta istituzionale dell'ASST o in una casella non istituzionale messaggi dal cui contenuto si rileva che sono stati erroneamente ricevuti, l'operatore di protocollo rispedisce il messaggio al mittente Tramite la funzione "notifica eccezione".

Torna al sommario

10.1.6 Ricezione di documenti cartacei a mezzo posta convenzionale

L'Ufficio Protocollo apre tutte le buste pervenute, compresa la corrispondenza nominativamente intestata qualora essa sia riferibile ad attività istituzionale, ed è registrata e sottoscritta tramite segnatura con apposizione di targhetta adesiva sul documento, ad esclusione della corrispondenza esclusa dalla protocollazione.

In considerazione dell'art. 616 C.P. fanno eccezione, e pertanto non vengono aperte, le buste con le caratteristiche seguenti:

1. Riportanti le seguenti diciture: "riservato", "personale", "confidenziale" o comunque dalla cui confezione si evinca il carattere di corrispondenza privata.

La corrispondenza personale viene consegnata al destinatario, il quale, dopo averne preso visione, se reputa che i documenti ricevuti debbano essere comunque protocollati perché riguardanti problematiche istituzionali, provvede a trasmetterli all' Ufficio Protocollo per la protocollazione. In caso di corrispondenza personale ricevuta tramite raccomandata o corriere, al momento del ritiro il destinatario firma un registro istituito allo scopo.

2. Riportanti le seguenti diciture: "offerta", "bando", "gara d'appalto" o simili, o comunque dalla cui confezione si evinca la partecipazione ad una gara (ad esempio: presenza di sigilli in ceralacca, firme apposte sui lembi della busta, ecc.).
3. Riconducibili a corrispondenza dal contenuto prettamente sanitario: per questa casistica i documenti sono consegnati in busta chiusa direttamente ai medici interessati, facendo firmare, per ricevuta, il apposito registro interno cartaceo. Tale registro viene utilizzato per registrare tutta la corrispondenza in busta chiusa registrata non aperta. In particolare vengono inserite le seguenti informazioni:
    a. Data
    b. mittente
    c. destinatario interno
    d. tipo di spedizione

copia informatica per consultazione

e. nominativo di chi ritira e firma

4. Indirizzate al personale ecclesiastico in servizio presso l'ASST.
5. Indirizzate ad Enti diversi dall'ASST.
6. Indirizzate a una delle Associazioni operanti all'interno dell'ASST.

Torna al sommario

10.1.7 Rilascio di ricevute attestanti la ricezione di documenti cartacei

Qualora un documento su supporto cartaceo venga consegnato allo sportello personalmente dal mittente o da altra persona incaricata, l'operatore dell'Ufficio Protocollo procede immediatamente alla registrazione del documento e provvede a consegnare al vettore una copia con apposto un timbro recante data e ora di ricezione e firma dell'operatore.

Torna al sommario

10.1.8 Conservazione delle buste o altri contenitori di documentazione

Le buste pervenute tramite posta raccomandata, corriere o altra modalità per la quale si renda rilevante evidenziare il mezzo di trasmissione, la data o il riferimento della spedizione, sono pinzate assieme al documento e trasmesse alla U.O./Servizio di competenza.
Tutte le altre buste non sono conservate.

Torna al sommario

10.2 Flusso dei documenti inviati dalla AOO

10.2.1 Trasmissione dei documenti informatici

La trasmissione dei documenti informatici soggetti alla registrazione di protocollo può essere effettuata dalla ASST mediante messaggi di posta elettronica certificata.

Per documenti in uscita s'intendono quelli prodotti dagli uffici dell'ASST nell'esercizio delle proprie funzioni, aventi rilevanza giuridico-probatoria e destinati a essere trasmessi a soggetti terzi o ad altre amministrazioni.

Per la spedizione dei documenti informatici, l'ASST si avvale della casella di posta elettronica certificata istituzionale (protocollogenerale@pec.asst-mantova.it).
I documenti in partenza verso destinatari esterni ad ASST sono classificati secondo il titolario di classificazione, ed allegati in formato pdf ai dati di registrazione di protocollo e protocollati con il sistema Prisma dal personale dell'UO addetto alla protocollazione in partenza, che ha altresì la responsabilità:

- del loro inserimento nel fascicolo relativo al procedimento
- della loro archiviazione.

In particolare, al momento della protocollazione degli atti in uscita vanno inserite nel sistema tutte quelle informazioni ritenute necessarie per favorire una agevole ricerca degli atti, nonché un eventuale successivo monitoraggio delle pratiche stesse.
I documenti informatici sono trasmessi di norma per posta elettronica certificata. La trasmissione dalla casella di pec istituzionale ad una casella pec del destinatario costituisce evidenza giuridico-probatoria dell'invio e della consegna del messaggio (art.47 CAD).

copia informatica per consultazione

Al fine di garantire la riservatezza dei dati sensibili o giudiziari di cui all'articolo 4, comma l, lettere d) ed e), del decreto legislativo 30 giugno 2003, n. 196, l' art. 46 del CAD dispone che "i documenti informatici trasmessi ad altre pubbliche amministrazioni per via telematica possono contenere soltanto le informazioni relative a stati, fatti e qualità personali previste da legge o da regolamento e indispensabili per il perseguimento delle finalità per le quali sono acquisite."
Torna al sommario

10.2.2 Trasmissione di documenti analogici

Nei casi in cui il destinatario sia sprovvisto di un indirizzo di posta elettronica certificata, il documento può essere prodotto in formato analogico (sebbene debba essere sempre sottoposto a scansione in fase di protocollazione). I mezzi di recapito della corrispondenza, in quest'ultimo caso, sono:

1. il servizio di posta ordinaria o posta raccomandata;
2. ed il servizio telefax o telegramma;
3. consegna diretta al destinatario.

Per ogni documento cartaceo destinato ad essere spedito in originale vengono prodotti, di norma, tanti esemplari quanti sono i destinatari.
L'originale rappresenta la redazione definitiva, perfetta e autentica negli elementi sostanziali e formali.
Qualora si renda necessario, per ragioni amministrative, si possono produrre copie di un medesimo documento. Su ciascuna copia va apposta la dicitura "copia" a cura della struttura.
Le copie trasmesse per ragioni amministrative ad altre strutture organizzative sono conservate per tutto il tempo necessario allo svolgimento del procedimento cui il documento si riferisce e quindi eliminate secondo le norme previste.

L'originale del documento trasmesso deve essere conservato dal soggetto che lo ha formato, e che deve provvedere ad inserirlo nel fascicolo relativo al procedimento o affare cui si riferisce e/o ad archiviarlo.
Torna al sommario

10.3 Formazione dei documenti - Aspetti operativi

Il contenuto minimo dei documenti formati dall'ASST deve garantire la presenza delle seguenti informazioni:

a. la denominazione e il logo
b. l'indirizzo completo
c. il codice fiscale
d. l'indicazione completa dell'ufficio che ha prodotto il documento corredata dai numeri di telefono ed indirizzo di posta elettronica.

Il documento, inoltre, deve recare almeno le seguenti informazioni:

e. il luogo di redazione del documento;
f. la data (giorno, mese, anno);
g. il numero di protocollo;
h. l'oggetto del documento;
i. il numero degli allegati (se presenti);
j. se trattasi di documento informatico, la firma elettronica qualificata da parte del RPA;

copia informatica per consultazione

k. se trattasi di documento cartaceo, la sigla autografa da parte del RPA e/o del responsabile del provvedimento finale.

Torna al sommario

10.4 Registrazione e segnatura di protocollo dei documenti ricevuti

I documenti dai quali possano nascere diritti, doveri o legittime aspettative di terzi vanno registrati. La numerazione delle registrazioni di protocollo è unica e rigidamente progressiva. Essa si chiude al 31 dicembre di ogni anno e ricomincia da 1 all'inizio dell'anno successivo.

La ratio che deve governare il comportamento di un operatore durante la fase di registrazione di un documento in arrivo deve essere improntata alla avalutatività. In altre parole, l'operatore di protocollo deve attestare che un determinato documento così come si registra è pervenuto. Si tratta dunque di una delicata competenza di tipo notarile, attestante la certezza giuridica di data, forma e provenienza per ogni documento.

La registrazione della documentazione ricevuta durante l'orario di apertura dell'Ufficio Protocollo viene effettuata di norma entro la giornata di arrivo.

La corrispondenza ricevuta durante l'orario di chiusura dell'Ufficio, è protocollata il giorno lavorativo successivo. Il sistema di protocollazione Prisma dispone comunque di un apposito campo in cui indicare l'ora effettiva di ricezione. In caso di ricezione di PEC, il sistema le acquisisce completando automaticamente il suddetto campo. L'unica eccezione prevista è l'utilizzo del protocollo differito.

Poiché la data di registrazione di un documento è parte integrante della segnatura di protocollo non è necessario apporre al documento stesso altri timbri che riportino l'indicazione della data di ricezione.

E' fatto divieto alle UU.OO./Servizi dell'ASST di utilizzare protocolli di ufficio o di settore, diversi dalla numerazione di protocollo ufficiale dell'ASST.
L'Ufficio Protocollo provvede alla protocollazione dei documenti utilizzando il sistema informatico, di cui al paragrafo 7.2.
La registrazione dei documenti ricevuti, spediti o interni è effettuata in un'unica operazione.
L'operazione di registrazione può essere di 3 tipi:

- Registrazione in Entrata o in Uscita
- Registrazione di emergenza in Entrata o in Uscita
- Recupero di una registrazione di emergenza in Entrata o in Uscita

Su ogni documento ricevuto dall'ASST è effettuata una registrazione di protocollo con il sistema di gestione del protocollo informatico, consistente nella memorizzazione dei dati obbligatori. Tale registrazione è eseguita in un'unica operazione, senza possibilità per l'operatore di inserire le informazioni in più fasi successive.

Ciascuna registrazione di protocollo contiene ai sensi dell'art. 53 del Testo Unico, i seguenti dati obbligatori in forma non modificabile:

a) il numero di protocollo, generato automaticamente dal sistema e registrato in forma non modificabile;
b) la data di registrazione di protocollo, assegnata automaticamente dal sistema e registrata in forma non modificabile;
c) il mittente per i documenti ricevuti o, in alternativa, il destinatario o i destinatari per i documenti spediti, registrati in forma non modificabile;

copia informatica per consultazione

d) l'oggetto del documento, registrato in forma non modificabile;
e) la data e il numero di protocollo del documento ricevuto, se disponibili;
f) l'impronta del documento informatico, se trasmesso per via telematica, costituita dalla sequenza di simboli binari in grado di identificarne univocamente il contenuto, registrata in forma non modificabile.

L'assegnazione ad un destinatario interno avviene indicando l'Unità Operativa o il Servizio competente in merito alla trattazione del procedimento di cui il documento fa parte così come previsto dagli artt. 4-6 della Legge 7 agosto 1990, n. 241, modificata dalla Legge 15/2005. Il Responsabile del procedimento coincide con il Responsabile dell'U.O./Servizio competente.
Dati obbligatori, da registrare in forma non modificabile, qualora essi siano disponibili al momento della registrazione stessa:

- data e numero di protocollo del documento ricevuto;
- Dati accessori da registrare, anche se non espressamente richiesto dalla normativa:
- numero degli allegati;
- descrizione degli allegati;
- mezzo di spedizione/ricezione (posta ordinaria, raccomandata, raccomandata R/R, a mano, telegramma, fax, email, ecc.);
- altre note (tra cui: estremi provvedimento differimento termini di registrazione, elementi identificativi del procedimento amministrativo ecc.).

I documenti pervenuti alla casella di posta elettronica istituzionale, registrati automaticamente, sono sottoposti a segnatura automaticamente dal sistema di protocollo informatico.

L'UP provvede, contestualmente alla segnatura dei documenti ricevuti, a classificare il documento nelle modalità descritte.
Torna al sommario

10.5 Segnatura di protocollo

Contestualmente alla registrazione, non viene apposta/associata la segnatura di protocollo.
Al documento protocollato viene assegnato un ID univoco.

La registrazione e la segnatura costituiscono un'operazione unica e contestuale aventi entrambe la natura di atto pubblico.

La segnatura di protocollo è l'apposizione o l'associazione al documento, in forma permanente non modificabile, delle informazioni riguardanti la registrazione di protocollo per consentire di individuare ciascun documento in modo inequivocabile.

Per i documenti cartacei, la segnatura viene apposta utilizzando un'etichetta autoadesiva prodotta da una stampante termica al momento della registrazione; l'etichetta, di norma, va applicata sul recto del documento nel primo spazio libero. Il sistema consente di produrre più esemplari dell'etichetta da utilizzare, ad esempio, nel caso di documenti uguali indirizzati a destinatari plurimi.
Per i documenti informatici, la segnatura viene associata al documento attraverso la produzione di un file conforme alle specifiche XML.
La segnatura riporta le informazioni seguenti:

copia informatica per consultazione

a. il progressivo di protocollo (composto da 7 cifre numeriche riempite con zeri a sinistra);
b. la data di protocollo (nel formato gg/mm/aaaa);
c. l'identificazione in forma sintetica dell'Ente come AOO ("ASST Mantova);
d. tipologia di registrazione ("A" per registrazione in arrivo, "P" per registrazione in partenza)

La segnatura di protocollo di un documento cartaceo avviene attraverso l'apposizione su di esso di un "segno" grafico sul quale vengono riportate le informazioni relative alla registrazione di protocollo.
Torna al sommario

10.6 Scansione dei documenti cartacei

Dopo la registrazione e la segnatura, le immagini dei documenti pervenuti su supporto cartaceo vengono acquisite tramite scanner e automaticamente associate alla registrazione di protocollo corrispondente attraverso il codice a barre apposto contestualmente alla segnatura.
Torna al sommario

10.7 Protocollazione differita

Nel caso di eccezionale carico di lavoro, che non permette di evadere la corrispondenza ricevuta nei tempi sopra indicati e qualora dalla mancata registrazione di protocollo del documento nella medesima giornata lavorativa di ricezione possa risultare leso un diritto di terzi (es. partecipazione concorso), è autorizzato l'uso del protocollo differito.
In particolare, vengono individuati i documenti da ammettere alla registrazione differita, le cause e il termine entro il quale la registrazione di protocollo deve essere comunque effettuata. Si applica solo ai documenti in arrivo e per tipologie omogenee che il dirigente dell'UP deve descrivere nel provvedimento.

In caso di mancata registrazione dei documenti entro eventuali scadenze:

- documenti cartacei: viene apposto un timbro con la data di ricezione effettiva con l'indicazione dell'orario scritto a penna. Tali estremi saranno poi inseriti manualmente a sistema con una nota.
- Corrispondenza: per i documenti ricevuti tramite PEC, non viene riportato sul sistema l'orario di ricezione, ma soltanto la data dal momento che tale documentazione viene acquisita automaticamente dal sistema Prisma. In questo caso l'Ufficio Protocollo inserisce manualmente una nota con l'ora effettiva di ricezione e successivamente acquisisce manualmente la PEC, in modo da permettere la visione del certificato di avvenuta ricezione.
-

Torna al sommario

copia informatica per consultazione

10.8 Registro giornaliero di protocollo

Il registro di protocollo è un atto pubblico originario che fa fede della tempestività e dell'effettivo ricevimento e spedizione di un documento, indipendentemente dalla regolarità del documento stesso ed è idoneo a produrre effetti giuridici a favore o a danno delle parti.
Il registro di protocollo è inoltre soggetto alle forme di pubblicità e di tutela di situazioni giuridicamente rilevanti previste dalla normativa vigente.
Giornalmente il sistema di protocollo produce in automatico il Registro Giornaliero di Protocollo, contenente tutte le protocollazioni/registrazioni effettuate il giorno precedente.

Torna al sommario

10.9 Documenti soggetti a protocollo riservato

Tutti i documenti vengono registrati utilizzando il protocollo informatico unico dell'Ente. Non sono quindi previsti documenti soggetti a protocollazione riservata.
Nei casi in cui sia necessario adottare misure di riservatezza ulteriori (ad esempio, nei casi seguenti: documenti legati a vicende di persone o a fatti privati, documenti contenenti informazioni sensibili, documenti dalla cui contestuale pubblicità possa derivare pregiudizio a terzi o al buon andamento dell'attività amministrativa ecc.) nell'oggetto del documento si indicano le generalità degli individui coinvolti utilizzando le iniziali del nome e del cognome anziché riportarle per esteso. In questi casi, inoltre, il documento non viene scansionato.

Torna al sommario

10.10 Casistica

Qui di seguito vengono fornite alcune indicazioni pratiche riguardo ai comportamenti organizzativi da adottare di fronte ad alcune situazioni che accadono comunemente negli uffici di registratura in relazione a particolari casi di corrispondenza in entrata.

Torna al sommario

10.10.1 Allegati

Tutti gli allegati pervenuti all'Ufficio Protocollo vanno registrati indicando nella registrazione del documento di accompagnamento il loro numero (effettiva quantità di allegati ricevuta) e la loro descrizione. Su ogni singolo allegato andrà trascritto il numero e l'anno di protocollo del documento di accompagnamento. Si osserva che sugli allegati non vanno applicate copie dell'etichetta utilizzata come segnatura di protocollo del documento di accompagnamento.
Il sistema informatico prevede una funzione specifica che permette di gestire ogni singolo allegato come un documento a sé stante; in alternativa, gli allegati vengono scansionati unitamente al documento principale. Questa indicazione vale, in particolare, per allegati quali, a titolo di esempio:

- contratti
- convenzioni
- relazioni tecniche
- verbali

copia informatica per consultazione

Non devono essere scansionati gli allegati che costituiscono documentazione a carattere prettamente sanitario/scientifico o il testo di articoli pubblicati.

Torna al sommario

10.10.2 Allegati pervenuti senza lettera di accompagnamento

Per i documenti da considerare ai fini procedimentali come documenti allegati, ma pervenuti senza lettera di accompagnamento, si procede registrandoli secondo l'usuale procedura.

Torna al sommario

10.10.3 Fax

Per i documenti ricevuti e inviati via fax si seguono le medesime indicazioni fornite relativamente ai documenti pervenuti o trasmessi attraverso altri mezzi di spedizione e quindi, nei casi già descritti, devono essere registrati dall'Ufficio Protocollo.
Si ponga attenzione a riportare la segnatura non tanto sulla copertina di trasmissione, quanto piuttosto sul documento. A questo proposito si sottolinea l'inutilità della copertina di trasmissione qualora essa abbia una funzione prevalentemente informativa e non giuridico-probatoria. Se la copertina del fax riporta un commento, un'indicazione o una frase significativa, la segnatura va posta sulla copertina e il documento dovrà essere trattato come allegato.
Si osserva che ogni documento deve essere individuato all'interno dell'Ente da un solo numero di protocollo, indipendentemente dal supporto e dal mezzo di trasmissione; qualora successivamente al fax pervenisse anche l'originale del documento, a questo dovrà essere attribuito lo stesso numero di protocollo e su di esso dovrà essere applicata l'etichetta con la segnatura (comprensiva di codice a barre). Il fax potrà quindi essere distrutto tranne nel caso in cui su di esso siano state apposte informazioni ritenute importanti (note del dirigente, appunti, ecc.) o si discosti significativamente dal documento pervenuto in seguito.

Torna al sommario

10.10.4 Documenti pervenuti in copie plurime

Nel caso di documenti pervenuti in più copie (documenti uguali indirizzati a destinatari plurimi) si darà ad ognuno di essi lo stesso numero di protocollo (applicando l'etichetta con la segnatura solo sul primo documento originario ricevuto e apponendo sulle altre copie a penna gli estremi del protocollo) e successivamente dovranno essere assegnati ai singoli destinatari.

Torna al sommario

10.10.5 Invio massivo

Qualora il medesimo documento debba essere inviato a un numero considerevole di destinatari, per esigenze di semplificazione verrà seguita la procedura di seguito descritta:

- nel campo "Destinatari" della procedura di protocollo informatico andrà riportato solo il nominativo del primo destinatario e la frase *"trattasi di invio massivo di comunicazione a …"* specificando la tipologia di destinatari
- nel campo "Descrizione allegati" andrà riportata la dicitura "Elenco altri destinatari";
- l'elenco dei destinatari viene gestito come allegato alla registrazione di protocollo;

copia informatica per consultazione

- il numero di protocollo è il medesimo per tutte le note inviate che vengono inserite nello stesso fascicolo.
-

Torna al sommario

10.10.6 Documenti anonimi o con firma non identificabile

I documenti anonimi (lettere/email) indirizzati alle Direzioni aziendali e/o genericamente all'ASST vengono inoltrati alla Direzione Strategica, che valuta l'opportunità della protocollazione e dell'eventuale seguito.
Qualora la Direzione dia l'indicazione per la protocollazione, nel campo mittente va indicata la denominazione "Anonimo".
Per i documenti con firma illeggibile e mittente non identificabile, nel campo «mittente» viene apposta la dicitura "firma non identificabile". Tali documenti vengono assegnati all'UO competente per materia.

Torna al sommario

10.10.7 Lettere con mittente non identificabile

Le lettere (non anonime) per le quali non sia identificabile il mittente devono essere protocollate. Nel campo mittente va indicata l'anagrafica "Mittente non identificato" o qualsiasi altro elemento utile all'identificazione del mittente.
Nel caso in cui siano PEC in cui non viene rilevato il mittente, va indicato nell'anagrafica del mittente l'indirizzo della PEC di provenienza.

Torna al sommario

10.10.8 Atti giudiziari

Con il termine "atti giudiziari" si intende tutta la corrispondenza proveniente da:

- Procure della Repubblica
- Tribunali di ogni ordine e grado
- Commissariati di Polizia
- Arma dei Carabinieri
- Polizia locale

Tale corrispondenza deve essere protocollata al pari della corrispondenza ordinaria.

Torna al sommario

10.10.9 Documenti indirizzati nominalmente al personale dell'ASST

La posta indirizzata nominalmente al personale dell'ASST è regolarmente aperta e registrata al protocollo, a meno che sulla busta non sia riportata la dicitura "personale" - "riservata personale" o espressione equivalente.
In questo caso la corrispondenza viene consegnata in busta chiusa al destinatario, che se reputa che i documenti acquisiti debbano essere, comunque, protocollati provvede a trasmetterli all'UP.

Torna al sommario

copia informatica per consultazione

10.10.10 Documenti non firmati

I documenti in arrivo identificabili ma privi di firma del mittente sono regolarmente sottoposti alle operazioni di registrazione di protocollo e di segnatura e nel campo «mittente» viene apposta la dicitura "firma mancante".
Analogamente si registrano al protocollo i documenti in arrivo privi della firma del mittente, per essi nel campo «mittente» viene apposta la dicitura "documento non sottoscritto". Tali documenti vanno assegnati all'UO competente per materia.

Torna al sommario

10.10.11 Documenti recanti oggetti plurimi

Nel caso di acquisizione di un documento indicante più oggetti, relativi a procedimenti diversi e quindi a differenti fascicoli, si dovranno produrre copie autentiche dello stesso documento e successivamente registrarle, classificarle e fascicolarle indipendentemente una dall'altra.
L'originale verrà inviato al destinatario indicato nel documento, oppure, nel caso di destinatari plurimi, al primo in indirizzo.
Torna al sommario

10.10.12 Protocolli urgenti

Il dirigente dell'UP può disporre la protocollazione immediata di documenti in entrata urgenti, nel caso in cui il carattere d'urgenza emerge dal contenuto del documento stesso.
Torna al sommario

10.10.13 Integrazioni documentarie

In caso di acquisizione all'Ufficio Protocollo di integrazioni documentarie il personale addetto non è tenuto a verificare la completezza sostanziale della documentazione pervenuta.
Torna al sommario

11 Flussi di lavorazione dei documenti non Protocollati

In questo capitolo sono descritti i processi di formazione e gestione dei documenti della ASST non soggetti a protocollazione. I processi legati alla fase di conservazione sono descritti nel Manuale di conservazione della ASST e del Conservatore.
Per quanto attiene alla formazione dei documenti Sanitari e Socio Sanitari ed, in particolare, agli aspetti inerenti i requisiti funzionali e di contenuto, si fa rinvio al "Manuale per la gestione della documentazione Sanitaria e Sociosanitaria della Regione Lombardia" di cui alla D.G.R. n. IX/4659 del 09.01.2013 ed al documento "Immagini, suoni e biosegnali: Manuale nei percorsi di cura" di cui alla D.G.R. n.X/3001 del 09.01.2015
La Tabella successiva riassume i flussi documentali gestiti, gli applicativi utilizzati e le UO coinvolte. Mentre nei paragrafi successivi sono brevemente descritti i flussi documentali.

Flusso Documentale	Classe Documentale	Applicativi utilizzati (Fornitore)	UO Coinvolte
Fatture	Fatture Attive e Notifiche		SEF (Struttura Risorse Economico Finanziarie)
		Hub Regionale (ARIA)	
	Fatture Passive e Notifiche		SEF (Struttura Risorse Economico Finanziarie)
		Hub Regionale (ARIA)	
DAE	Cedolini, Cartellini	Sigma/GPI	SRU (Struttura Risorse Umane)

copia informatica per consultazione

	e CU risorse Umane		UO interessata
	Delibere	Sfera	Affari Generali e Direzione Tutte le UO
	Determine	Sfera	Affari Generali e Direzione Tutte le UO
	Repertori	Prisma	Ufficio protocollo
	Documenti Protocollati	Prisma	Ufficio Protocollo Uffici protocollo decentrati
	LOG di trasmissione di cedolini e CU RU	Sigma	SRU (Struttura Risorse Umane) UO interessata
	RT	Mypay	Aria
	RPT	Mypay	Aria
	SINTEL 5/10/20 anni e illimitati	Sintel	Aria
RD	Ricette Dematerializzate Erogate	Applicativo EP	UO Sanitarie
	Ricette Dematerializzate Erogate Annullate	Applicativo EP	UO Sanitarie
	Ricette Dematerializzate Prescritte	PRR – Dataprocessing SISS (ARIA)	UO Sanitarie (visita ambulatoriale, ricovero, PS, laboratorio, radiologia)
	Ricette Dematerializzate Prescritte Annullate	Applicativo EP	Reparti, Ufficio Ricovero, Gestione operativa e sistemi informativi
		SISS (ARIA)	
DCE	Lettere di Dimissione	Recovery (Data processing)	Reparti e PS
		Galileo (Dedalus)	
	Referti di Documenti Clinici Generici	Health Meeting (Woezen)	Reparto competente
		PMA (Itamedical)	
		Galileo (Dedalus)	
	Referti Ambulatoriali	View Point (Medas)	Reparto competente (diabetologia, endoscopia, ostetricia, radiologia)
		Smart Digital Clinic (Meteda)	
		Endox (Tesi)	
		RA2000 (Siemens) PACS aziendale (Siemens/Kodak)	
		Delaus (Galileo)	
	Referti Anatomia Patologica	Armonia (Dedalus)	Anatomia Patologica
		Galileo (Dedalus)	
	Referti di Laboratorio	DN Lab	Laboratorio
		DN Firma	
		Galileo (Dedalus)	

copia informatica per consultazione

	Referti di Radiologia	RA2000 (Siemens) PACS aziendale (Siemens/Kodak)	Radiologia
		Galileo (Dedalus)	
	Verbali di Pronto Soccorso	Pronto Soccorso Web (Data Processing)	Medico UO competente
		Galileo (Dedalus)	
	Verbali Operatori	Ormaweb (Dedalus)	UO competenti
		Galileo (Dedalus)	
DICOM	DICOM	RA2000 (Siemens)	UO competenti
		PACS aziendale (Siemens/Kodak)	

Torna al sommario

11.1 Fatture

I flussi documentali delle Fatture si riferiscono alla produzione dei seguenti documenti:

- **Fatture Attive e Notifiche:** La UOC Struttura Risorse Economico Finanziarie (SEF) crea la fattura attiva tramite apposita funzionalità dell'applicativo Smart*Financial. La UOC firma digitalmente la fattura solamente in caso di fatturazione a PA e la invia all'Hub Regionale tramite apposita funzionalità dell'applicativo. A fronte della fattura attiva ASST riceve le relative notifiche da SDI tramite l'Hub Regionale e gli EP.
- **Fatture Passive e Notifiche:** Il documento è ricevuto dalla UOC Struttura Risorse Economico Finanziarie (SEF), giornalmente (o più volte al giorno). L'ufficio effettua un controllo formale sul documento e, nel caso in cui la fattura presentasse dati non corretti questa viene rifiutata immediatamente, senza il caricamento sul gestionale.
  Se la fattura è corretta viene autorizzato il pagamento previa verifica del servizio di competenza. L'ufficio di competenza, infatti, verifica la fattura e approva o rifiuta la fattura. In caso di rifiuto l'ufficio comunica, entro 15 gg, il motivo del rifiuto (tramite mail). In caso di rifiuto, l'UOC Struttura Risorse Economico Finanziarie (SEF), tramite apposita funzionalità e integrazione con l'Hub Regionale, rifiuta la fattura. In caso di approvazione, l'UOC Struttura Risorse Economico Finanziarie (SEF), convalida la fattura e genera l'OPI per il pagamento. Il documento è inviato all'hub regionale tramite apposita integrazione. Tramite apposita integrazione le notifiche sono ricevute dall'HUB Regionale e periodicamente l'UOC verifica le notifiche ricevute e gestisce gli scarti.

Torna al sommario

11.2 Documenti Amministrativi Elettronici (DAE)

I flussi documentali dei documenti amministrativi elettronici si riferiscono alla produzione dei seguenti documenti:

- **Documenti Protocollati:** Per il dettaglio del flusso si fa riferimento al Capitolo 10.
- **Registro giornaliero di Protocollo:** Per il dettaglio del flusso si fa riferimento al Capitolo 10.
- **Decreto:** Il redattore dello schema di decreto è l'utente incaricato dell'inserimento dei dati alfanumerici e del testo della proposta (Strutture abilitate). L'accesso al sistema (Sfera) avviene tramite utenze nominali e tutti i componenti della stessa Struttura con

copia informatica per consultazione

il ruolo di redattore hanno la possibilità di inserire proposte per la Struttura di appartenenza (principali informazioni da inserire sono: responsabile del procedimento, firmatario, oggetto, classificazione/fascicolo, testo del documento, allegati). Il redattore, come tutti gli attori del flusso, possono inserire allegati alla proposta di decreto, che formeranno parte integrante dell'atto. È possibile associare alla proposta ulteriori documenti informatici (riferimenti), conservati nel fascicolo come documenti istruttori. I redattori, come tutti gli attori del flusso, possono inserire note al testo, visibili in apposita sezione. L'applicativo consente altresì, di inviare la comunicazione di avvenuta pubblicazione sia ad utenti interni registrati nel flusso, sia ad utenti esterni tramite mail. Il numero attribuito alla proposta al momento della registrazione è un progressivo annuale, indipendente dalla Struttura proponente, che identifica univocamente la proposta.
Il Responsabile del Procedimento verifica la proposta e, se corretta, appone un visto con firma debole al prosieguo dell'iter della proposta.
L'RdP può, altresì, modificare/integrare la proposta e gli allegati, annullarla o re-inviarla al redattore.
La proposta giunge sulla scrivania virtuale del Direttore della Struttura o suo delegato (firmatario) che ne verifica il contenuto e, se approva, sottoscrive ed invia per le fasi successive. Il firmatario può re-inviare la proposta al redattore o al RdP, con eventuali note.
La proposta giunge quindi al SEF per l'apposizione del visto contabile, se previsto. Nella fase di gestione del parere contabile sarà nella disponibilità degli utenti SEF anche la funzionalità di "re-invia a unità proponente", con possibilità di inserire note: l'azione procederà alla ri-generazione della proposta, riportando la proposta sulle scrivanie virtuali degli utenti dell'unità proponente completamente modificabile (storicizzando i documenti). Una volta che gli utenti dell'unità proponente avranno terminato le modifiche, la proposta ripercorrerà i passaggi previsti prima di tornare al parere contabile.
Tutti i passaggi vengono storicizzati e resi visibili nell'apposita sezione.
Gestita la fase istruttoria, la proposta viene posta nella disponibilità degli utenti di AAGG, i quali hanno la possibilità di verificare la congruità della proposta e di modificarla.
L'Ufficio AAGG effettua una verifica formale su: sintassi, forma, coerenza degli allegati, aderenza alle linee guida, conformità al regolamento vigente, elementi essenziali dell'atto. Completata la verifica, se corretta viene inviata per i pareri dei Direttori (amministrativo, sanitario, sociosanitario), se presenta anomalie viene modificata o re-inviata sulla scrivania virtuale del redattore o del RDP, con possibilità di inserire note.
Gli utenti AAGG hanno la possibilità di sottoporre la proposta al Responsabile AAGG.
La proposta inizia il percorso di acquisizione dei pareri, a partire dal primo Direttore indicato. Ognuno avrà la possibilità di firmare la proposta di Decreto o di creare un parere contrario, il parere contrario diviene parte integrante del Decreto. Anche ogni Direttore ha la possibilità di modificare il testo, di inserire note e re-inviare la proposta ad AAGG.
Acquisiti i pareri dei Direttori, AAGG procede alla creazione della seduta e alla compilazione dell'ordine del giorno e sottopone la proposta di Decreto alla firma del Direttore Generale che può firmare l'atto o rimandarlo ad AAGG.

copia informatica per consultazione

Contestualmente alla firma digitale del Direttore Generale il sistema effettua la produzione di un documento in formato PDF/A contenente numero e data del Decreto e la numerazione dell'atto nel registro di riferimento.
Con l'apposizione della firma digitale il Decreto viene adottato e convertito in formato p7m.
L'adozione coincide con l'esecutività dell'atto, a meno che lo stesso non preveda il controllo regionale (in questo caso, l'esecutività sarà indicata a seguito della comunicazione della Regione, tramite apposita funzionalità applicativa).
Il documento è classificato secondo titolario e massimario di scarto di Regione Lombardia.
La pubblicazione è automatica: è il flusso documentale che si occupa di pubblicarne le informazioni sull'Albo Pretorio e sul sito dell'Amministrazione Trasparente
Il sistema SFERA invia in automatico gli atti in conservazione al termine del periodo di pubblicazione sull'albo pretorio.

- **Determine:**
  Il redattore dello schema di determina è l'utente incaricato dell'inserimento dei dati alfanumerici e del testo della proposta, l'accesso al sistema avviene tramite utenti nominali .
  Tutti i componenti della stessa Struttura con il ruolo di redattore hanno la possibilità di inserire proposte per il servizio di appartenenza (principali informazioni da inserire sono: responsabile del procedimento, firmatario, oggetto, classificazione/fascicolo, testo del documento, allegati).
  È possibile associare alla proposta ulteriori documenti informatici (riferimenti), conservati nel fascicolo come documenti istruttori.
  Il numero attribuito alla proposta al momento della registrazione è un progressivo annuale, indipendente dal servizio proponente, che identifica univocamente la proposta.
  Il Responsabile del Procedimento verifica la proposta e, se corretta, appone un visto con firma debole al prosieguo dell'iter della proposta .
  L'RdP può, altresì, modificare/integrare la proposta e gli allegati, annullarla o re-inviarla al redattore .
  La proposta giunge quindi al SEF per l'apposizione del visto contabile. Nella fase di gestione del parere contabile sarà nella disponibilità degli utenti SEF anche la funzionalità di "re-invia a unità proponente", con possibilità di inserire note: l'azione procederà alla ri-generazione della proposta, riportando la proposta sulle scrivanie virtuali degli utenti dell'unità proponente completamente modificabile (storicizzando i documenti). Una volta che gli utenti dell'unità proponente avranno terminato le modifiche, la proposta ripercorrerà i passaggi previsti prima di tornare al parere contabile.
  L'Ufficio Affari Generali effettua una verifica formale su: sintassi, forma, coerenza degli allegati, aderenza alle linee guida, conformità al regolamento vigente, elementi essenziali dell'atto.
  Completata la verifica: se corretta viene inviata per la firma del Dirigente, se presenta anomalie viene modificata o re-inviata sulla scrivania virtuale del redattore o del RDP, con possibilità di inserire note.
  Il documento viene firmato dal Direttore (o suo delegato) della Struttura che ha generato la Determina. Il Direttore, indicato come firmatario, può: firmare il

copia informatica per consultazione

documento con firma digitale oppure annullare la proposta. Può anche Re-inoltrare all'unità proponente con possibilità di inserire note: la proposta viene "rigenerata" e, dopo la revisione dell'unità proponente, il flusso ripercorre i passi relativi al passaggio presso il RDP e SEF per l'apposizione del visto contabile.
In caso di adozione il sistema effettua la numerazione dell'atto nel registro di riferimento e la produzione di un documento in formato PDF/A contenente numero e data della determina.
Con l'apposizione della firma digitale la determina viene adottata, diventa esecutiva e convertita in formato p7m.
Tutti i passaggi vengono storicizzati e resi visibili nell'apposita sezione.
Il documento viene classificato secondo titolario e massimario di scarto di Regione Lombardia.
La pubblicazione è automatica: è il flusso documentale che si occupa di pubblicarne le informazioni sull'Albo Pretorio e sul sito dell'Amministrazione Trasparente**.** Sul sistema SFERA gli atti vengono inviati automaticamente in conservazione al termine del periodo di pubblicazione sull'albo pretorio.

- **RT:** A seguito del pagamento viene creato il documento da parte del PSP che invia il documento a PAGO PA. Il documento viene inviato da PAGO PA a MyPay e archiviato su MyPay.
- **RPT:** A seguito della richiesta di pagamento del cittadino (o tramite interfaccia MyPay o tramite PSP) viene creato il documento. Il documento creato è inviato a PAGO PA che invia l'esito della richiesta che viene gestita da MyPay.
- **SINTEL 5/10/20 anni e illimitati: vengono gestiti diversi tipi di documenti dettagliati di seguito.**
  - Documenti di gara SA: Lato EP avviene il caricamento su una apposita sezione della piattaforma dei documenti di gara (es. disciplinare, capitolato, eventuali allegati). I documenti sono archiviati sul sistema e, a seconda della tipologia di gara e dalla configurazione della gara effettuata dalla SA, sono resi disponibili ai fornitori e/o pubblicati sul portale di Aria. L'EP può aggiungere dei documenti (es. risposte chiarimenti) e possono disattivare i documenti e allegarne di nuovi (per tutto il corso della gara). Per alcune Gare, è generata e inviata in automatico una mail PEC a tutti i fornitori invitati o che hanno partecipato.
  - Report: Tramite la piattaforma è possibile generare due tipologie di report: 1 - Report generati automaticamente dal sistema. A conclusione della gara (aggiudicazione), se la SA ha scelto la modalità dedicata, i fornitori visualizzano la Graduatoria..
    2 - Report generati su richiesta delle SA. In fase di valutazione è possibile scaricare report provvisori che, per accettazione possono essere firmati e ricaricati dall'EP (non è obbligatorio).E' effettuato un controllo non bloccante sulla validità della firma. A seconda della procedura, il report è semplificato (singolo lotto). Per il multilotto (esistono report per singolo lotto o multilotto).
  - Verbali: Una apposita funzionalità permette alle SA di inserire i nomi della commissione giudicatrice. I membri della commissione possono aggiungere i propri commenti. Il sistema li memorizza e li traccia all'interno di un report. Le SA (RUP o delegato della procedura) possono generare il verbale. Il file è generato, scaricato ed è possibile firmarlo digitalmente (ed eventualmente marcarlo temporalmente) e ricaricarlo. È effettuato un controllo non bloccante sulla validità della firma.

copia informatica per consultazione

- Documentazione di offerta: In questa tipologia documentale si distinguono due tipi di documenti:
  1- La documentazione di offerta caricata dai fornitori sulla base di quanto richiesto dalla SA, nella maggior parte dei casi richiede pdf firmati e/o marcati. In questa fase il fornitore può caricare i vari documenti richiesti. I formati non sono soggetti a controlli bloccanti tranne se configurato dalla SA il controllo bloccante sulla validità di firma e/o marca.
  2- Il Report sulle attività e le informazioni inserite dai fornitori. A conclusione del caricamento dell'offerta, è generato un report con le info caricate dal fornitore. Il documento è firmato e ricaricato firmato dal fornitore.
- Comunicazioni di procedura: Sia lato fornitore sia lato SA è possibile scambiare comunicazioni e/o eventuali allegati, tramite apposita funzionalità della piattaforma. Contestualmente è inviata una mail PEC con la stessa comunicazione. Il sistema, per ciascuna comunicazione scambiata, genera un report pdf contenente l'inbox e l'outbox della comunicazione ed eventualmente gli allegati.
- Report messaggi PEC: Il documento Report messaggi PEC è generato dal sistema in formato .pdf e contiene tuttle le mail PEC spedite relative alla gara.
- File Psw: Il documento è un file zip contenente un file txt, in cui è indicata la Password specifica del fascicolo (semi-chiave di decifratura) per le offerte che necessitano la cifratura. L'altra semi-chiave è in possesso di Aria. Il file è generato quando è prodotto il fascicolo (prima della creazione del pdv).
- Indice: Il file è generato quando è prodotto il fascicolo (prima della creazione del pdv) e contiene i metadati dei documenti presenti nei fascicoli.

- **Cedolini, Cartellini e CU RU: Cartellino presenze:** Per il personale del comparto afferente al SITRA è previsto un programma di rilevazione presenze (SigmaPlanner) in cui si possono verificare anomalie, rispetto orari, ecc. Le operazioni devono essere concluse dal coordinatore entro i primi giorni del mese successivo a quello di riferimento per permettere all'Ufficio Rilevazione Presenze di chiudere i cartellini e di passare le voci accessore nei cedolini. Per il personale non afferente al SITRA, le operazioni vengono svolte dal personale dell'ufficio rilevazione presenze: mensilmente viene effettuato un controllo sulle anomalie e comunicate, tramite invio del cartellino provvisorio al Responsabile (medici e comparto non SITRA) indicando un termine entro il quale il cartellino dovrà essere restituito con le correzioni da apportare, debitamente firmato. Se i cartellini restituiti con le correzioni presentano altre anomalie, si richiede nuovamente al responsabile di giustificare le eventuali anomalie.
  Per quanto riguarda i cedolini, da parte del servizio ER avviene l'elaborazione definitiva dei cedolini del mese che produce: file degli stipendi, (definito secondo tracciato record concordato, che viene trasmesso al Tesoriere Aziendale tramite PEC), file che viene trasmesso alla SEF tramite mail contenente l'indicazione degli importi da pagare per ruolo e conto economico di riferimento. Il file viene utilizzato dalla SEF per l'elaborazione degli ordinativi di pagamento ed il versamento delle ritenute.
  Prima dell'invio dei cedolini, vengono effettuati controlli di sistema (correttezza dati) e d'ufficio. Prima dell'elaborazione definitiva il settore ER controlla la coerenza dell'importo netto rilevato dal file con il netto di quanto viene trasmesso in tesoreria.
  Con cadenza mensile, al termine dello scarico delle voci accessorie nel cedolino paga, il cartellino definitivo viene pubblicato sull'Angolo del Dipendente e messo a disposizione del dipendente mentre, per i cedolini, l'attività mensile si conclude con la pubblicazione sul portale (angolo del dipendente) dei cedolini del mese.

copia informatica per consultazione

La SRU mette a disposizione le CU sul Portale aziendale (Angolo del Dipendente) per i dipendenti in essere e invia i modelli in cartaceo ai dipendenti cessati; per i cartacei, verifica il ricevimento da parte del lavoratore e in caso di mancato recapito le rispedisce.

- **LOG di trasmissione di Cedolini e CU Risorse umane:** I log di trasmissione vengono generati dal sistema e pubblicati sul portare (angolo del dipendente).

Torna al sommario

11.3 Ricette Dematerializzate

I flussi documentali delle ricette dematerializzate si riferiscono alla produzione dei seguenti documenti:

- **Ricette Dematerializzate Prescritte:** La prescrizione delle ricette dematerializzate viene effettuata dai medici al termine dell'evento di cura (visita ambulatoriale, ricovero, passaggio PS, laboratorio, radiologia) eseguito presso l'ente. Tramite gli applicativi dedicati (PRR) il medico seleziona le prestazioni/farmaci da prescrivere ed invia le Ricette Dematerializzate prescritte tramite servizi dedicati esposti dal SISS. Il modulo GSSC.PRSC trasmette al MEF l'xml della ricetta prescritta, gestisce la risposta di esito del MEF e memorizza i dati sul SISS. Il modulo GSSC.PRSC crea i messaggi jms e popola una coda centralizzata. Il modulo Conservare gestisce la creazione del PdV e l'invio in conservazione. Il documento inviato in conservazione è un file .zip contenente i file xml di invio, risposta e, solo per la farmaceutica, le credenziali dell'operatore che ha creato la ricetta. Il modulo Conservare interroga il servizio del sistema di conservazione per l'avvenuta conservazione. In caso di errori e scarto del PdV, il modulo Conservare interroga il sistema di conservazione per richiedere il Rapporto di Versamento e lo memorizza sul SISS.
- **Ricette Dematerializzate Prescritte Annullate:** L'annullamento delle ricette dematerializzate può essere effettuato in qualsiasi momento solo dal medico che le ha prescritte. Gli applicativi specifici degli ASST inviano le Ricette Dematerializzate Prescritte Annullate tramite servizi dedicati esposti dal SISS. Il modulo GSSC.PRSC trasmette al MEF l'xml della ricetta Prescritta Annullata, gestisce la risposta di esito del MEF e memorizza i dati sul SISS. Il modulo GSSC.PRSC crea i messaggi jms e popola una coda centralizzata. Il modulo Conservare gestisce la creazione del PdV e l'invio in conservazione. Il documento inviato in conservazione è un file .zip contenente i file xml di invio, risposta e, solo per la farmaceutica, le credenziali dell'operatore che ha creato la ricetta. Il modulo Conservare interroga il servizio del sistema di conservazione per l'avvenuta conservazione. In caso di errori e scarto del PdV, il modulo Conservare interroga il sistema di conservazione per richiedere il Rapporto di Versamento e lo memorizza sul SISS.
- **Ricette Dematerializzate Erogate:** L'erogazione delle ricette dematerializzate è un processo in carico all'ASST. In base ai messaggi che riceve dai vari dipartimentali, l'ASST invia le Ricette Dematerializzate erogate tramite servizi dedicati esposti dal SISS. Per quanto riguarda le RD erogate specialistiche, il modulo Erogaspec trasmette al MEF l'xml della ricetta erogata, gestisce la risposta di esito del MEF e memorizza i dati sul SISS. Per quanto riguarda le RD erogate farmaceutiche, il modulo TSAR trasmette al MEF l'xml della ricetta erogata, gestisce la risposta di esito del MEF e memorizza i dati sul SISS. Il modulo Erogafarm memorizza i dati relazionali sul SISS. I moduli Erogaspec e Erogafarm creano i messaggi jms e popolano una coda

copia informatica per consultazione

centralizzata. Il modulo Conservare gestisce la creazione del PdV e l'invio in conservazione. Il documento inviato in conservazione è un file .zip contenente i file xml di invio, risposta e, solo per la farmaceutica, le credenziali dell'operatore che ha creato la ricetta. Il modulo Conservare interroga il servizio del sistema di conservazione per l'avvenuta conservazione. In caso di errori e scarto del PdV, l'applicativo Conservare interroga il sistema di conservazione per richiedere il Rapporto di Versamento e lo memorizza sul SISS.

- **Ricette Dematerializzate Erogate Annullate:** L'annullamento dell'erogazione delle ricette dematerializzate è un processo in carico all'EP. In base ai messaggi che riceve dai vari dipartimentali, l'EP invia le Ricette Dematerializzate erogate annullate tramite servizi dedicati esposti dal SISS. Per quanto riguarda le RD erogate annullate specialistiche, il modulo Erogaspec trasmette al MEF l'xml della ricetta erogata annullata, gestisce la risposta di esito del MEF e memorizza i dati sul SISS. Per quanto riguarda le RD erogate annullate farmaceutiche, il modulo TSAR trasmette al MEF l'xml della ricetta erogata annullata, gestisce la risposta di esito del MEF e memorizza i dati sul SISS. Il modulo Erogafarm memorizza i dati relazionali sul SISS. Il modulo Erogaspec e Erogafarm creano i messaggi jms e popolano una coda centralizzata. Il modulo Conservare gestisce la creazione del PdV e l'invio in conservazione. Il documento inviato in conservazione è un file .zip contenente i file xml di invio, risposta e, solo per la farmaceutica, le credenziali dell'operatore che ha creato la ricetta. Il modulo Conservare interroga il servizio del sistema di conservazione per l'avvenuta conservazione. In caso di errori e scarto del PdV, il modulo Conservare interroga il sistema di conservazione per richiedere il Rapporto di Versamento e lo memorizza sul SISS.

Torna al sommario

11.4 Documenti clinici

I flussi documentali dei documenti clinici si riferiscono alla produzione dei seguenti documenti:

- **Referti Ambulatoriali:** Le worklist create sul sistema CUP, in base alle richieste pervenute dal CCR e tramite le accettazioni CUP, sono inviate agli applicativi di destinazione dedicati a seconda della tipologia di richiesta. I sistemi delle UO di competenza recepiscono le worklist inviate dal CUP mentre e le richieste che sono inserite manualmente. Il medico, a seguito della prestazione ambulatoriale redige il referto. Il referto in formato .pdf è firmato dal medico tramite carta SISS e marcato temporalmente. Il referto firmato e marcato temporalmente è archiviato nel repository aziendale Galileo. Il referto firmato e marcato temporalmente è archiviato nel repository regionale e pubblicato nel Fascicolo Sanitario del Paziente, che potrà consultare il documento accedendo con le proprie credenziali. Non verrà pubblicato sul FSE se il referto corrisponde ad una visita richiesta da UO interna per un paziente già ricoverato. L'archiviazione avviene tramite procedure schedulate dedicate.
- **Referti Anatomia Patologica:** Le worklist create sul sistema CUP sono inviate all'applicativo di destinazione. A seguito dell'esame acquisito dall'integrazione viene redatto il referto. Il referto in formato .pdf è firmato dal medico tramite carta SISS e marcata temporalmente. Il referto firmato e marcato temporalmente è archiviato nel repository aziendale Galileo. Il referto firmato e marcato temporalmente è archiviato nel repository regionale e pubblicato nel Fascicolo Sanitario del Paziente, che potrà

copia informatica per consultazione

consultare il documento accedendo con le proprie credenziali. Non verrà pubblicato sul FSE se il referto corrisponde ad una visita richiesta da UO interna per un paziente già ricoverato. L'archiviazione avviene tramite procedure schedulate dedicate.

- **Referti di Documenti Clinici Generici:** I documenti afferenti a questa classe documentale, sono referti generati da Health Meeting (per i referti multidisciplinari: caso clinico per il quale è necessario il consulto tra più specialisti), PMA (procreazione medicalmente assistita), Galileo (per ECG: il documento consiste nel referto del cardiologo e nel tracciato rilevato in sede di esame). Al termine della prestazione (o prestazioni in caso di terapie prolungate), il referto in formato .pdf è prodotto e firmato dal medico tramite carta SISS e marcato temporalmente. Il referto firmato e marcato temporalmente è archiviato nel repository aziendale Galileo. L'archiviazione avviene tramite procedure schedulate dedicate.
- **Referti di Laboratorio:** Per i pazienti esterni, all'accettazione viene utilizzato DN Territorio mentre gli altri due canali (PS o order entry da Galileo) sono dedicati ai clienti ricoverati. DN Lab genera i referti ed è integrato con i vari strumenti di laboratorio da cui riceve i dati. Al termine dell'esame, gli esiti sono caricati dagli strumenti di laboratorio sul sistema. Il medico redige il referto tramite apposita funzionalità. Il referto in formato .pdf è firmato dal medico tramite carta SISS (DNFirma) e marcata temporalmente. Il referto firmato e marcato temporalmente è archiviato nel repository aziendale e pubblicato nel Fascicolo Sanitario del Paziente, che potrà consultare il documento accedendo con le proprie credenziali. Non verrà pubblicato sul FSE se il referto corrisponde ad una visita richiesta da UO interna per un paziente già ricoverato. L'archiviazione avviene tramite procedure schedulate dedicate.
- **Referti di Radiologia**: Le worklist sono create in base alle richieste provenienti dai diversi applicativi integrati o, ove possibile, inserite manualmente. Le richieste contengono tutte le informazioni necessarie del paziente, della prestazione da erogare, del reparto e del presidio di provenienza. I referti di Radiologia vengono generati dall'applicativo RA2000, integrato con il CUP per i pazienti esterni. RA2000 è utilizzato per la refertazione mentre l'attvitità di imaging è gestita dal PACS aziendale. Se la richiesta deriva da PS c'è integrazione tra PS, data processing e sistema di refertazione RA2000 oppure per order entry e, in tal caso, la richiesta viene effettuata da Galileo, gestita all'interno di un'interfaccia legata al CUP per pianificare la prestazione e compare sul sistema RIS per poi essere refertata a seguito dell'esame. Il medico radiologo redige il referto, tramite apposita funzionalità del RIS, che ha una struttura definita e validata. Il medico ha la possibilità di visualizzare le immagini tramite integrazione nativa del RIS con il PACS. Il RIS gestisce la prestazione aggiuntiva con modulo prescrittivo interno e restituisce al CUP la prescrizione della prestazione aggiunta per la rendicontazione (solo per gli ambulatoriali esterni). Il referto in formato .pdf è firmato dal medico tramite carta SISS e marcato temporalmente. Il referto firmato e marcato temporalmente è archiviato nel repository aziendale e nel repository regionale e pubblicato nel Fascicolo Sanitario del Paziente, che potrà consultare il documento accedendo con le proprie credenziali. Non verrà pubblicato sul FSE se il referto corrisponde ad una visita richiesta da UO interna per un paziente già ricoverato. L'archiviazione avviene tramite procedure schedulate dedicate.
- **Verbali di Pronto Soccorso:** Il personale infermieristico, in fase di accettazione del paziente, inserisce l'anagrafica del paziente e crea l'episodio (Pronto Soccorso Web). Una volta creato l'episodio, medici e infermieri abilitati possono accedere all'episodio e richiedere consulenze mediche oppure, tramite integrazione con gli applicativi

copia informatica per consultazione

dedicati, esami di laboratorio e prestazioni radiologiche. Durante la permanenza del paziente, sono inserite nella scheda dedicate le richieste effettuate (consulenze, esami radiologici, esami di laboratorio) per il paziente. Tramite le integrazioni dedicate è possibile visualizzare le eventuali immagini radiologiche e il referto. Alla chiusura dell'episodio è generato un documento .pdf. Il verbale in formato .pdf è firmato dal medico tramite carta SISS e marcato temporalmente. Il referto firmato e marcato temporalmente è archiviato nel repository aziendale Galileo. Il referto firmato e marcato temporalmente è archiviato nel repository regionale e pubblicato nel Fascicolo Sanitario del Paziente, che potrà consultare il documento accedendo con le proprie credenziali. Come da indicazioni regionali sul FSE viene pubblicato il Verbale di Pronto soccorso ma non vengono pubblicato sul FSE le prestazioni a corredo effettuate durante l'episodio di Pronto soccorso come esami di laboratorio, consulenze specialistiche, referti di radiologia o strumentali. L'archiviazione avviene tramite procedure schedulate dedicate.

- **Verbali Operatori:** La produzione di Verbali Operatori avviene a seguito di ricoveri ordinari, d'urgenza oppure BIC (Bassa Intensità Chirurgica: prestazioni di chirurgia semplice in day hospital poi trasformate in prestazioni semi-ambulatoriali). Il posizionamento in lista operatoria è formato su Ormaweb a seguito di visita specialistica e valutazioni mediche che producono il modulo inserito nel sistema. Per il ricovero d'urgenza invece il PS chiude il verbale con esito di ricovero e il paziente viene portato in sala operatoria. Al termine della prestazione operatoria il verbale deve essere validato da tutti gli attori coinvolti dei diversi dipartimenti (Infermieristica, Anestesia, Chirurgia e talvolta Radiologia) tramite firma debole (utente-password che blocca la parte di ogni ente). Il documento viene poi firmato dal medico responsabile di sala, marcato e archiviato sul Repository aziendale Galileo.
- **Lettere di Dimissione:** L'accettazione del paziente per il successivo ricovero può avvenire in due modalità: 1. accettazione in reparto (ricovero programmato o pre-ricovero da PS), 2. accettazione allo sportello dell'ufficio ricoveri. Se l'accettazione avviene in reparto, il personale infermieristico inserisce l'anagrafica del paziente altrimenti l'attività è in capo all'amministrativo dell'ufficio ricovero di competenza.
  In entrambi successivamente viene creata la cartella clinica. Durante il ricovero del paziente, sono inserite nella scheda dedicate le richieste effettuate per il paziente. Tramite le integrazioni dedicate è possibile visualizzare le eventuali immagini radiologiche e il referto. Alla conclusione del ricovero è prodotta la lettera di dimissione. La lettera di dimissione in formato .pdf è firmata dal medico tramite carta SISS e marcata temporalmente. Il referto firmato e marcato temporalmente è archiviato nel repository aziendale Galileo e pubblicato nel Fascicolo Sanitario del Paziente, che potrà consultare il documento accedendo con le proprie credenziali. L'archiviazione avviene tramite procedure schedulate dedicate.

Torna al sommario

11.5 DICOM

Nel Sistema Informatico Radiologico - RIS sono create le worklist in base alle richieste provenienti dai diversi applicativi integrati e al paziente viene associato un ID Patient. Le richieste contengono tutte le informazioni necessarie del paziente, della prestazione da

copia informatica per consultazione

erogare, del reparto e del presidio di provenienza. Sono consentite inoltre richieste esterne. Le worklist create popolano le macchine radiologiche.
A seguito della prestazione radiografica sono create le immagini. Le immagini create sono corredate dai dati recepiti dal RIS, dai tag DICOM e sono inviate dalla macchina al PACS e archiviate secondo la tipologia di immagine, anagrafica, id studio, presidio di competenza. È possibile recuperare tutte le informazioni relative ad uno specifico paziente tramite l'ID Patient associato.
Torna al sommario

12 Organizzazione dei documenti informatici, dei fascicoli informatici e delle serie informatiche

All'interno del sistema di gestione informatica dei documenti vengono formati, gestiti e utilizzati tipologie di aggregazioni documentali informatiche diverse dai fascicoli: serie che aggregano documenti e serie che aggregano fascicoli.

L'aggregazione documentale consiste nell'insieme di documenti o insieme di fascicoli riuniti per caratteristiche omogenee, in relazione alla natura e alla forma dei documenti o in relazione all'oggetto e alla materia o in relazione alle funzioni dell'ente. Distinguiamo tre tipi di aggregazioni documentali, di seguito descritte: i fascicoli, le serie documentali e le serie di fascicoli.

Fascicolo: aggregazione documentale strutturata e univocamente identificata. Si possono costituire diverse tipologie di fascicoli (per affare, per persona fisica o giuridica, per attività, per procedimento). I fascicoli sono aperti di norma al livello più basso del titolario di classificazione. Nel caso del fascicolo per persona fisica o giuridica il fascicolo può essere aperto anche al livello di titolo (primo livello), quindi esso potrà contenere documenti appartenenti a classi diverse.

Serie documentale: aggregazione di documenti con caratteristiche omogenee, raggruppati ad esempio in base alla tipologia documentaria (es. delibere, decreti, fatture) o alla provenienza o all'oggetto. I documenti all'interno di una serie, non essendo aggregati utilizzando il titolario di classificazione come nel caso dei fascicoli, possono appartenere a titoli e classi differenti tra loro.

Serie di fascicoli: Le serie di fascicoli possono essere utilizzate per aggregare fascicoli omogenei per oggetto o tipologia o comunque per ragioni funzionali all'organizzazione del lavoro. I fascicoli accorpati per ragioni funzionali in base alla classe di riferimento (es. tutti i fascicoli aperti all'interno del titolo I classe 6) o alla tipologia di fascicoli (es. tutti i fascicoli del personale).

13 Misure di sicurezza e protezione dei dati personali

Per le misure di sicurezza e protezione dei dati personali si fa riferimento al documento di Piano di sicurezza allegato al presente documento.

Torna al sommario

copia informatica per consultazione

14 Piano di conservazione

Per il piano di conservazione si fa riferimento alle informazioni inserite nel Manuale di conservazione allegato al presente documento.

Torna al sommario

copia informatica per consultazione

DECRETO N. 1496 DEL 28/12/2021
DEL DIRETTORE GENERALE

OGGETTO: ATTUAZIONE DELLE REGOLE PREVISTE DAL "CODICE DELL'AMMINISTRAZIONE DIGITALE": NOMINA DEL RESPONSABILE DELLA GESTIONE DOCUMENTALE

Riproduzione cartacea del documento informatico sottoscritto digitalmente da
MARA AZZI il 28/12/2021 18:38:59 ai sensi dell'art. 20 e 23 del D.lgs 82/2005

copia informatica per consultazione

IL DIRETTORE GENERALE

PREMESSO che negli ultimi anni il Legislatore ha introdotto importanti disposizioni in materia di digitalizzazione della pubblica amministrazione volte a dare completa attuazione alle regole stabilite dal D.lgs. 82/2005 "Codice dell'amministrazione digitale" o, per abbreviazione, "CAD", con l'obiettivo di realizzare la compiuta digitalizzazione dell'attività della P.A. attraverso l'adozione di adeguate procedure di gestione documentale e di conservazione sostitutiva che portino al completo *switch off* dalla carta al digitale per tutti i documenti della pubblica amministrazione;

RICHIAMATE le disposizioni vigenti in materia e in particolare, oltre al già citato D.Lgs. 7 marzo 2005 n. 82:

- Regolamento eIDAS (electronic Identification Authentication and Signature) - Regolamento UE n°910/2014 emanato il 23 luglio 2014, è entrato in vigore direttamente in tutti gli Stati Membri il17 settembre 2014;
- DPR 28 dicembre 2000 n. 445 - Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa;
- L. 7/08/1990 n. 241 - Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi;
- D.Lgs. 30/06/2003 n. 196 - Codice in materia di protezione dei dati personali ed il Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali;
- "Linee Guida sulla formazione, gestione e conservazione dei documenti informatici" emanate da AGID, come previsto dall'art. 71 del CAD modificato dal D.Lgs.n.217/2017, entrate in vigore il 12.09.2020, che raggruppano in un "corpo unico" le regole tecniche concernenti la formazione, protocollazione, gestione e conservazione dei documenti informatici e aggiornano la precedente normativa di cui ai DPCM 2013 e 2014 e successivi aggiornamenti;

ATTESO che il D.P.R. 28.12.2000 n. 445 dispone che le Pubbliche Amministrazioni individuino, nell'ambito dei propri ordinamenti, "*gli uffici da considerare ai fini della gestione unica o coordinata dei documenti per grandi aree organizzative omogenee, assicurando criteri uniformi di classificazione e archiviazione*" (art. 50 comma 4);

ATTESO che il citato DPR n. 445/2000 dispone inoltre che "*ciascuna amministrazione istituisce un servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi in ciascuna delle grandi aree organizzative omogenee individuate ai sensi dell'articolo 50*", prevedendo che al servizio sia preposto un dirigente ovvero un funzionario (art. 61) in possesso di idonei requisiti professionali o di professionalità tecnico-archivistica, definendo altresì i compiti attribuiti al servizio stesso;

CONSIDERATO che l'attività del Responsabile della gestione documentale deve essere svolta in collaborazione ed intesa con gli altri soggetti individuati dalle citate normative in materia - responsabile della conservazione, responsabile per la transizione digitale e responsabile del trattamento dei dati personali – per la definizione e l'applicazione di criteri uniformi di trattamento del documento informatico con particolare riguardo alla

Riproduzione cartacea del documento informatico sottoscritto digitalmente da
MARA AZZI il 28/12/2021 18:38:59 ai sensi dell'art. 20 e 23 del D.lgs 82/2005
DECRETO DEL DIRETTORE GENERALE: 2021 / 1496 del 28/12/2021

copia informatica per consultazione

comunicazione interna tra le aree organizzative omogenee, alla classificazione, all'archiviazione e successiva formazione del pacchetto di versamento e quindi del transito del documento nel sistema di conservazione, nonché a provvedere alla stesura del manuale di gestione documentale;

PRESA VISIONE, inoltre, dell'attuale assetto del sistema di gestione documentale in atto in Azienda:

- con Decreto n. 213 del 19.02.2021 è stato nominato il Responsabile della Transizione Digitale dell'ASST di Mantova;
- con deliberazione dell'ex A.O. "C. Poma" n.1080 del 6.10.2015 è stato nominato in via provvisoria, quale Responsabile della tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi, l'addetto dell'ufficio protocollo;
- con deliberazione dell'ex A.O. "C. Poma" n.1081 del 6.10.2015 è stato approvato il manuale di gestione documentale aziendale;

RITENUTO opportuno, in considerazione dell'importanza e centralità del tema della gestione documentale e dell'ormai non più procrastinabile utilizzo generalizzato del documento informatico presso le pubbliche amministrazioni e alla luce della mutata realtà aziendale, aggiornare il sistema di gestione dei documenti informatici come di seguito specificato:

- individuare quale Responsabile della gestione documentale il Direttore della Struttura Complessa Affari Generali e Controlli Interni, in considerazione del fatto che il vigente POAS colloca le suddette funzioni nell'ambito della struttura da lui diretta;
- confermare il *"Manuale per la gestione del protocollo informatico, dei flussi documentali e degli archivi aziendali* già approvato con Deliberazione dell'ex A.O. "C. Poma" n. 1081/2015, fino alla sua revisione a cura del nuovo Responsabile;

RICORDATO che il Responsabile della Gestione Documentale deve porre in essere le azioni più opportune per il costante monitoraggio ed aggiornamento periodico, in presenza di cambiamenti normativi, organizzativi, procedurali o tecnologici rilevanti, del manuale di gestione documentale, provvedendo, altresì alla pubblicazione dello stesso sul sito web aziendale;

PRESO ATTO dell'attestazione di regolarità e di legittimità del presente provvedimento espressa da ALBINI GIUSEPPE Direttore della Struttura AFFARI GENERALI E CONTROLLI INTERNI, e da CASARI ANTONELLA, responsabile del procedimento;

DATO ATTO che il presente provvedimento non comporta oneri o proventi a carico dell'Azienda;

ACQUISITI i pareri del Direttore Amministrativo, del Direttore Sanitario e del Direttore Socio Sanitario;

copia informatica per consultazione

DECRETA

1. di nominare il Direttore della Struttura Complessa Affari Generali e Controlli Interni quale Responsabile della gestione documentale ai sensi dell'articolo 61, comma 2, del DPR n. 445/2000 e del D.lgs. n.82 del 7.03.2005;

2. di incaricare il Responsabile della Gestione Documentale ed il Responsabile della Transizione Digitale, per quanto di rispettiva competenza, di dare attuazione alle Linee Guida Agid emanate il 12.09.2020, e successive modifiche ed aggiornamenti, nei termini previsti;

3. di confermare in via transitoria il "Manuale di gestione del protocollo informatico dei flussi documentali e degli archivi" approvato con deliberazione dell'ex A.O.C. Poma n.1081 del 6.10.2015, incaricando il Responsabile della Gestione Documentale di provvedere, in tempi brevi, all'aggiornamento del manuale stesso;

4. di pubblicare il presente provvedimento all'Albo on line sul sito istituzionale aziendale, ai sensi dell'art. 32 della L. n. 69/2009 e dell'art. 17 della L.R. 33/2009, nel rispetto del Regolamento UE 2016/679.

PRESO ATTO dei pareri di

DIRETTORE AMMINISTRATIVO	FERRARI GIUSEPPE
DIRETTORE SANITARIO	BELLOMETTI SIMONA AURELIA
DIRETTORE SOCIOSANITARIO	BOSCAINI RENZO

DIRETTORE GENERALE
AZZI MARA
(atto firmato digitalmente ai sensi
delle vigenti disposizioni di legge)

copia informatica per consultazione

DECRETO N. 549 DEL 23/06/2022
DEL DIRETTORE GENERALE

OGGETTO: ATTUAZIONE DELLE REGOLE PREVISTE DAL "CODICE DELL'AMMINISTRAZIONE DIGITALE": NOMINA DEL RESPONSABILE DELLA CONSERVAZIONE DEI DOCUMENTI INFORMATICI DELL'ASST DI MANTOVA

IL DIRETTORE GENERALE

Riproduzione cartacea del documento informatico sottoscritto digitalmente da
MARA AZZI il 23/06/2022 14:36:23 ai sensi dell'art. 20 e 23 del D.lgs 82/2005
DECRETO DEL DIRETTORE GENERALE: 2022 / 549 del 23/06/2022

copia informatica per consultazione

PREMESSO che dal 1° gennaio 2022 sono entrate in vigore le "Linee Guida sulla formazione, gestione e conservazione dei documenti informatici" emanate da AGID, rilevanti per affrontare il processo di trasformazione digitale delineato nel Codice dell'Amministrazione Digitale, D.Lgs. n.82/2005 e nel Testo Unico sulla documentazione amministrativa, D.P.R.n.445/2000 che prevedono, tra l'altro, l'obbligo di nominare all'interno di ogni organizzazione aziendale la figura del Responsabile della Conservazione dei documenti informatici, definendone il ruolo, le competenze e le responsabilità;

RICHIAMATI, in particolare:
- l'art.43 e seguenti del D.Lgs. n. 82/2005 che prescrivono che i documenti informatici siano conservati in modo permanente con modalità digitali e prevedono l'adozione di regole, procedure e tecnologie che garantiscano caratteristiche di autenticità, integrità, affidabilità, leggibilità e reperibilità dei documenti, affidandone la gestione al Responsabile della conservazione;
- il DPCM 3 dicembre 2013 "Regole tecniche in materia di sistemi di conservazione" e le linee guida AGID, con cui sono state emanate le specifiche regole tecniche in base alle quali nelle pubbliche amministrazioni il ruolo del Responsabile della Conservazione ha il compito di gestire il processo di conservazione, generare il rapporto di versamento, generare e sottoscrivere il pacchetto di distribuzione e predisporre il manuale di conservazione;
- l'art. 44, comma 1-bis del D.Lgs. n. 82/2005 che stabilisce "*Il sistema di gestione dei documenti informatici delle pubbliche amministrazioni è gestito da un responsabile che opera d'intesa con il dirigente dell'ufficio per la transizione alla modalità digitale, con il responsabile del trattamento dati personali di cui al D.Lgs. n.196/2003 e con il responsabile della conservazione dei documenti informatici delle P.A., nella definizione e gestione delle attività di rispettiva competenza*";
- l'art 44, comma 1 quater del del D.Lgs. n. 82/2005 che prevede la possibilità di affidare il sistema di conservazione all'esterno, in *outsourcing*, in modo totale o parziale, a soggetti terzi anche privati che offrano idonee garanzie organizzative e tecnologiche, sempre nel rispetto del *manuale di conservazione* adottato dall'Azienda, pur mantenendo in capo al Responsabile della conservazione l'attività di verifica e controllo;
- "Linee Guida sulla formazione, gestione e conservazione dei documenti informatici" emanate da AGID il 12.09.2020, come previsto dall'art. 71 del CAD modificato dal D.Lgs.n.217/2017, che raggruppano in un "corpo unico" le regole tecniche concernenti la formazione, protocollazione, gestione e conservazione dei documenti informatici e aggiornano la precedente normativa di cui ai DPCM 2013 e 2014 e successivi aggiornamenti;

Riproduzione cartacea del documento informatico sottoscritto digitalmente da
MARA AZZI il 23/06/2022 14:36:23 ai sensi dell'art. 20 e 23 del D.lgs 82/2005
DECRETO DEL DIRETTORE GENERALE: 2022 / 549 del 23/06/2022

copia informatica per consultazione

- Regolamento eIDAS (electronic Identification Authentication and Signature Regolamento UE n°910/2014 emanato il 23 luglio 2014, entrato in vigore direttamente in tutti gli Stati Membri il17 settembre 2014;

PRESA VISIONE dell'attuale assetto del sistema di gestione documentale in atto in Azienda:

- con Decreto n. 213 del 19.02.2021 è stato nominato il Responsabile della Transizione Digitale dell'ASST di Mantova;
- con Decreto n.1496 del 28.12.2021 è stato nominato Responsabile della gestione documentale dell'Azienda il Direttore della Struttura Complessa Affari Generali e Controlli Interni;
- con deliberazione dell'ex A.O. "C. Poma" n.1080 del 6.10.2015 veniva nominato, in via provvisoria, quale Responsabile della conservazione il responsabile dei sistemi informativi aziendali;
- Regione Lombardia ha fornito un sistema unico di conservazione digitale a norma a favore degli enti sanitari e amministrativi dislocati sul territorio e, a seguito di specifica gara, ha affidato il relativo servizio alla società ARUBA, gara a cui questa Azienda ha aderito, e sottoscritto con ARUBA il contratto;

RITENUTO opportuno, in considerazione dell'importanza e centralità del tema della gestione documentale e dell'ormai non più procrastinabile utilizzo generalizzato del documento informatico presso le pubbliche amministrazioni e alla luce della mutata realtà aziendale, ridefinire tutti i ruoli e responsabilità al fine di migliorare l'intero processo della gestione documentale dell'Azienda e revocare, quindi, le precedenti nomine effettuate con deliberazione n.1080 del 06.05.2015;

RITENUTO, pertanto, di individuare quale Responsabile della conservazione digitale a norma dell'intera documentazione dell'Azienda, il dirigente della Struttura Complessa Sistemi Informativi, Ing.Paolo Garbossa, in possesso della professionalità necessaria per ricoprire tale ruolo:
-competenze informatiche, atteso il contenuto altamente tecnico e specialistico dei manuali di gestione e conservazione che governano i processi dell'Azienda;
-conoscenza specifica degli applicativi in uso in Azienda;
-capacità di coordinamento e di condivisione delle scelte con gli attori coinvolti nel processo;

PRESO ATTO dell'attestazione di regolarità e di legittimità del presente provvedimento espressa da CANINO PIERO Direttore della Struttura AFFARI GENERALI E CONTROLLI INTERNI, e da CANINO PIERO, responsabile del procedimento;

Riproduzione cartacea del documento informatico sottoscritto digitalmente da
MARA AZZI il 23/06/2022 14:36:23 ai sensi dell'art. 20 e 23 del D.lgs 82/2005
DECRETO DEL DIRETTORE GENERALE: 2022 / 549 del 23/06/2022

copia informatica per consultazione

DATO ATTO che il presente provvedimento non comporta oneri o proventi a carico dell'Azienda;

ACQUISITI i pareri del Direttore Amministrativo, del Direttore Sanitario e del Direttore Socio Sanitario;

DECRETA

1. di nominare l'ing. Paolo Garbossa, dirigente della Struttura Complessa Sistemi Informativi Aziendali, quale Responsabile della conservazione dei documenti informatici dell'Azienda Socio Sanitaria Territoriale di Mantova, così come previsto dal D.Lgs..n.82/2005, a decorrere dalla data di approvazione del presente atto;

2. di incaricare il Responsabile della conservazione affinché ponga in essere le azioni conseguenti alla sua nomina e previste dalla normativa di settore;

3. di precisare che tale incarico è differenziato ed aggiuntivo rispetto al ruolo ricoperto nella struttura di appartenenza e che tale incarico non comporta oneri a carico dell'ASST;

4. di revocare le precedenti nomine effettuate con Deliberazione n. 1080 del 06.10.2015;

5. di pubblicare il presente provvedimento all'Albo on line sul sito istituzionale aziendale, ai sensi dell'art. 32 della L. n. 69/2009 e dell'art. 17 della L.R. 33/2009, nel rispetto del Regolamento UE 2016/679.

Riproduzione cartacea del documento informatico sottoscritto digitalmente da
MARA AZZI il 23/06/2022 14:36:23 ai sensi dell'art. 20 e 23 del D.lgs 82/2005
DECRETO DEL DIRETTORE GENERALE: 2022 / 549 del 23/06/2022

copia informatica per consultazione

PRESO ATTO dei pareri di

DIRETTORE AMMINISTRATIVO	FERRARI GIUSEPPE
DIRETTORE SANITARIO	MALINGHER ALESSANDRO
DIRETTORE SOCIOSANITARIO	BOSCAINI RENZO

DIRETTORE GENERALE
AZZI MARA
(atto firmato digitalmente ai sensi
delle vigenti disposizioni di legge)

Riproduzione cartacea del documento informatico sottoscritto digitalmente da
MARA AZZI il 23/06/2022 14:36:23 ai sensi dell'art. 20 e 23 del D.lgs 82/2005
DECRETO DEL DIRETTORE GENERALE: 2022 / 549 del 23/06/2022

copia informatica per consultazione

Deliberazione n. 1037

VERBALE DI DELIBERAZIONE

del DIRETTORE GENERALE

L'anno **DUEMILADICIASSETTE (2017)** il giorno **QUATTRO** del mese di **OTTOBRE** alle ore **11:00** presso la sede legale il Direttore Generale dr. Luca Filippo Maria Stucchi ha adottato la seguente deliberazione:

OGGETTO: ADOZIONE DEL REGOLAMENTO PER L'ESERCIZIO DEL DIRITTO DI ACCESSO AI DOCUMENTI AMMINISTRATIVI, DEL DIRITTO DI ACCESSO CIVICO AI DOCUMENTI OGGETTO DEGLI OBBLIGHI DI PUBBLICAZIONE, DEL DIRITTO DI ACCESSO GENERALIZZATO DELL'ASST DI MANTOVA

copia informatica per consultazione

Affari Generali

IL DIRETTORE GENERALE

PREMESSO:

che il decreto legislativo 25 maggio 2016, n. 97, recante "Revisione e semplificazione delle disposizioni in materia di prevenzione della corruzione pubblicità e trasparenza correttivo della legge 6 novembre 2012, n. 190 e del decreto legislativo 14 marzo 2013, n. 33, ai sensi dell'articolo 7 della legge 7 agosto 2015, n. 124, in materia di riorganizzazione delle amministrazioni pubbliche", ha modificato ed integrato il decreto legislativo 14 marzo 2013, n.33, con particolare riferimento al diritto di accesso civico;

che il novellato art. 1 co. 1 del D. Lgs. n. 33/2013, come modificato dal D. Lgs. 25 maggio 2016, n. 97, ridefinisce la trasparenza, come: accessibilità totale dei dati e documenti detenuti dalle pubbliche amministrazioni, non più solo al fine di favorire forme diffuse di controllo sul perseguimento delle funzioni istituzionali e sull'utilizzo delle risorse pubbliche, ma soprattutto come strumento di tutela dei diritti dei cittadini e di promozione della partecipazione degli interessati all'attività amministrativa;

che il nuovo comma 1 dell'art. 2 del D. Lgs. n. 33/2013, così come modificato dall'art.3 del Decreto 97/2016, chiarisce che: "Le disposizioni del presente decreto disciplinano la libertà di accesso di chiunque ai dati e ai documenti detenuti dalle pubbliche amministrazioni e dagli altri soggetti di cui all'articolo 2-bis, garantita, nel rispetto dei limiti relativi alla tutela di interessi pubblici e privati giuridicamente rilevanti, tramite l'accesso civico e tramite la pubblicazione di documenti, informazioni e dati concernenti l'organizzazione e l'attività delle pubbliche amministrazioni e le modalità per la loro realizzazione", ampliando l'oggetto del decreto in un ottica accentuata di trasparenza e pubblicità;

che, al fine di dare attuazione a tale nuovo principio di trasparenza, introdotto dal legislatore, l'ordinamento giuridico prevede tre distinti istituti:

- "accesso documentale" di cui agli artt. 22 e seguenti della legge 7 agosto 1990, n. 241, riconosciuto ai soggetti che dimostrino di essere titolari di un "interesse diretto, concreto e attuale, corrispondente a una situazione giuridicamente tutelata e collegata al documento al quale è chiesto l'accesso", con lo scopo di porre i soggetti interessati in grado di esercitare al meglio le facoltà (partecipative, oppositive e difensive) che l'ordinamento attribuisce loro, a tutela delle posizioni giuridiche qualificate di cui sono titolari,

copia informatica per consultazione

- "accesso civico semplice", previsto dall'art. 5 co. 1 del citato decreto n. 33/2013, riconosciuto a chiunque, indipendentemente dalla titolarità di una situazione giuridica soggettiva connessa, ma circoscritto ai soli atti, documenti e informazioni oggetto di obblighi di pubblicazione, al fine di offrire al cittadino un rimedio alla mancata osservanza degli obblighi di pubblicazione imposti dalla legge, sovrapponendo al dovere di pubblicazione il diritto del privato di accedere ai documenti, dati e informazioni,

- "accesso civico generalizzato" (FOIA), disciplinato dall'art. 5 co. 2 e dall'art. 5 bis del decreto trasparenza, anch'esso a titolarità diffusa, potendo essere attivato da chiunque e non essendo sottoposto ad alcuna limitazione quanto alla legittimazione soggettiva del richiedente, avente ad oggetto tutti i dati, i documenti e le informazioni detenuti dalle pubbliche amministrazioni, ulteriori rispetto a quelli per i quali è stabilito un obbligo di pubblicazione;

che in attuazione dell'art. 5 – bis, comma 6, del D.lgs n.33/2013 introdotto dal D.lgs 97/2016 l'Autorità Nazionale Anti Corruzione ha, di seguito, adottato la Deliberazione n.1309 del 28 dicembre 2016, relativa a : "Linee Guida recanti indicazioni operative ai fini della definizione delle esclusioni e dei limiti all'accesso civico di cui all'art.5 comma 2 del D.lgs. 33/2013", che fornisce una prima serie di indicazioni, riguardanti prevalentemente le esclusioni e i limiti all'accesso civico generalizzato, disciplinati dall'art. 5-bis, co. 1-3, del D.lgs 33/2013;

che il Dipartimento della Funzione Pubblica in raccordo con l'Autorità Nazionale Anti Corruzione (A.N.A.C.), nell'esercizio della sua funzione generale di "coordinamento" delle iniziative di riordino della Pubblica Amministrazione e di organizzazione dei relativi servizi" (art. 27, n.3, legge n.93 del 1983), ha adottato la Circolare n.2/2017, in tema di "Attuazione delle norme sull'accesso civico generalizzato (c.d. FOIA)";

DATO ATTO che le "Linee Guida recanti indicazioni operative ai fini della definizione delle esclusioni e dei limiti all'accesso civico di cui al più volte richiamato art. 5 co. 2 D.lgs. 33/2013, predisposto dall'Autorità Nazionale Anticorruzione ai sensi del co. 6 dell'art. 5-bis, invita i soggetti tenuti all'applicazione del decreto trasparenza ad adottare: nel più breve tempo possibile, adeguate soluzioni organizzative, al fine di coordinare la coerenza delle risposte sui diversi tipi di accesso, una disciplina organica e coordinata delle tre tipologie di accesso, anche nella forma di uno specifico regolamento, al fine di evitare comportamenti disomogenei tra gli uffici che vi devono dare attuazione e di disciplinare compiutamente i casi di esclusione ed i limiti al diritto di accesso nelle sue diverse forme;

copia informatica per consultazione

RITENUTO pertanto di adottare il Regolamento per l'esercizio del diritto di accesso ai documenti amministrativi, del diritto di accesso civico ai documenti oggetto degli obblighi di pubblicazione e del diritto di accesso generalizzato" allegato alla presente deliberazione, per formarne parte integrante e sostanziale,

RITENUTO altresì opportuno rendere coerente anche con la nuova organizzazione aziendale il Regolamento, definendo gli adeguamenti organizzativi occorrenti per consentire un idoneo coordinamento dei comportamenti delle varie articolazioni organizzative dell'Azienda;

ACQUISITI i pareri favorevoli del Direttore Amministrativo, Sanitario e Socio Sanitario;

D E L I B E R A

Per le motivazioni di cui in premessa che si intendono qui integralmente riportate:

1. di adottare il "Regolamento per l'esercizio del diritto di accesso ai documenti amministrativi - del diritto di accesso civico ai documenti oggetto degli obblighi di pubblicazione - del diritto di accesso generalizzato" allegato alla presente deliberazione, per formarne parte integrante e sostanziale,

2. di rendere coerente anche con la nuova organizzazione aziendale il Regolamento, definendo gli adeguamenti organizzativi occorrenti per consentire un idoneo coordinamento dei comportamenti delle varie articolazioni organizzative dell'Azienda;

3. di trasmettere il presente provvedimento al Collegio Sindacale, ex art. 3 ter del D.Lgs. n. 502/92 e smi e art. 12, comma 1, L.R. n. 33/09;

copia informatica per consultazione

4. di disporre la pubblicazione on line a cura del Responsabile della pubblicazione, ai sensi dell'art. 32 L. n. 69/2009 e dell'art. 18, comma 9 L.R. 33/2009.

IL DIRETTORE GENERALE
Dr. Luca Filippo Maria Stucchi

IL DIRETTORE AMMINISTRATIVO
Dr.ssa Anna Gerola

IL DIRETTORE SANITARIO
Dr. Maurizio Galavotti

IL DIRETTORE SOCIOSANITARIO
Dr. Renzo Boscaini

copia informatica per consultazione

Si dichiara che la presente deliberazione:

- viene affissa all'albo pretorio dal 11.10.2017 e vi rimarrà per quindici giorni consecutivi;
- è immediatamente esecutiva ai sensi della Legge Regionale 11/07/1997 n. 31;
- viene trasmessa al Collegio Sindacale in data 11.10.2017.

IL DIRETTORE AMMINISTRATIVO
(dr.ssa Anna Gerola)

copia informatica per consultazione

REGOLAMENTO PER L'ESERCIZIO

- **DEL DIRITTO DI ACCESSO AI DOCUMENTI AMMINISTRATIVI**
- **DEL DIRITTO DI ACCESSO CIVICO AI DOCUMENTI OGGETTO DEGLI OBBLIGHI DI PUBBLICAZIONE**
- **DEL DIRITTO DI ACCESSO GENERALIZZATO**

Sommario

copia informatica per consultazione

copia informatica per consultazione

PRINCIPI GENERALI

Fonti normative

- L. 7 agosto 1990, n. 241 e ss.mm.ii., “Nuove norme in materia di procedimento amministrativo e
  di diritto di accesso ai documenti amministrativi”;
- D.P.R. 28 dicembre 2000, n. 445 e ss.mm.ii., “Testo Unico in materia di documentazione amministrativa”;
- D.Lgs. 30 giugno 2003, n. 196 e ss.mm.ii., “Codice in materia di protezione dei dati personali”;
- D.Lgs. 7 marzo 2005, n. 82 e ss.mm.ii., “Codice dell'amministrazione digitale”;
- D.P.R. 12 aprile 2006, n. 184, “Regolamento recante disciplina in materia di accesso ai documenti amministrativi”;
- L. 6 novembre 2012, n. 190 e ss.mm.ii., “Disposizioni per la prevenzione e la repressione della corruzione e dell'illegalità nella Pubblica Amministrazione”;
- D.Lgs. 14 marzo 2013, n. 33 e ss.mm.ii., “Riordino della disciplina riguardante gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni”;
- L. 7 agosto 2015, n. 124, “Deleghe al Governo in materia di riorganizzazione delle amministrazioni pubbliche”;
- Decreto Legislativo 18 aprile 2016, n.50, “Codice degli appalti”;
- D.Lgs. 25 maggio 2016, n. 97, “Revisione e semplificazione delle disposizioni in materia di prevenzione della corruzione, pubblicità e trasparenza, correttivo della Legge 6 novembre 2012,
  n. 190 e del Decreto Legislativo 14 marzo 2013, n. 33, ai sensi dell'articolo 7 della Legge 7 agosto 2015, n. 124, in materia di riorganizzazione delle amministrazioni pubbliche”;
- Delibera ANAC n.1309 del 28 dicembre 2016 Linee Guida recanti indicazioni operative ai fini della definizione delle esclusioni e dei limiti all'accesso civico di cui all’art. 5 co. 2 del d.lgs. 33/2013.
- L. 8 marzo 2017, n. 24, “Disposizioni in materia di sicurezza delle cure e della persona assistita, nonché in materia di responsabilità professionale degli esercenti le professioni sanitarie”.
- D.Lgs. 19 aprile 2017, n. 56, “Disposizioni integrative e correttive al decreto legislativo 18 aprile 2016, n. 50”.
- Circolare n.2/2017, del Ministero per la semplificazione e la pubblica amministrazione, “Attuazione delle norme sull’accesso civico generalizzato (c.d. FOIA).

copia informatica per consultazione

Finalità

Il presente Regolamento disciplina le diverse tipologie di accesso: ai documenti, civico semplice e civico generalizzato, con la finalità di incidere effettivamente sul rapporto tra cittadini e PA. In questo contesto il potere esecutivo delegato è stato chiamato ad attenersi al principio di trasparenza, intesa come accessibilità totale dei dati e dei documenti detenuti dalla PA, ciò al fine di implementare forme diffuse di controllo dell'agire pubblico, a tutela dei diritti fondamentali di garanzia delle libertà individuali e collettive, costituzionalmente garantiti dall'art.2 della Carta. Il Consiglio di Stato, con proprio parere del 24 febbraio 2016, n.515/2016, ha già sottolineato l'importanza storica del passaggio da un regime sinora fondato sull'accesso dei soggetti legittimati e sull'obbligo di pubblicazione a un regime nuovo di *freedom of information*, che consente a chiunque (non più, quindi, a chi abbia una particolare situazione legittimante), la piena conoscenza degli atti amministrativi (cd. *full disclosure*), con il rinnovato istituto dell'"accesso civico".

Definizioni

Pubblica Amministrazione tutti i soggetti di diritto pubblico e i soggetti di diritto privato, limitatamente alla loro attività di pubblico interesse disciplinata dal diritto nazionale e comunitario. |Art. 22, comma 1 lett. e) L.241/90|

Accesso ai documenti amministrativi: è il diritto degli interessati, di prendere visione o di estrarre copia di documenti amministrativi |Art. 22, comma 1 lett. a) L.241/90|

Interessato all'accesso ai documenti amministrativi: tutti i soggetti privati, compresi quelli portatori di interessi pubblici o diffusi, che abbiano un interesse, diretto, concreto e attuale, corrispondente ad una situazione giuridicamente tutelata e collegata al documento al quale è richiesto l'accesso |Art. 22, comma 1 lett. b) L.241/90|;

Controinteressato: tutti i soggetti individuati o facilmente individuabili in base alla natura del documento richiesto, che dall'esercizio del diritto di accesso potrebbero vedere pregiudicato il loro diritto alla riservatezza. |Art. 22, comma 1 lett. c) L.241/90|;

Documento amministrativo: ogni rappresentazione, comunque formata, del contenuto di atti, anche interni, delle pubbliche amministrazioni o, comunque, utilizzati ai fini dell'attività amministrativa; ogni rappresentazione grafica, fotocinematografica, elettromagnetica o di qualunque altra specie del contenuto di atti, anche interni o non relativi ad uno specifico procedimento, detenuti da una pubblica amministrazione e concernenti attività di pubblico interesse, indipendentemente dalla natura pubblicistica o privatistica della loro disciplina sostanziale |Art. 22, comma 1 lett. d) L.241/90|;

Dato: elemento conoscitivo come tale, indipendentemente dal supporto fisico su cui è incorporato e a prescindere dai vincoli derivanti dalle sue modalità di organizzazione e conservazione;

Informazione: rielaborazione di dati detenuti dall'Azienda effettuata per propri fini e contenuti in distinti documenti;

copia informatica per consultazione

Accesso civico: è il diritto di chiunque di richiedere la pubblicazione di documenti, informazioni o dati per i quali sussistono specifici obblighi di trasparenza, nei casi in cui sia stata omessa la loro pubblicazione - |Art.5, comma1 D.lgs 33/13 smi|;

Pubblicazione: divulgazione, attraverso la sezione AMMINISTRAZIONE TRASPARENTE del sito istituzionale dei documenti, delle informazioni e dei dati concernenti l'organizzazione e l'attività dell'Azienda.

Accesso civico generalizzato: è il diritto di chiunque di accedere ai dati e ai documenti detenuti dalle pubbliche amministrazioni, ulteriori rispetto a quelli oggetto di pubblicazione, nel rispetto dei limiti relativi alla tutela di interessi giuridicamente rilevanti, secondo quanto previsto dall'art. 5 bis del D.lgs 33/2013 (come modificato dal D.lgs 97/2016) - |Art.5, comma2 D.lgs 33/13 smi|;

Interessato all'accesso civico o generalizzato: chiunque abbia interesse ad accedere ai dati e ai documenti detenuti dalle pubbliche amministrazioni senza alcuna limitazione |Art.5, comma 2 e 3 D.lgs 33/13 smi|;

Controinteressato all'accesso civico: tutti i soggetti che subirebbero un pregiudizio concreto alla tutela di uno dei seguenti interessi privati: protezione dei dati personali, in conformità con la disciplina legislativa in materia; libertà e segretezza della corrispondenza; interessi economici e commerciali, ivi compresi la proprietà intellettuale, il diritto d'autore e i segreti commerciali - |Art.5bis, comma2 D.lgs 33/13 smi|;

Sezione 1 - ACCESSO DOCUMENTALE

Articolo 1 - Ambito oggettivo

1. Oggetto del diritto di accesso sono i documenti amministrativi, materialmente esistenti e detenuti dalla Pubblica Amministrazione, ad eccezione di quelli indicati all'articolo 24, commi 1, 2, 3, 5 e 6 L.241/90. |Art.2, DPR 184/2006 – Art. 22, comma 3, L.241/90|
2. L'accesso è consentito sia a documenti originali sia a copie di essi; possono inoltre formare oggetto del diritto di accesso singole parti di documenti ovvero copie parziali degli stessi; ove opportuno le copie parziali comprendono la prima e l'ultima pagina del documento, con indicazione delle parti omesse.
3. Il diritto di accesso è esercitato relativamente a documenti individuati o facilmente individuabili; non rientrano pertanto nell'ambito del diritto di accesso le richieste volte non ad acquisire documenti preesistenti, ma a promuovere una ricognizione che obblighi l'Azienda ad effettuare un'apposita elaborazione di dati. |Art. 2, comma 2, D.P.R. 184/2016|
4. Non sono accessibili le informazioni in possesso di una pubblica amministrazione che non abbiano forma di documento amministrativo, salvo quanto previsto dal decreto legislativo 30 giugno 2003, n. 196, in materia di accesso a dati personali da parte della persona cui i dati si riferiscono. |Art. 22, comma 4, L.241/90|
5. Il diritto di accesso è esercitabile fino a quando la Pubblica Amministrazione ha l'obbligo di detenere i documenti amministrativi ai quali si chiede di accedere. |Art. 22, comma 6, L.241/90|
6. Le domande d'accesso devono essere circoscritte nel loro oggetto e i documenti cui si chiede di accedere devono essere specificatamente individuati.

copia informatica per consultazione

Articolo 2 - Legittimazione soggettiva

2.1 Interessati

1. Il diritto di accesso ai documenti relativi ad attività amministrative e/o sanitarie, è riconosciuto a chiunque, sia esso persona fisica o giuridica, abbia un interesse diretto, concreto e attuale corrispondente ad una situazione giuridicamente tutelata e collegata al documento al quale è chiesto di accedere. |Art. 22 comma 1 lett b), L. n. 241/1990|
2. Tale diritto è riconosciuto anche ad associazioni e comitati portatori di interessi pubblici o diffusi, previo accertamento della legittimazione e della natura dell'interesse giuridico di cui sono portatori per finalità normativa o statutaria. |4 del DPR 184/2006|

2.2 Controinteressati

1. Sono controinteressati tutti coloro i quali, anche se non sono nominati o coinvolti nel documento che incorpora le informazioni cui si vuole accedere, potrebbero vedere pregiudicato il loro diritto alla riservatezza. |Art. 22 comma 1 lett c), L. n. 241/1990|

2.3 Responsabile del procedimento di accesso

1. Il Responsabile del procedimento di accesso è il dirigente del servizio/struttura o dell'ufficio competente a formare l'atto o a detenerlo stabilmente ovvero, su designazione di questi, un altro dipendente addetto alle predette unità organizzative competenti a formare l'atto o a detenerlo stabilmente. |Art 6, comma 6 DPR 184/2006|
2. Nel caso di atti infra-procedimentali, responsabile del procedimento è, parimenti, il dirigente o il funzionario da lui delegato, competente all'adozione dell'atto conclusivo, ovvero a detenerlo stabilmente.
3. Il Responsabile del procedimento cura i rapporti con i soggetti legittimati a richiedere l'accesso e provvede a quanto necessario per l'esercizio del loro diritto, secondo le modalità stabilite dal presente Regolamento.
4. In particolare, il suddetto Responsabile deve:
    - ricevere la richiesta di accesso;
    - provvedere alla identificazione del richiedente ed alla verifica della sua legittimazione ad esercitare il diritto;
    - decidere sull'ammissibilità della richiesta;
    - verificare l'esistenza di eventuali controinteressati e comunicare agli stessi l'avvio del procedimento;
    - comunicare agli interessati l'esclusione, il differimento o la limitazione del diritto di accesso. |Art. 6, L. n. 241/1990|
5. Il Responsabile del procedimento può affidare ad altro dipendente l'attività istruttoria ed ogni altro adempimento inerente il procedimento, mantenendone comunque la responsabilità.

copia informatica per consultazione

Articolo 3 - Potere sostitutivo

1. In caso di inerzia, il potere sostitutivo previsto dall'art.2, comma 9 bis della L. 241/90 è attribuito al DIRETTORE AMMINISTRATIVO. L'interessato, decorso inutilmente il termine per la conclusione del procedimento o quello superiore di cui al comma 7, può rivolgersi al responsabile di cui al comma 9-bis perché, entro un termine pari alla metà di quello originariamente previsto, concluda il procedimento attraverso le strutture competenti o con la nomina di un commissario.

   Allegato: Fac simile di istanza all'Autorità sostitutiva

Articolo 4 - Modalità di Accesso

1. Il diritto di accesso può essere esercitato in via informale o formale, su richiesta motivata e si realizza attraverso l'esame del documento o l'estrazione di copia ovvero mediante altra modalità idonea a consentire l'esame dell'atto in qualsiasi forma ne sia rappresentato il contenuto.
2. Il richiedente deve indicare gli estremi del documento oggetto della richiesta ovvero gli elementi che ne consentano l'individuazione, specificare e, ove occorra, comprovare l'interesse diretto, concreto ed attuale corrispondente ad una situazione giuridicamente rilevante direttamente collegata al documento per il quale è chiesto l'acceso, nonché, dimostrare la propria identità e, ove occorra, i propri poteri di rappresentanza dei soggetti interessati.
3. Coloro che presentano richiesta di accesso per conto di enti, persone giuridiche, associazioni o altri organismi, devono qualificarsi legali rappresentanti degli stessi ovvero dichiarare la carica ricoperta o la funzione svolta, che legittima l'esercizio del diritto per conto dei soggetti rappresentati.
4. Qualora la richiesta pervenga mediante servizio postale o posta elettronica, potrà essere evasa previa esibizione del documento di identità o trasmissione di copia del medesimo.

Articolo 5 - Accesso informale

1. L'accesso informale esercitato mediante richiesta, anche verbale, all'amministrazione competente a formare l'atto conclusivo del procedimento o a detenerlo stabilmente o per il tramite dell'Ufficio Relazioni con il Pubblico, è consentito qualora non risulti l'esistenza di controinteressati, non vi siano dubbi sulla legittimazione del richiedente, sulla sua identità, sui suoi poteri rappresentativi, sulla sussistenza dell'interesse ed il documento sia immediatamente disponibile.
2. La richiesta di accesso, esaminata immediatamente e senza formalità, è accolta dal Responsabile del procedimento mediante esibizione del documento, eventuale trascrizione manuale dello stesso, estrazione di copia o esperimento congiunto di tali operazioni, ovvero altra modalità ritenuta idonea.
3. Il Responsabile del procedimento, qualora in base al contenuto del documento richiesto riscontri l'esistenza di controinteressati, invita l'interessato a presentare richiesta formale di accesso.

copia informatica per consultazione

Articolo 6 - Accesso formale

1. Qualora non sia possibile l'accoglimento immediato della richiesta in via informale, ovvero sorgano dubbi sulla legittimazione del richiedente, sulla sua identità, sui suoi poteri rappresentativi, sulla sussistenza dell'interesse meritevole di tutela alla stregua delle informazioni e della documentazione fornita o sull'accessibilità del documento o per l'esistenza di controinteressati, oppure nel caso in cui venga richiesto il rilascio di un documento in copia conforme all'originale, l'interessato è invitato a presentare richiesta d'accesso formale |Art. 6, L. n. 241/1990|.
2. L'interessato può in ogni caso presentare richiesta formale d'accesso ai documenti.
3. La richiesta di accesso deve contenere:
    a) le complete generalità del richiedente e dell'eventuale accompagnatore, con relativi recapiti e numeri di telefono;
    b) gli estremi del documento di identificazione del richiedente o la dichiarazione di conoscenza personale da parte dell'addetto alla ricezione;
    c) l'eventuale titolo di rappresentanza del soggetto interessato;
    d) gli estremi del documento oggetto della richiesta ed eventualmente del procedimento in cui è inserito, ovvero, in caso di mancata conoscenza di essi, indicazione di tutti gli elementi che ne consentano l'individuazione;
    e) l'indicazione delle modalità con cui si intende esercitare il diritto di accesso, specificando se si tratta di visione, di estrazione di copia o di entrambe ovvero di richiesta di copia conforme;
    f) l'indicazione delle modalità con cui si intende eventualmente ricevere la documentazione;
    g) l'idonea motivazione da cui sia possibile valutare la legittimità dell'accesso;
    h) la data e la sottoscrizione.
4. Ove pervenga una richiesta formale che riguardi un'Amministrazione diversa nei cui confronti il diritto di accesso deve essere esercitato, la stessa viene immediatamente trasmessa all'Amministrazione competente e di tale trasmissione è data comunicazione all'interessato.
5. Qualora la richiesta pervenga mediante servizio postale, via fax o posta elettronica, la stessa potrà essere evasa previa esibizione del documento di identità o trasmissione di copia del medesimo.
6. Ove la richiesta risulti irregolare o incompleta, il Responsabile del procedimento è tenuto a darne comunicazione al richiedente entro dieci giorni con raccomandata con avviso di ricevimento o con altro mezzo idoneo a comprovarne la ricezione. In tale caso, il termine del procedimento ricomincia a decorrere dalla data di presentazione della richiesta corretta.
7. Il procedimento di accesso formale deve concludersi entro il termine di trenta giorni dalla data di protocollazione in arrivo della richiesta.

Articolo 7 - Accesso per via telematica

1. Le pubbliche amministrazioni di cui all'articolo 22, comma 1, lettera e), della legge, assicurano che il diritto d'accesso possa essere esercitato anche in via telematica. Le modalità di invio delle domande e le relative sottoscrizioni sono disciplinate dall'articolo 38 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, e successive modificazioni, dagli articoli 4 e 5 del decreto del Presidente della Repubblica 11 febbraio 2005, n. 68, e dal decreto legislativo 7 marzo 2005, n. 82, e successive modificazioni.

copia informatica per consultazione

Articolo 8 - Accoglimento della richiesta

1. Ove non sussistano ragioni per differire o negare il diritto d'accesso, la richiesta viene accolta. La comunicazione dell'accoglimento della richiesta formale di accesso contiene l'indicazione della sede e dell'ufficio presso cui rivolgersi, nonché di un congruo periodo di tempo, comunque non inferiore a quindici giorni, per prendere visione dei documenti o per ottenerne copia.
2. L'accoglimento della richiesta d'accesso ad un documento comporta, di norma, anche la facoltà di accesso agli altri documenti in esso richiamati e appartenenti al medesimo procedimento, fatte salve le eccezione di legge e di regolamento.
3. L'esame del documento avviene presso l'ufficio indicato nell'atto di accoglimento della richiesta, nelle ore di ufficio, alla presenza del personale addetto, ovvero nel giorno concordato dall'ufficio con il richiedente.
4. L'esercizio dei diritti di visione degli atti e documenti amministrativi e di accesso alle strutture ed ai servizi è gratuito La copia dei documenti è rilasciata subordinatamente al pagamento degli importi dovuti secondo le modalità determinate all'art. 10. Su richiesta dell'interessato, le copie possono essere autenticate.
5. Il richiedente ha la facoltà di prendere appunti, di fotografare e di trascrivere manualmente qualsiasi parte del documento ottenuto in visione.
6. I documenti sui quali è consentito l'accesso non possono essere asportati dal luogo presso cui sono dati in visione o comunque alterati in qualsiasi modo.
7. L'esame dei documenti è effettuato dal richiedente o da persona da lui incaricata, munita di delega scritta, con l'eventuale accompagnamento di altra persona di cui vanno specificate le generalità, che devono poi essere registrate in calce alla richiesta.
8. Trascorsi trenta giorni dalla comunicazione al richiedente dell'accettazione della richiesta di accesso senza che questi abbia preso visione del documento, il richiedente è considerato rinunciatario.
   |Art. 7, DPR n. 184/2006|.

Articolo 9 - Notifica ai controinteressati

1. Qualora, in base alla natura del documento richiesto o degli altri documenti in esso richiamati, risulti l'esistenza di controinteressati, il Responsabile del procedimento è tenuto a dare comunicazione agli stessi dell'istanza di accesso mediante raccomandata a/r oppure, per via telematica, per coloro che abbiano consentito tale forma di comunicazione.
2. Entro dieci giorni dalla ricezione della suddetta comunicazione, i controinteressati possono presentare, anche per via telematica, motivata opposizione alla richiesta di accesso. Decorso tale termine, il Responsabile del procedimento provvede in merito all'istanza di accesso dopo aver accertato la ricezione della comunicazione della medesima da parte dei controinteressati.
   |Art. 3, DPR n. 184/2006|.

Articolo 10 - Costi di riproduzione e di spedizione

1. L'esame dei documenti è gratuito.
2. Il rilascio di copie, anche se parziali, dei documenti è subordinato al rimborso del costo di riproduzione, fatte salve le vigenti disposizioni in materia di bollo per il rilascio di copie in forma autentica, nonché dei diritti di ricerca e visura.
3. Sono esentati dal pagamento di qualsivoglia costo i soggetti di cui alle lettere da f) a p) indicati nella successiva sezione 4, art. 2, punto 2.1.

copia informatica per consultazione

Costi di riproduzione

- L'imposta di bollo è dovuta per il rilascio della copia conforme su eventuale richiesta dell'interessato, ai sensi del DPR 642/72, come modificato dal DPR 955/82.
  I costi delle marche sono calcolati per foglio, composto da quattro facciate unite o rilegate tra di loro in modo da costituire un atto unico recante nell'ultima facciata la dichiarazione di conformità all'originale, e sono determinati periodicamente per legge.
  Per i tabulati meccanografici e fogli scritti a mezzo stampa, l'imposta di bollo è dovuta per ogni 100 linee o frazione di 100 linee effettivamente utilizzate.
  L'importo (stabilito per legge, alla quale si rinvia per successivi adeguamenti) è pari a euro 16,00 per marca da bollo ogni 4 fogli/facciate ovvero 100 linee scritte a mezzo stampa. (Art.5 DPR 642/1972).
  Gli importi a carico del richiedente per il rilascio di copie, che comprendono i diritti di ricerca e visura, sono così determinati:
- L'estrazione di copie di atti è sottoposta a rimborso nella misura di Euro 0,30 a pagina per riproduzioni fotostatiche formato UNI A4 e nella misura di Euro 0,50 a pagina per riproduzioni fotostatiche formato UNI A3.
- Per gli importi inferiori a Euro 0,50 non è dovuto alcun rimborso. Al di sopra di tale importo, deve essere effettuata la riscossione dell'intera cifra. Ai fini dell'esenzione del rimborso, non è consentito frazionare la richiesta di copie relative agli stessi documenti da parte del medesimo soggetto.

  Il costo della spedizione dei documenti è a totale carico del richiedente.

  La spedizione è di norma effettuata con raccomandata postale A.R. o altro mezzo idoneo, secondo le tariffe applicate dalle Poste italiane o altra società di spedizioni e consegna. Il richiedente provvederà al pagamento contrassegno dell'importo complessivo (spese di spedizione più i costi di rimborso fotocopie più un ulteriore importo corrispondente alla cifra trattenuta da Poste italiane per la conversione del vaglia postale.)

- Per la spedizione via telefax i costi sono determinati in base ad un rimborso fisso di Euro 1,30 a pagina formato UNI A4.

  Nel caso di richiesta di copie di documenti in bollo, al pagamento dell'imposta di bollo provvede direttamente il richiedente, fornendo direttamente all'ufficio competente al rilascio la marca da bollo. Resta salvo il diverso regime fiscale previsto da speciali disposizioni di legge.
  È prevista la possibilità di inoltro tramite posta elettronica dei documenti per i quali l'Amministrazione ha già provveduto ad effettuare archiviazione ottica in formato non modificabile.
  Per la spedizione tramite posta elettronica (PEC o posta elettronica ordinaria), i costi sono determinati in base ad un rimborso fisso di Euro 0,25 a pagina.

Il pagamento deve essere effettuato all'atto della richiesta e, comunque, non oltre il momento del ritiro delle copie, mediante:

a) Pagamenti tramite bonifici bancari
Banco Popolare Società Cooperativa, Via Filzi, 25| 46100 Mantova IBAN | IT 65 S 05034 11501 000000072000
b) Pagamenti a mezzo conto corrente postale
Bollettino ccp sul conto 12058467 Bonifico postale IBAN | IT 86 H 07601 11500 000012058467|

copia informatica per consultazione

Articolo 11 - Diniego di accesso

1. Il diniego espresso deve essere motivato a cura del responsabile del procedimento di accesso, con riferimento alla normativa vigente, alla individuazione delle categorie di cui all'art. 24 della Legge e alle circostanze di fatto per cui la richiesta non può essere accolta così come proposta.
2. Il diritto di accesso è sempre escluso laddove non si riscontri la sussistenza di un interesse personale, concreto, diretto ed attuale, per la tutela di situazioni giuridicamente rilevanti.
3. Ai sensi dell'art. 24 della L. 241/1990, il diritto di accesso viene altresì escluso nei confronti di:

   - documenti riguardanti l'attività dell'Ente diretta all'adozione di atti amministrativi generali, di pianificazione e di programmazione;
   - documenti amministrativi contenenti informazioni di carattere psicoattitudinale relativi a terzi nelle procedure selettive;
   - documenti che riguardano la vita privata o la riservatezza di persone fisiche, persone giuridiche, gruppi, imprese e associazioni, con particolare riferimento agli interessi epistolare, sanitario, professionale, finanziario, industriale e commerciale di cui siano in concreto titolari, ancorché i relativi dati siano stati forniti all'Ente dagli stessi soggetti cui si riferiscono.

4. Deve comunque essere garantito ai richiedenti l'accesso ai documenti amministrativi la cui conoscenza sia necessaria per curare o per difendere i propri interessi giuridici.
5. Nel caso di documenti contenenti dati sensibili e giudiziari, l'accesso è consentito nei limiti in cui sia strettamente indispensabile e, in caso di dati idonei a rivelare lo stato di salute, se la situazione giuridicamente rilevante che si intende tutelare con la richiesta di accesso ai documenti amministrativi è di rango almeno pari ai diritti dell'interessato, ovvero consiste in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile.
6. In ogni caso, i documenti non possono essere sottratti all'accesso ove sia sufficiente far ricorso al potere di differimento per assicurare una tutela agli interessi dei soggetti coinvolti nel provvedimento richiesto, ovvero per salvaguardare esigenze di riservatezza dell'Ente specie nella fase preparatoria di provvedimenti, in relazione a documenti la cui conoscenza possa compromettere il buon andamento dell'azione amministrativa |Art. 60 Dlgs. n.196/2003|.
7. L'atto che dispone il differimento dell'accesso ne indica la motivazione e la durata, nei limiti strettamente necessari al rispetto delle finalità previste nel precedente comma ed è comunicato al richiedente, per iscritto, entro il termine stabilito per l'accesso.
8. Non sono ammissibili istanze di accesso preordinate ad un controllo generalizzato dell'operato delle pubbliche amministrazioni. |Art. 24, comma 3, L.241/90|.

Articolo 12 - Differimento accesso agli atti delle procedure di affidamento e di esecuzione dei contratti pubblici

1. Fatta salva la disciplina prevista dall'art. 162 del D.Lgs 50/2016 per gli appalti secretati o la cui esecuzione richiede speciali misure di sicurezza, il diritto di accesso agli atti delle procedure di affidamento e di esecuzione dei contratti pubblici, ivi comprese le candidature e le offerte, è differito:

   - nelle procedure aperte, in relazione all'elenco dei soggetti che hanno presentato offerte, fino alla scadenza del termine per la presentazione delle medesime;

copia informatica per consultazione

- nelle procedure ristrette e negoziate e nelle gare informali, in relazione all'elenco dei soggetti che hanno fatto richiesta di invito o che hanno manifestato il loro interesse, e in relazione all'elenco dei soggetti che sono stati invitati a presentare offerte e all'elenco dei soggetti che hanno presentato offerte, fino alla scadenza del termine per la presentazione delle offerte medesime; ai soggetti la cui richiesta di invito sia stata respinta, è consentito l'accesso all'elenco dei soggetti che hanno fatto richiesta di invito o che hanno manifestato il loro interesse, dopo la comunicazione ufficiale, da parte delle stazioni appaltanti, dei nominativi dei candidati da invitare;
- in relazione alle offerte, fino all'aggiudicazione;
- in relazione al procedimento di verifica della anomalia dell'offerta, fino all'aggiudicazione.

2. Gli atti di cui sopra indicati non possono essere comunicati a terzi o resi in qualsiasi altro modo noti fino alla scadenza dei termini ivi previsti.
3. L'inosservanza di quanto previsto dai due precedenti commi rileva ai fini dell'applicazione dell'articolo 326 del codice penale sulla rivelazione ed utilizzazione di segreti di ufficio per i pubblici ufficiali o per gli incaricati di pubblici servizi. |Art.53 D.lgs n.50/2016|
4. Il differimento dell'accesso è disposto ove sia sufficiente per assicurare una temporanea tutela agli interessi di cui all'articolo 24, comma 6, della legge, o per salvaguardare specifiche esigenze dell'amministrazione, specie nella fase preparatoria dei provvedimenti, in relazione a documenti la cui conoscenza possa compromettere il buon andamento dell'azione amministrativa.
5. L'atto che dispone il differimento dell'accesso ne indica la durata.

Articolo 13 - Esclusione dell'accesso e divieto di divulgazione degli atti delle procedure di affidamento e di esecuzione dei contratti pubblici

1. Fatta salva la disciplina prevista dall'art. 162 del D.Lgs 50/2016 per gli appalti secretati o la cui esecuzione richiede speciali misure di sicurezza, sono esclusi il diritto di accesso e ogni forma di divulgazione degli atti delle procedure di affidamento e di esecuzione dei contratti pubblici in relazione:

   - alle informazioni fornite nell'ambito dell'offerta o a giustificazione della medesima che costituiscano, secondo motivata e comprovata dichiarazione dell'offerente, segreti tecnici o commerciali;

   - ai pareri legali acquisiti dai soggetti tenuti all'applicazione del nuovo codice dei contratti di cui al D.Lgs 50/2016, per la soluzione di liti, potenziali o in atto, relative ai contratti pubblici;

   - alle relazioni riservate del direttore dei lavori, del direttore della esecuzione e dell'organo di collaudo sulle domande e sulle riserve del soggetto esecutore del contratto;

   - alle soluzioni tecniche e ai programmi per elaboratore utilizzati dalla stazione appaltante o dal gestore del sistema informatico per le aste elettroniche, ove coperti da diritti di privativa intellettuale.

2. In relazione alle informazioni fornite nell'ambito dell'offerta o a giustificazione della medesima che costituiscano, secondo motivata e comprovata dichiarazione dell'offerente, segreti tecnici o commerciali, è consentito l'accesso al concorrente ai fini della difesa in giudizio dei propri interessi in relazione alla procedura di affidamento del contratto.

3. Le stazioni appaltanti possono imporre agli operatori economici condizioni intese a proteggere il carattere di riservatezza delle informazioni che le amministrazioni aggiudicatrici rendono disponibili durante tutta la procedura di appalto.

copia informatica per consultazione

Articolo 14 - Ricorso al T.A.R.

1. Il termine per evadere la richiesta di accesso è di trenta giorni. Decorso inutilmente tale termine, la richiesta si intende respinta.
2. Le controversie relative all'accesso ai documenti amministrativi sono disciplinate dal nuovo codice del processo amministrativo. Pertanto, l'interessato può presentare ricorso al Tribunale Amministrativo Regionale, entro trenta giorni in caso di diniego espresso o tacito o di differimento |Art. 25, L.241/90|.

Articolo 15 - Archiviazione delle richieste di accesso

1. Le richieste di accesso formale, debitamente protocollate, devono essere conservate in archivio secondo quanto previsto dal massimario di scarto dell'Azienda vigente al momento della richiesta stessa.

Sezione 2 - ACCESSO CIVICO

Articolo 1 - Ambito oggettivo

1. L'accesso civico è l'obbligo di pubblicare documenti, informazioni o dati in capo all'Azienda, nei casi in cui sia stata omessa la loro pubblicazione |Art. 5, comma 1 D.lgs.33/13|.
2. L'accesso civico è il diritto da parte di chiunque di accedere a documenti, dati o informazioni per i quali sussiste l'obbligo di pubblicità previsto dalla normativa vigente e in capo all'Azienda, nei casi in cui sia stata omessa la loro pubblicazione |Art. 5, comma 1 D.lgs.33/13|.

Articolo 2 - Legittimazione soggettiva

1. Chiunque può chiedere, senza alcuna limitazione quanto alla legittimazione soggettiva del richiedente, anche indipendentemente dall'essere cittadino italiano o residente nel territorio dello Stato, senza motivazione e gratuitamente, la pubblicazione sul sito web istituzionale di documenti, informazioni o dati di cui l'Azienda ha omesso la pubblicazione, nei casi in cui vi era obbligata, ai sensi della normativa vigente. pubblicazione |Art. 5, comma 2 D.lgs.33/13 - All. Deliberazione ANAC n.1309 del 28/12/2016|.

Articolo 3 - Istanza di accesso civico

1. L'istanza di accesso, contenente le complete generalità del richiedente con i relativi recapiti e numeri di telefono, identifica i dati, le informazioni o i documenti richiesti.
2. L'istanza può essere trasmessa dal soggetto interessato per via telematica secondo le modalità previste dal decreto legislativo 7 marzo 2005, n. 82 recante il «Codice dell'amministrazione digitale». Pertanto, ai sensi dell'art. 65 del CAD, le istanze presentate per via telematica sono valide se:
   - sottoscritte mediante la firma digitale o la firma elettronica qualificata il cui certificato è rilasciato da un certificatore qualificato;

copia informatica per consultazione

- l'istante o il dichiarante è identificato attraverso il sistema pubblico di identità digitale (SPID), nonché la carta di identità elettronica o la carta nazionale dei servizi;
- sono sottoscritte e presentate unitamente alla copia del documento d'identità;
- trasmesse dall'istante o dal dichiarante mediante la propria casella di posta elettronica certificata purché le relative credenziali di accesso siano state rilasciate previa identificazione del titolare, anche per via telematica secondo modalità definite con regole tecniche adottate ai sensi dell'art. 71 (CAD), e ciò sia attestato dal gestore del sistema nel messaggio o in un suo allegato.

3. Resta fermo che l'istanza può essere presentata anche a mezzo posta, fax o direttamente presso gli uffici e che laddove la richiesta di accesso civico non sia sottoscritta dall'interessato in presenza del dipendente addetto, la stessa debba essere sottoscritta e presentata unitamente a copia fotostatica non autenticata di un documento di identità del sottoscrittore, che va inserita nel fascicolo (cfr. art. 38, commi 1 e 3, d.P.R. 28 dicembre 2000, n. 445).
4. L'istanza deve essere presentata al Responsabile della prevenzione della corruzione e della trasparenza, i cui riferimenti sono indicati nella Sezione "Amministrazione trasparente" del sito web istituzionale del Azienda. Ove tale istanza venga presentata ad altro ufficio del Azienda, il responsabile di tale ufficio provvede a trasmetterla al Responsabile della prevenzione della corruzione e della trasparenza nel più breve tempo possibile. |All. - Determinazione n. 1309 del 28/12/2016|
5. L'Azienda, entro trenta giorni, procede alla pubblicazione nel sito del documento, dell'informazione o del dato richiesto e lo trasmette contestualmente al richiedente ovvero comunica al medesimo l'avvenuta pubblicazione, indicando il collegamento ipertestuale a quanto richiesto. Se il documento, l'informazione o il dato richiesti risultano già pubblicati nel rispetto della normativa vigente, l'Azienda indica al richiedente il relativo collegamento ipertestuale. |Art. 5, comma 6 D.lgs.33/13|.
6. Nei casi di ritardo o mancata risposta il richiedente può ricorrere al titolare del potere sostitutivo di cui all'articolo 2, comma 9 della Legge 7 agosto 1990, n.241 e successive modificazioni e integrazioni, che, verificata la sussistenza dell'obbligo di pubblicazione, entro quindici giorni provvede ai sensi del precedente comma 5.
7. il Responsabile della prevenzione della corruzione e trasparenza ha l'obbligo di segnalare, in relazione alla loro gravità, i casi di inadempimento o adempimento parziale all'ufficio di disciplina del Azienda ai fini dell'eventuale attivazione del procedimento disciplinare; la segnalazione degli inadempimenti viene effettuata anche al vertice politico dell'amministrazione e all'OIV ai fini dell'attivazione dei procedimenti rispettivamente competenti in tema di responsabilità. |Art. 5, comma 10 D.lgs.33/13|.

Sezione 3 - ACCESSO CIVICO GENERALIZZATO

Articolo 1 - Ambito oggettivo

1. L'accesso civico generalizzato è esercitabile relativamente ai dati, le informazioni o i documenti detenuti dalle pubbliche amministrazioni, ulteriori rispetto a quelli oggetto di pubblicazione, ossia per i quali non sussista uno specifico obbligo di pubblicazione nel rispetto della tutela degli interessi pubblici/e/o privati indicati dall'art.5bis, commi 1 e 2 D.lgs. 33/13 e delle specifiche esclusioni come previsto dall'art.5 bis c3 |Art. 5, comma 2 D.lgs.33/13|.

copia informatica per consultazione

Articolo 2 - Legittimazione soggettiva

2.1 Interessati

1. Chiunque può chiedere, senza alcuna limitazione quanto alla legittimazione soggettiva del richiedente anche indipendentemente dall'essere cittadino italiano o residente nel territorio dello Stato, senza motivazione e gratuitamente, l'accesso di documenti, informazioni o dati detenuti dalle pubbliche amministrazioni, ulteriori rispetto a quelli oggetto di pubblicazione, nel rispetto dei limiti relativi alla tutela. |Art. 5, comma 2 D.lgs.33/13|.

2.2 Controinteressati

1. I soggetti controinteressati sono esclusivamente le persone fisiche e giuridiche portatrici dei seguenti interessi privati di cui all'art. 5-bis, c. 2 del decreto trasparenza:
    a) protezione dei dati personali, in conformità al D.Lgs. n. 196/2003;
    b) libertà e segretezza della corrispondenza intesa in senso lato ex art.15 Costituzione;
    c) interessi economici e commerciali, ivi compresi la proprietà intellettuale, il diritto d'autore e i segreti commerciali.

2.3 Responsabili del procedimento

1. Responsabile dei procedimenti di accesso è il Dirigente/Responsabile:
    - dell'Ufficio che detiene i dati, le informazioni o i documenti;
    - dell'Ufficio relazioni con il pubblico (ove istituito);
    - dell'ufficio indicato dall'amministrazione nella sezione "Amministrazione trasparente" del sito web istituzionale. |art.5 co. 3 let. a), b), e c) D.Lgs. n. 33/2013.

   il quale può affidare ad altro dipendente l'attività istruttoria ed ogni altro adempimento inerente il procedimento, mantenendone comunque la responsabilità.
2. I Dirigenti/Responsabili dell'Amministrazione ed il Responsabile della prevenzione della corruzione e della trasparenza controllano ed assicurano la regolare attuazione dell'accesso sulla base di quanto stabilito dal presente regolamento.

Articolo 3 - Istanza di accesso

1. L'istanza di accesso, contenente le complete generalità del richiedente con i relativi recapiti e numeri di telefono, identifica i dati, le informazioni o i documenti richiesti.
2. Le istanze non devono essere generiche ma consentire l'individuazione del dato, del documento o dell'informazione di cui è richiesto l'accesso.
3. Non è ammissibile una richiesta meramente esplorativa volta a scoprire di quali informazioni l'Amministrazione dispone.
4. Allo stesso modo, non è consentita una domanda di accesso per un numero manifestamente irragionevole di documenti, tale da impedire il buon andamento dell'amministrazione o la proposta di più domande entro un periodo di tempo limitato da parte di uno stesso soggetto (o una pluralità di soggetti riconducibili ad un medesimo ente), nel caso di manifesta irragionevolezza dell'onere complessivo che ne deriva.

copia informatica per consultazione

5. Qualora il medesimo richiedente abbia formulato una richiesta identica o sostanzialmente coincidente, l'Azienda ha la facoltà di non rispondere alla nuova richiesta, a condizione che la precedente sia stata integralmente soddisfatta.
6. L'Azienda deve consentire l'accesso ai documenti nei quali siano contenute le informazioni già detenute e gestite dalla stessa, è escluso che, per rispondere alla richiesta di accesso, sia tenuto a formare o raccogliere o altrimenti procurarsi informazioni che non siano già in suo possesso, ovvero a rielaborare i dati ai fini dell'accesso generalizzato.
7. L'istanza può essere trasmessa dal soggetto interessato per via telematica secondo le modalità previste dal decreto legislativo 7 marzo 2005, n. 82 recante il «Codice dell'amministrazione digitale». Pertanto, ai sensi dell'art. 65 del CAD, le istanze presentate per via telematica sono valide se:
   a) sottoscritte mediante la firma digitale o la firma elettronica qualificata il cui certificato è rilasciato da un certificatore qualificato;
   b) l'istante o il dichiarante è identificato attraverso il sistema pubblico di identità digitale (SPID), nonché la carta di identità elettronica o la carta nazionale dei servizi;
   c) sono sottoscritte e presentate unitamente alla copia del documento d'identità;
   d) trasmesse dall'istante o dal dichiarante mediante la propria casella di posta elettronica certificata purché le relative credenziali di accesso siano state rilasciate previa identificazione del titolare, anche per via telematica secondo modalità definite con regole tecniche adottate ai sensi dell'art. 71 (CAD), e ciò sia
   attestato dal gestore del sistema nel messaggio o in un suo allegato.
8. Resta fermo che l'istanza può essere presentata anche a mezzo posta, fax o direttamente presso gli uffici e che laddove la richiesta di accesso civico non sia sottoscritta dall'interessato in presenza del dipendente addetto, la stessa debba essere sottoscritta e presentata unitamente a copia fotostatica non autenticata di un documento di identità del sottoscrittore, che va inserita nel fascicolo (cfr. art. 38, commi 1 e 3, d.P.R. 28 dicembre 2000, n. 445).

Allegato: Fac simile di istanza di accesso

Articolo 4 - Notifica ai contro interessati

1. L'ufficio cui è indirizzata la richiesta di accesso generalizzato, se individua soggetti controinteressati è tenuto a dare comunicazione agli stessi, mediante invio di copia della stessa, a mezzo di raccomandata con avviso di ricevimento o per via telematica per coloro che abbiano acconsentito a tale forma di comunicazione. |All. - Determinazione n. 1309 del 28/12/2016|
2. Entro dieci giorni dalla ricezione della comunicazione, i controinteressati possono presentare una motivata opposizione, anche per via telematica, alla richiesta di accesso. Decorso tale termine, l'Azienda provvede sulla richiesta di accesso, accertata la ricezione della comunicazione da parte dei controinteressati. |All. - Determinazione n. 1309 del 28/12/2016|
3. La comunicazione ai soggetti controinteressati non è dovuta nel caso in cui l'istanza riguardi l'accesso civico, cioè dati, documenti ed informazioni oggetto di pubblicazione obbligatoria.

Articolo 5 - Termini del procedimento

1. Il procedimento di accesso civico deve concludersi con provvedimento espresso e motivato nel termine di trenta giorni (art. 5, c. 6, del d.lgs. n. 33/2013) dalla presentazione dell'istanza con la comunicazione del relativo esito al richiedente e agli eventuali soggetti controinteressati. Tali termini sono sospesi nel caso di comunicazione dell'istanza ai controinteressati durante il tempo stabilito dalla norma per consentire agli stessi di presentare eventuale opposizione (10 giorni dalla ricezione della comunicazione).

copia informatica per consultazione

2. In caso di accoglimento, l'ufficio competente di cui alla Sez. 3 Art. 1.3 del presente Regolamento provvede a trasmettere tempestivamente al richiedente i dati o i documenti o le informazioni richieste.
3. Qualora vi sia stato l'accoglimento della richiesta di accesso generalizzato nonostante l'opposizione del controinteressato, l'Azienda è tenuta a darne comunicazione a quest'ultimo. I dati o i documenti richiesti possono essere trasmessi al richiedente non prima di quindici giorni dalla ricezione della stessa comunicazione da parte del controinteressato, ciò anche al fine di consentire a quest'ultimo di presentare eventualmente richiesta di riesame o ricorso al difensore civico, oppure ricorso al giudice amministrativo. |All. - Determinazione n. 1309 del 28/12/2016|
4. Nel caso di richiesta di accesso generalizzato, l'Azienda deve motivare l'eventuale rifiuto, differimento o la limitazione dell'accesso con riferimento ai soli casi e limiti stabiliti dall'art. 5-bis del decreto trasparenza.

Articolo 6 - Eccezioni assolute all'accesso generalizzato

1. Il diritto di accesso generalizzato è escluso:

   - nei casi di segreto di Stato (cfr. art. 39, legge n. 124/2007)
   - nei casi in cui l'accesso è subordinato dalla disciplina vigente al rispetto di specifiche condizioni, modalità o limiti, inclusi quelli di cui all'art. 24, c. 1, legge n. 241/1990.

2. Ai sensi di quest'ultima norma il diritto di accesso è escluso:
   - nei procedimenti tributari locali, per i quali restano ferme le particolari norme che li regolano;
   - nei confronti dell'attività dell'Azienda diretta all'emanazione di atti normativi, amministrativi generali, di pianificazione e di programmazione, per i quali restano ferme le particolari norme che ne regolano la formazione;
   - nei procedimenti selettivi, nei confronti dei documenti amministrativi contenenti informazioni di carattere psicoattitudinale relativi a terzi.
3. Nei casi di divieti di accesso o divulgazione previsti dalla legge tra cui:
   - il segreto militare (R.D. n.161/1941);
   - il segreto statistico (D.Lgs 322/1989);
   - il segreto bancario (D.Lgs. 385/1993);
   - il segreto scientifico e il segreto industriale (art. 623 c.p.);
   - il segreto istruttorio (art.329 c.p.p.);
   - il segreto sul contenuto della corrispondenza (art.616 c.p.);
   - i divieti di divulgazione connessi al segreto d'ufficio (art.15, D.P.R. 3/1957)
   - i dati idonei a rivelare lo stato di salute, ossia a qualsiasi informazione da cui si possa desumere anche indirettamente, lo stato di malattia o l'esistenza di patologie dei soggetti interessati, compreso qualsiasi riferimento alle condizioni di invalidità, disabilità o handicap fisici e/o psichici (art. 22, comma 8, del Codice; art. 7-bis, c. 6, D.Lgs.. n. 33/2013);
   - i dati idonei a rivelare la vita sessuale (art. 7-bis, c. 6, D.Lgs.. n. 33/2013);
   - i dati identificativi di persone fisiche beneficiarie di aiuti economici da cui è possibile ricavare informazioni relative allo stato di salute ovvero alla situazione di disagio economico-sociale degli interessati (divieto previsto dall'art. 26, comma 4, D.Lgs. n. 33/2013).
4. Tale categoria di eccezioni all'accesso generalizzato è prevista dalla legge ed ha carattere tassativo. In presenza di tali eccezioni l'Azienda è tenuto a rifiutare l'accesso trattandosi di eccezioni poste da una norma di rango primario, sulla base di una valutazione preventiva e generale, a tutela di interessi pubblici e privati fondamentali e prioritari rispetto a quello del diritto alla conoscenza diffusa.

copia informatica per consultazione

5. Nella valutazione dell'istanza di accesso, l'Azienda deve verificare che la richiesta non riguardi dati, documenti o informazioni sottratte alla possibilità di ostensione in quanto ricadenti in una delle fattispecie indicate al primo comma.
6. Per la definizione delle esclusioni all'accesso generalizzato di cui al presente articolo, si rinvia alle Linee guida recanti indicazioni operative adottate dall'Autorità Nazionale Anticorruzione ai sensi dell'art. 5-bis del decreto trasparenza, che si intendono qui integralmente richiamate.

Articolo 7 - Eccezioni relative all'accesso generalizzato

1. I limiti all'accesso generalizzato sono posti dal legislatore a tutela di interessi pubblici e privati di particolare rilievo giuridico che l'Azienda deve necessariamente valutare con la tecnica del bilanciamento, caso per caso, tra l'interesse pubblico alla divulgazione generalizzata e la tutela di altrettanto validi interessi considerati dall'ordinamento.

2. L'accesso generalizzato è rifiutato se il diniego è necessario per evitare un pregiudizio concreto alla tutela di uno degli interessi pubblici inerenti:

- la sicurezza pubblica e l'ordine pubblico;
- la sicurezza nazionale;
- la difesa e le questioni militari;
- le relazioni internazionali;
- la politica e la stabilità finanziaria ed economica dello Stato;
- la conduzione di indagini sui reati e il loro perseguimento;
- il regolare svolgimento di attività ispettive, preordinate ad acquisire elementi conoscitivi necessari per lo svolgimento delle funzioni di competenza dell'Azienda

3. In particolare sono sottratti all'accesso, ove sia rilevata la sussistenza del pregiudizio concreto:

- gli atti, i documenti e le informazioni concernenti segnalazioni, atti o esposti di privati, di organizzazioni sindacali e di categoria o altre associazioni fino a quando non sia conclusa la relativa fase istruttoria o gli atti conclusivi del procedimento abbiano assunto carattere di definitività,, qualora non sia possibile soddisfare prima l'istanza di accesso senza impedire o gravemente ostacolare lo svolgimento dell'azione amministrativa o compromettere la decisione finale;
- le notizie sulla programmazione dell'attività di vigilanza, sulle modalità ed i tempi del suo svolgimento, le indagini sull'attività degli uffici, dei singoli dipendenti o sull'attività di enti pubblici o privati su cui l'ente esercita forme di vigilanza;
- verbali ed atti istruttori relativi alle commissioni di indagine il cui atto istitutivo preveda la segretezza dei lavori;
- verbali ed atti istruttori relativi ad ispezioni, verifiche ed accertamenti amministrativi condotti su attività e soggetti privati nell'ambito delle attribuzioni d'ufficio;
- pareri legali redatti dagli uffici comunali, nonché quelli di professionisti esterni acquisiti, in relazione a liti in atto o potenziali, atti difensivi e relativa corrispondenza.

4. L'accesso generalizzato è altresì rifiutato se il diniego è necessario per evitare un pregiudizio concreto alla tutela di uno dei seguenti interessi privati:

a) la protezione dei dati personali, in conformità con la disciplina legislativa in materia, fatto salvo quanto previsto dal precedente articolo. In particolare, sono sottratti all'accesso, ove sia rilevata la sussistenza del pregiudizio concreto, i seguenti atti, documenti ed informazioni:

- documenti di natura sanitaria e medica ed ogni altra documentazione riportante notizie di salute o di malattia relative a singole persone, compreso qualsiasi riferimento alle condizioni di invalidità, disabilità o handicap fisici e/o psichici;

- relazioni dei Servizi Sociali ed Assistenziali in ordine a situazioni sociali, personali, familiari di persone assistite, fornite dall'Autorità giudiziaria e tutelare o ad altri organismi pubblici per motivi specificatamente previsti da norme di legge;

copia informatica per consultazione

- la comunicazione di dati sensibili e giudiziari o di dati personali di minorenni, ex D.Lgs. n. 193/2003;
- notizie e documenti relativi alla vita privata e familiare, al domicilio ed alla corrispondenza delle persone fisiche, utilizzati ai fini dell'attività amministrativa;
b) la libertà e la segretezza della corrispondenza.
In particolare sono sottratti all'accesso, ove sia rilevata la sussistenza del pregiudizio concreto, i seguenti atti, documenti ed informazioni:
- gli atti presentati da un privato, a richiesta del Azienda, entrati a far parte del procedimento e che integrino interessi strettamente personali, sia tecnici, sia di tutela dell'integrità fisica e psichica, sia finanziari, per i quali lo stesso privato chiede che siano riservati e quindi preclusi all'accesso;
- gli atti di ordinaria comunicazione tra enti diversi e tra questi ed i terzi, non utilizzati ai fini dell'attività amministrativa, che abbiano un carattere confidenziale e privato;
c) gli interessi economici e commerciali di una persona fisica o giuridica, ivi compresi la proprietà intellettuale, il diritto d'autore e i segreti commerciali.

5. L'Azienda è tenuta a verificare e valutare, una volta accertata l'assenza di eccezioni assolute, se l'ostensione degli atti possa determinare un pregiudizio concreto e probabile agli interessi indicati dal legislatore; deve necessariamente sussistere un preciso nesso di causalità tra l'accesso ed il pregiudizio. Il pregiudizio concreto va valutato rispetto al momento ed al contesto in cui l'informazione viene resa accessibile. I limiti all'accesso generalizzato per la tutela degli interessi pubblici e privati individuati nei commi precedenti si applicano unicamente per il periodo nel quale la protezione è giustificata in relazione alla natura del dato.
6. L'accesso generalizzato non può essere negato ove, per la tutela degli interessi pubblici e privati individuati nei commi precedenti, sia sufficiente fare ricorso al potere di differimento.
7. Qualora i limiti di cui ai commi precedenti riguardano soltanto alcuni dati o alcune parti del documento richiesto deve essere consentito l'accesso parziale utilizzando, se del caso, la tecnica dell'oscuramento di alcuni dati; ciò in virtù del principio di proporzionalità che esige che le deroghe non eccedano quanto è adeguato e richiesto per il raggiungimento dello scopo perseguito.

Articolo 8 - Richiesta di riesame

1. Il richiedente, nei casi di diniego totale o parziale dell'accesso generalizzato o di mancata risposta entro il termine previsto dal precedente art.5, ovvero i controinteressati, nei casi di accoglimento della richiesta di accesso, possono presentare richiesta di riesame al Responsabile della prevenzione della corruzione e della trasparenza che decide con provvedimento motivato, entro il termine di venti giorni.
2. Nel caso in cui i dati o documenti richiesti siano detenuti dal responsabile della prevenzione della corruzione e della trasparenza la competenza a decidere in sede di riesame è attribuito al DIRETTORE AMMINISTRATIVO
3. Se l'accesso generalizzato è stato negato o differito a tutela della protezione dei dati personali in conformità con la disciplina legislativa in materia, il Responsabile della prevenzione della corruzione e della trasparenza, provvede sentito il Garante per la protezione dei dati personali, il quale si pronuncia entro il termine di dieci giorni dalla richiesta.
4. A decorrere dalla comunicazione al Garante, il termine per l'adozione del provvedimento da parte del RPCT è sospeso, fino alla ricezione del parere del Garante e comunque per un periodo non superiore ai predetti dieci giorni.

Allegato: Fac simile di istanza all'Autorità sostitutiva
Allegato: Fac simile di riesame

copia informatica per consultazione

Articolo 9 - Motivazione del diniego all'accesso

1. Sia nei casi di diniego, anche parziale, connessi all'esistenza di limiti all'accesso generalizzato, sia per quelli connessi alle eccezioni assolute, sia per le decisioni del RPCT, gli atti sono adeguatamente motivati.

Articolo 10 - Impugnazioni

1. Avverso la decisione del responsabile del procedimento o, in caso di richiesta di riesame, avverso la decisione del RPCT, il richiedente l'accesso generalizzato può proporre ricorso al Tribunale Amministrativo Regionale ai sensi dell'art. 116 del Codice del processo amministrativo di cui al D.Lgs. n. 104/2010.
2. Se l'accesso generalizzato è negato o differito a tutela della protezione dei dati personali in conformità con la disciplina legislativa in materia, si adisce il Garante per la protezione dei dati personali, il quale si pronuncia entro dieci giorni dalla richiesta.

Sezione 4 - ACCESSO ALLA DOCUMENTAZIONE CLINICA

Fatta salva in via generale la normativa di cui alle sezioni 1 -2 -3 del presente Regolamento, l'accesso alla documentazione clinica detenuta dall' Azienda è altresì regolata dalle seguenti norme integrative o derogatorie

Articolo 1 - Ambito oggettivo

Costituiscono oggetto del diritto di accesso la documentazione clinica ed ad ogni documentazione contenente dati inerenti alla salute (lastre radiografiche, referti diagnostici, referti analitici, verbali di prestazioni di pronto soccorso e, più in generale, tutte le certificazioni riguardanti i pazienti assistiti presso le strutture dell'Azienda).

Articolo 2 - Legittimazione soggettiva

2.1 Interessati

Per le categorie dei documenti di cui al comma precedente, i soggetti legittimati all'accesso sono individuati come segue:

a) Paziente maggiorenne o minorenne emancipato al quale la documentazione clinica si riferisce;
b) Soggetti che esercitano la potestà dei genitori, nel caso in cui il paziente sia minorenne. Il genitore, in caso di separazione o divorzio, deve specificare, all'atto della richiesta di accesso, di essere o non essere genitore affidatario del minore, al fine di qualificare la propria posizione giuridica. Nel caso di revoca della potestà ad entrambi i genitori, è da ritenere che il diritto di accesso debba essere esercitato esclusivamente dal tutore nominato, unico soggetto responsabile della tutela degli interessi del minore;
c) Tutore, nei casi di paziente interdetto giudiziale (art.414 c.c.) o nel caso di cui al precedente punto b). Per le persone inabilitate (art. 415 c.c.) la volontà del richiedente deve essere integrata da quella del curatore, che deve parimenti sottoscrivere la richiesta. La qualità di tutore o curatore può anche essere attestata a mezzo dichiarazione sostitutiva di certificazione, ai sensi dell'art.46 del DPR 445/00;

copia informatica per consultazione

d) Terze persone, purché munite di delega scritta da parte del paziente o da chi esercita la potestà o la tutela.
In tali casi, quando la sottoscrizione dell'atto di delega non avviene innanzi al funzionario incaricato dell'azienda ospedaliera, dovrà essere prodotta copia del documento di identità del delegante che ha sottoscritto l'atto e del delegato, identificato al momento del ritiro;
e) in caso di paziente deceduto, eredi legittimi o testamentari del paziente deceduto, previa fornitura della prova della propria qualità di erede anche mediante dichiarazione sostitutiva di certificazione ovvero chi abbia un interesse proprio o agisca a tutela dello interessato o per ragioni familiari meritevoli di tutela, previa adeguata fornitura delle motivazioni per cui agisce (art. 9, comma 3, D.Lgs. n. 196/2003)
f) Autorità giudiziaria (artt. 210-211-261 c.p.c.; artt. 70 e 370 c.p.p.);
g) Polizia giudiziaria (artt. 55, 348 e 370 c.p.p.);
h) I.N.A.I.L., nei casi di infortunio occorso ad un assicurato (artt. 94 e 95 del DPR 1124/65 e art.5 del DM 15.3.1991);
i) I.N.P.S., nei casi di competenza per le spese di spedalità (artt. 17 e 18 del DPR 2316/34);
j) Enti esteri o sopra nazionali, legittimati all'accesso sulla base di convenzioni internazionali;
k) Ispettori del Lavoro, per conto dell'Ispettorato del lavoro e/o enti con funzioni analoghe (art.64 del DPR 303/56);
l) Prefetture, per spese di ricovero ospedaliero urgente di cittadini stranieri indigenti (L. 6972/90; RD 99/1991 art.. 114) ;
m) Dirigenti o organi di gestione dell'ente presso cui il paziente trovasi ricoverato, per ragioni di ufficio (assicurative, di spedalità, di responsabilità civile ect..), previa richiesta motivata dalle ragioni che giustificano l'accesso;
n) Legale rappresentante o Direttore sanitario o delegato di altri ospedali o cliniche, a seguito di trasferimento di pazienti in tali strutture, previa richiesta motivata della necessità di disporre di tali dati utili al trattamento morboso in atto;
o) Medico curante se munito di espressa delega rilasciatagli dal paziente;
p) Enti di ricerca e studio, le cui richieste motivate dovranno essere valutate caso per caso e soddisfatte compatibilmente con la esigenza di anonimità dei pazienti cui i dati si riferiscono;

2.2 Controinteressati

1. Sono controinteressati il paziente e altri familiari del paziente ai cui atti è richiesto lo accesso.

2.3 Responsabile del procedimento di accesso

1. In tema di documentazione sanitaria i Responsabili del procedimento di accesso sono il Direttore Sanitario di Presidio o il dirigente del servizio/struttura competente a formare l'atto o a detenerlo stabilmente a cui vanno indirizzate le relative domande.

copia informatica per consultazione

3. Modalità, tempi di rilascio della documentazione ed oneri finanziari

1. In conformità a quanto prescritto dall' art. 4 comma 2 della L. n. 24/2017 il rilascio della documentazione sanitaria, nella misura immediatamente disponibile, è eseguito entro sette giorni dalla presentazione della relativa richiesta da parte degli aventi diritto.
   Le eventuali integrazioni sono fornite, in ogni caso, entri il termine massimo di trenta giorni dalla presentazione della richiesta stessa.
2. Preferibilmente la richiesta è evasa in formato elettronico.
3. Gli obblighi in tema di imposta di bollo non si applicano in caso di rilascio di copie autenticate di cartelle cliniche.

Tariffario

Copie documenti sanitari (verbale P.S. – refertazioni – impegnative –ecc.)

- formato A4 Euro 2,00 forfettari per tipologia di documento da rilasciare
- formato A3 Euro 2,50 forfettari per tipologia di documento da rilasciare

Riproduzione su supporto informatico di immagini e/o documenti digitalizzati (compresa copia cartella clinica su file di stampa in pdf)

- CD Euro 10,00 cad.
- DVD Euro 10,00 cad.

Riproduzione lastre radiografiche

- formato 24x30 Euro 3,50 cad.
- formato 35,6x43,2 Euro 6,00 cad.
- formato 14x17" Euro 6,00 cad.

Cartella clinica:

tariffa unica forfetaria: € 25,00 (non assoggettata ad IVA) per fotocopia di cadauna cartella clinica in regime di ricovero ordinario o di Day Hospital con un massimo di Euro 50,00 in caso di rilascio di più cartelle, quando il costo delle medesime superi tale limite)

pagamento anticipato, da effettuarsi prima della consegna dei documenti;

Il pagamento deve essere effettuato mediante bonifico bancario intestato a: _____- tramite le seguenti coordinate: conto corrente di tesoreria c/o Codice IBAN: IT NN L NNNNN NNNNN NNNNNNNNNN con indicazione specifica della causale: *rilascio documenti sanitari* + nome e cognome.

Se l'interessato chiede di ricevere copia della documentazione sanitaria al suo domicilio a mezzo servizio postale, questa è trasmessa tramite raccomandata AR, all'indirizzo indicato nella richiesta. L'invio avverrà con tassa a carico del destinatario ed in

copia informatica per consultazione

contrassegno secondo le tariffe applicate dalle Poste italiane o altra società di spedizioni o consegna.

In questo ultimo caso l'importo da pagare corrisponderà al costo di riproduzione dei documenti, più i costi di spedizione, più un ulteriore importo corrispondente alla cifra trattenuta da Poste italiane per la conversione del vaglia postale.

Sezione 5 – DISPOSIZIONI FINALI

Articolo 1 - Abrogazioni

1. Dalla data di entrata in vigore del presente regolamento sono abrogate tutte le precedenti disposizioni aziendali in materia.

Articolo 2 - Norme di rinvio

1. Per tutto quanto non espressamente previsto dal presente Regolamento, si fa rinvio alle norme in materia previste dalle disposizioni normative vigenti o sopravvenienti, incompatibili con i presenti articoli.

Articolo 3 - Entrata in vigore

1. Il presente Regolamento entra in vigore alla data di adozione del provvedimento e tempestiva pubblicazione sul sito web aziendale nell'area amministrazione trasparente Amministrazione Trasparente", nella sotto sezione – Altri contenuti – Corruzione – Accesso civico.

copia informatica per consultazione

ISTANZA PER LA RICHIESTA DI ACCESSO CIVICO (F.O.I.A.) (*) (**)

alternativamente

All'Ufficio che detiene i dati, le informazioni o i documenti,
All'Ufficio relazioni con il pubblico,
Altro ufficio indicato dall'amministrazione nella sezione "Amministrazione trasparente" del sito web istituzionale, ai sensi del co. 3 let. a), b), e c) dell'art.5 del D.Lgs. n. 33/2013

OGGETTO: **Richiesta di accesso "generalizzato" ai documenti, dati e informazioni non soggetti a obbligo di pubblicazione (ai sensi dell'art. 5, comma 2 e ss. del D.Lgs. n. 33/2013).**

sottoscritt

Dati anagrafici*	nome	cognome	codice fiscale	luogo di nascita	/ / data di nascita

Residenza*	indirizzo	CAP	Comune	Prov/Stato estero

Recapiti*	@ indirizzo PEC/e-mail	telefono

nella propria qualità di soggetto interessato

CHIEDE

ai sensi e per gli effetti dell'art. 5, comma 2 e ss. del D.Lgs. n. 33/2013, come modificato dal D.Lgs. 25 maggio 2016, n. 97, di:
☐ prendere visione;
☐ ottenere copia semplice in formato elettronico con invio tramite posta elettronica;
☐ ottenere copia autentica (istanza e copie sono soggette all'assolvimento delle disposizioni in materia di bollo);

relativamente ai seguenti documenti, dati o informazioni detenuti da codesta Amministrazione:

copia informatica per consultazione

Documento	descrizione del contenuto*		
	autore	destinatario	data

Dato	descrizione del contenuto*	
	fonte del dato (es., denominazione della banca dati)	dal al periodo di riferimento

Informazione	descrizione del contenuto*	
	fonte (es. pagina web dove l'informazione è citata)	dal al periodo di riferimento

A tal fine dichiara di essere a conoscenza quanto prevede il seguente modello di istruttoria e le attività endoprocedimentali stabilite dalla nuova disciplina e in particolare che:

• come stabilito dall'art. 5, comma 5 del D.Lgs. 33/2013, modificato dal D.Lgs. 25 maggio 2016, n. 97, qualora l'amministrazione alla quale è indirizzata la presente richiesta dovesse individuare dei controinteressati ex art. 5-bis, comma 2 del medesimo D.Lgs., è tenuta a dare comunicazione agli stessi, mediante invio di copia della presente istanza;

• qualora venga effettuata la sopra citata comunicazione, il termine di conclusione del presente procedimento di accesso è sospeso fino all'eventuale opposizione dei controinteressati, e comunque non oltre 10 giorni;

• a norma dell'art. 5, comma 4 del D.Lgs. n. 33/2013, il rilascio di dati in formato elettronico è gratuito, salvo il rimborso del costo effettivamente sostenuto e documentato dall'amministrazione per la riproduzione su supporti materiali.

Con la presente il sottoscritto autorizza formalmente il trattamento dei dati personali nel rispetto del decreto legislativo n.196/2003.

ALLEGA

copia di documento di identità (non occorre per le istanze sottoscritte con firma digitale)

Luogo e data

Distinti saluti

Firma del richiedente

* I campi contrassegnati con l'asterisco sono obbligatori. Fonte : Sito web del Dipartimento della Funzione Pubblica

Il presente modulo ha validità di autodichiarazione a' sensi del DPR 445/2000 dei dati e fatti ivi riportati.

**Chiunque rilasci dichiarazioni mendaci o fornisca atti falsi incorrerà nelle sanzioni ex art. 76 DPR 445/2000.

copia informatica per consultazione

Al Direttore Amministrativo
(in qualità di Autorità Sostitutiva
ex art. 2 comma 9-bis L. 241/'90 e ss. mm. e ii.)

Istanza all'Autorità Sostitutiva per inerzia/diniego accesso civico1
(ex art. 2 comma 9-bis L. 241/'90 e Delibera ANAC n. 1310 del 28.12.2016)

sottoscritt

Dati anagrafici*	nome	cognome	codice fiscale	luogo di nascita	data di nascita / /

Residenza*	indirizzo	CAP	Comune	Prov/Stato estero

Recapiti*	indirizzo PEC/e-mail @	telefono

avendo presentato istanza di accesso civico con nota del _____ _____ volta ad esercitare l'accesso civico per i seguenti: dati/informazioni/ documenti:
_____ _____
_____

e, in riferimento a tale istanza (barrare la casella corrispondente):
☐ non avendo ottenuto alcuna risposta nei termini previsti (30 giorni)
☐ avendo ricevuto diniego totale all'istanza con comunicazione Prot. n. _ _ del _ ___
☐ avendo ricevuto diniego parziale all'istanza con comunicazione Prot. n. _ del __ ___
☐ avendo ricevuto diniego alla propria richiesta di riesame con comunicazione Prot. n. del _

PRESENTA ISTANZA
alla S.V., quale **soggetto titolare del potere sostitutivo** ai sensi dell'art.2 comma 9-bis L. 241/'90 e ss. mm. e ii., affinché sia data attuazione agli obblighi previsti dalla normativa vigente, entro termini stabiliti per il procedimento di cui trattasi.

Luogo e data

Firma del richiedente

[1] Il presente modulo ha validità di autodichiarazione a' sensi del DPR 445/2000 dei dati e fatti ivi riportati. Chiunque rilasci dichiarazioni mendaci o fornisca atti falsi incorrerà nelle sanzioni ex art. 76 DPR 445/2000.

copia informatica per consultazione

Al Responsabile della Prevenzione della Corruzione e della Trasparenza

Richiesta di riesame istanza di accesso civico[1]

(ex art. 5 comma 7 d.lgs. n. 33/2013, come modificato dal d.lgs. 25 maggio 2016, n. 97)

sottoscritt

Dati anagrafici*	nome	cognome	codice fiscale	luogo di nascita	/ / data di nascita
Residenza*	indirizzo		CAP	Comune	Prov/Stato estero
Recapiti*	@ indirizzo PEC/e-mail		telefono		

e, in riferimento a tale istanza (barrare la casella corrispondente):

☐ non avendo ottenuto alcuna risposta nei termini previsti (30 giorni)

☐ avendo ricevuto diniego totale all'istanza con comunicazione Prot. n. ____ _____ del ___ _____

☐ avendo ricevuto diniego parziale all'istanza con comunicazione Prot. n. _____ ___ del _____ _____

CHIEDE

alla S.V. di procedere al riesame dell'istanza stessa, adottando provvedimento motivato al riguardo entro 20 giorni, ai sensi dell'art. 5 comma 7 del d.lgs. 33/2013.

In caso di accoglimento della presente richiesta di riesame, il sottoscritto chiede altresì che:

☐ quanto oggetto di pubblicazione obbligatoria sia reso disponibile sul sito

☐ i dati/informazioni/documenti richiesti vengano consegnati al sottoscritto:

- ☐ a mano
- ☐ al proprio indirizzo come sopra indicato
- ☐ al proprio indirizzo di posta elettronica come sopra indicato

Luogo e data

Firma del richiedente

[1] Il presente modulo ha validità di autodichiarazione a' sensi del DPR 445/2000 dei dati e fatti ivi riportati. Chiunque rilasci dichiarazioni mendaci o fornisca atti falsi incorrerà nelle sanzioni ex art. 76 DPR 445/2000.

copia informatica per consultazione

Titolario e Massimario del Sistema Sociosanitario lombardo già Sistema Sanitario e Sociosanitario di Regione Lombardia

Revisione 04

Nel presente Titolario e Massimario di scarto in revisione 04 le modifiche inserite, rispetto alla versione precedente, sono riportate in carattere corsivo.

copia informatica per consultazione

Titolario di classificazione

Revisione 04

copia informatica per consultazione

TITOLARIO DEL SISTEMA SOCIOSANITARIO LOMBARDO
GIÀ SISTEMA SANITARIO E SOCIOSANITARIO DI REGIONE LOMBARDIA rev04

Titolo 1 - Area Amministrativa		
Classe	**Sottoclasse**	**Descrizione**
1	**.00**	**Amministrazione generale**
1	.01	Normativa e provvedimenti
1	.02	Programmazione, disposizioni, indirizzi e obiettivi dell'ente, atti di organizzazione
1	.03	Protocolli di intesa, convenzioni con enti pubblici e privati, no profit
1	.04	Controlli interni ed esterni
1	.05	Sistema Qualità e Risk Management
1	.06	Progetti di ricerca
1	.07	Associazioni di volontariato e di tutela dei diritti del malato
1	.08	Politiche ed interventi per le pari opportunità
2	**.00**	**Organi e organismi**
2	.01	Legale Rappresentante
2	.02	Organismi direttivi e scientifici
2	.03	Organismi di controllo interno ed esterno
2	.04	Collegi, Comitati e Commissioni
3	**.00**	**Attività giuridico-legale**
3	.01	Pareri, informative giuridiche e attività tecnico-legali
3	.02	Contenzioso legale
3	.03	Procedure concorsuali ed esecutive
3	.04	Assicurazioni e gestione sinistri
4	**.00**	**Risorse umane**
4	.01	Dotazione organica e gestione del personale
4	.02	Concorsi e selezioni
4	.03	Assunzioni, inquadramenti, incarichi e cessazioni
4	.04	Istituti contrattuali sospensivi della prestazione lavorativa
4	.05	Organizzazioni sindacali e contrattazione
4	.06	Retribuzione e compensi
4	.07	Trattamenti fiscali, contributivi e assicurativi
4	.08	Inabilità al lavoro, invalidità, infermità, indennizzo
4	.09	Presenze e assenze
4	.10	Quiescenza e relativo trattamento
4	.11	Servizi a richiesta individuale
4	.12	Valutazione del personale
4	.13	Formazione e aggiornamento del personale
4	.14	Deontologia professionale ed etica del lavoro
4	.15	Personale non strutturato o convenzionato
5	**.00**	**Risorse finanziarie e gestione contabile**
5	.01	Attività finanziaria e contabile
5	.02	Bilancio e rendicontazione
5	.03	Gestione entrate-uscite
5	.04	Gestione fiscale e imposte
6	**.00**	**Gestione e organizzazione del patrimonio**
6	.01	Progettazione e costruzione di beni immobili con relativi impianti
6	.02	Acquisizione e gestione beni immobili e relativi servizi
6	.03	Acquisizione e gestione beni mobili / generi di consumo e di servizi
6	.04	Manutenzione ordinaria, straordinaria, ristrutturazione, destinazione d'uso
6	.05	Attività contrattuale e tutela della proprietà intellettuale
6	.06	Sicurezza degli ambienti di lavoro
6	.07	Gestione dei rifiuti
7	**.00**	**Sistemi Informativi e comunicazione**
7	.01	Sistema documentale
7	.02	Rapporti con il pubblico, sportelli informativi e trasparenza
7	.03	Tutela della riservatezza
7	.04	Biblioteche e centri di documentazione
7	.05	Sistema informatico, reti e sicurezza
7	.06	Statistiche e reporting

copia informatica per consultazione

TITOLARIO DEL SISTEMA SOCIOSANITARIO LOMBARDO
GIÀ SISTEMA SANITARIO E SOCIOSANITARIO DI REGIONE LOMBARDIA rev04

Titolo 2 - Area Sanitaria e Socio-Sanitaria Territoriale		
Classe	**Sottoclasse**	**Descrizione**
1	**.00**	**Organizzazione territoriale**
1	.01	Gestione e organizzazione dipartimentale e interdipartimentale, distrettuale ed interdistrettuale
1	.02	Progetti, interventi e iniziative varie dipartimentali / distrettuali
1	.03	Coordinamento e gestione personale infermieristico, tecnico-assistenziale, di prevenzione
2	**.00**	**Prevenzione e sicurezza negli ambienti di lavoro**
2	.01	Aspetti generali, organizzativi e gestionali
2	.02	Medicina del lavoro e malattie professionali
2	.03	Igiene e sicurezza sul lavoro
2	.04	Sicurezza e impiantistica
3	**.00**	**Prevenzione medico - sanitaria**
3	.01	Aspetti generali, organizzativi e gestionali
3	.02	Educazione sanitaria
3	.03	Epidemiologia e profilassi malattie infettive e parassitarie
3	.04	Prevenzione malattie cronico-degenerative
3	.05	Igiene urbana, ambientale e sanità pubblica
3	.06	Tutela salute attività sportive
3	.07	Igiene degli alimenti
3	.08	Igiene della nutrizione
3	.09	Laboratorio di prevenzione
4	**.00**	**Prevenzione veterinaria**
4	.01	Aspetti generali, organizzativi e gestionali
4	.02	Sanità animale
4	.03	Anagrafe zootecnica e movimentazione animale
4	.04	Igiene alimenti di origine animale
4	.05	Igiene allevamenti e produzioni zootecniche
4	.06	Randagismo e tutela animali da affezione
5	**.00**	**Assistenza sanitaria**
5	.01	Aspetti generali, organizzativi e gestionali
5	.02	Emergenza sanitaria territoriale
5	.03	Assistenza sanitaria di base
5	.04	Assistenza protesica e integrativa
5	.05	Assistenza psichiatrica e neuropsichiatrica infantile
6	**.00**	**Assistenza socio-sanitaria integrata**
6	.01	Aspetti generali, organizzativi e gestionali
6	.02	Dipendenze
6	.03	Famiglia, infanzia ed età evolutiva
6	.04	Assistenza domiciliare
6	.05	Disabilità
6	.06	Fragilità
7	**.00**	**Governo sanitario e sociosanitario**
7	.01	Aspetti generali, organizzativi e gestionali
7	.02	Osservatorio epidemiologico
7	.03	Flussi informativi sanitari e sociosanitari
7	.04	Accreditamento e controllo strutture sanitarie
7	.05	Autorizzazione e controllo strutture sociosanitarie
7	.06	Acquisto e controllo prestazioni sanitarie
7	.07	Acquisto e controllo prestazioni sociosanitarie
8	**.00**	**Medicina legale**
8	.01	Aspetti generali, organizzativi e gestionali
8	.02	Attività medico-legale e necroscopica
8	.03	Invalidità civile, sordomutismo e menomazioni visive
8	.04	Istanze di indennizzo
9	**.00**	**Assistenza e governo farmaceutica**
9	.01	Aspetti generali, organizzativi e gestionali
9	.02	Controllo spesa farmaceutica
9	.03	Controllo farmacie, parafarmacie e distributori
9	.04	Autorizzazione e governo farmacie
9	.05	Farmacovigilanza
9	.06	Assistenza farmaceutica diretta
9	.07	Sperimentazione farmaci e dispositivi
9	.08	Gestione stupefacenti

copia informatica per consultazione

TITOLARIO DEL SISTEMA SOCIOSANITARIO LOMBARDO
GIÀ SISTEMA SANITARIO E SOCIOSANITARIO DI REGIONE LOMBARDIA rev04

Titolo 3 - Area Ospedaliera		
Classe	**Sottoclasse**	**Descrizione**
1	**.00**	**Direzione ospedaliera**
1	.01	Aspetti generali, organizzativi e gestionali
1	.02	Rapporti con l'autorità giudiziaria
1	.03	Igiene ospedaliera
1	.04	Radioprotezione
2	**.00**	**Pronto soccorso**
2	.01	Gestione organizzativa P.S.
2	.02	Attività emergenza-urgenza
3	**.00**	**Assistenza ospedaliera**
3	.01	Aspetti generali, organizzativi e gestionali
3	.02	Ricovero (ordinario, day hospital, day surgery)
3	.03	Day service
3	.04	Assistenza al parto
3	.05	Assistenza domiciliare
3	.06	Medicina penitenziaria
3	.07	Assistenza psichiatrica e neuropsichiatrica infantile
4	**.00**	**Assistenza ambulatoriale**
4	.01	Prestazioni ambulatoriali
5	**.00**	**Riabilitazione**
6	**.00**	**Attività immuno-trasfusionale**
6	.01	Aspetti generali, organizzativi e gestionali
6	.02	Valutazione idoneità donatori sangue ed emocomponenti
7	**.00**	**Attività di trapianto d'organi e tessuti**
7	.01	Aspetti generali, organizzativi e gestionali
7	.02	Donazione e prelievo
8	**.00**	**Farmaceutica ospedaliera**
8	.01	Farmaceutica
8	.02	Stupefacenti
9	**.00**	**Medicina legale ospedaliera**
9	.01	Medicina necroscopica
9	.02	Indennizzo danni
9	.03	Consulenze medico-legali
10	**.00**	**Medicina del lavoro**
10	.01	Cartella sanitaria e di rischio del lavoratore
10	.02	Malattia professionale e infortunio sul lavoro
11	**.00**	**Sperimentazione clinica dei medicinali e dei dispositivi**

copia informatica per consultazione

Massimario di scarto

Revisione 04

copia informatica per consultazione

CLASSE	COD. SOTTO CLASSE	SOTTOCLASSE	TIPO DOCUMENTO	TEMPO CONSERVAZIONE	RIFERIMENTI NORMATIVI / NOTE
1. Amministrazione Generale	.01	Normativa e provvedimenti	Normativa e relativa attuazione di carattere generale riferita ad atti esterni (normativa statale, regionale, pareri, circolari, direttive, delibere di altri Enti)	5 anni	
	.02	Programmazione, disposizioni, indirizzi e obiettivi aziendali, atti di organizzazione	Registro Deliberazioni / Determinazioni	ILLIMITATO	Circ.44/2005 Ministero per i Beni e le Attività Culturali. Deliberazioni (raccolta)
	.02	Programmazione, disposizioni, indirizzi e obiettivi aziendali, atti di organizzazione	Atti e provvedimenti emessi dall'Ente *originali* (Deliberazioni, Determinazioni, *corrispondenza di natura istituzionale* , ecc.)	ILLIMITATO	Circ.44/2005 Ministero per i Beni e le Attività Culturali. Circolari interne esplicative e direttive / Ordinanze
	.02	Programmazione, disposizioni, indirizzi e obiettivi aziendali, atti di organizzazione	Regolamenti aziendali e le relative fasi procedimentali (dalla proposta all'adozione del testo definitivo)	ILLIMITATO	Circ.44/2005 Ministero per i Beni e le Attività Culturali. Circolari interne esplicative e direttive / Ordinanze
	.02	Programmazione, disposizioni, indirizzi e obiettivi aziendali, atti di organizzazione	Documento di Programmazione	ILLIMITATO	Circ.44/2005 Ministero per i Beni e le Attività Culturali
	.02	Programmazione, disposizioni, indirizzi e obiettivi aziendali, atti di organizzazione	Piani Aziendali (Piano dei Controlli, Piano Salute, Strategici, Piano delle Performance, Piano anticorruzione, Modello organizzativo ecc.)	ILLIMITATO	Circ.44/2005 Ministero per i Beni e le Attività Culturali
	.02	Programmazione, disposizioni, indirizzi e obiettivi aziendali, atti di organizzazione	Disposizioni e comunicazioni a carattere transitorio *(convocazioni, inviti, corrispondenza varia, ecc.)*	5 anni	
	.02	Programmazione, disposizioni, indirizzi e obiettivi aziendali, atti di organizzazione	RAR, Progetti speciali, obiettivi regionali e aziendali	15 anni	
	.02	Programmazione, disposizioni, indirizzi e obiettivi aziendali, atti di organizzazione	Sperimentazioni gestionali	ILLIMITATO	
	.02	Programmazione, disposizioni, indirizzi e obiettivi aziendali, atti di organizzazione	Deleghe (di funzioni, attività, di firma) e Funzioni delegate da altri enti (Stato, Regioni, Comuni)	15 anni	
	.02	Programmazione, disposizioni, indirizzi e obiettivi aziendali, atti di organizzazione	Piano di organizzazione e funzionamento aziendale (*POAS* , POFA)	ILLIMITATO	
	.03	Protocolli di intesa, convenzioni con enti pubblici e privati, no profit	Convenzioni / collaborazioni con istituzioni varie (incluse convenzioni di tirocinio e convenzioni per accertamento d'ufficio PA certificanti)	ILLIMITATO	Circ.44/2005 Ministero per i Beni e le Attività Culturali
	.04	Controlli interni ed esterni	Documenti relativi ai controlli interni (es. controllo di gestione, contabilità analitica, controllo strategico, auditing, controllo di regolarità formale e contabile, ecc.)	10 anni; ILLIMITATO se allegate a delibere o a documenti di programmazione	
	.04	Controlli interni ed esterni	Documenti relativi ai controlli esterni (es. ispezioni e controlli effettuati da soggetti come la Corte dei Conti, Ministero della Salute, ecc.)	ILLIMITATO	
	.05	Sistema Qualità e Risk Management	Documenti relativi al sistema di gestione per la qualità (Verbali audit ISO, procedure aziendali, certificati ISO, riesame direzione, *questionari* customer satisfaction, piani qualità, ecc.)	10 anni	
	.05	Sistema Qualità e Risk Management	Scheda di incident reporting, raccolta e analisi dei rischi clinici, incident reporting, analisi statistica di principali sinistri, piano annuale di risk management	ILLIMITATO	
	.06	Progetti di Ricerca	Progetti di ricerca regionali, aziendali, altri progetti	5 anni	
	.07	Associazioni di volontariato e tutela dei diritti del malato	Rapporti con il mondo associativo, del no-profit, di tutela malati, ecc.	ILLIMITATO	
	.08	Politiche e interventi per le pari opportunità	Politiche sulle pari opportunità compresi convegni, congressi, questionari, ecc.	10 anni	

copia informatica per consultazione

CLASSE	COD. SOTTO CLASSE	SOTTOCLASSE	TIPO DOCUMENTO	TEMPO CONSERVAZIONE	RIFERIMENTI NORMATIVI / NOTE
2. Organi e Organismi	.01	Legale Rappresentate	Documenti relativi a Presidente, Direttore Generale o altra figura (nomina, compiti, rinnovo, cessazione e atti inerenti, ecc.)	ILLIMITATO	
	.01	Legale Rappresentate	Documenti relativi a Commissario ad acta (nomina, compiti, rinnovo, cessazione e atti inerenti, ecc.)	ILLIMITATO	
	.02	Organismi direttivi e scientifici	Documenti relativi a Presidente e Consiglio di Amministrazione di Fondazione (nomina, compiti, rinnovo, cessazione e atti inerenti, convocazione, funzionamento, verbali sedute, ecc.)	ILLIMITATO	
	.02	Organismi direttivi e scientifici	Documenti relativi a Direttore Amministrativo, Sanitario, Sociale (nomina, compiti, rinnovo, cessazione e atti inerenti, ecc.)	ILLIMITATO	
	.02	Organismi direttivi e scientifici	Documenti relativi a Direttore Scientifico e componenti comitato (nomina, compiti, rinnovo, cessazione e atti inerenti, ecc.)	ILLIMITATO	
	.03	Organismi di controllo interno ed esterno	Documenti relativi a organi / organismi di controllo interno (nomina, sostituzioni, convocazioni, funzionamento, verbali sedute e atti inerenti, ecc.)	ILLIMITATO	
	.03	Organismi di controllo interno ed esterno	Documenti relativi a Organismo di vigilanza del Codice etico comportamentale (nomina, sostituzioni, convocazioni, ordini del giorno, verbali, ecc.)	ILLIMITATO	
	.03	Organismi di controllo interno ed esterno	Documenti relativi a organismi di controllo esterni (elezioni, sostituzioni, convocazioni, ordini del giorno, verbali, ecc.)	ILLIMITATO	
	.03	Organismi di controllo interno ed esterno	Documenti relativi al Collegio Sindacale (nomina, sostituzioni, convocazioni, funzionamento, verbali sedute e atti inerenti, ecc.)	ILLIMITATO	
	.04	Collegi, Comitati e Commissioni	Documenti relativi a Collegio di Direzione (nomina, sostituzioni, convocazioni, funzionamento, verbali sedute e atti inerenti, ecc.)	ILLIMITATO	
	.04	Collegi, Comitati e Commissioni	Documenti relativi a Consiglio dei sanitari (elezioni, sostituzioni, convocazioni, ordini del giorno, verbali, ecc.)	ILLIMITATO	
	.04	Collegi, Comitati e Commissioni	Documenti relativi a Collegi tecnici (elezioni, sostituzioni, convocazioni, ordini del giorno, verbali, ecc.). Compresa quella relativa alla direzione dei distretti.	ILLIMITATO	
	.04	Collegi, Comitati e Commissioni	Documenti relativi a Comitato Unico di Garanzia (elezioni, sostituzioni, convocazioni, ordini del giorno, verbali, ecc.)	ILLIMITATO	
	.04	Collegi, Comitati e Commissioni	Documenti relativi a Comitato Etico (nomina, compiti, rinnovo dei componenti, ecc.)	ILLIMITATO	
	.04	Collegi, Comitati e Commissioni	Documenti relativi a Conferenza dei Sindaci ed esecutivo (composizione ed elezione, cessazione e sostituzione, funzionamento, verbali sedute, interpellanze e mozioni, ecc.)	ILLIMITATO	
	.04	Collegi, Comitati e Commissioni	Schede votazioni ed elezioni di collegi, comitati e commissioni	10 anni	
	.04	Collegi, Comitati e Commissioni	Documenti relativi a Commissione farmaceutica aziendale (nomina, compiti, rinnovo dei componenti, ecc.)	ILLIMITATO	
	.04	Collegi, Comitati e Commissioni	Documenti relativi a Componenti Ufficio di Pubblica Tutela (nomina, compiti, rinnovo dei componenti, ecc.)	ILLIMITATO	

copia informatica per consultazione

CLASSE	COD. SOTTO CLASSE	SOTTOCLASSE	TIPO DOCUMENTO	TEMPO CONSERVAZIONE	RIFERIMENTI NORMATIVI / NOTE
3. Attività Giuridico-Legale	.01	Pareri, informative giuridiche e attività tecnico-legali	Pareri legali e relazioni tecniche, compresi quelli che la struttura predispone per altre strutture.	15 anni (se raccolta autonoma) se inserito in fascicolo per il tempo del procedimento	
	.02	Contenzioso legale	Contenzioso civile	ILLIMITATO	
	.02	Contenzioso legale	Contenzioso penale	ILLIMITATO	
	.02	Contenzioso legale	Contenzioso amministrativo	ILLIMITATO	
	.02	Contenzioso legale	Contenzioso giuslavoristico	ILLIMITATO	
	.02	Contenzioso legale	Contenzioso stragiudiziale (arbitrato, mediazione, ecc.)	ILLIMITATO	
	.02	Contenzioso legale	Contenzioso sanzioni amministrative attive (es.: sanzioni erogate dall'ente verso terzi in materia di igiene, veterinaria, sicurezza sul lavoro, osservanza normativa antifumo; sanzioni a strutture sanitarie, ecc.) e passive. Compresi gli scritti difensivi.	10 anni	
	.02	Contenzioso legale	Procedimento per riscossione ticket sanitari	10 anni (a partire dalla conclusione del procedimento)	
	.02	Contenzioso legale	Segnalazioni / Denunce / Querele all'Autorità Giudiziaria	ILLIMITATO	
	.03	Procedure concorsuali ed esecutive	Concordati, fallimenti, pignoramenti, recupero crediti, riscossione coatta, ecc.	10 anni	
	.03	Procedure concorsuali ed esecutive	Azioni di rivalsa	*15 anni* *(dal ricovero / infortunio) in caso di avvenuto pagamento.* *30 anni* *(dal ricovero / infortunio) negli altri casi.*	*In quanto l'azione di recupero del credito si prescrive in 5 anni, mentre il termine massimo di prescrizione del reato è di 30 anni.* *Se a seguito di azione di rivalsa è stato attivato un "contenzioso legale" si osserverà il termine previsto per tale categoria documentale.*
	.04	Assicurazioni e gestione sinistri	Rapporto di brokeraggio assicurativo, RCT/O, gestione sinistri, polizze assicurative, richieste risarcimenti danni, tutela giudiziaria, furto incendi, infortuni, ecc.	ILLIMITATO	
	.04	Assicurazioni e gestione sinistri	Sinistri KasKo e RCA in assenza di contezioso	10 anni dall'avvenuta liquidazione	

copia informatica per consultazione

CLASSE	COD. SOTTO CLASSE	SOTTOCLASSE	TIPO DOCUMENTO	TEMPO CONSERVAZIONE	RIFERIMENTI NORMATIVI / NOTE
4. Risorse Umane	.01	Dotazione organica e gestione del personale	Fabbisogni e Piante organiche del personale, Fluper, ecc. (si veda anche p. 7.05)	10 anni	
	.02	Concorsi e selezioni	Bandi, verbali di concorsi, selezioni, avvisi di mobilità, avvisi pubblici, graduatoria finale, ecc.	ILLIMITATO	
	.02	Concorsi e selezioni	Altri documenti inerenti la procedura concorsuale *(domande di partecipazione, documenti non ritirati dagli interessati, prove d'esame ed annesso materiale documentario)*	5 anni *dopo la scadenza della graduatoria*	
	.02	Concorsi e selezioni	Documentazione relativa alle procedure di valutazione comparativa per l'assunzione di personale sia a tempo determinato sia indeterminato.	10 anni (a partire dalla ratifica e salvo contenzioso in atto). I verbali conservazione ILLIMITATA.	
	.02	Concorsi e selezioni	Documentazione relativa all'elezione delle commissioni giudicatrici	10 anni (a partire dalla ratifica e salvo contenzioso in atto) ILLIMITATO i verbali	
	.03	Assunzioni, inquadramenti, incarichi e cessazione	Documenti relativi alla assunzione e prese in servizio dei dipendenti. Compresi i contratti, rinnovi, carteggio tra enti. Trattenimenti in servizio. Stato di servizio	ILLIMITATO	
	.03	Assunzioni, inquadramenti, incarichi e cessazione	Documentazione relativa al periodo di prova	ILLIMITATO (a conclusione, inserite nei fascicoli personali)	
	.03	Assunzioni, inquadramenti, incarichi e cessazione	Mobilità interna ed esterna (in entrata e in uscita)	ILLIMITATO	
	.03	Assunzioni, inquadramenti, incarichi e cessazione	Cessazione del rapporto per limiti di età, di servizio, volontarie	ILLIMITATO (a conclusione, da inserire nei fascicoli personali)	
	.03	Assunzioni, inquadramenti, incarichi e cessazione	Documentazione relativa alle mansioni tipiche di ciascun ruolo, contratti di incarico, autorizzazioni per incarichi esterni, comunicazioni relative alla variazione dei dati personali, opzione per il regime di impegno a tempo pieno o a tempo parziale, opzione per attività intra-muraria o extra-muraria, assegnazione alla sede di servizio, ordini di servizio, cambio del settore disciplinare, riconoscimento mansioni superiori, modifica rapporto di lavoro, progressioni economiche orizzontali (PEO) e progressioni economiche verticali (PEV). Attribuzione / revoca / rinnovo qualifica di UPG, trasferimenti interni, libera professione (autorizzazione e atti conseguenti), ecc.	ILLIMITATO *(a conclusione, da inserire nei fascicoli personali)*	
	.04	Istituti contrattuali sospensivi della prestazione lavorativa	Documentazione relativa ai comandi e ai distacchi e alla ripresa di servizio nella sede originaria, aspettativa, congedi e altri istituti	ILLIMITATO (a conclusione, da inserire nei fascicoli personali)	
	.05	Organizzazioni sindacali e contrattazione	Documenti legati ai rapporti con le rappresentanze sindacali e agli accordi di contrattazione nazionale e decentrata (verbali, *accordi*)	ILLIMITATO *(5 anni documentazione preparatoria: lettere di invito, comunicazioni e altra documentazione di supporto)*	
	.06	Retribuzioni e compensi	Atti e documenti in materia di inquadramento economico	ILLIMITATO	
	.06	Retribuzioni e compensi	Documentazione contabile relativa a: comandi, trasferimenti, mobilità, elementi accessori (lavoro straordinario, reperibilità, plus orario, incentivazioni, proventi, indennità rischio rx, missioni, trasferte, assegni famigliari, intramoenia, libera professione, altre competenze variabili), gestione buoni pasto, ecc.	*10 anni*	*Armonizzato con stessa documentazione prodotta da altri enti locali.*
	.06	Retribuzioni e compensi	Certificazioni dei redditi dipendenti e personale atipico	20 anni	
	.06	Retribuzioni e compensi	Documenti relativi a prestiti, cessioni di stipendio, delegazioni di pagamento, pignoramento presso terzi (a partire dall'estinzione del pagamento).	10 anni (dopo l'estinzione del debito)	
	.06	Retribuzioni e compensi	CUD	10 anni	
	.06	Retribuzioni e compensi	Tabulati mensili riepilogativi retribuzioni – variazioni *stipendiali* mensili *(cedolini paga)*	10 anni	
	.07	Trattamenti fiscali, contributivi e assicurativi	Trattamenti fiscali e contributivi del personale (Versamenti mensili CPDEL, INADEL, CPS, INPS/INPDAP, indennizzo INAIL per infortunio, ecc.)	ILLIMITATO	
	.07	Trattamenti fiscali, contributivi e assicurativi	Trattamento di fine rapporto/servizio (TFR, TFS)	ILLIMITATO (a conclusione, inserite nei fascicoli personali)	
	.07	Trattamenti fiscali, contributivi e assicurativi	Pratiche assicurative per infortunio	5 anni	
	.08	Inabilità al lavoro, invalidità, infermità, indennizzo	Dichiarazioni di infermità ed equo indennizzo, comprende le pratiche di riconoscimento di infermità per cause di servizio e l'equo indennizzo.	ILLIMITATO (a conclusione, da inserire nei fascicoli personali)	

copia informatica per consultazione

CLASSE	COD. SOTTO CLASSE	SOTTOCLASSE	TIPO DOCUMENTO	TEMPO CONSERVAZIONE	RIFERIMENTI NORMATIVI / NOTE
4. Risorse Umane	.09	Presenze e assenze	Documenti relativi a permessi orari, assenze, ritardi, congedi ordinari e straordinari, ferie, congedo, cartellini / tabulati di presenza, permessi brevi e sindacali, sciopero, ecc.	5 anni	
	.09	Presenze e assenze	Riepilogo mensile rilevazione orari personale – timbrature	10 anni	
	.09	Presenze e assenze	Documenti relativi a turni ed orari di servizio, visite fiscali ai dipendenti	10 anni	
	.09	Presenze e assenze	Certificati malattia personale	10 anni (da cessazione attività)	
	.10	Quiescenza e relativo trattamento	Atti e documenti in materia di trattamento di quiescenza e di previdenza del personale, pratiche pensionistiche, riscatto e ricongiunzione servizi/ruolo, ecc.	ILLIMITATO (a conclusione, da inserire nei fascicoli personali)	
	.11	Servizi a richiesta individuale	Pratiche di concessione benefici economici (ad es. per cure mediche) e di gestione delle provvidenze per il personale (contributi per asili nido, per centri estivi per figli di dipendenti, per abbonamenti ai mezzi di trasporto pubblico, ecc.), nonché le richieste di rilascio della tessera di riconoscimento e di certificati di servizio, l'assistenza fiscale su richiesta del dipendente.	10 anni	
	.12	Valutazione del personale	Procedimenti disciplinari, verbali ed atti del dirigente competente / ufficio procedimenti disciplinari	ILLIMITATO	
	.12	Valutazione del personale	Valutazione del personale (scheda valutazione)	ILLIMITATO (a conclusione, da inserire nei fascicoli personali)	
	.12	Valutazione del personale	Documentazione riferita alle segnalazioni e alle comunicazioni sull'inosservanza dei doveri d'ufficio.	ILLIMITATO (a conclusione, inserire nel fascicolo personale)	
	.12	Valutazione del personale	Mobbing (denunce e segnalazioni)	ILLIMITATO (se nel fascicolo personale, 10 anni da cessazione attività altri esemplari)	
	.12	Valutazione del personale	Note di encomio, le congratulazioni per il servizio svolto e riconoscimenti simili	ILLIMITATO (a conclusione, da inserire nei fascicoli personali)	
	.13	Formazione e aggiornamento del personale	Documentazione relativa ad attività formative (interna, esterna, a distanza) rivolte al personale (richieste, autorizzazioni, *documentazione presenze*, ecc.)	5 anni	
	.13	Formazione e aggiornamento del personale	Attestati di corsi di qualificazione e riqualificazione del personale	ILLIMITATO (a conclusione, da inserire nei fascicoli personali)	
	.13	Formazione e aggiornamento del personale	Gestione crediti formativi professionali (ECM, ecc.)	ILLIMITATO (a conclusione, da inserire nei fascicoli personali)	
	.13	Formazione e aggiornamento del personale	Piano annuale e triennale della formazione	10 anni	
	.14	Deontologia professionale ed etica del lavoro	Codici deontologici del personale, Codice Etico, codice di comportamento e iniziative connesse alla divulgazione, conoscenza e osservanza, iniziative di prevenzione in materia di anticorruzione.	ILLIMITATO	
	.15	Personale non strutturato o convenzionato	Pratiche di affidamento di incarichi di lavoro autonomo (incarichi libero professionali, incarichi di natura occasionale, co.co.co) e altre forme di lavoro atipico (incarichi, contratti e relazioni, ecc.).	ILLIMITATO (da inserire nel fascicolo *personale*)	
	.15	Personale non strutturato o convenzionato	Documenti relativi alla presa in servizio e alla cessazione di personale atipico (collaboratori, stagisti, specializzandi, frequentatori, dottorandi, tirocinanti, volontari, *borsisti,* ecc.). Compresi i contratti, affidamento di incarichi, rinnovi, carteggio tra enti.	ILLIMITATO (da inserire nel fascicolo *personale*)	
	.15	Personale non strutturato o convenzionato	Fascicolo rapporti convenzione (MMG, PdF, Sumai, ecc.)	ILLIMITATO	

copia informatica per consultazione

CLASSE	COD. SOTTO CLASSE	SOTTOCLASSE	TIPO DOCUMENTO	TEMPO CONSERVAZIONE	RIFERIMENTI NORMATIVI / NOTE
5. Risorse finanziarie e gestione contabile	.01	Attività finanziaria e contabile	Budget di cassa (rendiconto finanziario)	10 anni	
	.01	Attività finanziaria e contabile	Ordinativi / Distinte di incasso e di pagamento, documentazione relativa alla gestione della spese (impegno, liquidazione, ordinazione e pagamento) e altre registrazioni contabili di carattere transitorio (mandati / reversali, movimenti del tesoriere, ecc.)	10 anni dall'approvazione del bilancio (se esistono per gli anni corrispondenti i registri contabili)	Sarà possibile scartare dopo 2 anni eventuale documentazione prodotta in copia
	.01	Attività finanziaria e contabile	Verbali e verifiche Cassa	ILLIMITATO	
	.01	Attività finanziaria e contabile	Convenzioni, attivazione e cessazione con istituti di credito	10 anni	
	.01	Attività finanziaria e contabile	Servizi bancari telematici (internet banking)	10 anni	
	.01	Attività finanziaria e contabile	Estratti conto operazioni bancarie	10 anni	
	.01	Attività finanziaria e contabile	Registri contabili principali, anche sotto forma di banche dati (mastro, giornali di cassa, ecc.)	ILLIMITATO	
	.02	Bilancio e Rendicontazione	Bilanci e rendiconto della gestione con i relativi allegati	ILLIMITATO	
	.02	Bilancio e Rendicontazione	Bilancio: carteggio interlocutorio interno, assegnazione budget, ecc.	10 anni	
	.02	Bilancio e Rendicontazione	Situazioni contabili periodiche (CET)	15 anni (se raccolta autonoma, se invece inserito in fascicolo per il tempo del procedimento)	
	.02	Bilancio e Rendicontazione	Libro cespiti	ILLIMITATO	
	.03	Gestione entrate-uscite	Documentazione varie inerenti il flusso degli incassi (avvisi di riscossione)	10 anni	
	.03	Gestione entrate-uscite	Cartelle pagamenti esattoriali	10 anni (se esistono per gli anni corrispondenti i registri contabili / libro giornale)	
	.03	Gestione entrate-uscite	Fatture emesse e fatture ricevute	10 anni (se esistono per gli anni corrispondenti i registri contabili / libro giornale)	
	.03	Gestione entrate-uscite	Solleciti di pagamento	10 anni	
	.03	Gestione entrate-uscite	Documentazione relativa ricognizione debiti/crediti gestione liquidatoria	ILLIMITATO	
	.03	Gestione entrate-uscite	Cessioni del credito	10 anni	
	.03	Gestione entrate-uscite	Rimborsi spese non dovute	10 anni	
	.04	Gestione fiscale e imposte	Documenti relativi a imposte e tasse dell'azienda quale sostituto di imposta IRES, ICI, IMU, IRPEF, bollo virtuale, IVA ecc.	10 anni	
	.04	Gestione fiscale e imposte	Registro IVA vendite, acquisti	ILLIMITATO	
	.04	Gestione fiscale e imposte	Certificazioni ritenute d'acconto	10 anni	
	.04	Gestione fiscale e imposte	Modello 770 (dichiarazione sostituti d'imposta)	10 anni	
	.04	Gestione fiscale e imposte	Modello Unico (redditi IRAP e IVA)	10 anni	

copia informatica per consultazione

CLASSE	COD. SOTTO CLASSE	SOTTOCLASSE	TIPO DOCUMENTO	TEMPO CONSERVAZIONE	RIFERIMENTI NORMATIVI / NOTE
6. Gestione e organizzazione del patrimonio	.01	Progettazione e costruzione di beni immobili con relativi impianti	Documentazione relativa alla progettazione e realizzazione degli immobili dell'azienda e alla relativa impiantistica (progettazione, direzione lavori, collaudi, contratti, planimetrie, progetti di costruzione, ecc.). Comprese le procedure di gare d'appalto per la realizzazione di dette opere / impianti.	ILLIMITATO 10 anni (salvo contenzioso in atto) per documentazione preliminare e preparatoria	
	.02	Acquisizione e gestione beni immobili e relativi servizi	Documentazione relativa ai procedimenti per l'acquisto di terreni, edifici, strutture e immobili di vario tipo, nonché la loro destinazione d'uso e l'ordinaria gestione patrimoniale. Compresi gli atti e documenti comprovanti la proprietà di immobili, la gestione di lasciti, nonché l'inventario beni immobili.	ILLIMITATO 10 anni (salvo contenzioso in atto) per documentazione preliminare e preparatoria	
	.02	Acquisizione e gestione beni immobili e relativi servizi	Documentazione relativa agli adempimenti necessari per la gestione delle locazioni attive e passive di immobili, comodati, ecc.	ILLIMITATO 10 anni (salvo contenzioso in atto) per documentazione preliminare e preparatoria	
	.02	Acquisizione e gestione beni immobili e relativi servizi	Documentazione che si riferisce alla alienazione, vendita, cessione o permuta di immobili, compresa l'eventuale indizione e gestione di asta pubblica	ILLIMITATO 10 anni (salvo contenzioso in atto) per documentazione preliminare e preparatoria	
	.02	Acquisizione e gestione beni immobili e relativi servizi	Documentazione relativa a costituzione e/o trasferimento di diritti reali sugli immobili (superfici, servitù)	ILLIMITATO	
	.02	Acquisizione e gestione beni immobili e relativi servizi	Programma triennale ed elenco annuale lavori pubblici	ILLIMITATO	
	.03	Acquisizione e gestione di beni mobili / generi di consumo e di servizi	Documentazione relativa all'acquisizione e fornitura di beni mobili, di materiali e attrezzature tecniche, scientifiche, e non, e per la fornitura di servizi, compresi contratti RCA auto (richieste partecipazione e gare, bandi gara, offerte, verbali seduta, atti indizione e aggiudicazione, contratti, ecc.)	10 anni *dalla data di dismissione del bene*	
	.03	Acquisizione e gestione di beni mobili / generi di consumo e di servizi	Acquisizione e gestione di beni mobili da lasciti o donazioni	ILLIMITATO	*La documentazione relativa a donazioni di beni mobili anche a carattere artistico deve essere classificata all'interno della voce donazione e conservata a tempo illimitato.* *Eventuali raccolte documentali spurie relative all'acquisizione/gestione di beni mobili di carattere artistico è da conservare a tempo illimitato.*
	.03	Acquisizione e gestione di beni mobili / generi di consumo e di servizi	Servizi di vigilanza, portineria, automezzi, ecc.	ILLIMITATO	
	.03	Acquisizione e gestione di beni mobili / generi di consumo e di servizi	Inventario beni mobili: Libro cespiti ammortizzabili e trasferimenti interni beni inventariati.	ILLIMITATO (per Libro cespiti, altra documentazione 10 anni)	
	.03	Acquisizione e gestione di beni mobili / generi di consumo e di servizi	Albo fornitori	20 anni	
	.03	Acquisizione e gestione di beni mobili / generi di consumo e di servizi	Documentazione relativa agli adempimenti necessari per la gestione delle locazioni attive e passive di beni mobili e comodati	ILLIMITATO	
	.03	Acquisizione e gestione di beni mobili / generi di consumo e di servizi	Documentazione che si riferisce alla alienazione, cessione o permuta di beni mobili, compresa eventuale indizione e gestione di asta pubblica. Fuori uso.	10 anni	
	.03	Acquisizione e gestione di beni mobili / generi di consumo e di servizi	Utenze varie (telefono, acqua, gas, calore, illuminazione, ecc.;	10 anni	
	.03	Acquisizione e gestione di beni mobili / generi di consumo e di servizi	Servizio ristorazione, mensa e ticket pasti (rapporti con fornitore)	10 anni	
	.03	Acquisizione e gestione di beni mobili / generi di consumo e di servizi	Documentazione relativa all'attività dei magazzini (richieste a magazzino, documento di trasporto, ordini, inventario di magazzino, registri carico-scarico, ecc.)	5 anni (per richieste a magazzino; tutto il resto 10 anni)	

copia informatica per consultazione

CLASSE	COD. SOTTO CLASSE	SOTTOCLASSE	TIPO DOCUMENTO	TEMPO CONSERVAZIONE	RIFERIMENTI NORMATIVI / NOTE
6. Gestione e organizzazione del patrimonio	.04	Manutenzione ordinaria, straordinaria, ristrutturazione, destinazione d'uso	Documentazione relativa alle procedure di appalto per la ristrutturazione, manutenzione, restauro di immobili. Compresi progettazione e collaudi relativi a lavori effettuati su edifici.	ILLIMITATO 10 anni (salvo contenzioso in atto) per documentazione preliminare e preparatoria	
	.04	Manutenzione ordinaria, straordinaria, ristrutturazione, destinazione d'uso	Documenti relativi alle eventuali modifiche della destinazione d'uso, ecc.;	ILLIMITATO 10 anni (salvo contenzioso in atto) per documentazione preliminare e preparatoria	
	.04	Manutenzione ordinaria, straordinaria, ristrutturazione, destinazione d'uso	Documentazione relativa alle procedure di appalto per la ristrutturazione, manutenzione, restauro di impianti. Compresa certificazione di manutenzione di impianti.	ILLIMITATO 10 anni (salvo contenzioso in atto) per documentazione preliminare e preparatoria	
	.04	Manutenzione ordinaria, straordinaria, ristrutturazione, destinazione d'uso	Documenti che si riferiscono alla manutenzione e riparazione di tutti i beni mobili (arredi, fax PC, scanner, ecc.), compresi i collaudi relativi ad apparecchiature, contratti di manutenzione, esiti delle manutenzioni.	20 anni (salvo contenzioso in atto) per documentazione preliminare e preparatoria	
	.04	Manutenzione ordinaria, straordinaria, ristrutturazione, destinazione d'uso	Documenti che si riferiscono alla manutenzione e riparazione di apparecchiature elettromedicali, di laboratorio e biomediche	20 anni (salvo contenzioso in atto) per documentazione preliminare e preparatoria	
	.04	Manutenzione ordinaria, straordinaria, ristrutturazione, destinazione d'uso	Interventi abbattimento barriere architettoniche	20 anni	
	.04	Manutenzione ordinaria, straordinaria, ristrutturazione, destinazione d'uso	Documentazione inerente posizionamento e rimozione cartelli indicatori e segnaletica	10 anni	
	.04	Manutenzione ordinaria, straordinaria, ristrutturazione, destinazione d'uso	Documenti su piccoli interventi tecnici (falegnameria, idraulica, ecc.)	5 anni	
	.05	Attività contrattuale e tutela della proprietà intellettuale	Contratti attivi (Concessioni, sponsorizzazioni, ecc.)	ILLIMITATO 10 anni (salvo contenzioso in atto) per documentazione preliminare e preparatoria	
	.05	Attività contrattuale e tutela della proprietà intellettuale	Ricerca (contratti di ricerca, *contratti* di sperimentazione clinica, ecc.)	ILLIMITATO 10 anni (salvo contenzioso in atto) per documentazione preliminare e preparatoria	
	.05	Attività contrattuale e tutela della proprietà intellettuale	Brevetti (documentazione inerente il rilascio, la gestione, la titolarità, il deposito, la durata, gli atti di disposizione, ecc.)	ILLIMITATO 10 anni (salvo contenzioso in atto) per documentazione preliminare e preparatoria	
	.06	Sicurezza degli ambienti di lavoro	Documentazione relativa alla sicurezza dei luoghi di lavoro e degli impianti a essi afferenti (adempimenti, sicurezza apparecchiature elettriche, procedure 1° soccorso, gestione e valutazione del rischio, impianti antintrusione, nomina addetti prevenzione e protezione RSPP, formazione su sicurezza e squadre di emergenza).	20 anni (dalla cessazione dell'attività o modifica alla titolarità di esercizio e modifica dei locali)	
	.06	Sicurezza degli ambienti di lavoro	Documenti previsti dalla normativa in materia di sicurezza sul lavoro e prevenzione (ad es. i vari piani per la sicurezza dei luoghi di lavoro, la nomina dei responsabili per la sicurezza, ecc.), compresa la formazione specifica del personale dipendente.	20 anni (dalla cessazione dell'attività o modifica alla titolarità di esercizio e modifica dei locali)	
	.06	Sicurezza degli ambienti di lavoro	Sorveglianza sanitaria e sicurezza ambiente di lavoro: rapporti e verbali di sopralluogo	ILLIMITATO	
	.06	Sicurezza degli ambienti di lavoro	Visite mediche del personale e attestazioni di idoneità	ILLIMITATO	
	.07	Gestione dei rifiuti	Documenti che si riferiscono alla gestione e smaltimento dei rifiuti dell'ente, anche quelli speciali, tossici, nocivi e biologici. Rientra in questa classe anche la nomina degli addetti responsabili.	20 anni	

copia informatica per consultazione

CLASSE	COD. SOTTO CLASSE	SOTTOCLASSE	TIPO DOCUMENTO	TEMPO CONSERVAZIONE	RIFERIMENTI NORMATIVI / NOTE
7. Sistemi Informativi e comunicazione	.01	Sistema documentale	Documentazione relativa alla gestione del servizio archivistico e strumenti di corredo. Compresi: manuale di gestione documenti, gestione del protocollo, gestione degli archivi (procedure di scarto, titolari , massimari, richieste di consultazione), ecc.	ILLIMITATO	*Si conservano a tempo illimitato anche: registro di protocollo, repertorio dei fascicoli, registro albo on-line, registri: protocollo, fascicoli, albo on line, notifiche, ordinanze, decreti, deliberazioni, determinazioni, contratti e tutte le tipologie di registri e repertori previsti dalla legge o regolamenti. Nel caso di incertezza sulla loro conservazione si deve sempre esprimere la Soprintendenza archivistica.*
	.01	Sistema documentale	Albo on line e pubblicazioni su siti web aziendali relativamente alle leggi in materia di accesso e trasparenza nella pubblica amministrazione	2 anni per Albo on line; per altre tipologie di documentazione si deve fare riferimento alle leggi in materia e alle disposizione dei Garanti/Autorità	
	.01	Sistema documentale	Domande consultazione archivio	1 anno	
	.01	Sistema documentale	Richieste di accesso ai documenti e conseguenti provvedimenti	1 anno per fini amministrativi ILLIMITATO (per motivi di studio o informazione archivistica)	Se la domanda di accesso produce diniego, e conseguente ricorso, la documentazione deve essere trasferita nell'eventuale fascicolo di contenzioso e conservata per il tempo dello stesso. Per la gestione delle domande di accesso agli atti si possono prevedere due modelli: centralizzato e decentralizzato. Centralizzato: tutta la documentazione è gestita in un unico fascicolo da un ufficio preposto. Decentralizzato: ogni domanda è gestita all'interno del fascicolo del procedimento dal relativo responsabile, si conserva per il tempo del fascicolo stesso.
	.02	Rapporti con il pubblico, sportelli informativi e trasparenza	Relazioni con il pubblico: gestione segnalazioni, reclami e apprezzamenti, informazioni, pubbliche relazioni	10 anni	
	.02	Rapporti con il pubblico, sportelli informativi e trasparenza	Comunicazione con i media, rassegna stampa, conferenze stampa,	1 anno	
	.02	Rapporti con il pubblico, sportelli informativi e trasparenza	Pubblicazioni aziendali, Piano di Comunicazione, guida ai servizi	ILLIMITATO	
	.02	Rapporti con il pubblico, sportelli informativi e trasparenza	Documenti relativi alla rappresentanza istituzionale (eventi, patrocini, manifestazioni, ecc.)	5 anni	
	.03	Tutela della riservatezza	Aggiornamenti elenchi incaricati privacy, nomina incaricati	10 anni	
	.03	Tutela della riservatezza	Informativa dell'Azienda e consenso al trattamento dati	Medesimo tempo di conservazione della documentazione relativa al prestazione/procedimento reso	Se il consenso (e l'informativa) è collegato a più documentazione deve essere conservato fino all'avvenuto scarto di tutti i documenti a cui afferisce.
	.03	Tutela della riservatezza	Documentazione relativa ai Reclami per la tutela della Privacy. Compresa sia la domanda (reclamo presentato) sia la risposta fornita	10 anni	
	.04	Biblioteche e centri di documentazione	Documentazione relativa al servizio di biblioteca, acquisti, catalogazione, richieste di consultazione e prestito, ecc. Compresa la gestione del centro di documentazione.	5 anni	
	.05	Sistema informatico, reti e sicurezza	Documentazione relativa alla gestione delle banche dati (es. sistema di gestione del personale, sistema finanziario-contabile, ecc.)	ILLIMITATO	Si intende la documentazione relativa alle fasi di progettazione e di gestione delle banche dati come sistema in quanto tale; da non confondere con i dati immessi che possono essere assoggettati a tempi diversi di conservazione.
	.05	Sistema informatico, reti e sicurezza	Documentazione relativa alla realizzazione e gestione delle reti interne ed esterne (comprese le cablature, gli impianti di rete, etc.), nonché la loro manutenzione e gli interventi per il loro corretto funzionamento.	10 anni	
	.05	Sistema informatico, reti e sicurezza	Documentazione relativa alla sicurezza informatica	ILLIMITATO	
	.05	Sistema informatico, reti e sicurezza	Documentazione relativa alla gestione dell'attività di informatizzazione e richieste di abilitazione e intervento	5 anni	
	.05	Sistema informatico, reti e sicurezza	Documentazione relativa alla realizzazione e gestione del SISS (es. progettazione e architettura sistemi, integrazione, istallazione e configurazione sistemi, gestione carte, ecc.)	10 anni	
	.05	Sistema informatico, reti e sicurezza	Documentazione inerente i sistemi dedicati alle attività CUP/ Call Center Regionale anche per la libera professione	10 anni	
	.06	Statistiche e reporting	Statistiche e report istituzionali (es. flussi informativi ministeriali, regionali, ISTAT, ecc.) a fronte di richieste di enti esterni	ILLIMITATO	

copia informatica per consultazione

CLASSE	COD. SOTTO CLASSE	SOTTOCLASSE	TIPO DOCUMENTO	TEMPO CONSERVAZIONE	RIFERIMENTI NORMATIVI / NOTE
1. Organizzazione territoriale	.01	Gestione e organizzazione dipartimentale e interdipartimentale, distrettuale ed interdistrettuale	Atti di indirizzo, coordinamento e programmazione attività dipartimentali e distrettuali Progetti (atti di approvazione) Rapporti con organi interni ed esterni	ILLIMITATO	
	.01	Gestione e organizzazione dipartimentale e interdipartimentale, distrettuale ed interdistrettuale	Monitoraggio attività dipartimentali e distrettuali	5 anni	Si tratta di documentazione di carattere ordinario/routinario (fogli di lavoro e verbali di carattere operativo). I documenti relativi alla gestione delle attività, al funzionamento ed all'organizzazione dei dipartimenti e dei distretti rientrano in Atti di indirizzo, coordinamento e programmazione attività dipartimentali e distrettuali (II.1.01)
	.01	*Gestione e organizzazione dipartimentale e interdipartimentale, distrettuale ed interdistrettuale*	*Verbali incontri / riunioni interne di pianificazione e organizzazione*	*10 anni*	
	.02	Progetti, interventi e iniziative varie dipartimentali / distrettuali	Documentazione istruttoria relativa a progetti	10 anni	Il progetto è conservato illimitatamente (II.1.01) (decreto di approvazione progetto, approvazione graduatoria ed erogazione contributi); mentre la documentazione istruttoria concerne: istanze/domande; valutazioni si può scartare a 10 aa. Come "gare appalto" (Vedi I.6.03).
	.03	Coordinamento e gestione personale infermieristico, tecnico-assistenziale, di prevenzione	Documenti inerenti attività del personale (turni di attività, assegnazioni, segnalazioni, compiti assegnati, obiettivi, ecc.). La documentazione relativa al rapporto di lavoro, alla valutazione del personale, ecc. dovrà essere classificata e conservata secondo quanto specificato nelle voci di classificazione del titolo 1.	5 anni	

copia informatica per consultazione

CLASSE	COD. SOTTO CLASSE	SOTTOCLASSE	TIPO DOCUMENTO	TEMPO CONSERVAZIONE	RIFERIMENTI NORMATIVI / NOTE
2. Prevenzione e sicurezza negli ambienti di lavoro	.01	Aspetti generali, organizzativi e gestionali	Documenti strategici di programmazione, pianificazione, rendicontazione delle attività (Piani, programmi, calendari, registri, altri documenti strategici e di programmazione, ecc.)	ILLIMITATO	
	.01	Aspetti generali, organizzativi e gestionali	Documentazione istruttoria e corrispondenza ordinaria/routinaria interna ed esterna attività prevenzione e sicurezza negli ambienti di lavoro	5 anni	
	.01	Aspetti generali, organizzativi e gestionali	Documentazione inerente attività formativa da parte dei soggetti accreditati da Regione Lombardia	10 anni	
	.02	Medicina del lavoro e malattie professionali	Certificati idoneità lavorativa specifica alle mansioni rilasciati dallo PSAL	10 anni	
	.02	Medicina del lavoro e malattie professionali	Ricorso avverso giudizi idoneità / inidoneità specifica alla mansione rilasciati dal Medico Competente con relativa documentazione sanitaria sul lavoratore	ILLIMITATO	
	.02	Medicina del lavoro e malattie professionali	Certificato di idoneità lavorativa di minori (D.Lgs. 345/99)	10 anni	
	.02	Medicina del lavoro e malattie professionali	Accertamenti sanitari e strumentali di idoneità/inidoneità al lavoro effettuati da medici competenti delle ditte	10 anni	
	.02	Medicina del lavoro e malattie professionali	Inchieste sulle malattie professionali (richieste, relazione, sopralluogo, rapporto a procura, ecc.)	ILLIMITATO	
	.02	Medicina del lavoro e malattie professionali	Cartella sanitaria e di rischio del lavoratore (accertamenti sanitari, referti, giudizio di idoneità al lavoro o cambio mansioni lavorative, accertamenti specialistici ulteriori, ecc.)	10 anni dalla cessazione del rapporto di lavoro. Salvo nei casi di: - esposizione ad agenti biologici: 10 anni dalla cessazione, ma fino a 40 anni dalla cessazione per infezioni latenti, recrudescenti, ecc.; - esposizione a radiazioni ionizzanti: 30 anni dalla cessazione; - esposizione ad agenti cancerogeni: 40 anni dalla cessazione.	D.lgs. 81/2008 art. 243 - art. 280 - Decreto Ministero della Salute 12 Luglio 2007, n.155: art. 3
	.02	Medicina del lavoro e malattie professionali	Certificato medico di malattia professionale (Mod. 5 SS INAIL)	ILLIMITATO	
	.02	Medicina del lavoro e malattie professionali	Denunce / Segnalazione malattia professionale da parte del medico (Mod. 92 bis INAIL)	ILLIMITATO	
	.02	Medicina del lavoro e malattie professionali	Segnalazione dell'ISPEL (Sistema sorveglianza epidemiologica Mal. Prof. SW nazionale)	ILLIMITATO	
	.02	Medicina del lavoro e malattie professionali	Scheda OCCAM (OCcupational CAncer Monitoring) ISPESL - INT	ILLIMITATO	
	.02	Medicina del lavoro e malattie professionali	Questionario sulla storia di lavoro e sulle abitudini di vita - Centro Operativo Lombardia (mesotelioma)	ILLIMITATO se in fascicolo personale. 30 anni da cessazione attività	
	.02	Medicina del lavoro e malattie professionali	Questionario sulla storia di lavoro e sulle abitudini di vita - ReNaTuNS Registro Reg. Lombardia	ILLIMITATO se in fascicolo personale. 30 anni da cessazione attività	

copia informatica per consultazione

CLASSE	COD. SOTTO CLASSE	SOTTOCLASSE	TIPO DOCUMENTO	TEMPO CONSERVAZIONE	RIFERIMENTI NORMATIVI / NOTE
2. Prevenzione e sicurezza negli ambienti di lavoro	.03	Igiene e sicurezza sul lavoro	Attività di vigilanza sanitaria sull'applicazione delle norme in materia di sicurezza ed igiene del lavoro negli ambienti di lavoro (segnalazioni, denunce, verbali di sopralluogo, verbale sanzionatorio, ecc.)	ILLIMITATO	
	.03	Igiene e sicurezza sul lavoro	Certificazioni / pareri igienico-sanitari su progetti nuovi insediamenti produttivi di carattere industriale e artigianale (es. SCIA ambienti di lavoro)	30 anni	Insediamenti produttivi di tipo industriale / artigianale: 30 anni dalla certificazione / SCIA
	.03	Igiene e sicurezza sul lavoro	Certificazioni / pareri igienico-sanitari su progetti di altri insediamenti produttivi di carattere non industriale (es. SCIA ambienti di lavoro)	5 anni	Altri insediamenti di tipo commerciale: 5 anni dalla certificazione/SCIA (es. parrucchiere, estetista, tatuatori, ecc.)
	.03	Igiene e sicurezza sul lavoro	Trattamento rifiuti speciali non pericolosi / pareri (art. 208 d.lgs. 152/2006) e altra documentazione	ILLIMITATO	
	.03	Igiene e sicurezza sul lavoro	Campionamenti ambientali per la determinazione quali-quantitativa fattori di rischio (rumore, microclima, polveri, agenti chimici, vibrazioni)	ILLIMITATO verbali; 10 anni altra documentazione	
	.03	Igiene e sicurezza sul lavoro	Autorizzazione: lavoro in locali interrati /seminterrati. in deroga art. 65 D.lgs. 81/08	2 anni dalla data di cessazione di attività	
	.03	Igiene e sicurezza sul lavoro	Inchiesta infortuni (comprendente: denunce, relazione di sopralluogo, esecuzione di rilievi, verbale raccolta di sommarie informazioni testimoniali, verbale raccolta di dichiarazioni spontanee, certificato medico di infortunio lavorativo, invito a presentarsi, richiesta di documentazione, acquisizione di documentazione, scheda "Inchiesta infortuni", verbale di accertamento e contestazione illecito amministrativo, ecc.)	ILLIMITATO	
	.03	Igiene e sicurezza sul lavoro	Referti infortuni che non esitano in indagine	10 anni	
	.03	Igiene e sicurezza sul lavoro	Registro infortuni	4 anni dall'ultima registrazione e, se non usato, dalla data in cui è stato vidimato	D.M. 12/9/58, art.2
	.03	Igiene e sicurezza sul lavoro	Rapporto relativo all'infortunio sul lavoro alla Procura della Repubblica con allegato l'inchiesta	ILLIMITATO	
	.03	Igiene e sicurezza sul lavoro	Fascicolo prevenzione infortuni	ILLIMITATO	
	.03	Igiene e sicurezza sul lavoro	Bonifica amianto (segnalazioni dei casi esposti, certificato esposizione, certificato PSAL per accesso benefici INAIL- INPS,	ILLIMITATO	
	.03	Igiene e sicurezza sul lavoro	Bonifica amianto (notifica amianto in strutture o luoghi, piano di lavoro per la bonifica, verbale di controllo c/o siti con presenza amianto e/o ditte abilitate a smantellamento, verbale sanzionatorio, relazione annuale bonifica / smantellamento amianto delle ditte, ecc.).	ILLIMITATO	
	.03	Igiene e sicurezza sul lavoro	Registro esposti ed ex esposti amianto	ILLIMITATO	
	.03	Igiene e sicurezza sul lavoro	Registro degli esposti ad agenti cancerogeni e registro degli esposti ad agenti biologici	ILLIMITATO	
	.03	Igiene e sicurezza sul lavoro	Registro informatico "Progetto rilevazione amianto" / notifiche censimento amianto	ILLIMITATO	
	.03	Igiene e sicurezza sul lavoro	Patentino per bonificatore amianto	ILLIMITATO	
	.03	Igiene e sicurezza sul lavoro	Comunicazioni per detrazioni fiscali	10 anni	
	.03	Igiene e sicurezza sul lavoro	Comunicazioni aziende classe di rischio primo soccorso (dm 388/2008)	10 anni	
	.03	Igiene e sicurezza sul lavoro	Comunicazioni nomina RLS e RSPP	5 anni	
	.03	Igiene e sicurezza sul lavoro	Rilascio patentini di abilitazione utilizzo gas tossici (compresi verbali esami) e relative revisioni	5 anni	RD n. 147/1927
	.03	Igiene e sicurezza sul lavoro	Comunicazioni relative alla notifica preliminare cantieri	5 anni	
	.03	Igiene e sicurezza sul lavoro	Verbali di ispezione e controlli cantieri	5 anni; 10 anni nel caso di contenzioso (sanzioni) dalla proposta di archiviazione	
	.04	Sicurezza e impiantistica	Documentazione relativa alle attività di vigilanza sulla sicurezza dei luoghi di lavoro delle macchine / impianti / attrezzature di lavoro	ILLIMITATO verbali; 10 anni dalla demolizioni degli impianti e/o delle attrezzature altra documentazione	
	.04	Sicurezza e impiantistica	Documentazione inerente presunte non conformità macchine / attrezzature marcatura CE	ILLIMITATO	

copia informatica per consultazione

CLASSE	COD. SOTTO CLASSE	SOTTOCLASSE	TIPO DOCUMENTO	TEMPO CONSERVAZIONE	RIFERIMENTI NORMATIVI / NOTE
3. Prevenzione medico - sanitaria	.01	Aspetti generali, organizzativi e gestionali	Documenti strategici di programmazione, pianificazione, rendicontazione delle attività (Piani, programmi, calendari, registri, altri documenti strategici e di programmazione, ecc.)	ILLIMITATO	
	.01	Aspetti generali, organizzativi e gestionali	Documentazione istruttoria e corrispondenza ordinaria / routinaria interna ed esterna attività di prevenzione medico-sanitaria	5 anni	
	.02	Educazione sanitaria	Progetti di promozione della salute	ILLIMITATO	
	.02	Educazione sanitaria	Documentazione istruttoria e corrispondenza relativa a progetti ed interventi di educazione alla salute.	10 anni	
	.02	Educazione sanitaria	Materiale informativo (compresi i questionari) per promozione ed educazione alla salute	1 anno	
	.03	Epidemiologia e profilassi malattie infettive e parassitarie	Documenti su attività di disinfezione/disinfestazione (denunce / segnalazioni, convenzione con enti, verbale di controllo, scheda intervento, ecc.)	ILLIMITATO convenzioni, denunce e verbali; 10 anni altra documentazione	
	.03	Epidemiologia e profilassi malattie infettive e parassitarie	Notifiche e denunce malattie infettive (scheda notifica)	10 anni	DM 15/12/90 (Sistema informativo delle malattie infettive e diffusive) DM 29/7/98 (Modifiche relative alla TBC)
	.03	Epidemiologia e profilassi malattie infettive e parassitarie	Registro informativo malattie infettive (MAINF)	ILLIMITATO	DM 15/12/90 (Sistema informativo delle malattie infettive e diffusive) DM 29/7/98 (Modifiche relative alla TBC)
	.03	Epidemiologia e profilassi malattie infettive e parassitarie	Indagine / Inchiesta / Sorveglianza epidemiologica di malattia infettiva (esiti campionamento, relazione sanitaria, dati su epidemia, elenco contatti, profilassi prescritta, comunicazione a enti locali e/o H, ecc.)	10 anni da ultima registrazione	Circ. Min. Sanità n. 61 del 19/12/1986. In considerazione del termine di prescrizione del diritto al risarcimento del danno subito da un paziente che è di dieci anni, siffatta documentazione verrà conservata sino al compimento della prescrizione decennale
	.03	Epidemiologia e profilassi malattie infettive e parassitarie	Indagine / Inchiesta / Sorveglianza epidemiologica di malattia infettiva (referto visite, esami laboratorio e strumentali, ecc.)	10 anni da ultima registrazione	
	.03	Epidemiologia e profilassi malattie infettive e parassitarie	Attuazione campagne vaccinali (calendarizzazione, inviti e registrazione vaccinazioni, ecc.)	ILLIMITATO i Registri e le schede vaccinali; 2 anni altra documentazione (compresi i fogli di lavoro)	Nota RL prot. H1.2001.0033136 del 16.05.2001 Direzione generale degli archivi. Prontuari di scarto per le ASL
	.03	Epidemiologia e profilassi malattie infettive e parassitarie	Scheda anamnesi prevaccinale	ILLIMITATO	
	.03	Epidemiologia e profilassi malattie infettive e parassitarie	Consenso informato alla vaccinazione	ILLIMITATO	Circ. Min. Sanità n. 61 del 19/12/1986
	.03	Epidemiologia e profilassi malattie infettive e parassitarie	Registro vaccinazioni	ILLIMITATO	
	.03	Epidemiologia e profilassi malattie infettive e parassitarie	Scheda vaccinale individuale cartacea o informatizzata con i dati vaccinazioni eseguite (data, nome commerciale, lotto, controllo di stato, data di scadenza del prodotto, ecc.)	Collegato all'esistenza in vita del soggetto cui si riferisce la scheda (fino a 5 anni dopo il decesso del vaccinato)	
	.03	Epidemiologia e profilassi malattie infettive e parassitarie	Convocazione vaccinazioni obbligatorie (previste dal Piano aziendale vaccinale)	ILLIMITATO il Registro; 2 anni altra documentazione	
	.03	Epidemiologia e profilassi malattie infettive e parassitarie	Scheda informativa sui danneggiati da vaccinazioni	ILLIMITATO	Circolare del Ministero della Sanità 10 aprile 1992
	.03	Epidemiologia e profilassi malattie infettive e parassitarie	Segnalazione reazioni avverse a vaccini	ILLIMITATO	
	.03	Epidemiologia e profilassi malattie infettive e parassitarie	Richiesta forniture vaccini (ordinativo)	2 anni	Nota RL prot. H1.2001.0033136 del 16.05.2001 Direzione generale degli archivi. Prontuari di scarto per le ASL
	.03	Epidemiologia e profilassi malattie infettive e parassitarie	Registrazione temperature frigoriferi per vaccini	1 anno	Nota RL prot. H1.2001.0033136 del 16.05.2001
	.03	Epidemiologia e profilassi malattie infettive e parassitarie	Registrazione interruzione catena freddo per vaccini	10 anni	
	.03	Epidemiologia e profilassi malattie infettive e parassitarie	Vaccinazione in ambiente protetto (richieste, comunicazioni)	10 anni	
	.03	Epidemiologia e profilassi malattie infettive e parassitarie	Scheda AIDASS di valutazione funzionale globale pazienti AIDS	ILLIMITATO	DGR 7/6471 del 2001
	.03	Epidemiologia e profilassi malattie infettive e parassitarie	Piano di assistenza personalizzato per HIV/AIDS extra-H	5 anni dall'ultima prestazione	
	.03	Epidemiologia e profilassi malattie infettive e parassitarie	Registro Regionale SOFIA (dati scheda extra-H)	ILLIMITATO	DGR 7/6471 del 2001
	.03	Epidemiologia e profilassi malattie infettive e parassitarie	Anamnesi specifica per malattie a trasmissione sessuale	10 anni	Nota RL prot. H1.2001.0033136 del 16.05.2001 Direzione generale degli archivi. Prontuari di scarto per le ASL
	.03	Epidemiologia e profilassi malattie infettive e parassitarie	Fascicolo ambulatoriale per malattie a trasmissione sessuale (MTS / HIV) (Scheda accoglienza / informativa, diario clinico, referti, visite, esami laboratorio e strumentali, consenso informato al trattamento, ecc.)	10 anni dalla chiusura del fascicolo	
	.03	Epidemiologia e profilassi malattie infettive e parassitarie	Scheda sorveglianza infezione da HIV	10 anni da ultima registrazione	
	.03	Epidemiologia e profilassi malattie infettive e parassitarie	Scheda notifica MTS	10 anni	
	.03	Epidemiologia e profilassi malattie infettive e parassitarie	Scheda consulenza linea informativa telefonica MTS / HIV (help line telefonica)	5 anni	
	.03	Epidemiologia e profilassi malattie infettive e parassitarie	Bollettini epidemiologici malattie infettive (report di epidemia)	5 anni dalla cessazione dell'allerta	
	.04	Prevenzione malattie cronico-degenerative	Gestione screening (campagne, esito screening, referti, ecc.)	10 anni	
	.04	Prevenzione malattie cronico-degenerative	Gestione screening (inviti e solleciti)	3 anni	
	.04	Prevenzione malattie cronico-degenerative	Indagine / Inchiesta / Sorveglianza epidemiologica	10 anni dalla chiusura del fascicolo	
	.04	Prevenzione malattie cronico-degenerative	Registri anatomia patologica (copie)	5 anni	
	.04	Prevenzione malattie cronico-degenerative	Registro mortalità e schede morte ISTAT	ILLIMITATO	
	.04	Prevenzione malattie cronico-degenerative	Registro tumori	ILLIMITATO	

copia informatica per consultazione

CLASSE	COD. SOTTO CLASSE	SOTTOCLASSE	TIPO DOCUMENTO	TEMPO CONSERVAZIONE	RIFERIMENTI NORMATIVI / NOTE
3. Prevenzione medico - sanitaria	.05	Igiene urbana, ambientale e sanità pubblica	Documenti relativi a pareri su progetti di edilizia privata e pubblica (compreso rilascio pareri)	10 anni	Procedimento relativo al parere e non alla gestione dell'intera pratica edilizia in capo ad altri enti (comune, provincia, ARPA, ecc.)
	.05	Igiene urbana, ambientale e sanità pubblica	Tombe di privati (richiesta, pareri igienico-sanitari)	10 anni	
	.05	Igiene urbana, ambientale e sanità pubblica	Urbanistica (valutazione igienico sanitaria, richiesta e pareri da enti)	10 anni	
	.05	Igiene urbana, ambientale e sanità pubblica	Pareri, Autorizzazioni e relativi controlli su realizzazione ed esercizio strutture sanitarie, socio-sanitarie pubbliche e private (es. Centri Procreazione Medicalmente Assistita - PMA, Strutture di ricovero e cura, Residenzialità psichiatrica)	ILLIMITATO (fino a cessazione di attività o modifiche di titolarità di esercizio – subingressi)	
	.05	Igiene urbana, ambientale e sanità pubblica	Pareri per esercizio di attività commerciali, artigiane, alberghi e strutture extra alberghiere, sportive (piscine) e ludico-ricreative	ILLIMITATO (fino a cessazione di attività o modifiche di titolarità di esercizio – subingressi)	
	.05	Igiene urbana, ambientale e sanità pubblica	Certificati di idoneità dei carri funebri	10 anni	
	.05	Igiene urbana, ambientale e sanità pubblica	Pareri di insalubrità / inabitabilità edifici ad uso pubblico e/o privato	10 anni se civili abitazioni, ILLIMITATO se insediamenti produttivi	
	.05	Igiene urbana, ambientale e sanità pubblica	Certificati di idoneità igienico-sanitaria di edifici ad uso pubblico e privato	10 anni se civili abitazioni, ILLIMITATO se insediamenti produttivi	
	.05	Igiene urbana, ambientale e sanità pubblica	Accertamento delle condizioni igienico-sanitarie e di sicurezza edifici/strutture ad uso pubblico e privato, comprese le strutture scolastiche e penitenziarie (verbali di ispezione/sopralluogo) ed eventuali prescrizioni	ILLIMITATO	
	.05	Igiene urbana, ambientale e sanità pubblica	Documentazione sulle radiazioni ionizzanti - RI (per usi industriale, di ricerca, sanitario). Comunicazione preventiva ex art. 22 e 24 D.lgs. 230/95, nulla osta di cat. B ex art 29, procedimenti ex art 30, revoca autorizzazione ex art. 146, vigilanza radiazioni ionizzanti, ecc. Compresa la documentazione relativa ai dosimetri personali.	ILLIMITATO se in fascicolo personale / ditta o impresa; altrimenti 30 anni da cessazione attività	
	.05	Igiene urbana, ambientale e sanità pubblica	Documenti in tema ambientale, tossicologia, radioprotezione (denunce, esposti, accertamenti, verbali sopralluogo e sanzionatorio)	ILLIMITATO	
	.05	Igiene urbana, ambientale e sanità pubblica	Documentazione inerente ritrovamento, messa in sicurezza e smaltimento materiale radioattivo	10 anni dalla data di chiusura del procedimento	
	.05	Igiene urbana, ambientale e sanità pubblica	Analisi rischio siti contaminati	ILLIMITATO	
	.05	Igiene urbana, ambientale e sanità pubblica	Valutazione Impatto Ambientale (VIA) e Valutazione Ambientale Strategica (VAS)	ILLIMITATO	
	.05	Igiene urbana, ambientale e sanità pubblica	Parere per interventi di bonifica e ripristino ambientale	10 anni dall'avvenuta bonifica	D.Lgs. 152/2006 e s.m.i
	.05	Igiene urbana, ambientale e sanità pubblica	Documenti sulle radiazioni non ionizzanti (NIR) (elettrosmog). Denunce, esposti, segnalazioni, vigilanza di emissioni elettromagnetiche non ionizzanti (NIR)	ILLIMITATO se in fascicolo personale / ditta o impresa; altrimenti 30 anni da cessazione attività	
	.05	Igiene urbana, ambientale e sanità pubblica	Autorizzazione e installazione Risonanza Magnetiche (RM)	2 anni dalla data di comunicazione cessazione di utilizzo	
	.05	Igiene urbana, ambientale e sanità pubblica	Movimentazione sorgenti radiogene, trasporto e commercio sostanze radioattive	ILLIMITATO se in fascicolo personale / ditta o impresa; altrimenti 30 anni da cessazione attività	
	.05	Igiene urbana, ambientale e sanità pubblica	Registro carico - scarico rifiuti speciali, integrati con i formulari relativi al trasporto dei rifiuti	5 anni dalla data dell'ultima registrazione	D.Lgs. 22/97 art.12 e s.m.i. (art. 190 del D.Lgs 152/2006 come modificato dalla legge 125/2013)
	.05	Igiene urbana, ambientale e sanità pubblica	Ispezioni / controlli acque di balneazione	ILLIMITATO	
	.05	Igiene urbana, ambientale e sanità pubblica	Ispezioni / controlli gas tossici (e relativi pareri)	ILLIMITATO	

copia informatica per consultazione

CLASSE	COD. SOTTO CLASSE	SOTTOCLASSE	TIPO DOCUMENTO	TEMPO CONSERVAZIONE	RIFERIMENTI NORMATIVI / NOTE
3. Prevenzione medico - sanitaria	.05	Igiene urbana, ambientale e sanità pubblica	Ispezioni / controlli fitofarmaci	ILLIMITATO	
	.05	Igiene urbana, ambientale e sanità pubblica	Produzione e/o commercializzazione di prodotti cosmetici (notifica immissione in commercio o importazione, comunicazione cessazione ditte, elenco cosmetici commercializzati e importati)	2 anni dalla data di cessazione di attività o di modifica titolarità di esercizio (subingresso)	
	.05	Igiene urbana, ambientale e sanità pubblica	Ispezioni/controlli su prodotti cosmetici (verbale di controllo, prescrizioni, comunicazione a NAS e Polizia Giudiziaria, ecc.)	ILLIMITATO	
	.05	Igiene urbana, ambientale e sanità pubblica	Valutazioni di effetti sulla salute di esposizione a fattori di rischio ambientale	ILLIMITATO se in fascicolo personale / ditta o impresa; altrimenti 30 anni da cessazione attività	
	.05	Igiene urbana, ambientale e sanità pubblica	Ispezioni/controlli su piscine (parere igienico-sanitario per apertura piscine, verbale sopralluogo, prelevamento campioni, analisi ed eventuali prescrizioni, ecc.)	10 anni	
	.05	Igiene urbana, ambientale e sanità pubblica	Verbale di controllo / sopralluogo per idoneità alloggiativa ed eventuali prescrizioni	ILLIMITATO	
	.05	Igiene urbana, ambientale e sanità pubblica	Segnalazione all'autorità giudiziaria dei rischi connessi per gli impianti termici nei casi di intossicazione da CO	ILLIMITATO	
	.05	Igiene urbana, ambientale e sanità pubblica	Segnalazione intossicazione CO diagnosticati da parte dei Dipartimenti emergenza H	ILLIMITATO	
	.05	Igiene urbana, ambientale e sanità pubblica	Parere igienico-sanitario per rilascio autorizzazioni (istanze, relazioni tecniche, planimetrie, atti istruttori copie atti autorizzativi, ecc.)	30 anni dalla cessazione attività	
	.05	Igiene urbana, ambientale e sanità pubblica	Proposta ordinanza al Sindaco per inconvenienti igienico - sanitari (proposta, ordinanza, verifica ottemperanza, ecc.)	10 anni *dalla conclusione del procedimento*	
	.05	Igiene urbana, ambientale e sanità pubblica	Autorizzazione al seppellimento di feti e parti anatomiche e relativa richiesta	10 anni	
	.05	Igiene urbana, ambientale e sanità pubblica	Registro dei parti e Registro degli aborti	ILLIMITATO	L'adozione di questi due registri risale al R.D. 6 dicembre 1928 n. 3318 (Istituzione del Regolamento per l'esercizio ostetrico delle levatrici). La compilazione dei registri viene confermata dal R.D. 26 maggio 1940 n. 1364 (che abroga il R.D. n.3318/28) e successivamente richiamata dal D.P.R. n. 163 del 7/3/1975 (che abroga il R.D. n. 1364/40). Con la Legge n. 42 del 26/02/1999 viene abrogato il DPR n.163/75 e di conseguenza i due registri. I registri sono a conservazione illimitata e il loro contenuto deve rimanere segreto.
	.05	Igiene urbana, ambientale e sanità pubblica	Copie di Elenchi deceduti (*dai registri degli* enti locali)	*2 anni*	*Elenchi dei defunti per i quali è stato fissato il funerale il giorno dopo*
	.05	Igiene urbana, ambientale e sanità pubblica	Passaporti mortuari da parte di enti locali e relativa richiesta	10 anni	
	.05	Igiene urbana, ambientale e sanità pubblica	Passaporti mortuari rilasciati e relativa richiesta	10 anni	
	.05	Igiene urbana, ambientale e sanità pubblica	Pareri e relativa richiesta per scuole di formazione, strutture turistico ricreative, servizi alla persona	30 anni dalla cessazione attività	
	.05	Igiene urbana, ambientale e sanità pubblica	Ispezioni e controlli su scuole di formazione, strutture turistico ricreative, servizi alla persona (verbale di controllo / sopralluogo ed eventuali prescrizioni, denunce, esposti, ecc.)	ILLIMITATO	
	.05	Igiene urbana, ambientale e sanità pubblica	Verifica periodica condizioni igienico sanitarie casa di reclusione	ILLIMITATO	
	.05	Igiene urbana, ambientale e sanità pubblica	Autorizzazione all'esercizio dell'attività sanitaria (Dichiarazione Inizio Attività (DIA), comunicazione di inizio attività per privati, ecc.)	2 anni dalla data di cessazione di attività o di modifica titolarità di esercizio (subingressi) o modifica locali	
	.05	Igiene urbana, ambientale e sanità pubblica	Edilizia cimiteriale (aree di rispetto cimiteriale, pareri, osservazioni, regolamenti, ecc.)	ILLIMITATO	
	.05	Igiene urbana, ambientale e sanità pubblica	Pareri sanitari rilasciati agli Enti competenti in materia di scarichi, rifiuti, pozzi, ecc.	10 anni	

copia informatica per consultazione

CLASSE	COD. SOTTO CLASSE	SOTTOCLASSE	TIPO DOCUMENTO	TEMPO CONSERVAZIONE	RIFERIMENTI NORMATIVI / NOTE
3. Prevenzione medico - sanitaria	.06	Tutela salute attività sportive	Fascicolo accreditamento Centri Medicina dello Sport (domanda accreditamento, verbale sopralluogo, delibera accreditamento, prescrizioni)	ILLIMITATO	
	.06	Tutela salute attività sportive	Documenti relativi alla verifica attività sportive (verbale di accertamento, prescrizioni, ecc.)	ILLIMITATO	
	.06	Tutela salute attività sportive	Certificato medico di idoneità e inidoneità sportiva agonistica e non	5 anni	D.M. Sanità 18 febbraio 1982 ("Norme per la tutela sanitaria dell'attività sportiva agonistica")
	.06	Tutela salute attività sportive	Documentazione relativa alle pratiche di ricorso alla Commissione Regionale d'Appello contro il giudizio di non idoneità sportiva	ILLIMITATO	
	.07	Igiene degli alimenti	Autorizzazioni di attività di deposito/vendita di prodotti fitosanitari;	5 anni *dalla cessazione attività*	
	.07	Igiene degli alimenti	Controllo e vigilanza sul deposito/vendita ed utilizzo di prodotti fitosanitari	ILLIMITATO	
	.07	Igiene degli alimenti	Autorizzazioni sanitarie per locali e attrezzature per produzione, confezionamento, vendita e somministrazione di alimenti e bevande (es. copia Segnalazione Certificata di Inizio Attività - S.C.I.A. / Dichiarazione di Inizio Attività Produttiva - D.I.A.P.	2 anni dalla data di cessazione di attività o di modifica titolarità di esercizio (subingressi) o modifica locali	
	.07	Igiene degli alimenti	Pareri preventivi e tecnici per la realizzazione, attivazione o modifica di imprese alimentari	30 anni dalla cessazione attività	
	.07	Igiene degli alimenti	Certificazioni sanitarie per commercializzazione, esportazione ed importazione di prodotti alimentari	10 anni	
	.07	Igiene degli alimenti	Consulenza e controllo micologico	5 anni	
	.07	Igiene degli alimenti	Controllo e vigilanza sulla produzione, preparazione, confezionamento, deposito, trasporto, somministrazione e vendita di prodotti alimentari	ILLIMITATO	
	.07	Igiene degli alimenti	Campionatura alimenti e prodotti fitosanitari (verbale prelevamento campioni). Comprese richieste e certificato analisi. Verbali di controllo.	ILLIMITATO i verbali di controllo; 10 anni altra documentazione	
	.07	Igiene degli alimenti	Controllo sulle acque potabili destinate al consumo umano	ILLIMITATO i verbali di controllo; 10 anni altra documentazione (es. esiti)	
	.07	Igiene degli alimenti	Rilascio certificati di idoneità al consumo umano di acqua	5 anni	
	.07	Igiene degli alimenti	Procedimenti di sequestro a seguito di riscontro di non conformità alle normative sugli alimenti, sulla vendita deposito prodotti fitosanitari, sulle acque potabili destinate al consumo umano	ILLIMITATO	
	.07	Igiene degli alimenti	Interventi di polizia amministrativo/giudiziaria (es. vincoli, sequestri) nell'ambito dell'attività di controllo e vigilanza dei prodotti alimentari e prodotti fitosanitari	ILLIMITATO	
	.07	Igiene degli alimenti	Programmi di informazione-formazione abbinata all'igiene degli alimenti	10 anni; ILLIMITATO gli attestati; 1 anno attività informativa (compresi i questionari) con conservazione ILLIMITATA di un esemplare dépliant /manifesto / brochure	Si propone lo scarto di tutta l'attività istruttoria / interlocutoria relativa all'attività di formazione (cfr. I.4.13 conservazione di 5 per formazione personale dipendente e II.5.03 per MMG / PdF 10 anni). L' atto (decreto/determina) per iniziativa di formazione a conservazione ILLIMITATO Vengono conservati illimitatamente gli attestati e la brochure dell'iniziativa.
	.07	Igiene degli alimenti	Registro informativo tossinfezioni e malattie trasmissione alimentare	ILLIMITATO	
	.07	Igiene degli alimenti	Ispezioni e controlli acque minerali e termali	ILLIMITATO	
	.08	Igiene della nutrizione	Rilevamenti dello stato nutrizionale, dei consumi e delle abitudini nutrizionali per gruppi di popolazione (es. Registro sorveglianza nutrizionale scuole)	10 anni	
	.08	Igiene della nutrizione	Predisposizione, verifica e controllo delle tabelle dietetiche della ristorazione collettiva (es. Menù, segnalazione su menù, ecc.)	10 anni	
	.08	Igiene della nutrizione	Interventi di prevenzione nutrizionale per diffusione conoscenze di stili alimentari corretti e protettici	10 anni; 1 anno attività informativa (compresi i questionari) con conservazione ILLIMITATA di un esemplare dépliant / manifesto / brochure	Si tratta di campagne informative. Se le iniziative vengono formalizzate vengono assunti decreti/determine a conservazione illimitata. Viene conservata illimitatamente la brochure dell'iniziativa.
	.08	Igiene della nutrizione	Formazione / motivazione ad un corretto stile alimentare per gruppi di popolazione (counselling nutrizionale)	10 anni	Si tratta di campagne informative. Se le iniziative vengono formalizzate vengono assunti decreti/determine a conservazione illimitata. Viene conservata illimitatamente la brochure dell'iniziativa.
	.08	Igiene della nutrizione	Consulenze per il personale delle ristorazioni in tema nutrizionale	10 anni	
	.09	Laboratorio di prevenzione	Referti analisi campioni ufficiali (Rapporti di prova). Comprese le eventuali registrazioni (verbale prelievo, verbale di analisi, fogli di lavoro, stampate strumenti, risultati controlli di qualità, ecc.)	10 anni	
	.09	Laboratorio di prevenzione	Referti analisi campioni ed esami di laboratorio. Comprese le relative registrazioni (richiesta d'analisi, foglio di lavoro, liste analisi, schede pazienti per le indagini che prevedono risultati dei controlli di qualità, ecc.)	5 anni	nota regione Lombardia H1.2003.0001436

copia informatica per consultazione

CLASSE	COD. SOTTO CLASSE	SOTTOCLASSE	TIPO DOCUMENTO	TEMPO CONSERVAZIONE	RIFERIMENTI NORMATIVI / NOTE
4. Prevenzione veterinaria	.01	Aspetti generali, organizzativi e gestionali	Documenti strategici di programmazione, pianificazione, rendicontazione delle attività (Piani, programmi, calendari, registri, altri documenti strategici e di programmazione)	ILLIMITATO	
	.01	Aspetti generali, organizzativi e gestionali	Documentazione istruttoria e corrispondenza ordinaria/routinaria interna ed esterna attività di prevenzione veterinaria	5 anni	
	.02	Sanità animale	Rilascio pareri, autorizzazioni e nulla osta per attività / strutture oggetto di controllo e vigilanza Pareri per rilascio permessi di costruire insediamenti produttivi	10 anni	
	.02	Sanità animale	Rilascio attestazioni e certificazioni sanitarie previste da normative nazionali o regionali	10 anni	
	.02	Sanità animale	Interventi di profilassi delle malattie infettive degli animali	10 anni	
	.02	Sanità animale	Denunce malattie infettive e diffusive degli animali (zoonosi)	10 anni; ILLIMITATO i registri	
	.02	Sanità animale	Accertamenti diagnostici e campionamenti previsti da Piani Nazionali e/o Regionali su animali	10 anni	
	.02	Sanità animale	Controlli sanitari mirati a verificare l'eventuale presenza delle malattie degli animali (controlli diagnostici e di indagini sierologiche)	10 anni	
	.02	Sanità animale	Valutazione inconvenienti igienici connessi alla presenza di cani, gatti, piccioni, ecc.	10 anni	
	.02	Sanità animale	Ispezioni/controlli allevamenti e animali allevati	ILLIMITATO	
	.02	Sanità animale	Verbali di sopralluogo presso le strutture oggetto di vigilanza	ILLIMITATO	
	.02	Sanità animale	Indagini epidemiologiche a seguito di malattie infettive o casi sospetti	ILLIMITATO 10 anni per pratiche indennizzo	
	.02	Sanità animale	Interventi di polizia amministrativo/giudiziaria (es. vincoli, sequestri, dissequestri, prescrizioni) nell'ambito dell'attività di vigilanza	ILLIMITATO per verbali; 10 anni altra documentazione	
	.03	Anagrafe zootecnica e movimentazione animale	Rilascio certificazioni sanitarie / passaporti per la movimentazione	10 anni	
	.03	Anagrafe zootecnica e movimentazione animale	Dichiarazione di provenienza e destinazione degli animali (mod. IV)	3 anni	Unico riferimento normativo in vigore D.Lgs. 200/2010 relativo ai suini.
	.03	Anagrafe zootecnica e movimentazione animale	Controlli sanitari sugli animali introdotti da paesi comunitari ed extracomunitari	10 anni (salvo verbali di sequestro che ricadono nella voce precedente "Interventi polizia amm. / giudiziaria")	
	.03	Anagrafe zootecnica e movimentazione animale	Segnalazioni da ufficio veterinario adempimenti comunitari arrivi animali vivi e alimenti/mangimi	3 anni	In analogia con il termine del mod. IV
	.03	Anagrafe zootecnica e movimentazione animale	Gestione anagrafe animale (certificazioni, vidimazioni registri, Banca Dati Regionale, ecc.)	20 anni	
	.03	Anagrafe zootecnica e movimentazione animale	Assegnazione codici di stalla / Schede di stalla	2 anni dalla data di cessazione di attività o di modifica titolarità di esercizio (subingressi) o modifica locali	
	.03	Anagrafe zootecnica e movimentazione animale	Consistenza di stalla	10 anni	
	.03	Anagrafe zootecnica e movimentazione animale	Comunicazioni inerenti apiari (registrazione nuovi apiari, comunicazioni per apiari attivi, autorizzazioni per nomadismo…)	10 anni	
	.03	Anagrafe zootecnica e movimentazione animale	Passaporti capi macellati e deceduti in stalla	5 anni	Circolare DG Salute n. 11 del 13.03.2013 (per equini)
	.04	Igiene alimenti di origine animale	Rilascio autorizzazioni alla produzione / vendita di carni e derivati	10 anni *dalla cessazione attività*	
	.04	Igiene alimenti di origine animale	Rilascio pareri igienico-sanitari per l'attività di produzione, vendita e autotrasporto di carni e derivati	10 anni *dalla cessazione attività*	
	.04	Igiene alimenti di origine animale	Ispezioni / vigilanza / sopralluoghi stabilimenti produzione, lavorazione e deposito di carni e derivati	ILLIMITATO	
	.04	Igiene alimenti di origine animale	Certificazioni sanitarie spedizioni di carni e derivati (importazione / esportazione)	10 anni	
	.04	Igiene alimenti di origine animale	Rilascio pareri igienico-sanitari / idoneità / nulla osta per attività di macellazione animali negli stabilimenti e a domicilio	10 anni	
	.04	Igiene alimenti di origine animale	Documentazione relativa alle D.I.A. (Dichiarazioni Inizio Attività) / SCIA	2 anni dalla data di cessazione di attività o di modifica titolarità di esercizio (subingressi) o modifica locali	
	.04	Igiene alimenti di origine animale	Atti relativi e/o conseguenti agli interventi di polizia amministrativa/giudiziaria (es. vincoli, sequestri, ecc.)	ILLIMITATO	
	.04	Igiene alimenti di origine animale	Documentazione inerente la gestione degli stati di allerta - Relazione finale	ILLIMITATO	
	.04	Igiene alimenti di origine animale	Segnalazioni stati di allerta e conseguenti controlli per il ritiro dei prodotti	10 anni	
	.04	Igiene alimenti di origine animale	Campionamento per indagini microbiologiche e chimiche per la ricerca di residui pericolosi (ormoni, farmaci)	10 anni	
	.04	Igiene alimenti di origine animale	Rilascio autorizzazioni alla produzione/vendita dei prodotti della pesca, latte, uova, miele e loro derivati	10 anni *dalla cessazione attività*	
	.04	Igiene alimenti di origine animale	Rilascio pareri igienico-sanitari per l'attività di produzione/vendita/autotrasporto di prodotti della pesca, latte, uova, miele e loro derivati	10 anni *dalla cessazione attività*	
	.04	Igiene alimenti di origine animale	Vigilanza, tramite ispezioni e sopralluoghi, sui stabilimenti produzione, lavorazione e deposito alimenti di origine animale (prodotti della pesca, latte, uova, miele e loro derivati)	ILLIMITATO	
	.04	Igiene alimenti di origine animale	Rilascio certificazioni sanitarie per le spedizioni dei prodotti della pesca, latte, uova, miele e loro derivati	10 anni	
	.04	Igiene alimenti di origine animale	Campionamenti per indagini microbiologiche e chimiche per la ricerca di residui pericolosi (ormoni, farmaci) sui prodotti della pesca, latte, uova, miele e loro derivati	10 anni	
	.04	Igiene alimenti di origine animale	Indagine per sospetta tossi infezione alimentare a seguito di consumo di alimenti di origine animale	10 anni da ultima registrazione	
	.04	Igiene alimenti di origine animale	Analisi trichinella e altre analisi su capi macellati (esiti negativi)	1 anno	

copia informatica per consultazione

CLASSE	COD. SOTTO CLASSE	SOTTOCLASSE	TIPO DOCUMENTO	TEMPO CONSERVAZIONE	RIFERIMENTI NORMATIVI / NOTE
4. Prevenzione veterinaria	.05	Igiene allevamenti e produzioni zootecniche	Autorizzazioni e pareri igienico sanitari, nulla osta su allevamenti e le strutture zootecniche, automezzi e stabilimenti (es. mangimifici, produzione latte, acquicoltura, ambulatori, grossisti medicinali, farmacie)	2 anni dalla data di cessazione di attività o di modifica titolarità di esercizio (subingressi) o modifica locali	
	.05	Igiene allevamenti e produzioni zootecniche	Vigilanza e ai conseguenti provvedimenti su allevamenti e le strutture zootecniche, sugli automezzi e sugli stabilimenti oggetto di controllo (es. mangimifici, produzione latte, acquicoltura, ambulatori, grossisti medicinali, farmacie)	ILLIMITATO	
	.05	Igiene allevamenti e produzioni zootecniche	Gestione rapporti e rendicontazione con Agenzia per le Erogazioni in Agricoltura - AGEA	ILLIMITATO	
	.05	Igiene allevamenti e produzioni zootecniche	Autorizzazioni al trasporto degli animali	5 anni (se dati inseriti nella banca dati regionale delle anagrafi zootecniche)	
	.05	Igiene allevamenti e produzioni zootecniche	Attività di farmaco-vigilanza veterinaria (autorizzazioni, ispezioni)	ILLIMITATO	
	.05	Igiene allevamenti e produzioni zootecniche	Autorizzazioni alla scorta farmaci veterinari	2 anni dalla data di cessazione di attività o di modifica titolarità di esercizio (subingressi) o modifica locali o 2 anni dalla rinuncia all'autorizzazione	
	.05	Igiene allevamenti e produzioni zootecniche	Rilascio autorizzazioni alla riproduzione e fecondazione animale	10 anni	
	.05	Igiene allevamenti e produzioni zootecniche	Ispezioni e controlli sullo smaltimento dei rifiuti di origine animale	ILLIMITATO	
	.05	Igiene allevamenti e produzioni zootecniche	Attuazione dei piani nazionali e regionali di campionamento (PNR e PNAA)	ILLIMITATO in caso di non conformità campionamenti / rapporti di prova; 10 anni nei casi di conformità	
	.05	Igiene allevamenti e produzioni zootecniche	Campionamenti	10 anni	
	.05	Igiene allevamenti e produzioni zootecniche	Gestione degli stati di allerta nel settore della produzione zootecnica - Relazione finale	ILLIMITATO	
	.05	Igiene allevamenti e produzioni zootecniche	Segnalazioni stati di allerta e conseguenti controlli per il ritiro dei prodotti	10 anni	
	.05	Igiene allevamenti e produzioni zootecniche	Documenti relativi a interventi di formazione degli addetti in tema di benessere animale (allevamenti e trasporti)	10 anni	
	.05	Igiene allevamenti e produzioni zootecniche	Gestione farmaci veterinari (ricette)	5 anni	
	.05	Igiene allevamenti e produzioni zootecniche	Ispezioni / controlli sull'igiene delle produzioni animali da allevamento	ILLIMITATO	
	.06	Randagismo e tutela animali da affezione	Ispezioni e controlli sul benessere animale (visite ed esami)	ILLIMITATO	
	.06	Randagismo e tutela animali da affezione	Pratiche morsicature	10 anni	
	.06	Randagismo e tutela animali da affezione	Notifica vaccinazione antirabbica	10 anni; Registro ILLIMITATO	
	.06	Randagismo e tutela animali da affezione	Ispezioni/controlli sull'igiene delle produzioni animali da affezioni	ILLIMITATO	
	.06	Randagismo e tutela animali da affezione	Gestione del canile sanitario (registro carico-scarico, atti di cessione, ecc.)	10 anni	
	.06	Randagismo e tutela animali da affezione	Interventi sul territorio (richieste, programmazione, registrazione) / colonie feline	10 anni	
	.06	Randagismo e tutela animali da affezione	Rilascio certificazioni sanitarie	10 anni	
	.06	Randagismo e tutela animali da affezione	Ispezioni e sopralluoghi	ILLIMITATO	
	.06	Randagismo e tutela animali da affezione	Sterilizzazioni cani randagi e gatti appartenenti a colonie riconosciute	20 anni	Il termine di 20 anni è legato alla vita massima di un cane/gatto.
	.06	Randagismo e tutela animali da affezione	Gestione dell'anagrafe canina - Registro	ILLIMITATO	
	.06	Randagismo e tutela animali da affezione	Atti di trasferimento cani e documentazione correlata (compresi tatuaggi)	15 anni	
	.06	Randagismo e tutela animali da affezione	Schede / cartellini accalappiamento cani	15 anni	
	.06	Randagismo e tutela animali da affezione	Interventi contro il maltrattamento degli animali. Comprese segnalazioni e conseguenti provvedimenti	10 anni	

copia informatica per consultazione

CLASSE	COD. SOTTO CLASSE	SOTTOCLASSE	TIPO DOCUMENTO	TEMPO CONSERVAZIONE	RIFERIMENTI NORMATIVI / NOTE
5. Assistenza sanitaria	.01	Aspetti generali, organizzativi e gestionali	Documenti strategici di programmazione, pianificazione, rendicontazione delle attività (Piani, programmi, calendari, registri, altri documenti strategici e di programmazione)	ILLIMITATO	
	.01	Aspetti generali, organizzativi e gestionali	Documentazione istruttoria e corrispondenza ordinaria/routinaria interna ed esterna attività di assistenza sanitaria	5 anni	
	.01	Aspetti generali, organizzativi e gestionali	Documentazione istruttoria e corrispondenza ordinaria / routinaria interna ed esterna attività di assistenza sanitaria: appuntamenti per accertamento di idoneità e altri tipi di documentazione del genere	1 anno	
	.02	Emergenza sanitaria territoriale	Documentazione 118 compilata dalle équipe di soccorso dei MSB (Mezzi di Soccorso di Base, con soccorritori a bordo), dei MSI (Mezzi di Soccorso Intermedio, con infermiere a bordo) e dei MSA (Mezzi di Soccorso Avanzato, con medico e infermiere a bordo).	ILLIMITATO Conservazione da parte della Struttura ospedaliera di destinazione del paziente (in cartella clinica o quale parte integrante della documentazione di Pronto Soccorso)	
	.02	Emergenza sanitaria territoriale	Documentazione generata dall'applicativo gestionale di COEU (Centrale Operativa Emergenza Urgenza)/SOREU (Sala Operativa Regionale Emergenza Urgenza) e relativi allegati; registrazioni telefoniche intercorse tra la COEU (Centrale Operativa Emergenza Urgenza)/SOREU (Sala Operativa Regionale Emergenza Urgenza) e altri soggetti (utenti, équipe dei mezzi di soccorso, Forze di Polizia, ospedali, ecc.).	ILLIMITATO	
	.02	Emergenza sanitaria territoriale	Documentazione sanitaria utilizzata in occasione di maxi emergenze e di grandi eventi	30 anni	
	.02	Emergenza sanitaria territoriale	Trasferimento dei pazienti a bordo di mezzi di soccorso attrezzati	ILLIMITATO Conservazione da parte della Struttura ospedaliera di destinazione del paziente (in cartella clinica o quale parte integrante della documentazione di Pronto Soccorso)	
	.03	Assistenza sanitaria di base	Documentazione relativa alla gestione dei Medici di Medicina Generale - MMG e dei Pediatri di Famiglia - PdF (associazionismo medico, orari apertura, ecc.)	5 anni	
	.03	Assistenza sanitaria di base	Ricevute consegna ricettari	5 anni	Nota Regione Lombardia H1.2001.0033136 del 16/05//2001 Nota Regione Lombardia H1. 2005.0032866 del 05/07/2005 DM 17.03.2008 Le Matrici ricette compilate sono conservate a cura dei medici prescrittori per 5 anni
	.03	Assistenza sanitaria di base	Rendicontazione accessi Assistenza Domiciliare Integrata - ADI, Assistenza Domiciliare Programmata - ADP, Prestazioni di particolare Impegno Professionale - PIP, prestazioni erogate per adesione a progetti / iniziative e documentazione su competenze economiche dei Medici di medicina generale - MMG e Pediatri di Famiglia - PdF	5 anni	
	.03	*Assistenza sanitaria di base*	*Cartelle e fascicoli relativi all'assistenza domiciliare*	*5 anni dal termine dell'assistenza*	
	.03	Assistenza sanitaria di base	Controllo / sopralluogo studi Medici di Medicina Generale - MMG e Pediatri di Famiglia - PdF ed eventuali prescrizioni	ILLIMITATO	
	.03	Assistenza sanitaria di base	Controllo e valutazione assistenza erogata dai Medici di Medicina Generale - MMG e dai Pediatri di Famiglia - PdF (es. vaccinazioni, ADI, ADP, screening, assistenza farmaceutica)	10 anni	
	.03	Assistenza sanitaria di base	Formazione dei Medici di Medicina Generale - MMG e dei Pediatri di Famiglia - PdF	10 anni	
	.03	Assistenza sanitaria di base	Documentazione su scelta / revoca dei Medici di Medicina Generale - MMG e dei Pediatri di Famiglia - PdF (Iscrizione al SSR, domande autorizzazione, cambio, variazioni anagrafiche, ecc.)	5 anni. 1 anno se esiste l'anagrafe informatizzata degli assistiti 5 anni comunque per stranieri	

copia informatica per consultazione

CLASSE	COD. SOTTO CLASSE	SOTTOCLASSE	TIPO DOCUMENTO	TEMPO CONSERVAZIONE	RIFERIMENTI NORMATIVI / NOTE
5. Assistenza sanitaria	.03	Assistenza sanitaria di base	Ambiti carenti per la Medicina Generale, la Pediatria di Famiglia *e di Continuità Assistenziale* e relative coperture (*richieste conferimento*, assegnazione e accettazioni dei medici, ecc.)	10 anni	
	.03	Assistenza sanitaria di base	Documentazione per riconoscimento diritto all'esenzione (copia cartella clinica, verbale invalidità, certificati medici, archivio esenti, ecc.)	5 anni	
	.03	Assistenza sanitaria di base	*Autocertificazioni per esenzioni da ticket sanitario*	*10 anni*	*In ragione della prescrizione decennale del diritto di credito al recupero ticket (art. 2946 c.c.)*
	.03	Assistenza sanitaria di base	Documentazione relativa alla gestione dei medici di Continuità Assistenziale (avvisi, graduatorie, incarichi, ecc.)	ILLIMITATO	
	.03	Assistenza sanitaria di base	Documentazione relativa alla attività di Continuità Assistenziale (registro interventi, referti delle visite ecc.)	ILLIMITATO i Registri, 10 anni altra documentazione	
	.03	Assistenza sanitaria di base	Controllo e valutazione assistenza erogata dai medici di Continuità Assistenziale	10 anni	
	.03	Assistenza sanitaria di base	Documentazione relativa a Strutture per cure sub acute (consenso al trasferimento paziente, scheda sanitaria pazienti, documentazione trasferimento, ecc.)	10 anni	
	.03	Assistenza sanitaria di base	*Documentazione relativa alla presa in carico del paziente cronico e/o fragile (Piano di Assistenza Individuale - PAI, patto di cura, ecc.).* Documentazione relativa al Cronic Related Group - CReG.	10 anni dall'ultima registrazione	
	.03	Assistenza sanitaria di base	Documentazione prodotta per rimborsi assistenza indiretta in Italia (documentazione di spesa originale e quietanzata, copia cartelle cliniche, dichiarazione non convenzione con il SSN, ecc.)	10 anni	
	.03	Assistenza sanitaria di base	Documentazione prodotta per rimborsi cure all'estero (valutazione centri regionali di riferimento, fatture, copia cartelle cliniche, liquidazione, ecc.)	10 anni	
	.03	Assistenza sanitaria di base	Documentazione relativa a stranieri (Dichiarazione indigenza, tessera sanitaria STP e registro codici STP, richiesta rimborso ricovero alla Prefettura, iscrizione volontaria SSR, ecc.)	10 anni	
	.03	Assistenza sanitaria di base	Modelli esteri comunitari	10 anni	
	.03	Assistenza sanitaria di base	Assistenza all'estero (modelli esteri Paesi in convenzione bilaterale, AIRE, documentazione ex DPR 618/1980, ecc.)	10 anni	
	.03	Assistenza sanitaria di base	Rimborsi dializzati	10 anni	
	.03	Assistenza sanitaria di base	Gestione funzionalità tessera sanitaria (richieste duplicati, richiesta PIN / GASS, ecc.)	1 anno	
	.03	Assistenza sanitaria di base	Concessione forniture extra prontuario	5 anni dal decesso o dalla cessazione per fascicolo assistito 5 anni per verbali commissione ILLIMITATO per atto di concessione	
	.04	Assistenza protesica e integrativa	Documentazione relativa all'erogazione dei dispositivi medici, di protesi, ortesi, presidi, ausili e prodotti dietetici, presidi per diabetici (domanda, certificato attestante la patologia, prescrizione specialistica, Progetto riabilitativo individuale e/o piano terapeutico, copia verbale invalidità, ricevuta consegna, ecc.) e relativa autorizzazione.	1 anno dalla data del decesso o dal termine dell'erogazione	
	.04	Assistenza protesica e integrativa	Documentazione attestante la fornitura dei dispositivi medici, dei presidi e dei prodotti dietetici	5 anni	
	.04	Assistenza protesica e integrativa	Rendiconto periodico da parte delle farmacie per forniture indirette prodotti dietetici	5 anni	
	.04	Assistenza protesica e integrativa	Autorizzazione / Fornitura per pazienti ipossiemici	1 anno dalla data del decesso o dal termine dell'erogazione	
	.04	Assistenza protesica e integrativa	Documentazione inerente la valutazione e il controllo dell'assistenza integrativa erogata	10 anni	
	.04	Assistenza protesica e integrativa	Report dati relativo agli utenti e ai prescrittori per la fornitura protesi, ortesi ed ausili, dispositivi medici, presidi e prodotti dietetici, presidi per diabetici	5 anni	
	.04	Assistenza protesica e integrativa	Documentazione relativa a gestione magazzino protesi, ortesi ed ausili (atti preparatori alla gara d'appalto, ordini dei dispositivi di gara, bolle di consegna / ritiro ausili al domicilio dell'assistito)	5 anni	
	.05	Assistenza psichiatrica e neuropsichiatrica infantile	Cartella clinica di struttura semiresidenziale, Centro Diurno e Residenzialità Leggera. Documentazione relativa alla neuropsichiatria dell'infanzia e dell'adolescenza.	10 anni	
	.05	Assistenza psichiatrica e neuropsichiatrica infantile	Cartella clinica di struttura residenziale (diario clinico, visite psichiatriche, attività riabilitative, colloqui psicoterapeutici, ecc.). Documentazione relativa alla neuropsichiatria dell'infanzia e dell'adolescenza	ILLIMITATO	
	.05	Assistenza psichiatrica e neuropsichiatrica infantile	Documentazione del sistema informatizzato regionale PSICHE	Secondo tipologia di regime di erogazione della prestazione (residenziale / semiresidenziale)	

copia informatica per consultazione

CLASSE	COD. SOTTO CLASSE	SOTTOCLASSE	TIPO DOCUMENTO	TEMPO CONSERVAZIONE	RIFERIMENTI NORMATIVI / NOTE
6. Assistenza socio - sanitaria integrata	.01	Aspetti generali, organizzativi e gestionali	Documenti strategici di programmazione e pianificazione delle unità di offerta sociosanitarie (Piani, programmi, calendari, registri, altri documenti strategici e di programmazione)	ILLIMITATO	
	.01	Aspetti generali, organizzativi e gestionali	Documentazione istruttoria e corrispondenza ordinaria/routinaria interna ed esterna attività di assistenza socio sanitaria integrata	5 anni	
	.01	Aspetti generali, organizzativi e gestionali	Progetti sociosanitari (atti di approvazione)	ILLIMITATO	
	.01	Aspetti generali, organizzativi e gestionali	Documentazione istruttoria relativa a progetti.	10 anni	
	.02	Dipendenze	Accertamento dipendenza su richiesta di aziende (elenco soggetti sottoposti ad accertamento, esito accertamenti, referti esami di laboratorio, documentazione varia, ecc.)	ILLIMITATO in cartella sanitaria. 1 anno altri esemplari	D.P.C.M. 10.2.84; DPR 14 gennaio 1997
	.02	Dipendenze	Cartella sanitaria SERT (Cartella SESIT con percorso di cura, dati clinici, esami laboratorio, visite, consensi, piani terapeutici, ecc.)	ILLIMITATO	
	.02	Dipendenze	Adempimenti connessi agli inserimenti in comunità terapeutiche di alcolisti e tossicodipendenti (certificati tossicodipendenza, ecc.)	10 anni	
	.02	Dipendenze	Richieste di certificazione dello stato di tossicodipendenza	ILLIMITATO	
	.02	Dipendenze	Flussi informativi del SERT (Flussi regionali, Report di attività e per la remunerazione, ecc.)	10 anni. ILLIMITATO se allegate a delibere o a documenti di programmazione	Decr. Leg. 29/98 e successive modifiche ed integrazioni
	.02	Dipendenze	Comunicazione tra strutture per trasferimento di tossicodipendenti (pazienti "appoggiati")	10 anni	
	.02	Dipendenze	Procedimenti per utenti segnalati dagli uffici territoriali del governo (richieste di intervento / valutazione, convocazione, foglio firma presenze, relazioni, comunicazioni, decreti, ecc.)	ILLIMITATO	
	.02	Dipendenze	Segnalazioni dagli uffici territoriali del governo e altri enti/istituzioni senza seguito	10 anni	
	.02	Dipendenze	Adempimenti inerenti alle misure alternative alla detenzione	ILLIMITATO	
	.02	Dipendenze	Richieste di consulenza su dipendenza da parte dei reparti ospedalieri, MMG, familiari, ecc.	10 anni	
	.02	Dipendenze	Progetti su dipendenze (*compresi gli* atti di approvazione)	ILLIMITATO	
	.02	Dipendenze	Attività formativa su dipendenze	10 anni	
	.02	Dipendenze	Attività informativa (compresi i questionari)	1 anno con conservazione ILLIMITATA per un esemplare dell'iniziativa/manifesto/brochure	Si tratta di campagne informative. Se le iniziative vengono formalizzate vengono assunti decreti/determine a conservazione illimitata. Viene conservata illimitatamente la brochure dell'iniziativa.
	.02	Dipendenze	Documentazione istruttoria e corrispondenza relativa ad interventi di prevenzione su dipendenze	10 anni	
	.02	Dipendenze	Cartella sanitaria Alcologia - NOA (Documentazione sanitaria, consulti psicologici, valutazioni sociali, comprendenti anche documentazione con dati riguardanti i familiari, consensi informati, informazioni inerenti i ricoveri, dati clinici, esami laboratorio, visite, ecc.)	ILLIMITATO	
	.03	Famiglia, infanzia ed età evolutiva	Fascicolo socio-sanitario utente del Consultorio Famigliare (Documentazione sanitaria, consulti psicologici, valutazioni sociali, comprendenti anche documentazione con dati riguardanti i familiari, consensi informati, informazioni inerenti i ricoveri, referti, valutazioni cliniche e psicologiche, schede, questionari, documenti contenenti dati sanitari, copia certificazione per IVG, ecc.)	20 anni	
	.03	Famiglia, infanzia ed età evolutiva	Documentazione relativa a minori sottoposti all'autorità giudiziaria (Adozioni, affidi, abbandoni, maltrattamenti, abusi, interventi di sostegno, vicende giudiziarie, ecc.)	ILLIMITATO	
	.03	Famiglia, infanzia ed età evolutiva	Segnalazione donne vittima di violenza	20 anni	
	.03	Famiglia, infanzia ed età evolutiva	Documentazione relativa a minori non riconosciuti	ILLIMITATO	
	.03	Famiglia, infanzia ed età evolutiva	Richieste dell'autorità giudiziaria assistenza psicologica per audizioni protette minori	5 anni	
	.03	Famiglia, infanzia ed età evolutiva	Segnalazione da ospedale per dimissioni protette post partum	1 anno	
	.03	Famiglia, infanzia ed età evolutiva	Documentazione relativa a gruppi consultoriali (allattamento, pre parto, contraccezione, menopausa, ecc.): scheda iscrizione, consenso al trattamento dati, foglio presenza, ecc.	1 anno	

copia informatica per consultazione

CLASSE	COD. SOTTO CLASSE	SOTTOCLASSE	TIPO DOCUMENTO	TEMPO CONSERVAZIONE	RIFERIMENTI NORMATIVI / NOTE
6. Assistenza socio - sanitaria integrata	.04	Assistenza domiciliare	Documentazione relativa all'erogazione di contributi economici a favore delle famiglie che assistono in casa persone non autosufficienti	10 anni	
	.04	Assistenza domiciliare	Documentazione inerente l' erogazione di assistenza domiciliare (Assegnazione del credit o voucher socio-sanitario, autorizzazione, Piani individuali di assistenza, attivazione, cartella socio-sanitaria utenti , verbali di equipe valutazione multidimensionale, ecc.)	5 anni *dal termine dell'assistenza*	
	.04	Assistenza domiciliare	Controllo e valutazione assistenza domiciliare erogata (verbali di controllo ed eventuali prescrizioni, report dei controlli)	ILLIMITATO	
	.04	Assistenza domiciliare	Autorizzazione erogazione ADI per utenti extra regione	5 anni	
	.04	Assistenza domiciliare	Segnalazioni per ingresso cure palliative (hospice)	1 anno	
	.04	Assistenza domiciliare	Segnalazioni di valutazione multidimensionale non attivate	1 anno	
	.05	Disabilità	Documenti prodotti nell'ambito di programmi e progetti anche di vita indipendente del disabile	10 anni	
	.05	Disabilità	Interventi personalizzati di valutazione delle capacità, analisi delle mansioni, orientamento e successivo inserimento in contesto lavorativo (compresi i certificati di svantaggio)	10 anni dall'ultima registrazione	
	.05	Disabilità	Procedimento relativo all'inserimento di alunni disabili nel contesto scolastico (istanze, convocazioni accertamento collegiale, documentazione sanitaria, verbale di accertamento, certificazioni , ecc.)	10 anni dall'ultima registrazione	
	.05	Disabilità	Concessione di contributi economici alle famiglie	10 anni	
	.05	Disabilità	Richiesta contributi per le spese ai sensi dell'art. 27 della legge 104 (richieste, valutazione, autorizzazione, documentazione sanitaria allegata)	10 anni	
	.06	Fragilità	Documentazione in strutture residenziali o semiresidenziali sociosanitarie (Domande inserimento, autorizzazioni, schede ingresso e dimissioni, valutazione socio-sanitaria, piano di assistenza personalizzato, copie di documentazione sanitaria, ecc.)	10 anni	
	.06	Fragilità	Documentazione monitoraggio delle strutture residenziali e semiresidenziali	10 anni	
	.06	Fragilità	Flussi informativi (Scheda di Osservazione Intermedia Assistenza - SOSIA, Scheda Individuale Disabile - SIDi, Scheda Riabilitazione - RIA, ecc.	10 anni. ILLIMITATO se allegate a delibere o a documenti di programmazione	
	.06	Fragilità	Verbali di equipe per valutazione multidimensionale	5 anni dall'ultima registrazione	
	.06	Fragilità	Fascicolo Socio Assistenziale e Sanitario (FaSaS) (cartella utente)	10 anni dall'ultima registrazione	
	.06	Fragilità	Documentazione relativa all'amministrazione di sostegno, tutele e curatele	ILLIMITATO	

copia informatica per consultazione

CLASSE	COD. SOTTO CLASSE	SOTTOCLASSE	TIPO DOCUMENTO	TEMPO CONSERVAZIONE	RIFERIMENTI NORMATIVI / NOTE
7. Governo sanitario e sociosanitario	.01	Aspetti generali, organizzativi e gestionali	Documenti strategici di programmazione e pianificazione delle attività (Piani, programmi, calendari, registri, altri documenti strategici e di programmazione)	ILLIMITATO	
	.01	Aspetti generali, organizzativi e gestionali	Documentazione istruttoria e corrispondenza ordinaria/routinaria interna ed esterna attività di governo sanitario e sociosanitario	5 anni	
	.02	Osservatorio epidemiologico	Indagini e statistiche demografiche ed epidemiologiche	10 anni ILLIMITATO se allegate a delibere o a documenti di programmazione	
	.03	Flussi informativi sanitari e sociosanitari	Flussi informativi Ministeriali, Regionali, altri enti	10 anni. ILLIMITATO se allegate a delibere o a documenti di programmazione	Decr. Leg. 29/98 e successive modifiche ed integrazioni
	.04	Accreditamento e controllo strutture sanitarie	Documentazione relative a istanze di accreditamento / autorizzazioni / ampliamento (requisiti, planimetrie, procedure dell'ente, delibere di accreditamento, dichiarazioni di conformità, elenchi personale, ecc.)	ILLIMITATO	
	.04	Accreditamento e controllo strutture sanitarie	Documentazione relative a vigilanza / controllo accreditamento (segnalazioni, autocertificazioni, verbale di controllo e sanzionatorio, provvedimenti di sospensione / revoca, perizie asseverate, ecc.)	ILLIMITATO	
	.04	Accreditamento e controllo strutture sanitarie	Autocertificazioni periodiche sulla dotazione organica	5 anni	
	.05	Autorizzazione e controllo strutture sociosanitarie	Documentazione relative a istanze di accreditamento / autorizzazioni / ampliamento (requisiti, planimetrie, procedure dell'ente, delibere di accreditamento, dichiarazioni di conformità, elenchi personale, ecc.).	ILLIMITATO	
	.05	Autorizzazione e controllo strutture sociosanitarie	Documentazione relative a vigilanza / controllo accreditamento (segnalazioni, autocertificazioni, verbale di controllo, provvedimenti di sospensione / revoca, perizie asseverate, ecc.)	ILLIMITATO	
	.06	Acquisto e controllo prestazioni sanitarie	Documentazione relativa alle attività dei controlli sulle prestazioni (moduli di registrazione, campionamento e programmazione, copie cartelle e documentazione sanitaria, comunicazioni, ecc.)	10 anni	
	.06	Acquisto e controllo prestazioni sanitarie	Documentazione relativa agli esiti dei controlli sui ricoveri (Verbale di controllo e sanzionatorio, controdeduzioni, denunce / esposti / segnalazioni)	ILLIMITATO	
	.06	Acquisto e controllo prestazioni sanitarie	Documentazione relativa agli esiti dei controlli sulle prestazioni ambulatoriali (Verbale di controllo e sanzionatorio, controdeduzioni, denunce / esposti / segnalazioni)	ILLIMITATO	
	.06	Acquisto e controllo prestazioni sanitarie	Attività di autorizzazione, inserimento, proroga, trasferimento di pazienti psichiatrici in strutture residenziali e semiresidenziali (richieste, autorizzazioni, documentazione allegata)	10 anni	
	.06	Acquisto e controllo prestazioni sanitarie	Verbali di sopralluogo presso le strutture residenziali e semiresidenziali in ambito salute mentale	ILLIMITATO	
	.06	Acquisto e controllo prestazioni sanitarie	Contratti con strutture sanitarie	ILLIMITATO	
	.06	Acquisto e controllo prestazioni sanitarie	Documentazione relativa alle rendicontazione delle attività delle strutture sanitarie	10 anni	
	.07	Acquisto e controllo prestazioni sociosanitarie	Documentazione relativa alle attività dei controlli sulle prestazioni (moduli di registrazione, campionamento e programmazione, copie cartelle e documentazione sanitaria, comunicazioni, ecc.)	10 anni	
	.07	Acquisto e controllo prestazioni sociosanitarie	Documentazione relativa agli esiti dei controlli sui ricoveri (Verbale di controllo e sanzionatorio, controdeduzioni, denunce / esposti / segnalazioni)	ILLIMITATO	
	.07	Acquisto e controllo prestazioni sociosanitarie	Documentazione relativa agli esiti dei controlli sulle prestazioni (Verbale di controllo e sanzionatorio, controdeduzioni, denunce / esposti / segnalazioni)	ILLIMITATO	
	.07	Acquisto e controllo prestazioni sociosanitarie	Contratti con strutture ed enti gestori socio-sanitari	ILLIMITATO	
	.07	Acquisto e controllo prestazioni sociosanitarie	Documentazione relativa alle rendicontazione delle attività delle unità d'offerta sociosanitarie (RSA, RSD, Cure Domiciliari, ecc.)	10 anni	

copia informatica per consultazione

CLASSE	COD. SOTTO CLASSE	SOTTOCLASSE	TIPO DOCUMENTO	TEMPO CONSERVAZIONE	RIFERIMENTI NORMATIVI / NOTE
8. Medicina legale	.01	Aspetti generali, organizzativi e gestionali	Documenti strategici di programmazione, pianificazione, rendicontazione delle attività (Piani, programmi, calendari, registri, altri documenti strategici e di programmazione)	ILLIMITATO	
	.01	Aspetti generali, organizzativi e gestionali	Documentazione istruttoria e corrispondenza ordinaria/routinaria interna ed esterna attività di medicina legale	5 anni	
	.02	Attività medico-legale e necroscopica	Soggiorni climatici ex ONIG / invalidi di guerra e di servizio (richiesta autorizzazione, documentazione sanitaria, autorizzazione, richiesta rimborso e conseguente liquidazione)	10 anni dall'ultima autorizzazione	
	.02	Attività medico-legale e necroscopica	Accertamenti sanitari su lavoratori visite fiscali (richieste e referti)	5 anni se non in fascicolo personale	
	.02	Attività medico-legale e necroscopica	Documenti riguardanti visite collegiali di idoneità / inidoneità alla mansione lavorativa compresi atti (certificato medico, documentazione sanitaria, ecc.)	20 anni	
	.02	*Attività medico-legale e necroscopica*	*Accertamento medico e domanda in merito all'interdizione dal lavoro delle lavoratrici in stato di gravidanza*	*5 anni*	*Decreto Legislativo 26 marzo 2001, n.151.*
	.02	Attività medico-legale e necroscopica	Consulenza medico legale in tema di riconoscimento della dipendenza da causa di servizio	20 anni	
	.02	Attività medico-legale e necroscopica	Documentazione per accertamenti decessi (certificati necroscopici)	ILLIMITATO	
	.02	Attività medico-legale e necroscopica	Documentazione per rilascio / rinnovo delle patenti di guida in *caso di malattie o minorazioni anatomiche o funzionali* rilasciate dalla Commissione Medica Locale (*certificazione sanitaria* , dichiarazione precedenti morbosi, certificato anamnestico, ecc.)	*10 anni dalla visita*	*Armonizzazione con i tempi di conservazione di altri enti sanitari*
	.02	Attività medico-legale e necroscopica	Contabilità (atti di liquidazione componenti commissione medica e documentazione corredata)	10 anni	
	.02	Attività medico-legale e necroscopica	*Giudizio* di idoneità patente di guida e nautica, pratiche per il rilascio e rinnovo (compreso originale ricevuta versamento diritti e certificato anamnestico)	*1 anno*	*Decreto Ministero delle Infrastrutture e dei Trasporti n. 182 del 2 agosto 2016 (Note all'art. 3 di cui all'art. 36 c.3 del decreto ministeriale 29 luglio 2008, n. 146)*
	.02	Attività medico-legale e necroscopica	Documentazione per rilascio / rinnovo del porto d'armi, compresa la documentazione sanitaria acquisita dal paziente	5 anni	
	.02	Attività medico-legale e necroscopica	Atti contenuti nel fascicolo relativo all'accertamento medico legale, compresa la documentazione inerente i rapporti e i flussi informativi con enti esterni	ILLIMITATO	
	.02	Attività medico-legale e necroscopica	Richieste e referti di visita medico-legale	20 anni	
	.03	Invalidità civile, sordomutismo e menomazioni visive	Documentazione per riconoscimento o aggravamento stati invalidità civile, cecità e sordità, handicap e diritto al lavoro disabili (istanze di riconoscimento, certificato medico attestante la patologia invalidante, documentazione sanitaria, verbale di accertamento, verbale INPS, verbale handicap, ecc.).	ILLIMITATO	
	.03	Invalidità civile, sordomutismo e menomazioni visive	Documentazione per rilascio / rinnovo del contrassegno invalidi, compresa la documentazione acquisita dal paziente	5 anni	
	.04	Istanze di indennizzo	Documentazione relativa ai danneggiati da vaccinazioni obbligatorie: pratiche di indennizzo (copie conformi di: certificato vaccinale, cartella clinica, documentazione sanitaria comprovante l'entità delle lesioni, documentazione amministrativa, ecc.)	ILLIMITATO	art.3 L.210/1992 e L. 238/1997); Circ. 1 Ministero della sanità del 4-11-1996 n. 900
	.04	Istanze di indennizzo	Documentazione relativa ai danneggiati da trasfusione o somministrazione di emoderivati: pratiche di indennizzo (copie conformi di: cartella clinica riportante la prova delle avvenute trasfusioni o somministrazioni emoderivati, documentazione sanitaria indicante positività o diagnosi di malattia, analisi ematochimiche, documentazione amministrativa, ecc.)	ILLIMITATO	art.3 L.210/1992 e L. 238/1997); Circ. 1 Ministero della sanità del 4-11-1996 n. 900

copia informatica per consultazione

CLASSE	COD. SOTTO CLASSE	SOTTOCLASSE	TIPO DOCUMENTO	TEMPO CONSERVAZIONE	RIFERIMENTI NORMATIVI / NOTE
9. Assistenza e governo farmaceutica	.01	Aspetti generali, organizzativi e gestionali	Documenti strategici di programmazione, pianificazione, rendicontazione delle attività (Piani, programmi, calendari, registri, altri documenti strategici e di programmazione, regolamentazione dei rapporti tra il Servizio Sanitario Nazionale e le farmacie).	ILLIMITATO	
	.01	Aspetti generali, organizzativi e gestionali	Documentazione istruttoria e corrispondenza ordinaria/routinaria interna ed esterna attività assistenza e governo farmaceutica	5 anni	
	.01	Aspetti generali, organizzativi e gestionali	Gestione ricettari SSN (gestione ordini, rendicontazioni, consegna / registrazione ricettari MMG, PdF, MCA, RSA e strutture ospedaliere)	5 anni	
	.02	Controllo spesa farmaceutica	Monitoraggio / Report sul consumo / impiego di farmaci	5 anni	
	.02	Controllo spesa farmaceutica	Analisi sul consumo delle risorse per farmaci SSN da parte dei MMG, PdF, medici continuità assistenziale e specialisti ospedalieri	5 anni	
	.02	Controllo spesa farmaceutica	Analisi sul consumo delle risorse per farmaci di fascia H erogati in regime di file F	5 anni	
	.02	Controllo spesa farmaceutica	Verbale di controllo / sopralluogo file F	ILLIMITATO	
	.02	Controllo spesa farmaceutica	Analisi sulla corretta erogazione e pagamento di ricette di farmaci in regime di SSN	5 anni (in assenza di contenziosi)	
	.02	Controllo spesa farmaceutica	Contenzioso con Farmacie relativo a ricette contestate (verbale controllo, sanzionatorio, segnalazione autorità giudiziaria, ecc.)	ILLIMITATO	
	.02	Controllo spesa farmaceutica	Documenti relativi a interventi da parte dei NAS di richiesta di informazioni sulle modalità di prescrizione dei farmaci	ILLIMITATO	
	.03	Controllo farmacie, parafarmacie e distributori	Visita ispettiva ordinaria/straordinaria presso le farmacie (Verbale di controllo / sopralluogo, notifiche, ecc.)	ILLIMITATO	
	.03	Controllo farmacie, parafarmacie e distributori	Visita ispettiva sui depositi e magazzini all'ingrosso di medicinali	ILLIMITATO	
	.04	Autorizzazione e governo farmacie	Autorizzazione all'apertura di esercizio farmaceutico (richieste, autorizzazioni, decadenza autorizzazione, ecc.)	ILLIMITATO (sino alla cessazione dell'attività o modifiche alla titolarità dell'esercizio – subingressi)	
	.04	Autorizzazione e governo farmacie	Regolamentazione in ordine alla fissazione di orari, turni, ferie ecc. delle farmacie	ILLIMITATO (sino alla cessazione dell'attività o modifiche alla titolarità dell'esercizio – subingressi)	
	.04	Autorizzazione e governo farmacie	Tenuta del registro dei farmacisti (nuove assunzioni, cessazioni, stati di servizio, nomina titolari e sostituti, ecc.)	ILLIMITATO (sino alla cessazione dell'attività o modifiche alla titolarità dell'esercizio – subingressi)	
	.04	Autorizzazione e governo farmacie	Richiesta e autorizzazioni di modifiche dei locali	ILLIMITATO (sino alla cessazione dell'attività o modifiche alla titolarità dell'esercizio – subingressi)	
	.04	Autorizzazione e governo farmacie	Richiesta e autorizzazioni trasferimento farmacie	ILLIMITATO (sino alla cessazione dell'attività o modifiche alla titolarità dell'esercizio – subingressi)	
	.05	Farmacovigilanza	Utilizzo farmaci fuori dalle prescrizioni (off-label)	10 anni	
	.05	Farmacovigilanza	Indicazioni/attività in applicazione di note AIFA (comprese comunicazioni di sicurezza d'uso)	10 anni	
	.05	Farmacovigilanza	Scheda di segnalazione di sospetta reazione avversa e le relative richieste di registrazione nel sito della farmacovigilanza del Ministero della Salute	ILLIMITATO	
	.05	Farmacovigilanza	Documenti relativi a ritiri o revoche di medicinali così come gli interventi di prelievo di farmaci ritenuti difettosi	5 anni	
	.05	Farmacovigilanza	Attività di vigilanza effettuate presso ospedali o altre strutture relative a gestione farmaci (medicinali scaduti, giacenza farmaci, pulizia armadi, disposizione farmaci, grado di umidità, luce, temperatura, recipienti a norma, correttezza gas medicinali, ecc.)	ILLIMITATO	
	.06	Assistenza farmaceutica diretta	Documenti relativi a garantire la fornitura di dispositivi medici (DM), presidi, farmaci e dietetici tramite dispensazione diretta (Richiesta autorizzazione ed erogazione diretta trattamenti e farmaci, ordine farmaci, registro smaltimento farmaci, ecc.)	5 anni	
	.07	Sperimentazione farmaci e dispositivi	Documenti che riguardano la sperimentazione di nuovi farmaci o l'uso di farmaci conosciuti al fine di verificarne l'effetto (Proposte di sperimentazioni, pareri del Comitato Etico, sottoscrizioni dei protocolli di studio, autorizzazione sperimentazione, ecc.)	25 anni (si veda anche cod. 3.11.00)	L'art. 58, comma 1 del regolamento EU 536/14 sulla sperimentazione dei medicinali sull'uomo, dispone quanto segue: A meno che il diritto dell'Unione preveda un periodo di archiviazione maggiore, il promotore e lo sperimentatore conservano il contenuto del fascicolo permanente della sperimentazione clinica per almeno venticinque anni dalla conclusione della medesima. Tuttavia, le cartelle cliniche dei soggetti sono archiviate in conformità del diritto nazionale.
	.08	Gestione stupefacenti	Documenti che riguardano gli stupefacenti (tenuta e distribuzione dei ricettari, monitoraggio sul quantitativo di stupefacenti erogato dalle farmacie o strutture convenzionate, ecc.)	5 anni	
	.08	Gestione stupefacenti	Registri di entrata e uscita degli stupefacenti	10 anni dalla data dell'ultima registrazione per enti e imprese autorizzati alla fabbricazione 5 anni dalla data dell'ultima registrazione per le officine autorizzate all'impiego e per le imprese autorizzate al commercio all'ingrosso 2 anni dalla data dell'ultima registrazione per le farmacie aperte al pubblico e le farmacie ospedaliere	DPR n.390/90 art. 60 e s.i.m. comma 1 Nota Regione Lombardia H1.2014.0019108 del 27.05.2014 Legge n. 38 del 15.03.2010 art. 10
	.08	Gestione stupefacenti	Registri di carico e scarico degli stupefacenti (registro delle unità operative)	2 anni dalla data dell'ultima registrazione	DPR n.390/90 art. 60 e s.i.m. comma 3 e 6 Nota Regione Lombardia H1.2014.0019108 del 27.05.2014 Legge n. 38 del 15.03.2010 art. 10
	.08	Gestione stupefacenti	Buoni / ordini di acquisto stupefacenti e documenti trasporto / fatture	10 anni	

copia informatica per consultazione

CLASSE	COD. SOTTO CLASSE	SOTTOCLASSE	TIPO DOCUMENTO	TEMPO CONSERVAZIONE	RIFERIMENTI NORMATIVI / NOTE
1. Direzione ospedaliera	.01	Aspetti generali, organizzativi e gestionali	Contestazioni anomalie SDO	10 anni	
	.01	Aspetti generali, organizzativi e gestionali	Documentazione pagamenti ad altre strutture ospedaliere	5 anni	
	.01	Aspetti generali, organizzativi e gestionali	Pagamento ticket, ricevute	5 anni	Nota Regione Lombardia H1.2003.0001436. Allegato 3 alla DGRV1II8II78 del 18.02.2002
	.01	*Aspetti generali, organizzativi e gestionali*	*Pratiche amministrative per ricoveri (stranieri, comunitari,solventi)*	*10 anni*	
	.01	Aspetti generali, organizzativi e gestionali	Appropriatezza ricoveri (PRUO, ecc.)	10 anni	
	.01	Aspetti generali, organizzativi e gestionali	Volontariato, registri	10 anni	
	.01	Aspetti generali, organizzativi e gestionali	Registri viaggi ambulanza per trasferimento pazienti per esami in altre strutture; Autorizzazione trasporti in ambulanza	1 anno	
	.01	Aspetti generali, organizzativi e gestionali	Richieste copie di cartelle cliniche ed ambulatoriali, schede di P.S., certificati di ricovero, referto esami di laboratorio, ecc.	1 anno	
	.01	Aspetti generali, organizzativi e gestionali	Deleghe per il ritiro dei referti / *cartelle cliniche*	1 anno	
	.01	Aspetti generali, organizzativi e gestionali	Reclami	10 anni	
	.01	Aspetti generali, organizzativi e gestionali	CUP, prenotazione per prestazioni	1 anno	
	.01	Aspetti generali, organizzativi e gestionali	Gestioni reti di patologia (adesione e organizzazione), i dati relativi alle singole prestazioni di cura saranno classificati negli appositi sistemi gestionali	ILLIMITATO per la documentazione organizzativa; per la documentazione relativa ai sistemi gestionali si fa riferimento alla tipologia di assetto assistenziale erogato (prestazione ambulatoriale, ricovero)	
	.01	Aspetti generali, organizzativi e gestionali	Registrazioni audio, Videoregistrazioni, Fotografie digitali / analogiche relative a prestazioni sanitarie	Tempo di conservazione correlato al documento principale, massimo 10 anni.	
	.01	Aspetti generali, organizzativi e gestionali	Registrazioni informatiche di monitoraggio di parametri biologici (es. ECG, EEG, ecc.)	Tempo di conservazione correlato al documento principale, massimo 10 anni.	
	.02	Rapporti con l'autorità giudiziaria	Documentazione relativa a segnalazioni / denunce all'Autorità Giudiziaria	ILLIMITATO	
	.03	Igiene ospedaliera	Documentazione relativa ai controlli della sterilizzazione (prove Bowie Dick, Grafici dei cicli-rintracciabilità); modulistica carico/scarico strumentario, richieste dei reparti e documentazione della sterilizzazione in genere	2 anni	
	.03	Igiene ospedaliera	Registri ossido di etilene	2 anni	
	.03	Igiene ospedaliera	Inchieste o indagini epidemiologiche su malattie infettive di particolare rilevanza e/o soggette a sorveglianza	10 anni	Circ. Min. Sanità n. 61 del 19/12/1986. In considerazione del termine di prescrizione del diritto al risarcimento del danno subito da un paziente che è di dieci anni, siffatta documentazione verrà conservata sino al compimento della prescrizione decennale. Ministero per i Beni culturali e per le attività culturali -Direzione Generale per gli Archivi (prontuario scarto ASL)
	.03	Igiene ospedaliera	Malattie infettive, registri	ILLIMITATO	
	.03	Igiene ospedaliera	Registro carico e scarico rifiuti speciali, integrati con i formulari relativi al trasporto dei rifiuti	5 anni dalla data dell'ultima registrazione	D.Lgs. n.22/97 art.12 e s.m.i. (art. 190 del D.Lgs. n.152/2006 come modificato dalla legge 125/2013)
	.03	Igiene ospedaliera	Controlli microbiologici ambientali (schede, relazioni, verbali, conclusioni, comunicazioni)	5 anni	In considerazione del termine di prescrizione del diritto al risarcimento del danno subito da un paziente che è di dieci anni, siffatta documentazione verrà conservata sino al compimento della prescrizione decennale.
	.03	Igiene ospedaliera	Vaccinazioni, campagne vaccinali: danni da vaccini	ILLIMITATO	
	.04	Radioprotezione	Valutazioni di sorveglianza ambientale e valutazioni della dose ricevuta od impegnata dai lavoratori esposti non classificati in categoria A, nonché i verbali di controllo dei dispositivi e degli strumenti di protezione di cui allo stesso articolo.	5 anni dalla data di compilazione	D.Lgs. n.230/1995 (art.81, c.3)
	.04	Radioprotezione	Schede personali sulle quali devono essere annotati i risultati delle valutazioni delle dosi individuali e delle introduzioni individuali; relazioni sulle circostanze ed i motivi inerenti alle esposizioni accidentali di emergenza nonché alle altre modalità di esposizione.	Sino alla cessazione del rapporto di lavoro mantenendone successivamente copia per almeno cinque anni	D.Lgs. n.230/1995 (art.81, c.3)
	.04	Radioprotezione	Risultati delle misurazioni di sorveglianza fisica della radioprotezione	10 anni	D.Lgs. n.230/1995 (art.81, c.3)

copia informatica per consultazione

CLASSE	COD. SOTTO CLASSE	SOTTOCLASSE	TIPO DOCUMENTO	TEMPO CONSERVAZIONE	RIFERIMENTI NORMATIVI / NOTE
2. Pronto soccorso	.01	Gestione organizzativa P.S.	Verbale di Pronto Soccorso (Registri, schede triage, schede di pazienti accolti in PS e trasferiti in altro ospedale, Schede di pazienti entrati in PS che rifiutano il ricovero)	ILLIMITATO	
	.02	Attività emergenza - urgenza	Verbale di Pronto Soccorso (Referti)	ILLIMITATO	
	.02	*Attività emergenza - urgenza*	*Documentazione O.B.I. (Osservazione Breve Intensiva)*	*ILLIMITATO*	
	.02	Attività emergenza - urgenza	Documentazione 118 compilata dalle équipe di soccorso dei MSB (Mezzi di Soccorso di Base, con soccorritori a bordo), dei MSI (Mezzi di Soccorso Intermedio, con infermiere a bordo) e dei MSA (Mezzi di Soccorso Avanzato, con medico e infermiere a bordo)	ILLIMITATO Conservazione da parte della Struttura ospedaliera di destinazione del paziente (in cartella clinica o quale parte integrante della documentazione di Pronto Soccorso)	
	.02	*Attività emergenza - urgenza*	*Registrazioni audio della consulenza specialistica telefonica dei Centri Antiveleno*	*ILLIMITATO*	*Trattasi di documentazione nativa digitale che deve essere obbligatoriamente trasferita al conservatore dell'ente sulla base di quanto prescritto dal D.Lgs. 82/05 s.i.m.*
	.02	*Attività emergenza - urgenza*	*Documentazione sanitaria sia in formato cartaceo sia digitale relativa alla consulenza specialistica telefonica effettuata dai Centri Antiveleno*	*ILLIMITATO*	
	.02	*Attività emergenza - urgenza*	*Documentazione dei Centri Antiveleno*	*5 anni*	*Risoluzione CEE 90/C 329/03*
3. Assistenza ospedaliera	.01	Aspetti generali, organizzativi e gestionali	Registri nosologici / rubriche ricoverati	ILLIMITATO	Circ. Min. Sanità n. 61 del 19/12/1986
	.02	Ricovero (ordinario, day hospital, day surgery)	Cartella clinica di ricovero comprensiva di tutti i documenti costitutivi, es.: richiesta di ricovero / rapporto di pronto soccorso, consensi, scheda di dimissione ospedaliera (SDO), scheda infermieristica / ostetrica, lettera di dimissione, atti di nascita, referti indagini strumentali e di laboratorio, documenti inerenti la valutazione del dolore ai sensi della legge 38 del 2010, TSO, consulenze specialistiche, ecc.	ILLIMITATO	Circ. Min. Sanità n. 61 del 19/12/1986
	.02	Ricovero (ordinario, day hospital, day surgery)	Verbale - registro operatorio	ILLIMITATO	Circ. Min. Sanità n. 61 del 19/12/1986, Circ. Min. Sanità n. 900 del 14/03/96
	.02	Ricovero (ordinario, day hospital, day surgery)	Cartella clinica di ricovero diurno. Comprensiva di tutti i documenti costitutivi.	ILLIMITATO	Circ. Min. Sanità n. 61 del 19/12/1986 e DPR n. 1409 del 30/06/63 "Legge archivistica"
	.03	Day service	Documentazione inerente le attività ambulatoriali di Day Service	30 anni solo per il Day service chirurgico; 10 anni dalla chiusura del fascicolo per gli altri, assimilabili a documentazione ambulatoriale	
	.04	Assistenza al parto	Registro dei parti e Registro degli aborti	ILLIMITATO	Vedi anche II.3.05
	.04	Assistenza al parto	Certificato di Assistenza al Parto (CedAP)	ILLIMITATO se in cartella clinica; altrimenti 30 anni	
	.04	Assistenza al parto	PMA - Fecondazione eterologa: record relativi a ciascun donatore (screening e i risultati dei test)	30 anni dall'utilizzo	
	.05	Assistenza domiciliare	Cartella clinica di ospedalizzazione domiciliare	ILLIMITATO	DGR 7180 del 24 aprile 2008
	.06	Medicina penitenziaria	Cartella clinica di pazienti in regime detentivo	ILLIMITATO	
	.07	Assistenza psichiatrica e neuropsichiatrica infantile	Cartella clinica di struttura semiresidenziale, Centro Diurno e Residenzialità Leggera. Documentazione relativa alla neuropsichiatria dell'infanzia e dell'adolescenza.	10 anni	
	.07	Assistenza psichiatrica e neuropsichiatrica infantile	Cartella clinica di struttura residenziale (diario clinico, visite psichiatriche, attività riabilitative, colloqui psicoterapeutici, ecc.). Documentazione relativa alla neuropsichiatria dell'infanzia e dell'adolescenza.	ILLIMITATO	
	.07	Assistenza psichiatrica e neuropsichiatrica infantile	Documentazione del sistema informatizzato regionale PSICHE	Secondo tipologia di regime di erogazione della prestazione (residenziale / semiresidenziale)	

copia informatica per consultazione

CLASSE	COD. SOTTO CLASSE	SOTTOCLASSE	TIPO DOCUMENTO	TEMPO CONSERVAZIONE	RIFERIMENTI NORMATIVI / NOTE
4. Assistenza ambulatoriale	.01	Prestazioni ambulatoriali	Referto di singole prestazioni ambulatoriali. Fascicolo / *cartella* ambulatoriale con relativa documentazione a supporto	10 anni dalla chiusura del fascicolo per documentazione ambulatoriale. 30 anni solo per attività chirurgica.	
	.01	Prestazioni ambulatoriali	Prescrizione – proposta - ricetta per richieste di prestazioni sanitarie	ILLIMITATO se in cartella clinica; 5 anni altri esemplari	Nota Regione Lombardia H1.2003.0001436. Allegato 3 alla DGRV1Il8Il78 del 18.02.2002
	.01	Prestazioni ambulatoriali	Referti / documentazione a supporto dell'attività ambulatoriale - percorso chirurgico (Chirurgia a bassa complessità assistenziale)	30 anni	
	.01	Prestazioni ambulatoriali	Referti esami di laboratorio	5 anni	Nota Regione Lombardia H1.2003.0001436. Allegato 3 alla DGRV1Il8Il78 del 18.02.2002
	.01	Prestazioni ambulatoriali	Schede di emodialisi	10 anni da cessazione di trattamento	
	.01	Prestazioni ambulatoriali	Elenco emodializzati	10 anni da ultima dialisi	
	.01	Prestazioni ambulatoriali	Registro regionale di dialisi	10 anni da ultima dialisi	
	.01	Prestazioni ambulatoriali	Referti radiologici e di medicina nucleare. Compresi i referti strutturati	ILLIMITATO (in caso di ricovero da includere in cartella clinica)	D.M. Sanità 14/02/1997 Intesa Stato - Regioni del 04/04/2012 sul documento del Ministero della Salute recante "Linee guida per la dematerializzazione della documentazione clinica in diagnostica per immagini – Normativa e prassi"
	.01	Prestazioni ambulatoriali	Documentazione iconografica radiologica e di medicina nucleare. Compresa qualsiasi immagine diagnostica, indipendentemente dalle modalità di acquisizione (analogica o digitale) e dal regime di erogazione (ambulatoriale o ricovero)	10 anni	D.M. Sanità 14/02/1997 Circ. Min. Sanità n. 61 del 19/12/1986 Intesa Stato - Regioni del 04/04/2012 sul documento del Ministero della Salute recante "Linee guida per la dematerializzazione della documentazione clinica in diagnostica per immagini – Normativa e prassi"
	.01	Prestazioni ambulatoriali	Cartelle radioterapiche	ILLIMITATO	
	.01	Prestazioni ambulatoriali	Certificati di idoneità e inidoneità sportiva	5 anni	D.M. Sanità 18/02/1982 ("Norme per la tutela sanitaria dell'attività sportiva agonistica")

copia informatica per consultazione

CLASSE	COD. SOTTO CLASSE	SOTTOCLASSE	TIPO DOCUMENTO	TEMPO CONSERVAZIONE	RIFERIMENTI NORMATIVI / NOTE
4. Assistenza ambulatoriale	.01	Prestazioni ambulatoriali	Referti esami citologici e istologici	10 anni	
	.01	Prestazioni ambulatoriali	Riserva non campionata (residui di campioni bioptici / operatori / autoptici in liquido fissativo)	15 giorni dalla definizione della diagnosi (valido anche per campioni eseguiti durante ricovero)	Si fa riferimento a campioni per esclusive attività diagnostiche. Lo smaltimento può essere anche solo parziale nell'ipotesi di dover prelevare nuovamente o rivedere a distanza una parte del campione; in questo caso va registrato cosa non viene smaltito. LG "Tracciabilità, raccolta, trasporto, conservazione e archiviazione di cellule e tessuti per indagini diagnostiche di anatomia patologica" Consiglio Superiore di Sanità - Sez. 1 del maggio 2015
	.01	Prestazioni ambulatoriali	Inclusioni in paraffina di campioni istologici derivati da qualsiasi fonte (es. prelievo bioptico, operatorio, autoptico, ecc.)	50 anni (valido anche per campioni eseguiti durante ricovero)	
	.01	Prestazioni ambulatoriali	Campioni istologici allestiti (anche da citoinclusi)	50 anni (valido anche per campioni eseguiti durante ricovero) 15 giorni per i preparati colorati con immunofluorescenza (in quanto soggetti a decadimento. Valido anche per campioni eseguiti durante ricovero)	Per "campione istologico" o "sezione istologica" si fa riferimento sia a quella derivata da Surgical Pathology sia da procedura autoptica. Il fine della lunga conservazione dei campioni è la garanzia per il paziente e i suoi famigliari di poter accedere nel tempo, per scopi sanitari, a una fonte di DNA.
	.01	Prestazioni ambulatoriali	Campioni istologici digitalizzati	30 anni (dall'eliminazione del campione istologico "fisico") corrispondente. Valido anche per campioni eseguiti durante ricovero)	Il "vetrino digitale" può essere eseguito ed eliminato dopo il suo utilizzo innumerevoli volte sino a quando è presente il suo corrispettivo "fisico". Nel caso quest'ultimo venga eliminato allo scadere del suo tempo minimo di conservazione appare buona prassi effettuare una sua "scannerizzazione finale" da conservare per il tempo minimo definito. La digitalizzazione appare di particolare rilievo per i preparati in immunofluorescenza che decadono molto rapidamente nel tempo.
	.01	Prestazioni ambulatoriali	Campioni citologici allestiti (escluso Pap test)	50 anni se campione patologico unico, altrimenti 5 anni (valido anche per campioni eseguiti durante ricovero)	Il fine della lunga conservazione dei campioni è la garanzia per il paziente e i suoi famigliari di potere accedere nel tempo, per scopi sanitari, a una fonte di DNA e, quando positivo, per confrontare nel tempo l'istotipo e il grado di differenziazione della neoplasia. Nel caso il campione citologico positivo sia associato a un campione istologico o nell'archivio di una Anatomia Patologica sia presente almeno un campione istologico o autoptico dello stesso paziente, i campioni citologici possono essere smaltiti dopo 5 anni.
	.01	Prestazioni ambulatoriali	Pap test	10 anni (valido anche per campioni eseguiti durante ricovero)	
	.01	Prestazioni ambulatoriali	Campioni citologici digitalizzati	30 anni (dall'eliminazione del campione citologico corrispondente. Valido anche per campioni eseguiti durante ricovero)	Il "vetrino digitale" può essere eseguito ed eliminato dopo il suo utilizzo innumerevoli volte sino a quando è presente il suo corrispettivo "fisico". Nel caso quest'ultimo venga eliminato allo scadere del suo tempo minimo di conservazione appare buona prassi effettuare una sua "scannerizzazione finale" da conservare per il tempo minimo definito.
	.01	Prestazioni ambulatoriali	Residui di campioni citologici in fase liquida	3 mesi dall'emissione del referto diagnostico (valido anche per campioni eseguiti durante ricovero)	I campioni citologici in fase liquida possono essere utilizzati per indagini immunoistochimiche o biomolecolari, senza necessità di riprelevare il paziente. Il tempo minimo indicato di archiviazione considera i tempi che potrebbero intercorrere tra la diagnosi, il recepimento di questa da parte del clinico e la sua richiesta di approfondimenti diagnostici.
	.01	Prestazioni ambulatoriali	Residui di acidi nucleici estratti da campioni istologici o autoptici o da liquidi biologici risultati idonei alle indagini di patologia molecolare già effettuate.	2 anni (valido anche per campioni eseguiti durante ricovero)	

copia informatica per consultazione

CLASSE	COD. SOTTO CLASSE	SOTTOCLASSE	TIPO DOCUMENTO	TEMPO CONSERVAZIONE	RIFERIMENTI NORMATIVI / NOTE
5. Riabilitazione	.01	Riabilitazione	Cartella ambulatoriale di riabilitazione	10 anni da ultima registrazione	
6. Attività Immuno-trasfusionale	*.01*	*Aspetti generali, organizzativi e gestionali*	*Documentazione inerente il sistema qualità e le relative registrazioni del sangue ed emocomponenti*	*10 anni*	*D.M. 2 novembre 2015 "Disposizioni relative ai requisiti di qualità e sicurezza del sangue e degli emocomponenti". Art. 29, comma 4.*
	.02	*Valutazione idoneità donatori sangue ed emocomponenti*	*Cartella sanitaria del donatore di sangue ed emocomponenti*	*30 anni*	*D.M. 2 novembre 2015 "Disposizioni relative ai requisiti di qualità e sicurezza del sangue e degli emocomponenti". Art. 5, comma 8.*
	.02	*Valutazione idoneità donatori sangue ed emocomponenti*	*Le registrazioni dei risultati riguardanti le determinazioni del gruppo sanguigno ABO ed Rh, della presenza di anticorpi irregolari anti-eritrocitari, delle prove di compatibilità pre-trasfusionali relativi ai pazienti riceventi, nonché la documentazione inerente le reazioni ed eventi avversi gravi.*	*15 anni*	*D.M. 2 novembre 2015 "Disposizioni relative ai requisiti di qualità e sicurezza del sangue e degli emocomponenti". Art. 29, comma 3.*
	.02	*Valutazione idoneità donatori sangue ed emocomponenti*	*Documentazione che consente di ricostruire il percorso di ogni unità di sangue ed emocomponenti, il modulo di consenso informato relativo a ciascuna donazione, i risultati delle indagini di validazione prescritte dalla normativa vigente su ogni unità di sangue o emocomponenti*	*30 anni*	*D.M. 2 novembre 2015 "Disposizioni relative ai requisiti di qualità e sicurezza del sangue e degli emocomponenti". Art. 29, comma 2.*
	.02	Valutazione idoneità donatori sangue ed emocomponenti	Danni da trasfusione	ILLIMITATO	L. 210/1992 art.3 e L. 238/1997); Circ. 1 Ministero della Sanità del 4-11-1996 n. 900
7. Attività di trapianto d'organi e tessuti	.01	Aspetti generali, organizzativi e gestionali	Documentazione gestionale (Segnalazione alla Direzione Sanitaria di soggetto in morte cerebrale, Attivazione della commissione per l'accertamento dello stato di morte cerebrale, Verbale di accertamento della morte cerebrale, Richiesta di nulla osta dell'autorità giudiziaria)	30 anni	D.Lgs. n.16/2010. - 30 anni per i dati inerenti il donatore e il ricevente (art. 14 c. 2) - 10 anni per le registrazioni dell'istituto dei tessuti (all. V lett. E)
	.02	*Donazione e prelievo*	*Dati necessari ad assicurare la tracciabilità in tutte le fasi per la donazione, l'approvvigionamento, il controllo, la lavorazione, la conservazione, lo stoccaggio e la distribuzione di tessuti e cellule umani.*	*30 anni dopo l'uso clinico (l'archiviazione dei dati può avvenire anche in forma elettronica)*	*D.Lgs. 6 novembre 2007, n. 191 "Attuazione della direttiva 2004/23/CE sulla definizione delle norme di qualità e di sicurezza per la donazione, l'approvvigionamento, il controllo, la lavorazione, la conservazione, lo stoccaggio e la distribuzione di tessuti e cellule umani"*
	.02	*Donazione e prelievo*	*Dati per identificare donatore, donazione, tessuti / cellule, ecc. (di cui all'allegato X del D.Lgs. 25 gennaio 2010, n. 16)*	*30 anni*	*D.Lgs. 25 gennaio 2010, n. 16 "Attuazione delle direttive 2006/17/CE e 2006/86/CE, che attuano la direttiva 2004/23/CE per quanto riguarda le prescrizioni tecniche per la donazione, l'approvvigionamento e il controllo di tessuti e cellule umani, nonché per quanto riguarda le prescrizioni in tema di rintracciabilità, la notifica di reazioni ed eventi avversi gravi e determinate prescrizioni tecniche per la codifica, la lavorazione, la conservazione, lo stoccaggio e la distribuzione di tessuti e cellule umani". (Art. 14, comma 2).*
	.02	*Donazione e prelievo*	*I registri dei donatori, necessari ai fini di una completa tracciabilità,*	*30 anni dopo l'uso clinico o dopo la scadenza o eliminazione del tessuto o cellula in un archivio adeguato*	*D.Lgs. 25 gennaio 2010, n. 16 "Attuazione delle direttive 2006/17/CE e 2006/86/CE, che attuano la direttiva 2004/23/CE per quanto riguarda le prescrizioni tecniche per la donazione, l'approvvigionamento e il controllo di tessuti e cellule umani, nonché per quanto riguarda le prescrizioni in tema di rintracciabilità, la notifica di reazioni ed eventi avversi gravi e determinate prescrizioni tecniche per la codifica, la lavorazione, la conservazione, lo stoccaggio e la distribuzione di tessuti e cellule umani". (Allegato IV, Punto 1.4.4)*
	.02	*Donazione e prelievo*	*Tutte le registrazioni, dati grezzi compresi, critiche per la sicurezza e la qualità dei tessuti e cellule.*	*10 anni dopo la data di scadenza, l'uso clinico o lo smaltimento*	*D.Lgs. 25 gennaio 2010, n. 16 "Attuazione delle direttive 2006/17/CE e 2006/86/CE, che attuano la direttiva 2004/23/CE per quanto riguarda le prescrizioni tecniche per la donazione, l'approvvigionamento e il controllo di tessuti e cellule umani, nonché per quanto riguarda le prescrizioni in tema di rintracciabilità, la notifica di reazioni ed eventi avversi gravi e determinate prescrizioni tecniche per la codifica, la lavorazione, la conservazione, lo stoccaggio e la distribuzione di tessuti e cellule umani". (Allegato V, E, punto 7)*
	.02	*Donazione e prelievo*	*Tracciabilità del percorso di idoneità, assegnazione degli organi, prelievo e trapianto organi.*	*30 anni dopo la donazione*	*D.M. del 19 novembre 2015 "Attuazione della direttiva 2010/53/UE relativa alla norme di qualità e sicurezza degli organi umani destinati ai trapianti"*

copia informatica per consultazione

CLASSE	COD. SOTTO CLASSE	SOTTOCLASSE	TIPO DOCUMENTO	TEMPO CONSERVAZIONE	RIFERIMENTI NORMATIVI / NOTE
8. Farmaceutica ospedaliera	.01	Farmaceutica	Matrici ricette del SSN (a cura dei singoli medici dal 1/09/2005 e comunque per i ricettari "nominali")	5 anni dalla data dell'ultima prescrizione	Nota DG Sanità Regione Lombardia H1.2001.0033136 del 16/05/2001 Nota DG Sanità Regione Lombardia H1.2005.0032866 del 04/07/2005 Allegato (p. 3.3) al Decreto Ministeriale 18 maggio 2004
	.01	Farmaceutica	Documentazione relativa all'approvvigionamento farmaci	5 anni	
	.01	*Farmaceutica*	*Documenti di trasporto per consegna beni farmaceutici*	*10 anni*	
	.01	*Farmaceutica*	*Documentazione inerente alla gestione dei controlli di qualità sui gas medicinali*	*10 anni*	
	.01	Farmaceutica	Schede di prescrizione dei farmaci in file F	2 anni	Comunicazione DG Sanità prot. H12004.0057563 del 11.11.2004
	.01	Farmaceutica	Documentazione piani terapeutici farmaci	ILLIMITATO (in cartella clinica)	
	.01	Farmaceutica	Fogli di lavorazione delle preparazioni di farmaci oncologici	5 anni	Raccomandazione ministeriale sulla sicurezza dei farmaci antiblastici
	.01	*Farmaceutica*	*Grafici di rilevazione della temperatura registrazione linea del freddo (frigoriferi per medicinali)*	*1 anno*	
	.02	Stupefacenti	Registri di entrata e uscita degli stupefacenti	10 anni dalla data dell'ultima registrazione per enti e imprese autorizzati alla fabbricazione 5 anni dalla data dell'ultima registrazione per le officine autorizzate all'impiego e per le imprese autorizzate al commercio all'ingrosso 2 anni dalla data dell'ultima registrazione per le farmacie aperte al pubblico e le farmacie ospedaliere	DPR n.390/90 art. 60 e s.i.m. comma 1 Nota Regione Lombardia H1.2014.0019108 del 27.05.2014 Legge n. 38 del 15.03.2010 art. 10
	.02	Stupefacenti	Buoni / ordini di acquisto stupefacenti e documenti trasporto / fatture	10 anni	
	.02	Stupefacenti	Bollettario con moduli approvvigionamento (Reparti - Farmacia) di farmaci stupefacenti	2 anni dalla data dell'ultima registrazione	Decreto del Presidente della Repubblica del 9 ottobre 1990, n. 309 - art. 45 , comma 6. Testo unico delle leggi in materia di disciplina degli stupefacenti e sostanze psicotrope, prevenzione, cura e riabilitazione dei relativi stati di tossicodipendenza.
	.02	Stupefacenti	Bollettario con moduli di restituzione (Reparti - Farmacia) di farmaci stupefacenti	5 anni dalla data dell'ultima registrazione	Decreto del Presidente della Repubblica del 9 ottobre 1990, n. 309 - art. 45 , comma 6. Testo unico delle leggi in materia di disciplina degli stupefacenti e sostanze psicotrope, prevenzione, cura e riabilitazione dei relativi stati di tossicodipendenza.
	.02	Stupefacenti	Registro di carico e scarico dei medicinali contenenti sostanze stupefacenti o psicotrope delle Unita Operative (reparti) delle Aziende Sanitarie	2 anni dalla data dell'ultima registrazione	Decreto Ministeriale 3 agosto 2001 in riferimento a Decreto del Presidente della Repubblica del 9 ottobre 1990, n. 309 - art. 60 c. 3 e 6. Testo unico delle leggi in materia di disciplina degli stupefacenti e sostanze psicotrope, prevenzione, cura e riabilitazione dei relativi stati di tossicodipendenza.

copia informatica per consultazione

CLASSE	COD. SOTTO CLASSE	SOTTOCLASSE	TIPO DOCUMENTO	TEMPO CONSERVAZIONE	RIFERIMENTI NORMATIVI / NOTE
9. Medicina legale ospedaliera	.01	Medicina necroscopica	Certificato di morte, accertamento morte, cause di morte (ISTAT), referti autoptici	ILLIMITATO	
	.01	Medicina necroscopica	Registro dei decessi	ILLIMITATO	
	.02	Indennizzo danni	Giudizio medico-legale per danni da vaccinazioni e/o trasfusioni	ILLIMITATO	Circ. Min. Sanità 10 aprile 1992
	.03	Consulenze medico-legali	Certificazioni medico-legali; certificati inerenti accertamenti di laboratorio a valenza medico-legale; attività peritale; giudizio medico-legale per danni da vaccinazioni e/o trasfusioni	10 anni	In considerazione del termine di prescrizione del diritto al risarcimento del danno subito da un paziente che è di dieci anni, siffatta documentazione verrà conservata sino al compimento della prescrizione decennale.
10. Medicina del lavoro	.01	Cartella sanitaria e di rischio del lavoratore	Cartelle sanitarie e di rischio	Almeno sino alla cessazione del rapporto di lavoro; 40 anni dalla cessazione del lavoro comportante una esposizione ad agenti cancerogeni ; 30 anni dalla cessazione del lavoro comportante una esposizione a radiazioni ionizzanti	D.M. 12/07/07, n.155
	.01	Cartella sanitaria e di rischio del lavoratore	Schede delle prove allergologiche relative a malattie professionali	ILLIMITATO	Normativa di riferimento difforme, per lo più a carattere regionale.
	.02	Malattia professionale e infortunio sul lavoro	Registri vaccinazioni	ILLIMITATO	
	.02	Malattia professionale e infortunio sul lavoro	Registri infortuni	4 anni dall'ultima registrazione e, se non usato, dalla data in cui è stato vidimato	D.M. 12/9/58, art.2
11. Sperimentazione clinica dei medicinali e dei dispositivi	.00	Sperimentazione clinica dei medicinali e dei dispositivi	Documentazione relativa alla sperimentazione clinica *dei* farmaci e dei dispositivi (fascicolo della sperimentazione) *per uso umano*	25 anni dalla conclusione della sperimentazione	L'art. 58, comma 1 del regolamento EU 536/14 sulla sperimentazione dei medicinali sull'uomo, dispone quanto segue: "A meno che il diritto dell'Unione preveda un periodo di archiviazione maggiore, il promotore e lo sperimentatore conservano il contenuto del fascicolo permanente della sperimentazione clinica per almeno venticinque anni dalla conclusione della medesima. Tuttavia, le cartelle cliniche dei soggetti sono archiviate in conformità del diritto nazionale".
	.00	Sperimentazione clinica dei medicinali e dei dispositivi	Consenso informato relativo all'esposizione a radiazioni ionizzanti a scopo di ricerca scientifica e clinica e area sperimentazione di farmaci	ILLIMITATO	D.Lgs. n.230/1995 e D.M. 18/03/1998

copia informatica per consultazione

Aruba PEC S.p.A

Manuale di Conservazione

Versione: 1.5
Data approvazione: 11/10/2018
Redazione: Marco Menonna
Verificato da: Mauro Manetti, Roberta Giommoni
Approvato da: Simone Braccagni
Classificazione documento: Pubblico

VERSIONE N°	DATA	NATURA DELLA MODIFICA
1.0	26/11/2014	Prima versione documento
1.1	02/02/2016	Revisione del manuale a seguito della pubblicazione del nuovo schema sul sito istituzionale dell'Agid
1.2	04/04/2016	Modifiche su terminologie utilizzate
1.3	20/09/2017	Par.3.1: aggiornata normativa di riferimento Par.4.1: aggiornati Responsabili del Servizio e date di nomina Par.6.3: rimosso Par.7.6: modificata terminologia (da "materiali" a documenti"); Inserimento Par.7.7.3: Produzione copie o duplicati su supporti rimuovibili Par. 7.11: inserito paragrafo "audit log" Par.8.6: migliorata descrizione della soluzione di conservazione Par.8.6.1: migliorata descrizione change management e inserito riferimento test di Quality Assurance Par.9.2.: modificata cadenza verifica periodica dell'integrità degli archivi. Modificata descrizione procedura leggibilità archivi. Par.9.2.1 modificata frequenza verifica integrità degli archivi Cap.11: Cambiata descrizione specifiche tecniche per "invio in conservazione del PdA" Par.12.7: ridefinite modalità di isolamento delle componenti critiche Par.12.8.3: migliorata descrizione della sicurezza organizzativa e aggiornati riferimenti normativi 12.8.4: aggiornate regole password utente Tutto il documento: aggiornati riferimenti a documenti interni e procedure di sistema
1.4	11/12/2017	Tutto il documento: inseriti testi alternativi per le immagini e verificata accessibilità Par. 1.1: Specificata denominazione societaria del Conservatore Accreditato e inseriti dati identificativi della società Par. 2.1: Uniformata terminologia relativa a IdC, IPdA e IPdV Par. 6.3.2: Aggiornata tabella formati consigliati

Aruba PEC S.p.A.
Via San Clemente, 53
24036 Ponte San Pietro (BG)
P. IVA 01879020517

ARUBA GROUP

copia informatica per consultazione

		Par 6.6.1: Aggiornati riferimenti alle specifiche specifiche del Pacchetto di Versamento Par. 6.7.1: Aggiornata terminologia relativa a IdC Par.7.5.2: Inserito paragrafo relativo a gestione PdA incompleti o non validi Par. 7.6.1: Aggiornato paragrafo e corretto refuso di terminologia sul secondo punto Par. 7.8.3: Descritta procedura per scarto immediato Par.9.2: Modificato titolo paragrafo Par. 9.2.1: Rivista descrizione delle attività di verifica dell'integrità degli archvi Par 10.1.2: Aggiornati i contenuti della Scheda di Conservazione Cap. 11: Rivisti ed aggiornati livelli di servizio (SLA)
1.5	11/10/2018	Aggiornamenti Terminologia, Normativa e Standard di Riferimento Par.4.1: Aggiornati Ruoli e Reponsabilità Par.6.4: Precisazione su inserimento delle c.d. extrainfo nell' IdC. Par. 7.1: Aggiornamento modalità di acquisizione dei PdV. Inserito par. 7.5.3 Rettifica dei pacchetti di archiviazione Par.12.5: Rimosso riferimento a protocollo SSL Par. 12.6: Rivisti dettagli gestione dei backup del sistema Tutto il documento: aggiornamenti riferimenti a normativa trattamento dati personali

Aruba PEC S.p.A.
Via San Clemente, 53
24036 Ponte San Pietro (BG)
P. IVA 01879020517

copia informatica per consultazione

Indice del documento

Sommario

copia informatica per consultazione

copia informatica per consultazione

copia informatica per consultazione

1 Scopo e ambito del documento

Il presente documento è il Manuale del sistema di conservazione (di seguito per brevità chiamato anche "Manuale") del Conservatore Accreditato Aruba PEC S.p.a. (da ora in avanti "ARUBA"). Di seguito i dati identificativi della società:

Denominazione sociale:	**Aruba PEC S.p.A.**
Indirizzo della sede legale ed operativa:	**Via S. Clemente, 53** **I-24036 Ponte San Pietro (BG)**
Legale rappresentante:	**Simone Braccagni** (Amministratore Unico)
N° di iscrizione al Registro Imprese di Bergamo:	**01879020517 (REA n. 445886)**
Codice Fiscale e Partita IVA:	**01879020517**
N° di telefono (centralino):	**+39 0575 050.350**
ISO Object Identifier (OID):	**1.3.6.1.4.1.29741**
Sito web principale:	**https://www.pec.it**
E-mail (generale):	**info@arubapec.it**

Il Manuale illustra dettagliatamente l'organizzazione, i soggetti coinvolti e i ruoli svolti dagli stessi, il modello di funzionamento, la descrizione dei processi, in particolare le modalità di versamento, archiviazione e distribuzione, la descrizione delle architetture e delle infrastrutture utilizzate, le misure di sicurezza adottate ed ogni altra informazione utile alla gestione e alla verifica del funzionamento, nel tempo, del sistema di conservazione digitale di documenti informatici.

Il Manuale è costituito dalla versione corrente del presente documento.

In particolare, nel presente Manuale sono riportati:

a) i dati dei soggetti che nel tempo hanno assunto la responsabilità del servizio di conservazione, descrivendo in modo puntuale, in caso di affidamento, i soggetti, le funzioni e gli ambiti oggetto dell'affidamento stesso;
b) la struttura organizzativa comprensiva delle funzioni, delle responsabilità e degli obblighi dei diversi soggetti che intervengono nel processo di conservazione;
c) la descrizione delle tipologie dei documenti informatici sottoponibili a conservazione,
d) comprensiva dell'indicazione dei formati gestiti, dei metadati da associare alle diverse tipologie di documenti e delle eventuali eccezioni;
e) la descrizione delle modalità di presa in carico di uno o più pacchetti di versamento, comprensiva della predisposizione del rapporto di versamento e della descrizione dei controlli effettuati su ciascuno specifico formato adottato;
f) la descrizione del processo di conservazione e del trattamento dei pacchetti di archiviazione;
g) la modalità di svolgimento del processo di esibizione e di esportazione dal sistema di conservazione con la produzione del pacchetto di distribuzione;

copia informatica per consultazione

h) la descrizione del sistema di conservazione, comprensivo di tutte le componenti tecnologiche, fisiche e logiche, opportunamente documentate e delle procedure di gestione e di evoluzione delle medesime;
i) la descrizione delle procedure di monitoraggio della funzionalità del sistema di conservazione e delle verifiche sull'integrità degli archivi con l'evidenza delle soluzioni adottate in caso di anomalie;
j) la descrizione delle procedure per la produzione di duplicati o copie;
k) i tempi entro i quali le diverse tipologie di documenti informatici devono essere oggetto di scarto/cancellazione;
l) le modalità con cui viene richiesta la presenza di un pubblico ufficiale, indicando anche quali sono i casi per i quali è previsto il suo intervento;
m) le normative in vigore nei luoghi dove sono conservati i documenti;

Il Manuale recepisce le disposizioni di cui al D.Lgs. 7 marzo 2005, n. 82, e s.m.i. (Codice dell'amministrazione digitale), di seguito per brevità chiamato anche "Codice" o "CAD", oltre alle indicazioni riportate nei provvedimenti di legge o di prassi richiamati nel capitolo "Riferimenti normativi e di prassi" nonché i provvedimenti di natura tecnica richiamati nel capitolo "Riferimenti tecnici".

Il Cliente è tenuto a leggere con la massima attenzione il presente Manuale predisposto da ARUBA. Il Cliente in qualità di unico Responsabile della conservazione approva e fa propri i contenuti del presente Manuale di conservazione. Per una più agevole e scorrevole lettura del presente Manuale si raccomanda la consultazione del capitolo dedicato alle definizioni, abbreviazioni e termini tecnici.

Torna al sommario

2 Terminologia (glossario e acronimi)

Secondo la normativa vigente e ai fini dell'interpretazione del presente Manuale, i termini e le espressioni sotto elencate avranno il significato descritto nelle definizioni in esso riportate. Qualora le definizioni adottate dalla normativa di riferimento non fossero riportate nell'elenco che segue, si rimanda ai testi in vigore per la loro consultazione.
I termini e le espressioni non definiti avranno il significato loro attribuito all'interno del paragrafo o sezione che li contiene.
Ai fini della fruizione del Servizio di conservazione digitale dei documenti informatici descritto nel presente Manuale, valgono ad ogni effetto anche le definizioni contenute nel Contratto, da intendersi, pertanto, qui interamente riportate e trascritte, nonché le seguenti:

2.1 Glossario dei termini e acronimi

Glossario dei termini e Acronimi	
AgID	Agenzia per l'Italia Digitale
Accesso	Operazione che consente a chi ne ha diritto di prendere visione dei documenti informatici conservati
Accreditamento	Riconoscimento, da parte dell'Agenzia per l'Italia Digitale, del possesso dei requisiti del livello più elevato, in termini di qualità e sicurezza, ad un soggetto pubblico o privato che svolge attività di conservazione o di certificazione del processo di conservazione
Agente di alterazione	Qualsiasi codice contenuto in un documento informatico potenzialmente idoneo a modificare la rappresentazione dell'informazione senza alterarne il contenuto binario

copia informatica per consultazione

	(in via meramente esplicativa e non esaustiva: macro, codici eseguibili nascosti, formule di foglio di lavoro occulte in tutto o in parte, sequenze di caratteri occultate all'interno dei documenti informatici)
Aggregazione documentale informatica	Raccolta di documenti informatici o di fascicoli informatici, riuniti per caratteristiche omogenee, in relazione alla natura e alla forma dei documenti o in relazione all'oggetto e alla materia o in relazione alle funzioni dell'ente
Archivio	Complesso organico di documenti, di fascicoli e di aggregazioni documentali di qualunque natura e formato, prodotti o comunque acquisiti da un soggetto produttore durante lo svolgimento dell'attività
Archivio informatico	Archivio intestato dal Cliente al/i Titolare/i nel quale sono conservati costituito da documenti informatici, fascicoli informatici nonché aggregazioni documentali informatiche gestiti e conservati in ambiente informatico e di cui il/i medesimo/i è/sono giuridicamente responsabile/i
Area organizzativa omogenea	Un insieme di funzioni e di strutture, individuate dalla amministrazione, che opera su tematiche omogenee e che presenta esigenze di gestione della documentazione in modo unitario e coordinato ai sensi dell'articolo 50, comma 4, del D.P.R. 28 dicembre 2000, n. 445 e s.m.i.
Attestazione di conformità delle copie per immagine su supporto informatico di un documento analogico	Dichiarazione rilasciata da notaio o altro pubblico ufficiale a ciò autorizzato allegata o asseverata al documento informatico
Autenticità	Caratteristica di un documento informatico che garantisce di essere ciò che dichiara di essere, senza aver subito alterazioni o modifiche. L'autenticità può essere valutata analizzando l'identità del sottoscrittore e l'integrità del documento informatico
Base di dati	Collezione di dati registrati e correlati tra loro
Certificatore accreditato	Soggetto, pubblico o privato, che svolge attività di certificazione del processo di conservazione al quale sia stato riconosciuto, dell'Agenzia per l'Italia Digitale, il possesso dei requisiti del livello più elevato, in termini di qualità e di sicurezza
Ciclo di gestione	Arco temporale di esistenza del documento informatico, del fascicolo informatico, dell'aggregazione documentale informatica o dell'archivio informatico dalla sua formazione alla sua eliminazione o conservazione nel tempo
Chiusura del Pacchetto di Archiviazione	Operazione consistente nella sottoscrizione del Pacchetto di Archiviazione con firma digitale apposta da un Firmatario Delegato di ARUBA e apposizione di una validazione temporale con marca temporale alla relativa impronta
Classificazione	Attività di organizzazione logica di tutti i documenti secondo uno schema articolato in voci individuate attraverso specifici metadati
Codice o CAD	Decreto legislativo 7 marzo 2005, n. 82 e successive modificazioni e integrazioni
Codice eseguibile	Insieme di istruzioni o comandi software direttamente elaborabili dai sistemi informatici
Conservatore accreditato	Soggetto, pubblico o privato, che svolge attività di conservazione al quale sia stato riconosciuto, dall'Agenzia per l'Italia Digitale o da un certificatore accreditato, il possesso dei requisiti del livello più elevato, in termini di qualità e di sicurezza
Conservazione	Insieme delle attività finalizzate a definire ed attuare le politiche complessive del sistema di conservazione e a governarne la gestione in relazione al modello organizzativo adottato e descritto nel Manuale di conservazione
Contrassegno a stampa	Contrassegno generato elettronicamente, apposto a stampa sulla copia analogica di un documento amministrativo informatico per verificarne provenienza e conformità all'originale
Coordinatore della Gestione Documentale	Responsabile della definizione di criteri uniformi di classificazione ed archiviazione nonché di comunicazione interna tra le AOO ai sensi di quanto disposto dall'articolo

copia informatica per consultazione

	50 comma 4 del DPR 445/2000 e s.m.i. nei casi di amministrazioni che abbiano istituito più Aree Organizzative Omogenee
Copia informatica di documento analogico	Il documento informatico avente contenuto identico a quello del documento analogico da cui è tratto
Copia per immagine su supporto informatico di documento analogico	Il documento informatico avente contenuto e forma identici a quelli del documento analogico da cui è tratto
Copia informatica di documento informatico	Il documento informatico avente contenuto identico a quello del documento da cui è tratto su supporto informatico con diversa sequenza di valori binari.
Copia di sicurezza	Copia di backup degli archivi del sistema di conservazione.
Descrittore evidenze	Vedi pacchetto informativo.
Destinatario	Identifica il soggetto/sistema al quale il documento informatico è indirizzato.
DIRT	Documenti informatici rilevanti ai fini delle disposizioni tributarie.
Documento analogico	La rappresentazione non informatica di atti, fatti o dati giuridicamente rilevanti.
Documento analogico originale	Documento analogico che può essere unico oppure non unico se, in questo secondo caso, sia possibile risalire al suo contenuto attraverso altre scritture o documenti di cui sia obbligatoria la conservazione, anche se in possesso di terzi.
Documento originale unico	E' quel documento analogico il cui contenuto non può essere desunto da altre scritture o documenti di cui sia obbligatoria la tenuta, anche presso terzi e che non soddisfa, dunque, alcuna delle condizioni elencate nella definizione di "Documento analogico originale".
Documento informatico	La rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti.
Duplicato informatico	Il documento informatico ottenuto mediante la memorizzazione, sullo stesso supporto o su supporti diversi, della medesima sequenza di valori binari del documento originario.
Duplicazione dei documenti informatici	Produzione di duplicati informatici.
Elenco Persone	Elenco delle persone designate dal Cliente ad operare in suo nome, conto e interesse con ARUBA per l'esecuzione del contratto.
Esibizione	Operazione che consente di visualizzare un documento conservato e di ottenerne copia;
Estratto per riassunto	Documento nel quale si attestano in maniera sintetica ma esaustiva fatti, stati o qualità desunti da dati o documenti in possesso di soggetti pubblici
Evidenza informatica	Una sequenza di simboli binari (bit) che può essere elaborata da una procedura informatica.
Fascicolo informatico	Raccolta, individuata con identificativo univoco, di atti, documenti e dati informatici, da chiunque formati, del procedimento amministrativo, nell'ambito della pubblica amministrazione. Per i soggetti privati è da considerarsi fascicolo informatico ogni aggregazione documentale, comunque formata, funzionale all'erogazione di uno specifico servizio o prestazione.
Firma digitale	Un particolare tipo di firma elettronica avanzata basata su un certificato qualificato e su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici.
Fruibilità di un dato	La possibilità di utilizzare il dato anche trasferendolo nei sistemi informativi automatizzati di un'altra amministrazione.

copia informatica per consultazione

Firmatario delegato	Responsabile del servizio di conservazione o Persona formalmente delegata ad apporre la propria firma digitale sui Pacchetto di Archiviazione per conto di ARUBA; questa persona può essere interna o esterna ad ARUBA, laddove è giuridicamente possibile.
Formato	Modalità di rappresentazione del documento informatico mediante codifica binaria; comunemente è identificato attraverso l'estensione del file e/o il tipo MIME.
Fornitore esterno	Organizzazione che fornisce ad ARUBA servizi relativi al suo sistema di conservazione dei documenti.
Funzionalità aggiuntive	Le ulteriori componenti del sistema di protocollo informatico necessarie alla gestione dei flussi documentali, alla conservazione dei documenti nonché alla accessibilità delle informazioni.
Funzionalità interoperative	Le componenti del sistema di protocollo informatico finalizzate a rispondere almeno ai requisiti di interconnessione di cui all'articolo 60 del D.P.R. 28 dicembre 2000, n. 445 e s.m.i.
Funzionalità minime	La componente del sistema di protocollo informatico che rispetta i requisiti di operazioni ed informazioni minime di cui all'articolo 56 del D.P.R. 28 dicembre 2000, n. 445 e s.m.i.
Funzione di hash	Una funzione matematica che genera, a partire da una evidenza informatica, una sequenza di bit (impronta) in modo tale che risulti di fatto impossibile, a partire da questa, ricostruire l'evidenza informatica originaria e generare impronte uguali a partire da evidenze informatiche differenti.
Generazione automatica di documento informatico	Formazione di documenti informatici effettuata direttamente dal sistema informatico al verificarsi di determinate condizioni.
Identificativo univoco	Sequenza di caratteri alfanumerici associata in modo univoco e persistente al documento informatico, al fascicolo informatico, all'aggregazione documentale informatica, in modo da consentirne l'individuazione.
Indice di Conservazione (IdC)	L'Indice del Pacchetto di Archiviazione (IPdA)
Indice del Pacchetto di Archiviazione (IPdA)	Indice che contiene le informazioni relative al Pacchetto di Archiviazione in formato xml, anche indicato nello standard SInCRO come IdC (Indice di Conservazione)
Indice del Pacchetto di Versamento (IPdV)	Indice che contiene le informazioni relative al pacchetto di versamento in formato xml.
Immodificabilità	Caratteristica che rende la rappresentazione del documento informatico non alterabile nella forma e nel contenuto durante l'intero ciclo di gestione e ne garantisce la staticità nella conservazione del documento stesso.
Impronta	La sequenza di simboli binari (bit) di lunghezza predefinita generata mediante l'applicazione alla prima di una opportuna funzione di hash.
Insieme minimo di metadati del documento informatico	Complesso dei metadati da associare al documento informatico per identificarne provenienza e natura e per garantirne la tenuta.
Integrità	Insieme delle caratteristiche di un documento informatico che ne dichiarano la qualità di essere completo ed inalterato.
Interoperabilità	Capacità di un sistema informatico di interagire con altri sistemi informatici analoghi sulla base di requisiti minimi condivisi.
Leggibilità	Insieme delle caratteristiche in base alle quali le informazioni contenute nei documenti informatici sono fruibili durante l'intero ciclo di gestione dei documenti.
Log di sistema	Registrazione cronologica delle operazioni eseguite su di un sistema informatico per finalità di controllo e verifica degli accessi, oppure di registro e tracciatura dei cambiamenti che le transazioni introducono in una base di dati.
Manuale di gestione	Strumento che descrive il sistema di gestione informatica dei documenti.

copia informatica per consultazione

Memorizzazione	Processo di trasposizione su un qualsiasi idoneo supporto, attraverso un processo di elaborazione, di documenti analogici o informatici.
Marca temporale	Evidenza informatica che consente di rendere opponibile a terzi un riferimento temporale; la marca temporale prova l'esistenza in un certo momento di una determinata informazione, sotto forma di struttura dati firmata da una Time Stamping Authority.
Metadati	Insieme di dati associati a un documento informatico, o a un fascicolo informatico, o ad un'aggregazione documentale informatica per identificarlo e descriverne il contesto, il contenuto e la struttura, nonché per permetterne la gestione nel tempo nel sistema di conservazione.
Normativa regolante la conservazione digitale di documenti informatici	Si intende: il D.lgs. 7 marzo 2005, n. 82 e s.m.i. (Codice dell'amministrazione Digitale "CAD") e i relativi decreti attuativi, le regole tecniche e aggiungendo, per il documento informatico a rilevanza tributaria, le disposizioni di cui al DMEF 17 giugno 2014 e s.m.i., il DPR 26 ottobre 1972 n. 633 e s.m.i., il DPR 29 settembre 1973 n. 600 e s.m.i., i provvedimenti interpretativi emessi dagli organi competenti.
Originali non unici	I documenti per i quali sia possibile risalire al loro contenuto attraverso altre scritture o documenti di cui sia obbligatoria la conservazione, anche se in possesso di terzi.
Pacchetto di Archiviazione	Pacchetto informativo composto dalla trasformazione di uno o più pacchetti di versamento secondo le specifiche e le modalità riportate nel Manuale di conservazione.
Pacchetto di Distribuzione	Pacchetto informativo inviato dal sistema di conservazione all'utente in risposta ad una sua richiesta.
Pacchetto di invio documenti	Pacchetto informativo utilizzato per inviare i documenti fisici al sistema di conservazione a seguito dell'avvenuta accettazione di un pacchetto di versamento.
Pacchetto di versamento	Pacchetto informativo inviato dal produttore al sistema di conservazione secondo un formato predefinito e concordato descritto nel Manuale di conservazione;
Pacchetto informativo	Contenitore che racchiude uno o più oggetti da conservare (documenti informatici, documenti amministrativi informatici, documenti informatici rilevanti ai fini tributari, fascicoli informatici, aggregazioni documentali informatiche), oppure anche i soli metadati riferiti agli oggetti da conservare.
Piano della sicurezza del sistema di conservazione	Documento che, nel contesto del piano generale di sicurezza, descrive e pianifica le attività volte a proteggere il sistema di conservazione dei documenti informatici da possibili rischi nell'ambito dell'organizzazione di appartenenza.
Piano della sicurezza del sistema di gestione informatica dei documenti	Documento, che, nel contesto del piano generale di sicurezza, descrive e pianifica le attività volte a proteggere il sistema di gestione informatica dei documenti da possibili rischi nell'ambito dell'organizzazione di appartenenza.
Piano di conservazione	Strumento, integrato con il sistema di classificazione per la definizione dei criteri di organizzazione dell'archivio, di selezione periodica e di conservazione ai sensi dell'articolo 68 del D.P.R. 28 dicembre 2000, n. 445 e s.m.i.
Presa in carico	Accettazione da parte del sistema di conservazione di un pacchetto di versamento in quanto conforme alle modalità previste dal Manuale di conservazione;
Processo di conservazione	Insieme delle attività finalizzate alla conservazione dei documenti informatici;
Processo/servizio di marcatura temporale	E' il processo/servizio che associa in modo affidabile un'informazione e un particolare momento, al fine di stabilire prove attendibili che indicano il momento in cui l'informazione esisteva.
Produttore	E' il Cliente, di norma diverso dal Titolare, che in proprio o attraverso le persone fisiche da egli stesso incaricate produce il Pacchetto di versamento ed è responsabile del trasferimento del suo contenuto nel sistema di conservazione; nel caso di Pubblica Amministrazione è identificato nella figura del responsabile della gestione documentale.
Rapporto di versamento	Documento informatico che attesta l'avvenuta presa in carico da parte del sistema di conservazione dei pacchetti di versamento inviati dal produttore.

copia informatica per consultazione

Registrazione informatica	Insieme delle informazioni risultanti da transazioni informatiche o dalla presentazione in via telematica di dati attraverso moduli o formulari resi disponibili in vario modo all'utente.
Registro particolare	Registro informatico specializzato per tipologia o per oggetto; nell'ambito della pubblica amministrazione è previsto ai sensi dell'articolo 53, comma 5 del D.P.R. 28 dicembre 2000, n. 445 e s.m.i.;
Registro di protocollo	Registro informatico della corrispondenza in ingresso e in uscita che permette la registrazione e l'identificazione univoca del documento informatico all'atto della sua immissione cronologica nel sistema di gestione informatica dei documenti.
Referente/i del Cliente	E'/sono le persone fisiche che il Cliente indica ad ARUBA quali punti di riferimento tecnico ed organizzativo per gli aspetti che riguardano le comunicazioni relative all'erogazione del servizio di conservazione.
Repertorio informatico	Registro informatico che raccoglie i dati registrati direttamente dalle procedure informatiche che trattano il procedimento, ordinati secondo un criterio che garantisce l'identificazione univoca del dato all'atto della sua immissione cronologica.
Responsabile della gestione documentale o responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi	Dirigente o funzionario, comunque in possesso di idonei requisiti professionali o di professionalità tecnico archivistica, preposto al servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi.
Responsabile della sicurezza	Soggetto al quale compete la definizione delle soluzioni tecniche ed organizzative in attuazione delle disposizioni in materia di sicurezza.
Riferimento temporale	Informazione contenente la data e l'ora con riferimento al Tempo Universale Coordinato (UTC), della cui apposizione è responsabile il soggetto che forma il documento.
Scarto	Operazione con cui si eliminano, secondo quanto previsto dalla normativa vigente, i documenti ritenuti privi di valore amministrativo e di interesse culturale.
Scheda/e di conservazione	Elenco dei documenti informatici che il Cliente sottopone a conservazione con il Contratto.
Sistema di classificazione	Strumento che permette di organizzare tutti i documenti secondo un ordinamento logico con riferimento alle funzioni e alle attività dell'amministrazione interessata.
Sistema di conservazione	Insieme di hardware, software, politiche, procedure, linee guida, regolamenti interni, infrastrutture fisiche e organizzative, volto ad assicurare la conservazione elettronica dei documenti del Cliente per il periodo di tempo specificato nel Contratto. Detto sistema tratta i documenti informatici in conservazione in pacchetti informativi che si distinguono in pacchetti di versamento, pacchetti di archiviazione e pacchetti di distribuzione;
Sistema di gestione informatica dei documenti	Nell'ambito della pubblica amministrazione è il sistema di cui all'articolo 52 del D.P.R. 28 dicembre 2000, n. 445 e s.m.i.; per i privati è il sistema che consente la tenuta di un documento informatico.
Staticità	Caratteristica che indica l'assenza di tutti gli elementi dinamici, quali macroistruzioni, riferimenti esterni o codici eseguibili, e l'assenza delle informazioni di ausilio alla redazione, quali annotazioni, revisioni, segnalibri, gestite dal prodotto software utilizzato per la redazione;
Transazione informatica	Particolare evento caratterizzato dall'atomicità, consistenza, integrità e persistenza delle modifiche della base di dati.
Testo unico	Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, e successive modificazioni.

copia informatica per consultazione

Titolare/i	La/e persona/e fisica/che o giuridica/che o altro tipo di società o ente che è/sono giuridicamente responsabili/e della formazione dei documenti da conservare formati in proprio ovvero formati da terzi in suo/loro nome, conto e interesse.
Ufficio utente	Riferito ad un area organizzativa omogenea, un ufficio dell'area stessa che utilizza i servizi messi a disposizione dal sistema di protocollo informatico.
Utente	Persona, ente o sistema che interagisce con i servizi di un sistema di gestione informatica dei documenti e/o di un sistema per la conservazione dei documenti informatici, al fine di fruire delle informazioni di interesse.
Validazione temporale	Il risultato della procedura informatica con cui si attribuiscono, ad uno o più documenti informatici, una data ed un orario opponibili ai terzi.
Versamento agli archivi di stato	Operazione con cui il responsabile della conservazione di un'amministrazione statale effettua l'invio agli Archivi di Stato o all'Archivio Centrale dello Stato della documentazione destinata ad essere ivi conservata ai sensi della normativa vigente in materia di beni culturali.

Torna al sommario

copia informatica per consultazione

2.2 Abbreviazioni e termini tecnici

Abbreviazioni e termini tecnici	
Agenzia per l'Italia Digitale (già DigitPA)	Ente pubblico non economico, con competenza nel settore delle tecnologie dell'informazione e della comunicazione nell'ambito della pubblica amministrazione. L'Ente, opera secondo le direttive per l'attuazione delle politiche e sotto la vigilanza del Ministro per la pubblica amministrazione e l'innovazione, con autonomia tecnica e funzionale, amministrativa, contabile, finanziaria e patrimoniale;
ASP - Application Service Provider	Fornitore di Servizi Applicativi;
CAD	Decreto legislativo 7 marzo 2005, n. 82, e successive modificazioni - "Codice dell'amministrazione digitale";
CA - Certificatore Accreditato	Soggetto autorizzato dall'Agenzia per l'Italia Digitale che garantisce l'identità dei soggetti che utilizzano la firma digitale;
CC - Common Criteria	Criteri per la valutazione della sicurezza nei sistemi informatici, con riconoscimento internazionale in quanto evoluzione dei criteri europei (ITSEC), statunitensi (Federal Criteria), e canadesi (Canadian Criteria);
C.M.	Circolare Ministeriale;
CSCD - contratto di servizio di conservazione dei documenti	Contratto di servizio di conservazione dei documenti, ove sono esplicitate chiaramente l'ambito dell'affidamento conferito, le specifiche funzioni, le attività e le responsabilità affidate dal Cliente ad ARUBA;
D.LGS.	Decreto Legislativo;
D.M.	Decreto Ministeriale;
DNS – Domain Name System	Sistema di gestione dei nomi simbolici associati ad indirizzi di siti e domini Internet. Quando un messaggio di posta elettronica (e-mail), o un applicativo di consultazione di siti internet (browser) punta ad un dominio, il DNS traduce il nome inserito sotto forma di URL (es. http//www.....it)/ in un indirizzo costituito da una sequenza numerica convenzionale (es. 123.123.23.3).
D.P.C.M.	Decreto del Presidente del Consiglio dei Ministri;
D.P.R.	Decreto Presidente della Repubblica;
DPS	Documento Programmatico per la Sicurezza;
ETSI	European Telecommunications Standards Institute;
HSM - Hardware Security Module	Dispositivi hardware dedicati per la sicurezza crittografica e la gestione delle chiavi in grado di garantire un elevato livello di protezione;
HTTP (Hypertext Transfer Protocol)	Protocollo di trasmissione, che permette lo scambio di file (testi, immagini grafiche, suoni, video e altri documenti multimediali) su World Wide Web;
HTTPS (Secure Hypertext Transfer Protocol)	Protocollo di trasmissione, sviluppato da Netscape Communications Corporation, per la cifratura e decifratura dei dati trasmessi durante la consultazione di siti e pagine Internet. Corrisponde ad un'estensione del protocollo Internet standard HTTP (Hypertext Transfer Protocol), attraverso il protocollo SSL;
ICT - Information and Communication Technology	Tecnologia dell'Informazione e delle Telecomunicazioni. Il dipartimento che gestisce i sistemi informatici e telematici;
INTERNET	Un sistema globale di reti informatiche nel quale gli utenti di singoli computer possono ottenere informazioni da luoghi diversi. Lo sua grande diffusione è stata determinata principalmente dall'introduzione dei protocolli di trasmissione di documenti con riferimenti ipertestuali (HTTP) e dallo sviluppo del World Wide Web (WWW);
ISO – International Organization for Standardization	Organizzazione internazionale per la standardizzazione, costituita da organismi nazionali provenienti da più di 75 paesi. Ha stabilito numerosi standard nell'area dei sistemi informativi. L'ANSI (American National Standards Institute) è uno dei principali organismi appartenenti all'ISO;

copia informatica per consultazione

ITSEC – Information Technology Security Evaluation Criteria	Criteri europei per la valutazione della sicurezza nei sistemi informatici;
MEF	Ministero dell'Economia e delle Finanze;
NTP – Network Time Protocol	Protocollo per la sincronizzazione del tempo;
OID – Object IDentifier	Sequenza numerica univoca che identifica un oggetto (struttura, algoritmo, parametro, sistema) nell'ambito di una gerarchia generale definita dall'ISO;
PdV	Pacchetto di Versamento
PdA	Pacchetto di Archiviazione
PdD	Pacchetto di Distribuzione
PU	Pubblico Ufficiale
PIN – Personal Identification Number	Codice di sicurezza riservato che permette l'identificazione del soggetto abbinato ad un dispositivo fisico. Permette ad esempio l'attivazione delle funzioni del dispositivo di firma;
POP – Point of Presence	Punto di accesso alla rete internet;
PSCD - Prestatore di Servizi di Conservazione dei Dati	Nella fattispecie, ARUBA;
SSL – Secure Socket Layer	Protocollo standard per la gestione di transazioni sicure su Internet, basato sull'utilizzo di algoritmi crittografici a chiave pubblica;
TSA	***Time Stamping Authority;***
TSS	***Time Stamping Service;***
TUDA - DPR 28 dicembre 2000, n. 445, e successive modificazioni -	***"Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa";***
URL – Uniform Resource Locator	Sistema standard di nomenclatura specificante un sito, dominio o altro oggetto (file, gruppo di discussione, ecc.) su Internet. La prima parte dell'URL (http , ftp, file, telnet, news) specifica il protocollo di accesso all'oggetto;
XML	***Extensible Markup language;***
WWW – World Wide Web	Insieme di risorse interconnesse da hyperlink accessibili tramite Internet

Torna al sommario

copia informatica per consultazione

3 Normativa e standard di riferimento

3.1 Normativa di riferimento

Il sistema di conservazione digitale di ARUBA, è stato realizzato in conformità alla normativa vigente in materia di conservazione dei documenti informatici. Alla data l'elenco dei principali riferimenti normativi italiani in materia, ordinati secondo il criterio della gerarchia delle fonti, è costituito da:

- **Codice Civile** [Libro Quinto Del lavoro, Titolo II Del lavoro nell'impresa, Capo III Delle imprese commerciali e delle altre imprese soggette a registrazione, Sezione III Disposizioni particolari per le imprese commerciali, Paragrafo 2 Delle scritture contabili], articolo 2215 bis - Documentazione informatica;
- **Legge 7 agosto 1990**, n. 241 e s.m.i. – Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi;
- **Decreto del Presidente della Repubblica 28 dicembre 2000**, n. 445 e s.m.i. – Testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa;
- **Regolamento (UE) 2016/679** del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE.
- **Regolamento (UE) N. 910/2014** del Parlamento Europeo e del Consiglio del 23 luglio 2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE
- **Decreto Legislativo 30 giugno 2003, n. 196** e s.m.i. – Codice in materia di protezione dei dati personali;
- **Decreto Legislativo 22 gennaio 2004, n. 42** e s.m.i. – Codice dei Beni Culturali e del Paesaggio;
- **Decreto Legislativo 7 marzo 2005 n. 82** e s.m.i. – Codice dell'amministrazione digitale (CAD);
- **Decreto del Presidente del Consiglio dei Ministri 22 febbraio 2013** – Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma3, lettera b), 35, comma 2, 36, comma 2, e 71;
- **D.M. 17 giugno 2014** - Modalità di assolvimento degli obblighi fiscali relativi ai documenti informatici ed alla loro riproduzione su diversi tipi di supporto - articolo 21, comma 5, del decreto legislativo n. 82/2005;
- **Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013** - Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5-bis, 23-ter, comma 4, 43, commi 1 e 3, 44 , 44-bis e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005;
- **Circolare AGID 10 aprile 2014, n. 65** - Modalità per l'accreditamento e la vigilanza sui soggetti pubblici e privati che svolgono attività di conservazione dei documenti informatici di cui all'articolo 44-bis, comma 1, del decreto legislativo 7 marzo 2005, n. 82.
- **Il DPR nr. 1409 del 30 settembre 1963 -** (Legge archivistica) all'art. 30 prevede che le cartelle cliniche siano conservate illimitatamente. Secondo le norme vigenti, inoltre, gli originali cartacei delle cartelle cliniche in quanto originali unici, non possono essere distrutti;
- **Circolare Ministero della Sanità 19 dicembre 1986, n. 61 -** Circolare avente per oggetto il periodo di conservazione della documentazione sanitaria presso le istituzioni sanitarie pubbliche e private di ricovero e cura
- **DM 14.2.1997 -** Norma di attuazione del D.lgs n.230/95, "Determinazione delle modalità affinché i documenti radiologici e di medicina nucleare e i resoconti esistenti siano resi tempestivamente disponibili per successive esigenze mediche, ai sensi dell'art. 111, comma 10, del decreto legislativo 17 marzo 1995, n. 230"
- **D.lgs 26 maggio 2000, n. 187 -** Attuazione della direttiva 97/43/Euratom in materia di protezione

copia informatica per consultazione

sanitaria delle persone contro i pericoli delle radiazioni ionizzanti connesse ad esposizioni mediche
- **Prontuario di selezione per gli archivi delle aziende sanitarie locali e delle aziende ospedaliere, 2005** Atto di indirizzo che reca indicazioni sui tempi di conservazione dei documenti generati e/o custodita Aziende Sanitarie pubbliche ed accreditate, redatto dal Ministero per i Beni e la Attività Culturali
- **Consiglio dei Ministri – Conferenza Stato Regioni 02 Marzo 2012 -** Linee Guida per la dematerializzazione della documentazione clinica in diagnostica per immagini. Normativa e prassi.

Torna al sommario

3.2 Standard di riferimento

Dove non sono indicate una versione e/o una data specifica, si intende fare riferimento alla più recente versione disponibile del documento citato:

- **ISO 14721:2012 OAIS** (Open Archival Information System), Sistema informativo aperto per l'archiviazione;
- **ISO/IEC 27001:2013**, Information technology - Security techniques - Information security management systems – Requirements, Requisiti di un ISMS (Information Security Management System);
- **ETSI TS 101 533-1 V1.3.1 (2012-04)** Technical Specification, Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part 1: Requirements for Implementation and Management, Requisiti per realizzare e gestire sistemi sicuri e affidabili per la conservazione elettronica delle informazioni;
- **ETSI TR 101 533-2 V1.3.1 (2012-04)**Technical Report, Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part 2: Guidelines for Assessors, Linee guida per valutare sistemi sicuri e affidabili per la conservazione elettronica delle informazioni;
- **UNI 11386:2010 Standard SInCRO** - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali;
- **ISO 15836:2009** Information and documentation - The Dublin Core metadata element set, Sistema di metadata del Dublin Core.
- **Dicom 3.0** (Digital Imaging and Communications in Medicine, immagini e comunicazione digitali in medicina)
- **Health Level 7 (HL7)** versione 2.3.1 e 2.5
- Integrating the Healthcare Enterprise (IHE)
- **UNI ISO 15489-1: 2006** Information and documentation -- Records management -- Part 1: General
- **UNI ISO 15489-2: 2007** Information and documentation—Records management. Part 2: Guidelines
- **ISO 9001:2015** – Quality management systems – Requirements;

Torna al sommario

4 Ruoli e responsabilità

Nel sistema di conservazione si individuano i seguenti ruoli principali:

Ruolo	Organizzazione di appartenenza
Produttore	Cliente
Responsabile della conservazione	Cliente
Referenti del Cliente	Cliente
Responsabile del servizio di conservazione	ARUBA
Utente	Cliente/Terzi autorizzati

copia informatica per consultazione

ARUBA, quale **Responsabile del servizio di conservazione** digitale dei documenti informatici del Cliente, agisce nei limiti dell'affidamento conferito e nell'osservanza degli obblighi ivi previsti nonché nel rispetto della normativa regolante la conservazione digitale di documenti informatici e delle presenti prescrizioni; in particolare, essa agirà attraverso persone fisiche dalla stessa formalmente incaricate.

L'attività di ARUBA riguarda la sola conservazione digitale dei documenti informatici del Cliente, senza alcuna responsabilità e possibilità di intervento ed accesso al contenuto degli stessi.

A carico del Responsabile del servizio di conservazione, non è posto alcun obbligo/dovere di elaborare i documenti informatici versati in conservazione al fine di estrarre i relativi metadati che, pertanto, dovranno essere forniti e associati ai rispettivi documenti a cura e carico del Cliente.

Il Responsabile del servizio di conservazione opera altresì nell'osservanza di quanto stabilito nel presente *Manuale*, al quale, se necessario, è sin da ora autorizzato ad apportare le modifiche, le integrazioni e gli aggiornamenti ritenuti necessari e/o conseguenti al mutato contesto tecnico-giuridico della normativa in materia.

L'utente è il soggetto che richiede al sistema di conservazione l'accesso ai documenti per acquisire le informazioni di interesse nei limiti previsti dalla legge. Tali informazioni vengono fornite dal sistema di conservazione secondo le modalità previste nel presente *Manuale*.

Come già anticipato, il processo di conservazione impone al Cliente l'istituzione di una struttura ed una organizzazione interna, coerente con le proprie politiche di efficienza gestionale, che garantisca la piena osservanza alle disposizioni normative di riferimento e di quanto previsto dal presente *Manuale,* dal *Contratto* e dai rispettivi allegati.

A tale scopo, in base alle specifiche necessità, il Cliente deve, sia dal punto di vista dell'impostazione operativa delle attività propedeutiche alla conservazione digitale dei propri documenti informatici sia dal punto di vista della scelta delle risorse coinvolte nel processo, organizzare il lavoro all'interno della propria organizzazione affinché esso venga svolto secondo i principi stabiliti dalla normativa in materia nonché dalle specifiche regole tecniche.

Tutto il personale di ARUBA è stato assunto nel rispetto di politiche rigorose volte ad accertarne, tra l'altro, l'alto grado di professionalità nonché i requisiti morali e di onorabilità.

Torna al sommario

4.1 Profili professionali all'interno della struttura organizzativa ARUBA

Qui di seguito si da conto della struttura organizzativa del processo di conservazione adottato evidenziando, nel contempo, le funzioni, le responsabilità e gli obblighi dei diversi soggetti che intervengono nel suddetto processo. Il processo di conservazione prevede una serie di attività che implicano il concorso di numerosi soggetti, a differenti livelli e con diverse responsabilità.

Qui di seguito vengono dettagliate per singola attività i diversi compiti e responsabilità delle figure preposte alla gestione e controllo del sistema di conservazione.

Il processo di conservazione, prevede, le seguenti **figure responsabili** :

1. Responsabile del servizio di conservazione;
2. Responsabile della funzione archivistica di conservazione;
3. Responsabile del trattamento dei dati personali, ora Responsabile della protezione dei dati personali (DPO)
4. Responsabile della sicurezza dei sistemi per la conservazione;
5. Responsabile dei sistemi informativi per la conservazione;
6. Responsabile dello sviluppo e della manutenzione del sistema di conservazione

Qui di seguito si riportano le **attività associate a ciascuna delle figure sopra elencate**:

copia informatica per consultazione

- **Responsabile del servizio di conservazione**
  Le attività affidate dal Responsabile della conservazione con l'Atto di Affidamento.

- **Responsabile della funzione archivistica di conservazione**
  Definizione e gestione del processo di conservazione, incluse le modalità di trasferimento da parte del Cliente, di acquisizione, verifica di integrità e descrizione archivistica dei documenti e delle aggregazioni documentali trasferiti, di esibizione, di accesso e fruizione del patrimonio documentario e informativo conservato; definizione del set di metadati di conservazione dei documenti e dei fascicoli informatici; monitoraggio del processo di conservazione e analisi archivistica per lo sviluppo di nuove funzionalità del sistema di conservazione; collaborazione col Cliente ai fini del trasferimento in conservazione, della selezione e della gestione dei rapporti con il Ministero dei beni e delle attività culturali per quanto di competenza.

- **Responsabile del trattamento dei dati personali, ora Responsabile della protezione dei dati personali (DPO)**
  Garanzia del rispetto delle vigenti disposizioni in materia di trattamento dei dati personali; garanzia che il trattamento dei dati affidati dai Clienti avverrà nel rispetto delle istruzioni impartite dal titolare del trattamento dei dati personali, con garanzia di sicurezza e di riservatezza.
  In particolare tenuto a:
  a) informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal Regolamento UE 2016/679 nonché da altre disposizioni relative alla protezione dei dati;
  b) sorvegliare l'osservanza del Regolamento UE 2016/679, di altre disposizioni relative alla protezione dei dati nonché delle politiche del titolare del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
  c) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35 del Regolamento UE 2016/679;
  d) cooperare con l'autorità di controllo; e
  e) fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36 del Regolamento UE 2016/679, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.

  Nell'eseguire i propri compiti il responsabile della protezione dei dati considera debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo.

- **Responsabile della sicurezza dei sistemi per la conservazione**
  Rispetto e monitoraggio dei requisiti di sicurezza del sistema di conservazione stabiliti dagli standard, dalle normative e dalle politiche e procedure interne di sicurezza; segnalazione delle eventuali difformità al Responsabile del servizio di conservazione e individuazione e pianificazione delle necessarie azioni correttive.

- **Responsabile dei sistemi informativi per la conservazione**
  Gestione dell'esercizio delle componenti hardware e software del sistema di conservazione; monitoraggio del mantenimento dei livelli di servizio (SLA) concordati con il fornitore e segnalazione delle eventuali difformità degli SLA al Responsabile del servizio di conservazione e individuazione e pianificazione delle necessarie azioni correttive; pianificazione dello sviluppo delle infrastrutture tecnologiche del sistema di conservazione; controllo e verifica dei livelli di servizio erogati da terzi con segnalazione delle eventuali difformità al Responsabile del servizio di conservazione.

- **Responsabile dello sviluppo e della manutenzione del sistema di conservazione**
  Coordinamento dello sviluppo e manutenzione delle componenti hardware e software del sistema di conservazione; pianificazione e monitoraggio dei progetti di sviluppo del sistema di conservazione;

copia informatica per consultazione

monitoraggio degli SLA relativi alla manutenzione del sistema di conservazione; interfaccia col Cliente relativamente alle modalità di trasferimento dei documenti e fascicoli informatici in merito ai formati elettronici da utilizzare, all'evoluzione tecnologica hardware e software, alle eventuali migrazioni verso nuove piattaforme tecnologiche; gestione dello sviluppo di siti web e portali connessi al servizio di conservazione.

Ciascuno dei responsabili sopra elencati può avvalersi, per lo svolgimento delle attività al medesimo attribuite, di addetti ed operatori formalmente incaricati.

Nella pagina seguente sono riportati i dati dei soggetti che nel tempo hanno assunto particolari funzioni e responsabilità con riferimento al sistema di conservazione.

copia informatica per consultazione

Ruoli e responsabilità					
Ruolo	**Cognome**	**Nome**	**Responsabilità**	**Data nomina**	**Data cessazione**
Responsabile del servizio di conservazione	Braccagni	Simone	Definizione e attuazione delle politiche complessive del sistema di conservazione, nonché del governo della gestione del sistema di conservazione; definizione delle caratteristiche e dei requisiti del sistema di conservazione in conformità alla normativa vigente; corretta erogazione del servizio di conservazione al Cliente; gestione delle convenzioni, definizione degli aspetti tecnico-operativi e validazione dei disciplinari tecnici che specificano gli aspetti di dettaglio e le modalità operative di erogazione dei servizi di conservazione.	01/09/2014	
Responsabile della funzione archivistica di conservazione	Boschi	Serena	Definizione e gestione del processo di conservazione, incluse le modalità di trasferimento da parte del Cliente, di acquisizione, verifica di integrità e descrizione archivistica dei documenti e delle aggregazioni documentali trasferiti, di esibizione, di accesso e fruizione del patrimonio documentario e informativo conservato; definizione del set di metadati di conservazione dei documenti e dei fascicoli informatici; monitoraggio del processo di conservazione e analisi archivistica per lo sviluppo di nuove funzionalità del sistema di conservazione; collaborazione col Cliente ai fini del trasferimento in conservazione, della selezione e della gestione dei rapporti con il Ministero dei beni e delle attività culturali per quanto di competenza.	01/09/2014	
Responsabile del trattamento dei dati personali, ora Responsabile della protezione dei dati personali (DPO)	Giommoni	Roberta	Garanzia del rispetto delle vigenti disposizioni in materia di trattamento dei dati personali; garanzia che il trattamento dei dati affidati dai Clienti avverrà nel rispetto delle istruzioni impartite dal titolare del trattamento dei dati personali, con garanzia di sicurezza e di riservatezza.In particolare tenuto a: a) informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal Regolamento UE 2016/679 nonché da altre disposizioni relative alla protezione dei dati; b) sorvegliare l'osservanza del Regolamento UE 2016/679, di altre disposizioni relative alla protezione dei dati nonché delle politiche del titolare del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo; c) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35 del Regolamento UE 2016/679; d) cooperare con l'autorità di controllo; e e) fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36 del Regolamento UE 2016/679, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione. Nell'eseguire i propri compiti il responsabile della protezione dei dati considera debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo.	24/05/2018	

copia informatica per consultazione

Responsabile del trattamento dei dati personali	Braccagni	Simone	Garanzia del rispetto delle vigenti disposizioni in materia di trattamento dei dati personali; garanzia che il trattamento dei dati affidati dai Clienti avverrà nel rispetto delle istruzioni impartite dal titolare del trattamento dei dati personali, con garanzia di sicurezza e di riservatezza.	01/09/2014	23/05/2018
Responsabile della sicurezza dei sistemi per la conservazione	Corsi	Matteo	Rispetto e monitoraggio dei requisiti di sicurezza del sistema di conservazione stabiliti dagli standard, dalle normative e dalle politiche e procedure interne di sicurezza; segnalazione delle eventuali difformità al Responsabile del servizio di conservazione e individuazione e pianificazione delle necessarie azioni correttive.	06/09/2017	
	Santoni	Adriano	Come sopra	01/09/2014	05/09/2017
Responsabile dei sistemi informativi per la conservazione	Gaverini	Angelo	Gestione dell'esercizio delle componenti hardware e software del sistema di conservazione; monitoraggio del mantenimento dei livelli di servizio (SLA) concordati con il fornitore; segnalazione delle eventuali difformità degli SLA al Responsabile del servizio di conservazione e individuazione e pianificazione delle necessarie azioni correttive; pianificazione dello sviluppo delle infrastrutture tecnologiche del sistema di conservazione; controllo e verifica dei livelli di servizio erogati da terzi con segnalazione delle eventuali difformità al Responsabile del servizio di conservazione.	06/09/2017	
	Ravazza	Roberto	Come sopra	01/09/2014	05/09/2017
Responsabile dello sviluppo e della manutenzione del sistema di conservazione	Mauro	Manetti	Coordinamento dello sviluppo e manutenzione delle componenti hardware e software del sistema di conservazione; pianificazione e monitoraggio dei progetti di sviluppo del sistema di conservazione; monitoraggio degli SLA relativi alla manutenzione del sistema di conservazione; interfaccia col Cliente relativamente alle modalità di trasferimento dei documenti e fascicoli informatici in merito ai formati elettronici da utilizzare, all'evoluzione tecnologica hardware e software, alle eventuali migrazioni verso nuove piattaforme tecnologiche; gestione dello sviluppo di siti web e portali connessi al servizio di conservazione.	06/09/2017	
	Pulvirenti	Salvatore	Come sopra	01/09/2014	05/09/2017

Torna al sommario

copia informatica per consultazione

5 Struttura organizzativa per il servizio di conservazione

In questo capitolo sono indicate le strutture organizzative coinvolte nel servizio di conservazione comprese le responsabilità, che intervengono nelle principali funzioni che riguardano il servizio di conservazione

5.1 Organigramma

La figura in basso riporta le strutture organizzative coinvolte nel servizio di conservazione:

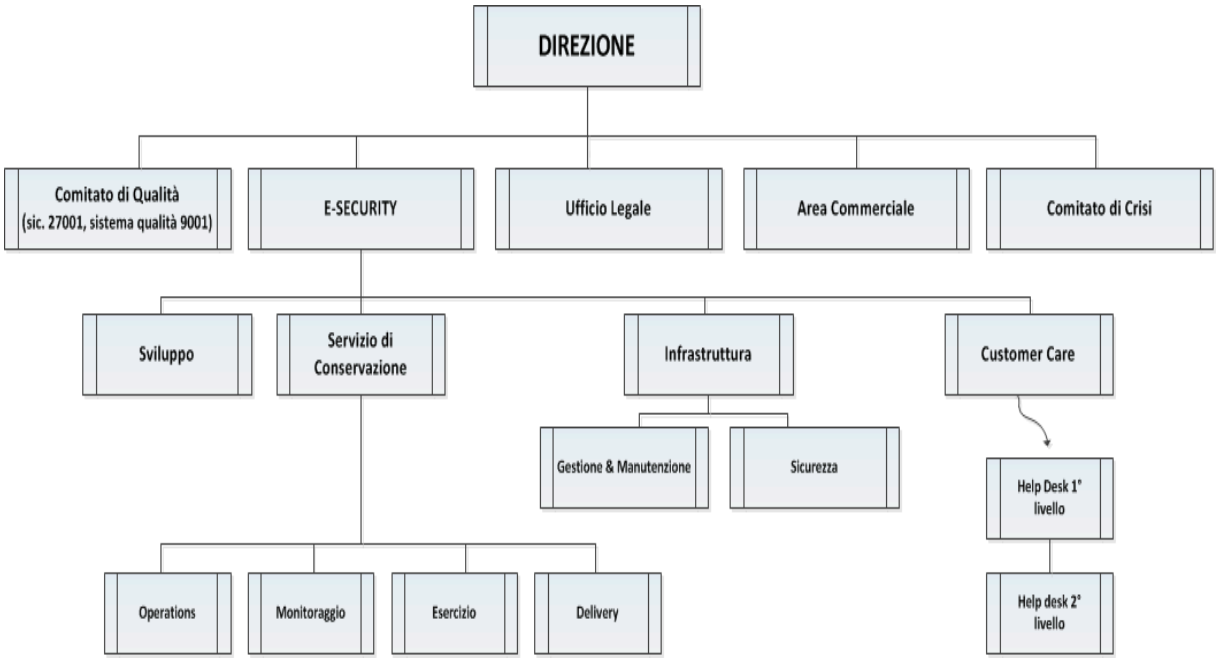


Figura 1: Rappresentazione delle strutture organizzative coinvolte nel servizio di conservazione

Torna al sommario

5.2 Strutture organizzative

Nello specifico le strutture funzionali dell'organizzazione operano in sinergia come segue:

- **Direzione**
  - ✓ la Direzione Aziendale garantisce la continuità generale dell'organizzazione
- **Comitato di Qualità**
  - ✓ garantisce la qualità operativa dei servizi ed il miglioramento di processi/procedure
- **E-Security**
  - ✓ rappresenta la Business Line che si occupa dei servizi e soluzioni di sicurezza in ambito digitale
- **Ufficio legale**
  - ✓ garantisce la verifica periodica di conformità a normativa e standard di riferimento

copia informatica per consultazione

- **Area Commerciale**
  - ✓ promuove il servizio di conservazione ai clienti
  - ✓ fornisce il supporto ai clienti in fase di prevendita (pre-sales)
  - ✓ partecipa attivamente al miglioramento dei servizi erogati in termini di definizione dell'offerta
- **Infrastruttura**
  - ✓ garantisce la sicurezza degli accessi logici e fisici, predisponendo appositi asset nel perimetro del data center
  - ✓ garantisce la sicurezza dell'infrastruttura tramite sistemi dedicati (video-sorveglianza, anti-intrusione, anti-incendio, etc)
  - ✓ designa, gestisce e provvede alla manutenzione delle aree sicure
- **Sviluppo**
  - ✓ fornisce know-how e supporto per lo sviluppo dei sistemi informativi
  - ✓ provvede alla progettazione di nuovi servizi e fornisce supporto per la manutenzione dei servizi attivi
  - ✓ si occupa dello studio di fattibilità per l'implementazione di nuovi servizi
  - ✓ fornisce interventi di analisi ed attività di assistenza nella fase di pre-vendita dei servizi
- **Servizio di Conservazione**
  - ✓ garantisce la gestione degli asset (hardware e software), occupandosi dell'intero processo di supply-chain del servizio di conservazione
  - ✓ provvede alla gestione delle informazioni, per l'intero ciclo di vita (dalla classificazione, al monitoraggio del sistema, fino alla protezione dei log)
  - ✓ si occupa della manutenzione ed assistenza, a garanzia della continuità operativa del servizio di conservazione
  - ✓ garantisce l'esecuzione del processo di conservazione in conformità ai requisiti tecnici normativi
  - ✓ provvede alla gestione operativa degli accessi logici e fisici, seguendo apposite procedure e mantenendo aggiornata la documentazione
  - ✓ garantisce l'attivazione e consegna dei servizi ai clienti, rispettando KPI e SLA concordati
- **Customer Care**
  - ✓ provvede all'assistenza tecnica rivolta ai clienti proprietari dei servizi
  - ✓ fornisce il supporto operativo sui servizi dei clienti
  - ✓ partecipa al miglioramento dei processi di comunicazione verso i clienti

Torna al sommario

copia informatica per consultazione

5.3 Responsabilità e funzioni nel processo di conservazione

Di seguito sono indicati i compiti, le responsabilità e le funzioni di firma in relazione alle diverse fasi del processo di conservazione digitale.

Fasi del processo	Descrizione delle fasi del processo di conservazione		COMPITI	RESPONSABILITA'	FIRMA
FASE 1	**Acquisizione da parte del sistema di conservazione del pacchetto di versamento per la sua presa in carico**				
	Descrizione sintetica	Il sistema di conservazione riceve l'indice del pacchetto di versamento contenente le informazioni sugli oggetti digitali che saranno inviati in conservazione.	**SC**	**RMGO**	**==**
FASE 2	**Verifica che il pacchetto di versamento e gli oggetti contenuti siano coerenti con le modalità previste nel presente Manuale di conservazione e con i formati di conservazione**				
	Descrizione sintetica	Viene verificato che l'oggetto ricevuto sia formalmente un indice xml in linea con lo standard DocFly. Viene verificato che il PdV è versato nei termini contrattuali e di servizio stabiliti col produttore	**SC**	**RMGO**	**==**
FASE 3	**Preparazione del rapporto di conferma**				
	Descrizione sintetica	Il sistema, una volta effettuate le verifiche dell'idPdV rimane in attesa dell'invio dei documenti	**SC**	**RMGO**	**==**
FASE 4	**Eventuale rifiuto del pacchetto di versamento, nel caso in cui le verifiche di cui alla FASE 2 abbiano evidenziato anomalie e/o non conformità**				
	Descrizione sintetica	Il sistema scarta l'intero pacchetto e invia notifica in automatico	**SC**	**RMGO**	**==**
FASE 5	**Ricezione e verifica dei documenti**				
	Descrizione sintetica	Per ognuno di documenti inviati viene verificato che l'hash del documento informatico sia corrispondente all'hash dichiarato all'interno del medesimo indice del pacchetto al fine di avere garanzia che la trasmissione del pacchetto sia avvenuta correttamente e che l'integrità del documento informatico ricevuto sia assicurata. Vengono inoltre effettuati controlli di leggibilità, integrità e che i documenti non siano già presenti a sistema	**SC**	**RMGO**	**==**
FASE 7	**Generazione automatica del rapporto di versamento relativo a ciascun pacchetto di versamento, univocamente identificato dal sistema di conservazione e contenente un riferimento temporale, specificato con riferimento al Tempo Universale Coordinato (UTC), e una o più impronte, calcolate sull'intero contenuto del pacchetto di versamento, secondo le modalità di seguito descritte**				
	Descrizione sintetica	Il sistema genera in automatico il rapporto di versamento per ognuno dei PdV che ha superato i controlli qualitativi	**SC**	**RMGO**	**==**
FASE 8	**Sottoscrizione del rapporto di versamento con firma digitale apposta da ARUBA**				
	Descrizione sintetica	Il sistema provvede in automatico alla sottoscrizione digitale del rapporto di versamento con certificato del RSC e alla marcatura temporale del rapporto.	**SC**	**RMGO**	**RSC**
FASE 9	**Preparazione e gestione del Pacchetto di Archiviazione (c.d. Pacchetto di Archiviazione)**				

copia informatica per consultazione

	Descrizione sintetica	Il sistema genera il Pacchetto di Archiviazione secondo le modalità descritte al cap. 7	**SC**	**RMGO**	**==**
FASE 10	**Sottoscrizione del Pacchetto di Archiviazione con firma digitale apposta da ARUBA e apposizione di una validazione temporale con marca temporale alla relativa impronta. Tale operazione viene in breve chiamata anche "Chiusura del Pacchetto di Archiviazione"**				
	Descrizione sintetica	Come previsto da normativa l'Indice di Conservazione, viene sottoscritto digitalmente dal RSC, una volta passato nello stato "conservato".	**SC**	**RMGO**	**RSC**
FASE 11	**Preparazione e sottoscrizione con firma digitale del Responsabile del servizio di conservazione del Pacchetto di Distribuzione ai fini dell'esibizione richiesta dall'utente**				
	Descrizione sintetica	Come previsto da normativa il PdD viene sottoscritto digitalmente dal RSC	**SC**	**RER**	**RSC**
FASE 12	**Produzione di duplicati informatici o di copie informatiche effettuati su richiesta del Cliente in conformità a quanto previsto dalle regole tecniche in materia di formazione del documento informatico**				
	Descrizione sintetica	Richieste di duplicati o copie informatiche vengono sottoscritte digitalmente dal RSC in modo da attestarne l'autenticità rispetto al documento sorgente	**SC**	**RER**	**RSC**
FASE 13	**Eventuale scarto del Pacchetto di Archiviazione dal sistema di conservazione alla scadenza dei termini di conservazione previsti dal contratto di servizio, dandone preventiva informativa al Cliente al fine di raccoglierne il consenso**				
	Descrizione sintetica	Una volta scaduti i termini di conservazione previsti dal contratto, il sistema provvede a inviare una mail di notifica al client, il quale potrà decidere in autonomia se cancellarli dal sistema.	**SC**	**RCD** **DPO**	**==**

Legenda:
- **RMGO** - responsabile del monitoraggio della gestione ordinaria del sistema e dei processi di base di conservazione
- **RER** - responsabile dell'esibizione/restituzione dei documenti informatici conservati
- **RIS** - responsabile dell'infrastruttura sistemistica, del piano di Disaster Recovery / Piano di continuità operativa (Business Continuity Plan) e della sicurezza
- **RCD** - responsabile della cancellazione dei documenti e dei dati digitali
- **DPO** - responsabile della protezione dei dati personali
- **RSC** - responsabile del servizio di conservazione
- **SC** - Sistema di conservazione

Torna al sommario

copia informatica per consultazione

6 Oggetti sottoposti a conservazione

6.1 Descrizione delle tipologie dei documenti sottoposti a conservazione

Come chiaramente esplicitato nel *Contratto*, il servizio di conservazione digitale dei documenti informatici non riguarda la conservazione di documenti analogici di alcun tipo e genere.

Prima dell'attivazione del servizio il Cliente esplicita la tipologia di documenti che intende sottoporre a conservazione mediante il servizio offerto da ARUBA, evidenziandone le caratteristiche nell'apposito allegato del *Contratto*.

Per ogni formato definito viene individuato anche il **software necessario per la visualizzazione** del documento informatico.

ARUBA configura sul servizio un profilo di conservazione per ogni tipologia/classe di documenti su indicazione del Cliente, classificato come omogeneo in base ai dati da utilizzare per l'indicizzazione ed i termini di conservazione (vedi apposito allegato al *Contratto*).

Ogni variazione di formato di documento e di software associato per la visualizzazione oppure dei dati utilizzati per l'indicizzazione deve essere preventivamente concordato con ARUBA e configurato sul servizio.

Il sistema di conservazione digitale è impostato per accettare le seguenti tipologie di documento:

- **documenti informatici** sono la "rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti" come definito dal Codice dell'Amministrazione Digitale;
- **documenti amministrativi** costituenti atti amministrativi con rilevanza interna al procedimento amministrativo;
- **documenti rilevanti ai fini tributari** come stabilito nel DM del MEF del 17 giugno 2014;
- **documenti clinici** che possono contenere informazioni su osservazioni cliniche dirette, quali rivelazioni di anamnesi, segni vitali o sintomi, osservazioni indirette, derivanti, ad esempio da diagnostica strumentale, esami di laboratorio o rappresentazione iconografica di resoconti radiologici, oppure opinioni mediche quali valutazioni di osservazioni cliniche, consulti e consulenze, obiettivi da raggiungere o piani diagnostico terapeutici, azioni di natura clinico-sanitaria atte a generare osservazioni cliniche ed opinioni mediche;
- **altri documenti in genere**

Le diverse tipologie di documenti sono prodotti/formati/emessi a cura e sotto l'esclusiva responsabilità del Cliente mediante una delle seguenti principali modalità:

a) redazione tramite l'utilizzo di appositi strumenti software;
b) acquisizione di un documento informatico per via telematica o su supporto informatico, acquisizione della copia per immagine su supporto informatico di un documento analogico, acquisizione della copia informatica di un documento analogico;
c) registrazione informatica delle informazioni risultanti da transazioni o processi informatici o dalla presentazione telematica di dati attraverso moduli o formulari;
d) generazione o raggruppamento anche in via automatica di un insieme di dati o registrazioni, provenienti da una o più basi dati, anche appartenenti a più soggetti interoperanti, secondo una struttura logica predeterminata e memorizzata in forma statica.

Al fine di garantire l'identificazione certa del soggetto che ha formato il documento, i documenti informatici posti in conservazione saranno in genere sottoscritti con firma digitale del Cliente e dovranno essere identificati in modo univoco e persistente.

E' prevista la possibilità di depositare in conservazione documenti informatici non sottoscritti. In tal caso deve necessariamente essere preventivamente dichiarata, per ogni classe/tipo di documento, nell'apposito allegato del *Contratto*.

Torna al sommario

copia informatica per consultazione

6.2 Copie informatiche di documenti analogici originali unici

Come noto, l'art. 22 del CAD stabilisce che:

a) (comma 2) le copie per immagine su supporto informatico di documenti originali formati in origine su supporto analogico hanno la stessa efficacia probatoria degli originali da cui sono estratte, se la loro conformità è attestata da un notaio o da altro pubblico ufficiale a ciò autorizzato, con dichiarazione allegata al documento informatico e asseverata secondo le regole tecniche stabilite ai sensi dell'articolo 71.
b) (comma 3) le copie per immagine su supporto informatico di documenti originali formati in origine su supporto analogico nel rispetto delle regole tecniche di cui all'articolo 71 hanno la stessa efficacia probatoria degli originali da cui sono tratte se la loro conformità all'originale non è espressamente disconosciuta.

Pertanto, alla luce di quanto sopra, il Cliente qualora intendesse depositare in conservazione copie per immagine su supporto informatico di documenti originali formati in origine su supporto analogico è tenuto, a propria cura e spese, a predisporre quanto necessario per ottemperare a quanto previsto dalle richiamate disposizioni.

In particolare, sarà cura e carico del Cliente:

a) produrre la copia per immagine su supporto informatico del documento analogico mediante processi e strumenti che assicurino che il documento informatico abbia contenuto e forma identici a quelli del documento analogico da cui è tratto;

successivamente:

b) (ai fini di quanto stabilito dall'articolo 22, co. 3, del CAD), dovrà sottoscrivere con firma digitale la copia per immagine del documento analogico;

oppure

c) laddove richiesto dalla natura dell'attività, (art. 22, comma 2, del CAD), dovrà inserire nel documento informatico contenente la copia per immagine, l'attestazione di conformità all'originale analogico. Il documento informatico così formato dovrà poi essere sottoscritto con firma digitale del notaio o con firma digitale o firma elettronica qualificata di pubblico ufficiale a ciò autorizzato.

Si tenga presente che l'attestazione di conformità delle copie per immagine su supporto informatico di uno o più documenti analogici, effettuata per raffronto dei documenti o attraverso certificazione di processo nei casi in cui siano adottate tecniche in grado di garantire la corrispondenza della forma e del contenuto dell'originale e della copia, può essere prodotta, sempre a cura e carico del Cliente, come documento informatico separato contenente un riferimento temporale e l'impronta di ogni copia per immagine. Tale documento informatico separato dovrà essere sottoscritto con firma digitale del notaio o con firma digitale o firma elettronica qualificata del pubblico ufficiale a ciò autorizzato.

In sostanza, in questi casi il Cliente dovrà alternativamente depositare in conservazione:

- la copia per immagine su supporto informatico dell'originale analogico contenente l'attestazione di conformità all'originale analogico debitamente sottoscritto come sopra riportato;

oppure

- le copie per immagine su supporto informatico unitamente all'attestazione di conformità prodotta come documento informatico separato contenente un riferimento temporale e l'impronta di ogni singola copia per immagine, debitamente sottoscritto come sopra riportato.

Torna al sommario

copia informatica per consultazione

6.3 Formati gestiti

Come noto, la leggibilità di un documento informatico dipende dalla possibilità e dalla capacità di interpretare ed elaborare correttamente i dati binari che costituiscono il documento, secondo le regole stabilite dal formato con cui esso è stato rappresentato. Il formato di un documento informatico è la convenzione usata per rappresentare il contenuto informativo mediante una sequenza di byte.

Il sistema di conservazione ARUBA garantisce la conservazione dei documenti prodotti nei formati previsti dall'allegato 2 "Formati" del DPCM 03-12-2013.

I formati ammessi alla conservazione, devono essere specificati dal Cliente prima del versamento in conservazione e per tale ragione vengono esplicitati all'interno di uno specifico allegato, facente parte del Contratto di servizio stipulato con ARUBA (come descritto al par 10.1.2).

Torna al sommario

6.3.1 Caratteristiche generali dei formati

I formati scelti devono essere, puntualmente richiamati nell'apposito allegato al *Contratto.* ARUBA, comunque raccomanda un insieme di formati che sono stati dalla stessa valutati in funzione di alcune caratteristiche quali:

CARATTERISTICA		DESCRIZIONE DELLA CARATTERISTICA
1	**APERTURA**	Un formato si dice "aperto" quando è conforme a specifiche pubbliche, cioè disponibili a chiunque abbia interesse ad utilizzare quel formato. La disponibilità delle specifiche del formato rende sempre possibile la decodifica dei documenti rappresentati in conformità con dette specifiche, anche in assenza di prodotti che effettuino tale operazione automaticamente. Questa condizione si verifica sia quando il formato è documentato e pubblicato da un produttore o da un consorzio al fine di promuoverne l'adozione, sia quando il documento è conforme a formati definiti da organismi di standardizzazione riconosciuti. In quest'ultimo caso tuttavia si confida che quest'ultimi garantiscono l'adeguatezza e la completezza delle specifiche stesse. In relazione a questo aspetto, ARUBA ha privilegiato formati già approvati dagli Organismi di standardizzazione internazionali quali ISO e OASIS.
2	**SICUREZZA**	La sicurezza di un formato dipende da due elementi: - il grado di modificabilità del contenuto del file; - la capacità di essere immune dall'inserimento di codice maligno.
3	**PORTABILITÀ**	Per portabilità si intende la facilità con cui i formati possano essere usati su piattaforme diverse, sia dal punto di vista dell'hardware che del software, inteso come sistema operativo. Di fatto si ottiene mediante l'impiego fedele di standard documentati e accessibili e dalla loro diffusione sul mercato.
4	**FUNZIONALITÀ**	Per funzionalità si intende la possibilità da parte di un formato di essere gestito da prodotti informatici, che prevedono una varietà di funzioni messe a disposizione del Cliente per la formazione e gestione del documento informatico.
5	**SUPPORTO ALLO SVILUPPO**	Il supporto allo sviluppo è la modalità con cui si mettono a disposizione le risorse necessarie alla manutenzione e sviluppo del formato e i prodotti informatici che lo gestiscono (organismi preposti alla definizione di specifiche tecniche e standard, società, comunità di sviluppatori, ecc.).
6	**DIFFUSIONE**	La diffusione è l'estensione dell'impiego di uno specifico formato per la formazione e la gestione dei documenti informatici. Questo elemento influisce sulla probabilità che esso venga supportato nel tempo, attraverso la disponibilità di più prodotti informatici idonei alla sua gestione e visualizzazione.

Torna al sommario

6.3.2 Formati consigliati per la conservazione

Oltre al soddisfacimento delle caratteristiche suddette, nella scelta dei formati idonei alla conservazione, ARUBA è stata estremamente attenta affinché i formati stessi fossero capaci a far assumere al documento le fondamentali caratteristiche di immodificabilità e staticità.
Pertanto, alla luce delle suddette considerazioni, **i formati indicati dalla normativa** per la conservazione delle diverse tipologie di documenti informatici sono i seguenti:

copia informatica per consultazione

FORMATO	DESCRIZIONE	
PDF - PDF/A	Il PDF (Portable Document Format) è un formato creato da Adobe nel 1993 che attualmente si basa sullo standard ISO 32000. Questo formato è stato concepito per rappresentare documenti complessi in modo indipendente dalle caratteristiche dell'ambiente di elaborazione del documento. Il formato è stato ampliato in una serie di sotto-formati tra cui il PDF/A.	
	Caratteristiche e dati informativi	
	Informazioni gestibili	Testo formattato, immagini, grafica vettoriale 2D e 3D, filmati.
	Sviluppato da	Adobe Systems - http://www.adobe.com/
	Estensione	.pdf
	Tipo MIME	Application/pdf
	Formato aperto	SI
	Specifiche tecniche	Pubbliche
	Standard	ISO 32000-1 (PDF) ISO 19005-1:2005 (vers. PDF 1.4) ISO 19005-2:2011 (vers. PDF 1.7)
	Altre caratteristiche	Assenza di collegamenti esterni
		Assenza di codici eseguibili
		Assenza di contenuti crittografati
		Il file risulta indipendente da codici e collegamenti esterni che ne possono alterare l'integrità e l'uniformità nel lungo periodo
		Le più diffuse suite d'ufficio permettono di salvare direttamente i file nel formato PDF/A
		Sono disponibili prodotti per la verifica della conformità di un documento PDF al formato PDF/A.
	Software necessario alla visualizzazione	Adobe Reader

FORMATO	DESCRIZIONE	
TIFF	Il TIFF è un formato utilizzato per la rappresentazione delle immagini mediante grafica raster (l'immagine digitale è formata da un insieme pixel, ordinate secondo linee e colonne).	
	Caratteristiche e dati informativi	
	Informazioni gestibili	Immagini
	Sviluppato da	Aldus Corporation in seguito acquistata da Adobe
	Estensioni	.tif
	Tipo MIME	image/tiff
	Formato aperto	NO
	Specifiche tecniche	Pubbliche
	Ultime versioni	TIFF 6.0 del 1992 TIFF Supplement 2 del 2002
	Standard	ISO 12639 (TIFF/IT) ISO 12234 (TIFF/EP)
	Altre caratteristiche	Formato immagine raster, in versione non compressa o compressa senza perdita di informazione
		Formato utilizzato per la conversione in digitale di documenti cartacei
		Esistono parecchie versioni, alcune delle quali proprietarie (che ai fini della conservazione nel lungo periodo sarebbe bene evitare)
		In genere le specifiche sono pubbliche e non soggette ad alcuna forma di limitazione
	Software necessario alla visualizzazione	ImageGlass

copia informatica per consultazione

FORMATO	DESCRIZIONE	
JPG	Il JPG è un formato utilizzato per la rappresentazione delle immagini mediante grafica raster (l'immagine digitale è formata da un insieme pixel, ordinate secondo linee e colonne).	
	Caratteristiche e dati informativi	
	Informazioni gestibili	Immagini
	Sviluppato da	Joint Photographic Experts Group
	Estensioni	.jpg, .jpeg
	Tipo MIME	image/jpeg
	Formato aperto	SI
	Specifiche tecniche	Pubbliche
	Ultima versione	2009
	Standard	ISO/IEC 10918:1
	Altre caratteristiche	Formato immagine raster, in versione compressa. Può comportare una perdita di qualità dell'immagine originale.
		JPG è il formato più utilizzato per la memorizzazione di fotografie ed è quello più comune su World Wide Web.
		Lo stesso gruppo che ha ideato il JPG ha prodotto il JPEG 2000 con estensione .jp2 (ISO/IEC 15444-1) che può utilizzare la compressione senza perdita di informazione. Il formato JPEG 2000 consente, inoltre, di associare metadati ad un'immagine. Nonostante queste caratteristiche la sua diffusione è tutt'oggi relativa.
	Software necessario alla visualizzazione	ImageGlass

FORMATO	DESCRIZIONE	
Office Open XML (OOXML)	Offine Open XML, comunemente abbreviato in OOXML, è un formato di file, sviluppato da Microsoft, basato sul linguaggio XML per la creazione di documenti di testo, fogli di calcolo, presentazioni, grafici e database.	
	Caratteristiche e dati informativi	
	Informazioni gestibili	Documenti di testo, fogli di calcolo, presentazioni, grafici e database
	Sviluppato da	Microsoft
	Estensioni principali	.docx, .xlsx, .pptx
	Tipo MIME	application/vnd.openxmlformats-officedocument.wordprocessingml.document,application/x-tika-ooxml,application/zip application/vnd.ms-powerpoint,application/vnd.openxmlformats-officedocument.presentationml.template,application/vnd.ms-powerpoint.addin.macroEnabled.12,application/vnd.ms-powerpoint.presentation.macroEnabled.12,application/vnd.ms-powerpoint.template.macroEnabled.12,application/vnd.ms-powerpoint.slideshow.macroEnabled.12 application/vnd.ms-excel,application/vnd.openxmlformats-officedocument.spreadsheetml.template,application/vnd.ms-excel.sheet.macroEnabled.12,application/vnd.ms-excel.template.macroEnabled.12,application/vnd.ms-excel.addin.macroEnabled.12,application/vnd.ms-excel.sheet.binary.macroEnabled.12,application/x-tika-msoffice application/vnd.openxmlformats-officedocument.spreadsheetml.sheet,application/x-tika-ooxml
	Formato aperto	SI
	Specifiche tecniche	Pubblicate da Microsoft dal 2007
	Ultima versione	1.1
	Standard	ISO/IEC DIS 29500:2008
	Altre caratteristiche	Open XML è adottato dalla versione 2007 della suite Office di Microsoft
		MS Office 2007 legge e scrive file conformi a ECMA-376 Edition 1
		MS Office 2010 legge e scrive file conformi a ISO/IEC 29500:2008 transitional (norme transitorie) e legge file conformi a ISO/IEC 29500:2008 strict (indicazioni fondamentali)

copia informatica per consultazione

		Documenti conformi ad ISO/IEC 29500:2008 strict sono supportati da diversi prodotti informatici disponibili sul mercato
		Il formato Office Open XML dispone di alcune caratteristiche che lo rendono adatto alla conservazione nel lungo periodo, tra queste l'embedding dei font, la presenza di indicazioni di presentazione del documento, la possibilità di applicare al documento la firma digitale XML.
		I metadati associabili ad un documento che adotta tale formato sono previsti dallo standard ISO 29500:2008
	Software necessario alla visualizzazione	https://openxmlviewer.codeplex.com/

FORMATO	**DESCRIZIONE**	
Open Document Format	ODF (Open Document Format, spesso referenziato con il termine OpenDocument) è uno standard aperto, basato sul linguaggio XML, sviluppato dal consorzio OASIS per la memorizzazione di documenti corrispondenti a testo, fogli elettronici, grafici e presentazioni.	
	Caratteristiche e dati informativi	
	Informazioni gestibili	Documenti di testo, fogli di calcolo, presentazioni e grafici.
	Sviluppato da	OASIS
	Estensioni principali	.ods, .odp, .odg, .odb
	Tipo MIME	application/vnd.oasis.opendocument.text
	Formato aperto	SI
	Specifiche tecniche	Pubblicate da OASIS dal 2005
	Ultima versione	1.0
	Standard	ISO/IEC 26300:2006 UNI CEI ISO/IEC 26300
	Altre caratteristiche	Formato basato sul linguaggio XML
		Un documento è descritto da più strutture XML, relative a contenuto, stili, metadati ed informazioni per l'applicazione
		Lo standard ISO/IEC IS 26300:2006 è ampiamente usato come standard documentale nativo, oltre che da OpenOffice.org, da una ampia serie di altri prodotti disponibili sulle principali piattaforme: Windows, Linux. Mac.
		È stato adottato come standard di riferimento da moltissime organizzazioni governative e da diversi governi ed ha una "penetrazione" di mercato che cresce giorno per giorno.
	Software necessario alla visualizzazione	Open Office

FORMATO	**DESCRIZIONE**	
XML	Extensible Markup Language (XML) è un formato di testo flessibile derivato da SGML (ISO 8879). Su XML si basano numerosi linguaggi standard utilizzati nei più diversi ambiti applicativi. Ad esempio: SVG usato nella descrizione di immagini vettoriali, XBRL usato nella comunicazione di dati finanziari, ebXML usato nel commercio elettronico, SOAP utilizzato nello scambio dei messaggi tra Web Service	
	Caratteristiche e dati informativi	
	Informazioni gestibili	Contenuto di evidenze informatiche, dei pacchetti di versamento, archiviazione e distribuzione, ecc.
	Sviluppato da	W3C - http://www.w3.org/
	Estensione	.xml
	Tipo MIME	Application/xml Text/xml
	Formato aperto	SI
	Specifiche tecniche	Pubblicate da W3C – http://www.w3.org/XML/
	Altre caratteristiche	Formato di testo flessibile derivato da SGML (ISO 8879).
	Software necessario alla visualizzazione Qualsiasi editor di testo. Inoltre è possibile, concordando con il Cliente le caratteristiche di un opportuno file xslt, produrne una copia human readable con Microsoft Internet Explorer / Firefox / Google Chrome o altri browser	

copia informatica per consultazione

FORMATO	DESCRIZIONE	
TXT	File di testo semplice, non strutturato, è adatto a contenuti puramente testuali e non richiede particolari possibilità di strutturazione o informazioni aggiuntive sulla struttura o la formattazione. Non contiene quindi indicazioni di formattazione nascoste o visibili (p. es. grassetto, rientri, colori ecc.) o indicazioni strutturali (p. es. titoli, sezioni, sottosezioni, indice ecc.). Questi file molto semplici offrono, sul lungo periodo, ottime garanzie per la conservazione e leggibilità dei dati.	
	Caratteristiche e dati informativi	
	Informazioni gestibili	Testo
	Estensione	.txt
	Tipo MIME	text/plain
	Formato aperto	SI
	Specifiche tecniche	Pubbliche
	Standard	ISO 646 RFC 3629 ISO/ IEC 10646
	Altre caratteristiche	Sono ammessi i seguenti set di caratteri: • US-ASCII; • ISO 8859-1 e 8859-15 (Latin-1 e Latin-9); • Unicode (UTF-8, UTF-16)
		Ai fini della conservazione nell'uso di tale formato, è importante specificare la codifica del carattere (Character Encoding) adottata.
	Software necessario alla visualizzazione	Notepad++

FORMATO	DESCRIZIONE	
EML	Electronic Mail Message (EML) è un formato di testo che definisce la sintassi di messaggi di posta elettronica scambiati tra utenti	
	Caratteristiche e dati informativi	
	Informazioni gestibili	Messaggi di posta elettronica e PEC
	Sviluppato da	Internet Engineering Task Force (IETF) - http://www.ietf.org/
	Estensione	.eml
	Tipo MIME	Message/rfc2822
	Formato aperto	SI
	Specifiche tecniche	Pubblicate da IETF - http://www.ietf.org/rfc/rfc2822.txt
	Altre caratteristiche	è un formato di testo flessibile derivato da SGML (ISO 8879).
	Software necessario alla visualizzazione	La maggior parte dei client di posta elettronica supportano la visualizzazione di file eml

Per quanto concerne il formato degli allegati al messaggio di posta elettronica, valgono le indicazioni di cui sopra. I formati XML ed EML sono accettati solamente per le classi documentali di tipo "PEC".

Torna al sommario

6.3.3 Identificazione

L'associazione del documento informatico al suo formato può avvenire, attraverso varie modalità, tra cui le più impiegate sono:

1. l'estensione: una serie di lettere, unita al nome del file attraverso un punto, ad esempio [nome del file].doc identifica un formato sviluppato dalla Microsoft;
2. il magic number: i primi byte presenti nella sequenza binaria del file, ad esempio 0xffd8 identifica i file immagine di tipo .jpeg;
3. verifica della corrispondenza tra il tipo MIME ricavato dall'estensione del file ed il tipo MIME ricavato dal magic number;
4. l'utilizzo di tool automatici specifici come Apache TIKA

Per identificare il formato dei files posti in conservazione occorre procedere all'analisi di ogni singolo documento

copia informatica per consultazione

informatico contenuto all'interno dei pacchetti di versamento. ARUBA procede come segue:

1	**Fase di IDENTIFICAZIONE**	Ogni documento che viene inviato al sistema di conservazione deve essere stato precedentemente ed espressamente indicato dal sistema versante. In questo modo tutti i documenti non noti vengono automaticamente non riconosciuti e quindi rifiutati
2	**Fase di RICEZIONE**	Il sistema Aruba, una volta noti i documenti che il Cliente vuole mettere in conservazione si mette in attesa, secondo i canali concordati, della loro ricezione
3	**Fase di VALIDAZIONE**	Una volta che i documenti vengono recepiti dal sistema di conservazione la prima elaborazione effettuata sugli stessi è quella del rilevamento della tipologia corretta del documento. Solo se questo esame restituisce esito positivo vengono realizzate ulteriori validazioni atte a garantire la correttezza formale del documento, secondo gli standard qui esposti e gli accordi convenuto col Cliente

Torna al sommario

6.4 Metadati da associare alle diverse tipologie di documenti

Con il termine "metadati" si indicano tutte le informazioni significative associate al documento informatico, escluse quelle che costituiscono il contenuto del documento stesso. I metadati riguardano principalmente, ma non esclusivamente, i modi, i tempi ed i soggetti coinvolti nel processo della formazione del documento informatico, della sua gestione e della sua conservazione.

Metadati sono anche le informazioni riguardanti gli autori, gli eventuali sottoscrittori e le modalità di sottoscrizione e la classificazione del documento. I metadati devono essere associati al documento dal Cliente prima del versamento in conservazione e per tale ragione vengono esplicitati all'interno di uno specifico allegato, facente parte del Contratto di servizio stipulato con ARUBA (come specificato al par 10.1.2).

I metadati forniti dal Cliente restano di proprietà del Cliente medesimo.

I metadati, seppur chiaramente associati al documento informatico, possono essere gestiti indipendentemente dallo stesso. In relazione ai diversi tipi di documenti informatici posti in conservazione, è previsto un "**set minimo"** di metadati.

Oltre al set minimo di metadati, il Cliente potrà decidere di associare al documento informatico eventuali ulteriori metadati c.d. "*extrainfo*". Le extra info verranno inserite, al pari degli altri metadati, nell'indice di conservazione che. I metadati *extrainfo* dovranno essere puntualmente individuati nello spazio ad essi riservato nell'apposito allegato del *Contratto* e verranno opportunamente gestiti da Aruba come in esso concordato.

Torna al sommario

6.5 Modalità di assolvimento dell'imposta di bollo sui documenti posti in conservazione

Il Cliente è tenuto al pagamento dell'imposta di bollo eventualmente dovuta sui documenti depositati in conservazione.

Pertanto, il versamento dell'imposta dovuta dovrà essere effettuata dal Cliente nei termini previsti dall'art. 6 del DMEF 17 giugno 2014 e nei modi di cui all'art. 17 del D.Lgs. 9 luglio 1997, n. 241 e loro successive modificazioni e/o integrazioni.

Tutti i relativi e conseguenti obblighi, adempimenti e formalità per l'assolvimento dell'imposta di bollo sui documenti informatici posti in conservazione sono ad esclusivo onere e carico del Cliente, il quale dovrà attenersi alle disposizioni di legge ed ai documenti di prassi emanati ed emanandi.

Allo stesso modo, sono ad esclusivo onere e carico del Cliente tutte le comunicazioni da presentare al

copia informatica per consultazione

competente Ufficio delle entrate in forza di quanto stabilito dalla normativa regolante la conservazione digitale di documenti informatici.

Torna al sommario

6.6 Pacchetto di versamento

In questo paragrafo sono fornite le tipologie di pacchetto di versamento gestite e per ciascuna di esse descritta la struttura dati.

Il nostro standard prevede l' indice di un pacchetto di versamento che si caratterizza per le seguenti parti:

- area di identificazione del PDV
- area di identificazione dei documenti costituenti il pacchetto e composta dai seguenti elementi:
  - metadato obbligatori
  - metadati extra-info

Nella prima parte il dato importante e obbligatorio è il *pdvid* ovvero l'identificativo del PDV. Esso deve essere unico all'interno dello spazio gestito dal produttore, quindi indipendentemente dall'archivio.

La seconda parte prevede una lista di elementi, uno per ogni documento da versare. Ogni singolo file deve essere per prima cosa identificato. A questo scopo sono necessari i seguenti dati:

- nome file
- algoritmo di hashing per la generazione dell'impronta
- impronta del documento

Inoltre, poiché il sistema deve controllare la tipologia di documento per valutarne l'aderenza alle condizioni espresse in fase di contratto, deve essere indicato il MIME type del documento.
Per rimanere poi aderenti alla norma vigente devono essere passati anche un id unico dei singoli documenti del pacchetto e la data di chiusura degli stessi.

L'ultima parte dell'Indice contiene un insieme di metadati extra-info, così come definiti in fase contrattuale col Produttore

Torna al sommario

6.6.1 Specifiche Pacchetto di Versamento

Le specifiche del Pacchetto di Versamento secondo lo standard definito da ARUBA, sono disponibili all'interno di specifiche sezioni pubblicate sui siti web www.pec.it e guide.pec.it.

Torna al sommario

6.7 Pacchetto di Archiviazione

In questo paragrafo viene resa la struttura del Pacchetto di Archiviazione nonché il trattamento dei pacchetti di archiviazione.

Torna al sommario

6.7.1 Specifiche Pacchetto di Archiviazione

Il Pacchetto di Archiviazione è composto da varie parti:

copia informatica per consultazione

- l'insieme degli elementi (documenti e/o altri PdA) che compongono il pacchetto
- l'Indice del Pacchetto di Archiviazione (IPdA) che elenca tutti gli elementi del pacchetto. Il formato dell'indice è aderente allo standard UNI SInCRO (nel quale è indicato come IdC – Indice di Conservazione) ed è marcato temporalmente e firmato elettronicamente con certificato del Responsabile del Sistema di Conservazione.

Torna al sommario

6.8 Pacchetto di Distribuzione

Il Pacchetto di Distribuzione contiene l'insieme degli elementi (documenti e/o PdA) precedentemente ricercati e selezionati dall'utente.

Viene offerto sotto forma di un archivio .zip che per ogni elemento contiene:

- una cartella contenente l'elemento stesso. Nel caso di un documento il documento stesso, nel caso di un PdA l'intero PdA, ovvero tutti gli elementi di cui è costituito
- un'altra cartella che contiene l'indice relativo all'elemento individuato, marcato temporalmente e firmato elettronicamente con certificato del Responsabile del Sistema di Conservazione

Torna al sommario

6.9 Documenti rilevanti ai fini delle disposizioni tributarie

In considerazione di quanto previsto dall'art. 21, co. 5, del CAD[1], i documenti informatici rilevanti ai fini delle disposizioni tributarie (di seguito, per brevità chiamati anche "**DIRT**") sono conservati nel rispetto di quanto previsto dalle disposizioni in materia, attualmente riconducibili al Decreto del 17 giugno 2014 del Ministero dell'Economia e delle Finanze e successive modificazioni ed integrazioni.

Il Cliente, pertanto, è tenuto a conoscere le disposizioni relative alla normativa regolante la conservazione digitale di documenti informatici in vigore ed a controllare l'esattezza dei risultati ottenuti con l'utilizzo del Servizio di conservazione fornito da ARUBA.

Formazione, emissione e trasmissione dei documenti fiscalmente rilevanti

Ai fini tributari, la formazione, l'emissione, la trasmissione, la copia, la duplicazione, la riproduzione, l'esibizione, la validazione temporale e la sottoscrizione dei documenti informatici, deve avvenire a cura del Cliente nel rispetto delle regole tecniche adottate ai sensi dell'art. 71 del decreto legislativo 7 marzo 2005, n. 82, e dell'art. 21, comma 3, del decreto del Presidente della Repubblica 26 ottobre 1972, n. 633, in materia di fatturazione elettronica

Immodificabilità, integrità, autenticità e leggibilità dei documenti fiscalmente rilevanti

I documenti informatici rilevanti ai fini tributari devono avere le caratteristiche dell'immodificabilità, dell'integrità, dell'autenticità e della leggibilità, e devono essere utilizzati i formati previsti dal decreto legislativo 7 marzo 2005, n. 82 e dai decreti emanati ai sensi dell'art. 71 del predetto decreto legislativo nonché quelli individuati nel presente Manuale. Detti formati devono essere idonei a garantire l'integrità, l'accesso e la leggibilità nel tempo del documento informatico.

Pertanto, tutti i DIRT che vengono versati in conservazione devono essere statici ed immodificabili, ossia privi di qualsiasi agente di alterazione.

Il Cliente dovrà assicurarsi e garantire che i DIRT che versa in conservazione abbiano le suddette caratteristiche sin dalla loro formazione e, in ogni caso, prima che siano depositati nel sistema di conservazione.

---

[1] Art. 21, co. 5 del CAD: "Gli obblighi fiscali relativi ai documenti informatici ed alla loro riproduzione su diversi tipi di supporto sono assolti secondo le modalità definite con uno o più decreti del Ministro dell'economia e delle finanze, sentito il Ministro delegato per l'innovazione e le tecnologie.";

copia informatica per consultazione

A tale fine, i DIRT, salvo diverso e circostanziato accordo col Responsabile del servizio di conservazione, devono essere prodotti nel formato PDF/A in conformità a quanto previsto nel capitolo 12 del presente *Manuale*.

Ordine cronologico e non soluzione di continuità per periodo di imposta

Posto che l'art. 3 del Decreto MEF 17.06.2014 stabilisce che i documenti informatici devono essere conservati in modo tale da rispettare le norme del codice civile, le disposizioni del codice dell'amministrazione digitale e delle relative regole tecniche e le altre norme tributarie riguardanti la corretta tenuta della contabilità, il Cliente deve farsi carico di versare in conservazione i propri documenti informatici assicurando, ove necessario e/o previsto dalle norme e/o dai principi contabili nazionali, l'ordine cronologico dei medesimi e senza che vi sia soluzione di continuità in relazione a ciascun periodo d'imposta o anno solare.

In altre parole, gli obblighi richiamati dall'art. 3 del DM 17.06.2014, essendo riferibili a norme riguardanti la corretta tenuta della contabilità, sono posti a completo ed esclusivo carico del Cliente.

Ciò comporta che il Cliente, nell'eseguire il versamento in conservazione dei DIRT, dovrà rispettare le regole di corretta tenuta della contabilità e procedere secondo regole uniformi, nell'ambito del medesimo periodo d'imposta o anno solare.

Funzioni di ricerca

ARUBA non fornisce, in fase di formazione dei documenti, alcuna funzionalità di indicizzazione degli stessi che, quindi, è posta ad esclusivo carico e sotto la responsabilità del Cliente il quale al documento informatico immodificabile il Cliente dovrà associare, in relazione ad ogni classe/tipologia documentale, i metadati previsti dalla legge (anche tributaria) e dalle regole tecniche di cui all'art. 71 del CAD e, più in generale, dalla vigente normativa in materia o gli eventuali ulteriori metadati riportati nell'Elenco documenti in conservazione; i suddetti metadati dovranno essere generati dal Cliente durante la fase di produzione/formazione/emissione dei documenti informatici.

Pertanto, è il Sistema di Gestione documentale del Cliente che deve assicurare l'indicizzazione dei DIRT in merito al formato, allo stato, alle caratteristiche (fiscali) di ogni singolo DIRT ed ai metadati "minimi" previsti dal Decreto MEF del 17 giugno 2014 (nome, cognome, denominazione, codice fiscale, partita IVA, data e associazioni logiche di questi) e dal presente *Manuale* nel capitolo 12.

Per sfruttare appieno le potenzialità del processo di conservazione dei DIRT non è sufficiente attenersi alle regole tecniche previste dalla norma, ma è necessario che il Cliente si attenga scrupolosamente ad un progettato ciclo di gestione dei DIRT, con il fine di predisporli ed organizzarli sin dalla loro formazione in modo tale da massimizzare la facilità del loro reperimento, prestando particolare attenzione alla fase di classificazione ed organizzazione. Dal puntuale svolgimento di quanto sopra dipende la facilità del loro reperimento.

A tale fine, è necessario che, in relazione ad ogni classe documentale, il Cliente associ ad ogni DIRT i metadati previsti dal presente *Manuale* (ed, eventualmente, degli ulteriori previsti nell'apposito allegato del *Contratto*) necessari per adempiere agli obblighi imposti dalle disposizioni in materia.

Il sistema di conservazione garantisce, come riportato nel capitolo 16, le necessarie funzioni di ricerca dei DIRT conservati sulla scorta dei metadati ad essi associati.

Classificazione dei DIRT secondo aggregazioni per "Tipo documento"

Il Sistema di Gestione documentale del Cliente, oltre ad assicurare il formato, l'indicizzazione, l'apposizione del riferimento temporale, la sottoscrizione con firma digitale di ogni DIRT dallo stesso prodotto, deve provvedere altresì alla classificazione per tipologia di documento in conformità a quanto previsto dall'Allegato 1 al presente Manuale.

Torna al sommario

6.9.1 Modalità di assolvimento dell'imposta di bollo sui DIRT

Come precisato nel precedente capitolo 12, l'imposta di bollo nonché tutti gli obblighi e le formalità per l'assolvimento dell'imposta sui DIRT, qualora dovuta, sono ad esclusivo onere e carico del Cliente, il quale dovrà attenersi alle disposizioni di legge (art. 6, del DMEF del 17 giugno 2014) ed ai documenti di prassi emanati ed emanandi.

copia informatica per consultazione

Torna al sommario

6.10 Trattamento dei pacchetti di archiviazione contenenti documenti rilevanti ai fini delle disposizioni tributarie

Il processo di conservazione dei DIRT è effettuato nel rispetto delle regole di cui al DMEF del 17 giugno 2014 e successive modificazioni ed integrazioni.

Nello specifico, il processo di conservazione, prende avvio con il versamento in conservazione del pacchetto di versamento prodotto dal Cliente e termina (ergo, "*viene chiuso in conservazione*") termina con l'apposizione di una marca temporale sul Pacchetto di Archiviazione.

Con riferimento ai DIRT, il processo di conservazione, in forza di quanto stabilito dall'art. 3 del DMEF del 17 giugno 2014, è effettuato entro il termine previsto dall'art. 7, comma 4-ter, del decreto-legge 10 giugno 1994, n. 357, convertito con modificazioni dalla legge 4 agosto 1994, n. 489 e s.m.i..

Pertanto, il Cliente dovrà provvedere a trasmettere ad ARUBA il pacchetto di versamento, contenente i DIRT da sottoporre a conservazione, rigorosamente entro i termini stabiliti nell'apposito allegato del *Contratto*; tale termine è necessario ad ARUBA per "chiudere" in conservazione il Pacchetto di Archiviazione entro i termini perentori previsti dalla legge.

Torna al sommario

copia informatica per consultazione

7 Il processo di conservazione

In questo capitolo sono riportate tutte le fasi inerenti il processo di conservazione dei documenti informatici

7.1 Modalità di acquisizione dei pacchetti di versamento per la loro presa in carico

Come già anticipato in altre parti del presente *Manuale*, unico responsabile del contenuto del pacchetto di versamento è il Cliente (Produttore), che deve formarlo, sottoscriverlo con firma digitale (ove previsto) e trasmetterlo al sistema di conservazione secondo le modalità operative di versamento definite nel presente *Manuale,* nel *Contratto* e nei rispettivi allegati.

L'operazione di versamento consiste nella trasmissione dei documenti da conservare e dei metadati che li specializzano, così come già accennato precedentemente.

La ricezione e presa in carico di un pacchetto di versamento segue uno schema logico di funzionamento che si articola in due fasi distinte: ricezione dell'Indice del Pacchetto di Versamento (IPdV) e ricezione dei documenti che fanno parte del Pacchetto di Versamento (PdV).

L'uno e gli altri possono essere trasmessi al sistema di conservazione attraverso canali diversi. Alternativamente essi possono essere:

- interfaccia web
- invocazione di metodi tramite web service REST
- trasferimento via protocollo FTP

Ogni canale messo a disposizione è provvisto di opportuni accorgimenti per la trasmissione dei dati in modalità sicura:

- l'interfaccia web viaggia su protocollo HTTPS
- il web service REST è contattabile tramite protocollo HTTPS
- la PEC nativamente garantisce autenticità della provenienza e notifica di consegna in modalità sicura
- il server FTP è raggiungibile via FTPS

Per il completamento delle operazioni di conservazione di un PdV non è necessario scegliere esclusivamente uno dei canali sopra citati. La ricezione, anche in maniera asincrona, dei singoli componenti di un PdV possono arrivare anche da canali diversi.

Il sistema di conservazione prende in carico un PdV solo dopo che tutte le sue parti (IPdV e relativi documenti) vengono correttamente ricevuti e superano con esito positivo i relativi controlli.

Tale operazione viene ufficialmente sancita dalla produzione del cosiddetto Rapporto di Versamento (RdV) che viene consegnato al cliente all'indirizzo PEC fornito nella fase contrattuale.

Poiché la produzione del RdV rappresenta formalmente la presa in carico del PdV da parte del sistema di conservazione, il RdV viene marcato temporalmente e firmato digitalmente direttamente o via delega dal Responsabile del servizio di Conservazione.

Torna al sommario

7.1.1 Ricezione dell'indice del pacchetto di versamento

L'IPdV è un'evidenza informatica, ovvero un file, che descrive il versamento stesso e i documenti che ne fanno parte attraverso l'uso di metadati. Questi sono di carattere diverso a seconda che descrivano proprietà e qualità del pacchetto in genere o dei singoli documenti.

E' bene sottolineare che ogni PdV può contenere esclusivamente documenti della stessa tipologia, ovvero della

copia informatica per consultazione

stessa Classe Documentale. In questo senso l'elenco dei metadati dei singoli documenti è in qualche modo omogeneo.

Per consentire l'elaborazione automatica dei metadati il sistema di conservazione Aruba richiede l'incapsulamento degli stessi in un determinato formato XML, che di fatto costituisce l'IPdV.

In tale file sono contenute sezioni diverse che identificano la qualità dei metadati. Essi infatti possono essere caratteristici del PdV e del soggetto versante, rappresentare direttive speciali di elaborazione per la conservazione, descrittivi dei singoli documenti che si vogliono conservare, a loro volta distinti in standard, come indicato nel paragrafo 12.4, o definiti insieme al Cliente in fase di stipula del contratto e infine caratteristici del formato del documento.

La struttura dell'indice del pacchetto di versamento è definita nel paragrafo 6.6.1.

La funzione di ricezione degli indici dei pacchetti di versamento nel sistema di conservazione effettua, per ogni indice, i seguenti controlli:

- abilitazione alla conservazione da parte del sistema di gestione documentale versante e in particolare dell'utente che effettua il versamento. In caso di esito negativo il sistema rifiuta il tentativo di versamento
- controllo formale dell'indice versato. In particolare viene verificato che sia un formato XML valido per una elle Classi Documentali registrate a sistema. In caso di esito negativo il sistema rifiuta il tentativo di versamento
- verifica, tramite l'id univoco contenuto nell'indice, dell'eventuale presenza del PdV già nel sistema. In caso di esito positivo il nuovo indice sostituisce in toto il vecchio. Di conseguenza vengono aggiornati tutti i metadati, tutti i documenti eventualmente versati e non più presenti nel nuovo indice vengono cancellati dal sistema
- controllo sulla completezza e correttezza formale dei metadati, in relazione alla Classe Documentale rilevata. In caso di esito negativo il sistema rifiuta il tentativo di versamento
- controllo sulla tipologia di documenti che si vuole versare. Ogni documento deve appartenere ad almeno uno dei formati ammessi dalla tipologia di Classe Documentale. In caso di esito negativo il sistema rifiuta il tentativo di versamento
- eventuali controlli supplementari definiti insieme al Cliente. La gestione degli esiti negativi va formalizzato in sede contrattuale

Torna al sommario

7.1.2 Ricezione documenti associati ad un pacchetto di versamento

La ricezione dell'IPdV permette al sistema di conservazione di registrare i metadati del PdV e di mettersi in attesa dei documenti per la conservazione del pacchetto.

Relativamente al singolo documento tra i metadati indicati nell'IPdV sono di particolare importanza quelli utili all'identificazione dello stesso. Essi sono principalmente due: un identificativo univoco utile all'identificazione human readable del documento e un hash del file stesso, ovvero una stringa di caratteri che normalizza con un particolare algoritmo in maniera univoca il documento stesso.

In particolare l'hash, che per il sistema di conservazione Aruba deve essere in formato SHA256 base64, garantisce la riconoscibilità e incorruttibilità del documento in forma automatica e univoca.

Nel momento in cui un documento viene ricevuto da uno qualsiasi dei canali esposti precedentemente, ne viene calcolato l'hash in SHA265 e base64. Se il risultato è tra quelli precedentemente comunicati in uno dei IPdV ricevuti e non ancora in conservazione, allora il file viene accettato.

Successivamente la funzione di ricezione dei documenti informatici nel sistema di conservazione effettua una serie di controlli atti a verificare formalmente leggibilità, integrità e la corrispondenza del documento alle regolamentazioni stabilite per la Classe Documentale di appartenenza. Per operare ciò il sistema determina il formato dello stesso sulla base di quanto esposto in precedenza (estensione e mimetype).

copia informatica per consultazione

La mancata identificazione del formato del file causa il rifiuto dello stesso con conseguente restituzione di un errore.

Una volta individuato il formato del documento viene controllato che questo sia tra i formati ammessi per la Classe Documentale di appartenenza. Nel caso di esito negativo il file viene rifiutato e viene restituito un errore. Superati i primi controlli, ne vengono operati degli altri relativamente alla qualità dello stesso.

In relazione a ciascun documento informatico infine:

- viene verificato che non sia già presente nel sistema di conservazione;
- viene verificato che il salvataggio avvenga correttamente all'interno del sistema di conservazione.

Tutti i documenti informatici che non superano anche uno solo dei precedenti controlli **vengono rifiutati**. In questo caso non viene salvata alcuna informazione sul sistema di conservazione ed il documento non conforme viene immediatamente eliminato.

Quando tutti i documenti di un pacchetto di versamento vengono ricevuti correttamente viene reso disponibile il rapporto di versamento sottoscritto con firma digitale dal Responsabile del servizio di Conservazione.

Tale rapporto viene anche inviato via email da un indirizzo PEC all'indirizzo PEC fornito dal cliente in fase contrattuale.

Torna al sommario

7.2 Verifiche effettuate sui pacchetti di versamento e sugli oggetti in essi contenuti

Le funzionalità attivate nel processo di versamento/acquisizione del pacchetto di versamento prevedono dei controlli sia nella fase di ricezione dell'indice del PdV che sui singoli documenti inviati e corrispondenti a quanto previsto nell'indice stesso. La tabella riportata in basso elenca le diverse tipologie di controlli effettuati e per ognuna di esse indica l'azione prevista da sistema. Quest'ultima può tradursi in una operazione di scarto o notifica di un warning.

Controlli dell'indice del Pacchetto di versamento

Il deposito di un pacchetto di versamento è distinto per ciascun pacchetto di documenti informatici omogenei (documenti omogenei, ossia aventi la stessa classe documentale). Pertanto, a classi documentali diverse corrispondono diversi PdV e versamenti, uno per ogni classe.

Controlli nella fase di ricezione dell'indice del PdV

ID	Oggetto del controllo	Azione in caso di check negativo
Verifica Autorizzazioni		
1.01	viene verificato che l'utente che effettua il versamento sia abilitato all'invio dei Pdv	Il sistema scarta l'intero pacchetto
Verifica formale indice del PdV		
2.01	viene verificato che l'oggetto ricevuto sia formalmente un indice xml in linea con lo standard DocFly	Il sistema scarta l'intero pacchetto
2.02	viene verificato che il PdV è versato nei termini contrattuali e di servizio stabiliti col produttore	WARNING: Il sistema accetta il PdV ma non garantisce la conservazione nei termini concordati
Verifica presenza dati-documenti nell'indice del PdV		

copia informatica per consultazione

3.01	viene verificato che l'indicazione del sistema di conservazione sia corretta	Il sistema scarta il PdV poiché il metadato contenuto nell'indice indica un sistema di conservazione diverso da DocFly
3.02	viene verificato che l'identificativo specificato nel Pdv non sia già presente nel sistema di conservazione	Il sistema verifica se il PdV (che contiene lo stesso ID) non sia già stato conservato. In questo caso il sistema considera il nuove indice in sostituzione del precedente. Viene invece scartato qualora il PdV risulta essere in stato 'conservato'.
3.04	viene effettuato un controllo semantico sui metadati presenti nell'indice del PdV	Il sistema scarta il PdV poiché uno o più metadati non rispettano il formato condiviso nel contratti di servizio
3.05	viene controllato che per ciascun documento dichiarato e descritto all'interno dell'indice del Pdv: a. tutti i metadati minimi obbligatori siano presenti e nel formato corretto; b. il formato del documento è un formato ammesso c. l'estensione del documento sia tra quelle ammesse per il tipo documento; d. il formato dichiarato sia corrispondente all'estensione del nome file	Il sistema scarta il PdV perché le verifiche formali sui documenti dichiarati nell'indice del PdV hanno avuto esito negativo
Verifiche Paternità		
4.01	viene verificato che il Pdv, nel caso abbia estensione P7M, sia firmato con certificato valido	Il sistema scarta il PdV perché le verifiche formali sui certificati di firma hanno avuto esito negativo
4.02	viene verificato che tutte le firme apposte al Pdv siano valide	Il sistema scarta il PdV perché le verifiche formali sui certificati di firma hanno avuto esito negativo

Controlli nella fase di ricezione dei documenti

A seguito della corretta ricezione dell'indice del PdV, il sistema di conservazione è pronto per la ricezione dei relativi documenti informatici (files) descritti nel pacchetto stesso

Controlli nella fase di ricezione dei documenti (files)

Controllo ricezione documenti		
1.01	viene verificato che l'hash del documento informatico inviato sia corrispondente all'hash dichiarato all'interno del medesimo indice del pacchetto al fine di avere garanzia che la trasmissione del pacchetto sia avvenuta correttamente e che l'integrità del documento informatico ricevuto sia assicurata	Il sistema scarta il documento poiché non atteso

copia informatica per consultazione

1.02	in caso di file P7M viene verificata la validità della firma apposta su ogni singolo documento: o Controllo di conformità. o Controllo Crittografico. o Controllo Catena Trusted. o Controllo Certificato. o Controllo CRL	Il sistema scarta il documento qualora il certificato di firma non sia valido WARNING: in caso di documenti firmati e il certificato di firma utilizzato è prossimo alla scadenza, il sistema evidenzia un warning.
1.03	viene verificato che il documento sia leggibile	Il sistema scarta il documento nel caso questo non sia leggibile
1.04	viene verificato che il formato del documento informatico sia effettivamente valido e corrispondente a quanto dichiarato nel pacchetto di versamento. In tal caso i controlli eseguiti variano in funzione del formato atteso per ciascuno specifico documento.	Il sistema scarta il documento poiché il formato non è quello atteso
1.05	viene verificato che i documenti ricevuti non siano già presenti nel sistema di conservazione;	WARNING: il documento viene accettato e il sistema invia una notifica
1.06	viene verificato che la ricezione dei documenti si sia correttamente conclusa entro la data limite di ricezione stabilita col produttore nel contratto di servizio	WARNING: il documento viene accettato ma il sistema non garantisce la conservazione nei termini concordati

Le eventuali anomalie e/o scarti riscontrate durante le verifiche effettuate sull'indice del pacchetto di versamento e documenti contenuti al suo interno, saranno comunicate via PEC sia al responsabile della conservazione indicato dal cliente (nel contratto di servizio) che all'utente che ha effettuato l'operazione di versamento.

Tali comunicazioni saranno conservate all'interno del sistema di posta per tutta la durata del contratto sottoscritto dal cliente.

Torna al sommario

7.3 Accettazione dei pacchetti di versamento e generazione del rapporto di versamento di presa in carico

Il sistema di conservazione predispone, per ciascun pacchetto di versamento, un **rapporto di versamento** che viene firmato dal Responsabile del Sistema di Conservazione. Lo schema del rapporto di versamento è illustrato nel paragrafo successivo (par. 7.3.1).

In particolare il rapporto di versamento contiene, tra l'altro, le seguenti informazioni:

- identificativo unico del PdV, come indicato nel relativo IPdV
- identificativo unico del PdV fornito dal sistema di conservazione
- data di ricezione dell'IPdV
- per ogni documento accettato viene indicato:
  - id univoco, come indicato nell'IPdV
  - id univoco fornito dal sistema di conservazione
  - hash
  - data di ricezione
  - esito della ricezione (accettato o warning)
  - descrizione warning, ove necessario

Torna al sommario

copia informatica per consultazione

7.3.1 *Specifiche rapporto di versamento*

Il Rapporto di Versamento è basilare nel processo di conservazione, in quanto è documento informatico che attesta l'avvenuta presa in carico da parte del sistema di conservazione dei pacchetti di versamento inviati dal produttore.

Esso viene prodotto nel momento in cui tutti gli elementi utili per la conservazione del pacchetto di versamento sono stati consegnati al sistema.

In esso sono presenti sempre i seguenti dati:

- id del Pacchetto di Versamento
- id del Rapporto di Versamento
- riferimento temporale (UTC) di generazione del Rapporto di Versamento
- lista dei documenti afferenti al pacchetto. Per ognuno di essi sono distinguibili:
- id come indicato nell'Indice del PdV
- id assegnato dal sistema
- impronta del documento
- nome del documento
- data di ricezione del file
- esito controllo firma digitale (ove previsto)
- esito controllo marca temporale (ove previsto)

Il Rapporto di Versamento viene sempre firmato digitalmente con certificato del Responsabile di Conservazione. In questo modo viene reso non modificabile.

Torna al sommario

7.4 Rifiuto dei pacchetti di versamento e modalità di comunicazione delle anomalie

Per la gestione dei rifiuti dei pacchetti di versamento e modalità di comunicazione delle anomalie si rimanda al par. 7.2.

Torna al sommario

7.5 Preparazione e gestione del Pacchetto di Archiviazione

Il Pacchetto di Archiviazione (PdA) è quello conservato dal sistema di conservazione e possiede un insieme completo di metadati utili alla conservazione a lungo termine.

Il Pacchetto di Archiviazione viene realizzato secondo lo standard di riferimento SInCRO - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali (UNI 11386:2010), che rappresenta lo standard nazionale riguardante la struttura dell'insieme dei dati a supporto del processo di conservazione.

Uno più pacchetti di versamento vengono trasformati in un Pacchetto di Archiviazione (PdA) in base alle regole tecniche standard del sistema conservazione previste e agli accordi contrattuali.

Il sistema di conservazione a lungo termine ha, fra le altre, la prerogativa di conservare l'autenticità dei documenti in esso contenuti.

La preservazione della suddetta autenticità non può però basarsi *tout court* sulla firma digitale in quanto quest'ultima:

- ha una validità slegata dall'architettura e dalla struttura del sistema di conservazione;
- ha una validità limitata nel tempo e pari al certificato emesso dalla CA;
- vede la propria sicurezza legata ad algoritmi soggetti ad obsolescenza tecnologica.

È pertanto fondamentale che il sistema di conservazione a lungo termine verifichi la validità ed il valore delle firme digitali apposte dal Cliente sui documenti informatici oggetto di conservazione.

copia informatica per consultazione

A tale fine, il Cliente dovrà accertarsi che le firme digitali apposte sui documenti informatici inviati in conservazione:

a) siano valide al momento di sottoscrizione del documento informatico;

b) e mantengano piena validità sino al termine ultimo convenuto con ARUBA per la "chiusura" del Pacchetto di Archiviazione.

Con la sottoscrizione dei pacchetti di archiviazione ARUBA non sottoscrive il contenuto e la semantica dei documenti conservati ma asserisce solamente che il processo di conservazione è stato eseguito correttamente, nel rispetto della normativa regolante la conservazione digitale di documenti informatici

Torna al sommario

7.5.1 Chiusura anticipata (in corso d'anno) del Pacchetto di Archiviazione

In caso di accessi, verifiche ed ispezioni in corso d'anno, il sistema consente, dietro specifica richiesta del Cliente, l'anticipata chiusura del Pacchetto di Archiviazione rispetto ai tempi programmati.

Torna al sommario

7.5.2 Gestione dei Pacchetti di Archiviazione non validi o non completi

Nel caso di versamento di un PdA che non viene completato entro 4 ore dalla sua creazione, il sistema invia una email al Responsabile della Conservazione per avvertire l'utente e chiedere il completamento o la modifica del PdA.

Qualora il PdA non venga completato entro 7 giorni dalla sua creazione, il sistema provvederà a:

a) Rimuovere i PdV incompleti presenti nel PdA e/o documenti non collegati a nessun IPdV;
b) Conservare il PdA con i soli PdV completi e validi (con conseguente RdC);
c) Eliminare l'intero PdA nel caso in cui non contenga alcun PdV valido;
d) Inviare una mail di notifica all'utente dell'avvenuta cancellazione dei PdV incompleti ed eventuale conservazione del PdA con i soli PdV validi e completi;
e) Registrare sui log il dettaglio di tutte le operazioni e dei file cancellati.

Torna al sommario

7.5.3 Rettifica dei pacchetti di archiviazione

Il sistema di conservazione prevede la possibilità di eseguire la rettifica del pacchetto di archiviazione, inviando un documento successivo rispetto a quello inviato in precedenza in conservazione. Tale operazione, riservata solamente al produttore o titolare con diritti di scrittura sulla classe documentale relativa, permette al cliente di sostituire un documento inviato in conservazione con un nuovo documento dello stesso tipo, lasciandone invariati i metadati.

Il cliente, una volta indicato il PDA sul quale applicare la rettifica, potrà procedere alla sostituzione di uno o più documenti ed inserire la motivazione relativa all'operazione. Il documento sarà sottoposto ai medesimi controlli di verifica previsti dal processo di conservazione sui documenti originariamente inviati al servizio di conservazione. Una volta sostituiti i documenti, il sistema mostrerà a video l'esito della rettifica: in caso di errori riscontrati, verrà indicato per ciascun documento la tipologia di errore, permettendo al cliente di apportare le modifiche necessarie per concludere l'operazione, altrimenti sarà confermato l'esito positivo della rettifica.

Il PDA rettificato conterrà l'IPDV ed i documenti modificati, mentre il PDA originale rimarrà a disposizione sul sistema di conservazione nel PDD e consultabile dal cliente in qualsiasi momento.

Le operazioni di rettifica verranno registrate nei log di sistema.

copia informatica per consultazione

7.6 Preparazione e gestione del Pacchetto di Distribuzione ai fini dell'esibizione

Nel modello OAIS e in linea con la normativa vigente, il Pacchetto di Distribuzione è strutturato nel modello dati come il Pacchetto di Archiviazione. La differenza sta nella sua destinazione in quanto esso viene concepito per essere fruito ed utilizzato dall'utente finale (esibizione).
In questo caso, un PdD può anche non coincidere con il Pacchetto di Archiviazione originale conservato: anzi, molto spesso, ragioni di opportunità inducono a distribuire pacchetti informativi che sono un'estrazione del contenuto informativo di un PdA. Può anche verificarsi il caso di Pacchetto di Distribuzione che sono il frutto di più PdA che vengono "spacchettati" e reimpacchettati per un più fruibile utilizzo da parte dell'utente.
Un utente autorizzato da un soggetto produttore, quindi, è in grado di interrogare il sistema per ricevere in uscita uno specifico Pacchetto di Distribuzione. L'utente utilizzerà le funzionalità di richiesta di esibizione di un documento o di un insieme di documenti, per ottenerne una replica esatta secondo i fini previsti dalla norma.
In risposta alla richiesta iniziale di esibizione, da parte dell'utente, il sistema di conservazione risponderà restituendo un PdD che nel caso più completo conterrà:

- I file/documenti richiesti così come sono stati archiviati dal sistema al momento della messa in conservazione
- Indici dei Pacchetti di Archiviazione, marcati temporalmente e firmati come all'origine, con cui sono stati conservati i documenti richiesti. Al loro interno sono contenuti tutti i metadati di tutti i documenti messi in conservazione nello stesso PdA

A fronte di una richiesta di produzione del Pacchetto di Distribuzione, il sistema effettua delle verifiche di coerenza e correttezza del pacchetto e dei documenti in esso contenuti. A tal proposito, il sistema di conservazione verifica che le impronte dei documenti restituiti nel PdD corrispondano a quelle presenti nel relativo indice del Pacchetto di Archiviazione; in modo da garantire che i documenti stessi non abbiano subito alterazioni o modifiche nei contenuti.
La richiesta di produzione di un PdD implica l'invio di una comunicazione via PEC all'utente finale e altri destinatari eventualmente comunicati dal cliente nel contratto di servizio. Le comunicazioni via PEC, relative alle ricevute di invio e consegna, vengono conservate al fine di tracciare l'intera trasmissione.
La richiesta di esibizione può avvenire da due tra i canali messi a disposizione: interfaccia web e web service.
In entrambi i casi il flusso di selezione dei documenti da esibire è il medesimo:

1. ricerca dei documenti attraverso opportuni filtri
2. selezione e spostamento dei riferimenti dei documenti individuati all'interno di un area di lavoro
3. richiesta di esibizione a partire dai documenti nell'area di lavoro
4. produzione del link di download da cui scaricare il Pacchetto di Distribuzione

La ricerca dei documenti avviene tramite la selezione di filtri sui metadati. Una volta individuata la classe documentale di interesse l'utente può effettuare le ricerche inserendo i valori su cui filtrare per uno o più metadati di riferimento.
La ricerca contemporanea su più metadati implica un filtro più forte, ovvero una restrizione del numero dei documenti risultanti.
Inoltre è possibile effettuare una ricerca tra documenti di classi documentali differenti ma che sono accomunati per un particolare metadato.
Se ad esempio si volessero cercare tutti i documenti afferenti a un determinato numero pratica, dotando classi documentali di tipo differente dello stesso metadato "numero pratica" è possibile effettuare una ricerca di questo tipo.
Tutti i documenti di interesse risultanti dalle ricerche vengono quindi spostati in un'area di lavoro. Finita l'operazione di selezione l'utente può ulteriormente chiedere di esibire solo una parte dei documenti messi nell'area di lavoro.
Il Pacchetto di Distribuzione risultante dalla richiesta di esibizione contiene:

- i documenti da esibire
- gli indici dei PdA, marcati temporalmente e firmati elettronicamente così come al momento della conservazione, del flusso di conservazione relativo ai documenti scelti

Nel caso in cui tra i documenti figurino interi PdA, il Pacchetto di Distribuzione contiene tutti i documenti che lo compongono.

Torna al sommario

copia informatica per consultazione

7.6.1 Attività conseguenti alla cessazione del contratto

In tutti i casi di cessazione del rapporto contrattuale, ARUBA consente al Cliente, nei termini previsti dalle Condizioni di fornitura, il recupero dei propri documenti.

Non incombe su ARUBA alcun obbligo di provvedere alla materiale restituzione dei documenti informatici conservati, dal momento che l'attività di recupero dovrà essere effettuata dal Cliente con le modalità descritte di seguito:

1. Accedendo al sistema, il Cliente effettua esplicita richiesta di chiusura dell'intero Archivio
2. Il sistema in automatico genera il Pacchetto di Distribuzione contenente tutte le evidenze dei PdA (Pacchetti di Archiviazione) conservati.
3. Il Cliente riceve comunicazione via mail PEC del buon esito della procedura
4. Il Cliente, da sistema, richiede la produzione del Pacchetto di Distribuzione relativo all'intero archivio
5. Entro i termini stabiliti da contratto, il sistema rende disponibile il Pacchetto di Distribuzione che potrà essere scaricato dal cliente

7.7 Produzione di duplicati e copie informatiche e descrizione dell'eventuale intervento del pubblico ufficiale nei casi previsti

Nei successivi paragrafi vengono descritte le procedure adottate per la produzione di duplicati o copie.

7.7.1 Produzione di duplicati

La produzione di duplicati informatici dei documenti conservati può avvenire a seguito di una richiesta proveniente dal dipartimento tecnico oppure da una richiesta effettuata direttamente all'interno del sistema di conservazione.

In entrambe le situazioni, il passo iniziale consiste nella ricerca del documento informatico di interesse sfruttando le funzionalità messe a disposizione dal sistema di conservazione. Individuato il documento informatico di interesse, una apposita funzione consente di effettuare il download del documento stesso, producendo quindi un duplicato.

Il documento informatico richiesto viene infatti estratto dal sistema in formato binario controllando che l'estrazione sia eseguita senza errori e quindi inviata all'utente che ne ha fatto richiesta.

Torna al sommario

7.7.2 Produzione di copie

La produzione di copie si rende necessaria solamente a seguito di obsolescenza tecnologica di un formato accettato in conservazione e determina, quale diretta conseguenza, l'avvio di una procedura di riversamento sostitutivo.

In tale contesto ARUBA, previo perfezionamento di specifico accordo scritto (dove saranno concordati ruoli, modalità, tempi e corrispettivi), si renderà disponibile a collaborare col Cliente nell'effettuare le copie informatiche dei documenti informatici depositati in conservazione secondo quanto stabilito dalle regole tecniche vigenti.

Torna al sommario

7.7.3 Produzione copie o duplicati su supporti rimuovibili

In caso di richiesta di produzione di copie o duplicati su supporto rimuovibile, viene prodotto un insieme di DVD (o altro supporto), ognuno autoconsistenze, e consegnati al responsabile della conservazione che ne ha fatto richiesta.

copia informatica per consultazione

Il processo prevede l'uso di un apposito applicativo che permette la generazione di immagini complete o parziali degli archivi di conservazione che poi vengono riversate su supporto ottico da un operatore. Il software richiede in input l'identificativo dell'archivio di conservazione, le classi documentali desiderate e il periodo temporale coinvolto. L'output generato è dato dal contenuto selezionato dagli archivi di conservazione, lottizzato in pacchetti di dimensione compatibile alla capienza del supporto ottico. I supporti creati vengono etichettati con una codifica generata automaticamente che in nessun modo riporta informazioni sul contenuto.

In ogni singolo pacchetto sono presenti i documenti protetti con criptazione e il software di ricerca e accesso. Il software di ricerca e accesso permette previo inserimento di una password da parte dell'utente, di poter visionare l'indice di quanto contenuto nei pacchetti prodotti, eseguire ricerche su metadati e decriptare e visionare i singoli documenti. Qualora il cliente desiderasse anche l'evidenza della conservazione verrà consentito lo scarico, ovviamente decriptando in linea, del documento con il relativo Indice di Conservazione e tutte le evidenze necessarie.

La protezione dei documenti è quindi ottenuta tramite criptazione con un certificato pubblico, generato allo scopo. La decriptazione è eseguita tramite la chiave privata, abbinata al certificato, rilasciata col software di ricerca e accesso, e un PIN che viene recapitato a mezzo telematico al responsabile della conservazione. Insieme al PIN viene anche recapitata una descrizione del contenuto di ogni supporto: codice del supporto, evidente sull'etichetta dello stesso, archivio, classi documentali data conservazione primo Pacchetto di Archiviazione, data conservazione ultimo Pacchetto di Conservazione.

7.7.4 Intervento del Pubblico Ufficiale

ARUBA richiede la presenza di un pubblico ufficiale nei casi in cui sia previsto il suo intervento assicurando allo stesso l'assistenza tecnica necessaria per l'espletamento delle attività al medesimo attribuite.

Ogni risorsa, comprese quelle di natura economica, necessaria per l'espletamento delle attività attribuite al pubblico ufficiale dovranno essere garantite e sostenute dal Cliente; pertanto, qualora il Cliente non se ne sia fatto carico direttamente, ARUBA è sin da ora autorizzata ad addebitare al Cliente tutti i costi e le spese, compresi gli onorari inerenti le attività prestate dal Pubblico Ufficiale, qualora la normativa ne richieda obbligatoriamente la presenza.

Torna al sommario

7.8 Scarto dei pacchetti di archiviazione

7.8.1 Trasferimento dei documenti informatici in conservazione

Nella scheda di conservazione, parte integrante del contratto di servizio e sottoscritta dal cliente, sono indicati i tempi entro i quali le diverse tipologie di documenti devono essere trasferite in conservazione, ove, nel caso delle pubbliche amministrazioni, non già presenti nel Manuale di gestione.

Torna al sommario

7.8.2 Scarto dei documenti informatici conservati

Relativamente alla possibilità di scarto, ossia di eliminare legalmente i documenti informatici conservati digitalmente a norma di legge, occorre distinguere preliminarmente la tipologia dei soggetti (Clienti) produttori, pubblici o privati.

Va preliminarmente osservato che in ambito privato, con l'eccezione degli archivi "dichiarati di notevole interesse storico", che divengono archivi specificatamente disciplinati, l'obbligo di conservazione dei documenti è disciplinato dall'ordinamento vigente e, in particolare, dai termini prescrittivi del codice civile nonché, per le scritture contabili, le fatture, le lettere e i telegrammi ricevuti e le copie delle fatture, delle lettere e dei telegrammi spediti, segnatamente dall'art. 2220 del c.c., il quale stabilisce l'obbligo di conservazione di dieci anni dalla data dell'ultima registrazione.

In ambito pubblico, oltre alle prescrizioni civilistiche, si rendono applicabili una serie di altre disposizioni specifiche, una su tutte, il Codice dei beni culturali e ambientali, emanato con il D.Lgs. 10 gennaio 2004, n. 42.

copia informatica per consultazione

Inoltre, con riferimento agli archivi pubblici o privati, che rivestono interesse storico-artistico particolarmente importante, lo scarto del Pacchetto di Archiviazione avviene previa autorizzazione del Ministero per i beni e le attività culturali rilasciata al produttore secondo quanto previsto dalla normativa vigente in materia.

Pertanto, alla luce di quanto sopra sinteticamente rappresentato, una volta scaduti i termini previsti dalla legge il Cliente riceve una notifica via PEC dal sistema di conservazione e in autonomia può decidere di eliminare i documenti conservati attraverso le funzionalità previste dal sistema di conservazione.

Torna al sommario

7.8.3 Richiesta di scarto immediato

I clienti possono richiedere ad ARUBA lo scarto di alcuni Pacchetti di Archiviazione dal sistema di conservazione. Fermo quanto definito nel precedente paragrafo, riguardante il rispetto della normativa vigente in materia, il Responsabile della Conservazione potrà, previa compilazione della modulistica messa a disposizione da ARUBA, richiedere lo scarto di uno o più PdA.

Il richiedente dovrà indicare nel modulo i riferimenti all'archivio ed ai pacchetti di archiviazione che intende scartare, unitamente alle motivazioni dello scarto ed alla conferma di disporre di tutte le autorizzazioni necessarie per l'operazione.

Il modulo dovrà essere accompagnato da firma valida ed inviato tramite email all'indirizzo pec scarto@docfly.it.

Le operazioni di scarto verranno registrate nei log di sistema.

Torna al sommario

7.9 Predisposizione di misure a garanzia dell'interoperabilità e trasferibilità ad altri conservatori

In analogia allo standard SInCRO, la struttura prevista per il PdV prevede una specifica al fine di raggiungere un soddisfacente grado d'interoperabilità nei processi di migrazione, la struttura dell'Indice di Conservazione viene realizzata da ARUBA in conformità con quanto previsto dallo standard "*Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali*", (c.d. SInCRO), ossia dalla norma UNI 11386 dell'ottobre 2010.

I pacchetti di archiviazione generati dal sistema di conservazione vengono trattati al solo scopo di soddisfare i requisiti della conservazione digitale dei documenti ed al soddisfacimento delle richieste di produzione di pacchetti di distribuzione e di esibizione.

Il soddisfacimento dei requisiti della conservazione digitale implica che i pacchetti di archiviazione vengano firmati digitalmente dal responsabile del servizio di conservazione o da un suo delegato e marcati temporalmente per assicurarne la validità nel corso del tempo.

La produzione di pacchetti di distribuzione o l'esibizione di pacchetti di archiviazione comporta invece la produzione di duplicati degli stessi che sono successivamente utilizzati nei processi. Il Pacchetto di Archiviazione memorizzato all'interno del sistema non subisce più alcuna modifica successiva alla firma digitale e all'apposizione della marca temporale.

Torna al sommario

7.10 Tabella riepilogativa delle fasi del processo di conservazione

Il processo di conservazione si articola nelle seguenti fasi:

FASE 1	**Acquisizione da parte del sistema di conservazione del pacchetto di versamento per la sua presa in carico**	
	Descrizione sintetica	Consiste nella ricezione dell'IPdV
FASE 2	**Verifica che il pacchetto di versamento e gli oggetti contenuti siano coerenti con le modalità**	

copia informatica per consultazione

	previste nel presente Manuale di conservazione e con i formati di conservazione	
	Descrizione sintetica	In questa fase vengono condotti i controlli sull'IPdV
FASE 3	**Preparazione del rapporto di conferma**	
	Descrizione sintetica	A seconda dell'esito del controllo sull'IPdV viene prodotto un rapporto di conferma che viene restituito al sistema versante. **NOTA BENE:** il rapporto di conferma non implica la presa in carico del versamento da parte del sistema
FASE 4	**Eventuale rifiuto del pacchetto di versamento, nel caso in cui le verifiche di cui alla FASE 2 abbiano evidenziato anomalie e/o non conformità**	
	Descrizione sintetica	Alternativamente alla fase 3 viene restituito al sistema versante l'indicazione di eventuali anomalie. In tale caso il versamento viene rifiutato
FASE 5	**Ricezione dei documenti**	
	Descrizione sintetica	Il sistema si mette in attesa dei documenti del PdV
FASE 6	**Verifica dei documenti**	
	Descrizione sintetica	In questa fase vengono condotti i controlli specifici del documento ricevuto
FASE 7	**Generazione automatica del rapporto di versamento relativo a ciascun pacchetto di versamento, univocamente identificato dal sistema di conservazione e contenente un riferimento temporale, specificato con riferimento al Tempo Universale Coordinato (UTC), e una o più impronte, calcolate sull'intero contenuto del pacchetto di versamento, secondo le modalità di seguito descritte**	
	Descrizione sintetica	Una volta ricevuti correttamente, o con warning, tutti i documenti del PdV viene prodotto il PdV
FASE 8	**Sottoscrizione del rapporto di versamento con firma digitale apposta da ARUBA**	
	Descrizione sintetica	Il RdV viene firmato digitalmente dal Responsabile del servizio di Conservazione o da un suo delegato. Infine il RdV viene inviato al Cliente via email PEC. In questa fase Aruba prende in carico il versamento ufficialmente
FASE 9	**Preparazione e gestione del Pacchetto di Archiviazione (c.d. Pacchetto di Archiviazione)**	
	Descrizione sintetica	Il Pacchetto di Archiviazione è un insieme di metadati in grado di fornire prova dell'integrità dell'insieme dei documenti, ad esso correlati la cui conservazione decorre da una data determinata, la cui prova di integrità è fornita tramite una firma elettronica qualificata, corroborata da una marca temporale. La struttura del Pacchetto di Archiviazione è costruita sulla base delle specifiche della struttura dati (UNI 11386:2010) contenute nell'allegato 4 alle regole tecniche e secondo le modalità riportate nel manuale della conservazione
FASE 10	**Sottoscrizione del Pacchetto di Archiviazione con firma digitale apposta da ARUBA e apposizione di una validazione temporale con marca temporale alla relativa impronta. Tale operazione viene in breve chiamata anche "Chiusura del Pacchetto di Archiviazione"**	
	Descrizione sintetica	Il Pacchetto di Archiviazione (PdA), che viene costruito dal versamento di uno o più PdV, viene "chiuso" nel momento in cui tutti i PdV sono stati presi in carico dal sistema. La chiusura viene sancita dall'apposizione di opportuna marca temporale, per stabilirne l'istante di creazione, e firma digitale del Responsabile del servizio di Conservazione o di un suo delegato, per garantirne l'immodificabilità. Con la suddetta firma apposta in calce al Pacchetto di Archiviazione e la suddetta dichiarazione il conservatore NON SOTTOSCRIVE il contenuto e la semantica dei documenti conservati ma asserisce solamente che il processo di conservazione è stato eseguito correttamente, nel rispetto delle norme giuridiche e delle indicazioni contrattuali di servizio.
FASE 11	**Preparazione e sottoscrizione con firma digitale di ARUBA del Pacchetto di Distribuzione ai fini dell'esibizione richiesta dall'utente**	
	Descrizione sintetica	Il Pacchetto di Distribuzione (PdD) è definito in base alle esigenze del richiedente e può contenere anche un set parziale di metadati. È generato a partire dai pacchetti di archiviazione. Nel caso più semplice il PdD contiene dei duplicati del PdA. In alternativa esso può essere costituito da una scelta di documenti conservati selezionati attraverso una o più interrogazioni. I risultati di tali ricerche possono essere raccolti in un'area di lavoro e da qui può essere prodotto il PdD voluto.
FASE 12	**Produzione di duplicati informatici effettuati su richiesta del Cliente in conformità a quanto previsto dalle regole tecniche in materia di formazione del documento informatico**	
	Descrizione	Per duplicato informatico si intende il documento informatico ottenuto mediante la

copia informatica per consultazione

	sintetica	memorizzazione, sullo stesso dispositivo o su dispositivi diversi, della medesima sequenza di valori binari del documento originario. I duplicati informatici hanno il medesimo valore giuridico, ad ogni effetto di legge, del documento informatico da cui sono tratti, se prodotti in conformità alle regole tecniche in materia di formazione del documento informatico, ovvero se contiene la stessa sequenza di bit del documento informatico di origine.
FASE 13	**Eventuale scarto del Pacchetto di Archiviazione dal sistema di conservazione alla scadenza dei termini di conservazione previsti dal *Contratto* di servizio, dandone preventiva informativa al Cliente al fine di raccoglierne il consenso**	
	Descrizione sintetica	Alla scadenza dei termini di conservazione, il cliente in autonomia può decidere di cancellar ei documenti in conservazione.

Torna al sommario

7.11 Audit Log

Il sistema di conservazione registra per ogni evento rilevante a quanto definito nella normativa relativa al processo di conservazione.

In particolare sono gestiti i seguenti eventi:

- Creazione PDA
- Conservazione PDA
- Invio Rapporto di Versamento
- Invio Rapporto di Conservazione
- Esibizione PDD
- Download Documento
- Scarto PDA
- Verifica Integrità PDA

Il log di audit è consultabile tramite applicativo dal produttore e attraverso il sistema di back office a chi gestisce il servizio o a pubblico ufficiale che ne faccia richiesta.

Il log viene salvato in apposito database e rimane disponibile nel tempo per consultazione. Oltre al log di audit sono presenti altri log di servizio relativi ad altri eventi generati dal sistema durante il processo di conservazione.

Torna al sommario

8 Il sistema di conservazione

8.1 Infrastruttura informatica datacenter

I Data Center dal quale sono erogati i servizi si trovano sul territorio nazionale e sono conformi ai requisiti della normativa ISO/IEC 27001:2013.

Nelle due strutture che verranno messe a disposizione per l'erogazione dei servizi viene data grande importanza alla sicurezza degli ambienti e dei dati in essi contenuti. Per questo sono presenti tutta una serie di sistemi che permettono di garantire integrità degli ambienti e dei servizi.

Torna al sommario

8.2 Caratteristiche generali della soluzione di conservazione

La soluzione, come meglio descritto in seguito, presenta le seguenti caratteristiche peculiari:

- architettura di produzione implementata su infrastruttura virtuale e storage dedicati predisposta totalmente ridondata (HA) presso il Data Center di proprietà del gruppo Aruba, certificato **ANSI/TIA 942-A Rating IV (ex Tier)**, sito in via Gobetti 96, Arezzo;

copia informatica per consultazione

- architettura secondaria predisposta per consentire la doppia scrittura del dato, effettuata attraverso procedura applicativa, e la replica sincrona storage based della piattaforma virtuale, inclusi i DB documentali e gestionali, situata presso il Data Center di proprietà del gruppo Aruba, sito in via Ramelli, Arezzo;

Il Sistema di Conservazione è sviluppato in modo modulare consentendo una facile scalabilità semplicemente aggiungendo unità e potenza elaborativa ai moduli sottoposti al maggior carico. Vista l'esperienza del Gruppo Aruba nell'ambito della gestione di grandi volumi di dati è sempre stato un obiettivo per il Gruppo creare architetture che possiamo definire elastiche: "espandibili" in caso di aumento del carico di lavoro oppure "limitabili" nel caso di una riduzione delle necessita.

L'intera soluzione è stata progettata per essere quindi in grado di gestire l'elaborazione di grandi volumi di dati, scalando sia verticalmente che orizzontalmente in ognuna delle sue singole componenti, con un elevato livello di affidabilità, distribuendo su più server fisici nodi con il medesimo ruolo ed evitando single point of failure.

L'architettura modulare del sistema è implementata al 100% su infrastruttura di virtualizzazione con hypervisor VMware e garantisce i sintesi i seguenti vantaggi:

Affidabilità - Totale ridondanza ai guasti HW

- Funzionalità di HA implementata dall'architettura virtuale.
- Almeno due moduli con il medesimo ruolo posizionati su server fisici separati.
- DBMS in configurazione Master-Master.
- Utilizzo di sistemi di firma e marca ad alte prestazioni in HA

Architettura scalabile

- Nodi di Front-End ed Application multipli e contemporaneamente attivi.
- Storage di livello Enterprise ad alte prestazioni per la piattaforma VMware e le componenti DB
- Funzionalità di replica

Torna al sommario

8.3 Componenti Logiche

Di seguito riportiamo l'immagine rappresentativa delle componenti logiche del sistema di conservazione:

copia informatica per consultazione

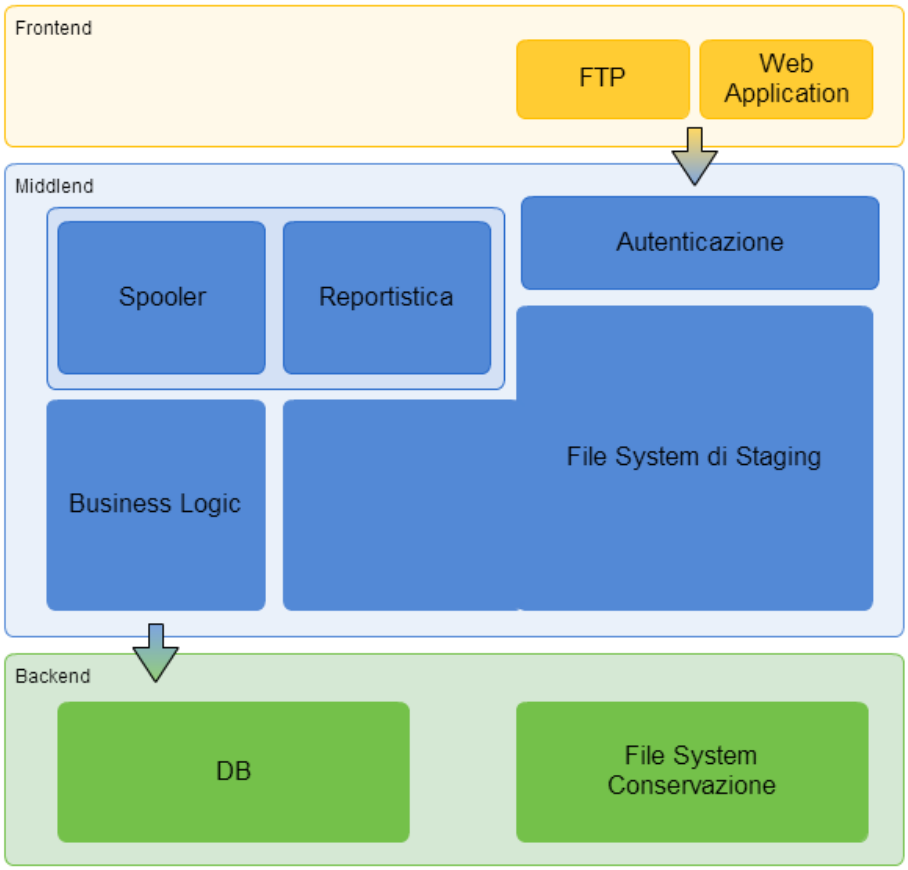


Figura 2: Rappresentazione delle componenti logiche

Come si evince dalla figura l'architettura è basata su una soluzione multi-tier a 3 livelli:

- **Presentation layer**: L'applicazione è pensata per essere scalabile, aumentando il numero dei Web container attraverso una logica di server clustering, gestita automaticamente dal sistema, che, a seconda del livello di carico di ciascun server, distribuirà al meglio le richieste dei client

- **Business logic (o application) layer**: La Business Logic implementa l'intelligenza necessaria per gestire le varie istanze di backend sia in scrittura, sia in fase di ricerca, distribuendo le query sulle varie istanze disponibili. Tutte le istanze backend sono sempre disponibili almeno in lettura

- **Store (& Database) layer**: la parte di back end è composta da diverse istanze. Ogni istanza è costituita dal DB e dal relativo file system. Il DB è duplicato in modalità Master-Master su due nodi predisposti sull'ambiente virtuale e contiene i metadati conservati; il FS contiene l'archivio (dati conservati) e viene replicato con strumenti di basso livello.

Torna al sommario

8.4 Componenti tecnologiche

Il sistema di conservazione Aruba PEC è composto da varie parti e tecnologie, con l'obiettivo di trarre il meglio dalla loro sinergia.

Le principali componenti software che interagiscono all'interno del sistema sono:

- Sistema documentale quale CMS di riferimento
- DB per la gestione dei dati di sistema e dei metadati legati ai materiali in conservazione
- Sistema LDAP per le operazioni di registrazione, autenticazione e controllo degli accessi degli utenti al

copia informatica per consultazione

sistema, indipendentemente dall'interfaccia scelta

- Web server e servlet container per le interfacce di frontiera (Web e Web Service)
- Un sistema di message broker per la gestione delle code in ingresso dei documenti in conservazione sulle interfacce di caricamento massivo (FTP e Web Service)
- Motore di Ricerca per la gestione dei dati di audit

Torna al sommario

8.5 Componenti fisiche

La soluzione è composta da due infrastrutture fra loro interconnesse:

- un sito di Produzione completamente autosufficiente e con tutte le componenti ridondate in HA e collegato tramite fibre ottiche dedicate e di proprietà, con doppia via, al sito secondario,
- un sito Secondario di DR predisposto alla replica dei dati e con le componenti necessarie ad una ripartenza del servizio.

Tutte le componenti utilizzate sono di tipologia enterprise e, come tutte le soluzioni implementate da ARUBA, utilizzano prodotti di marche ampliamente riconosciute e leader del mercato di riferimento.

Torna al sommario

8.5.1 Sito Primario (Produzione)

Il sito di produzione ospita una infrastruttura virtuale basata su soluzione VMware sul quale vengono istallati:

- i nodi di Front-End (almeno due) per le interfacce di caricamento, esibizione e gestione,
- gli Application o Business Logic server (almeno due),
- i backend server, un singolo nodo per ogni istanza,
- un nodo virtuale dedicato al DB server di ogni istanza di backend, la seconda copia in Master-Master è installata sul sito secondario,
- un nodo virtuale per la gestione delle code del sistema di caricamento,
- un nodo virtuale che implementa il DB che contiene tutte le informazioni per la gestione dell'infrastruttura (configurazione, accounting, etc.), la seconda copia in Master-Master è installata sul sito secondario,
- Storage di livello enterprise per l'archiviazione dei documenti;
- Link ed interfacce verso i sistemi di Firma e Marcatura presenti nel medesimo data Center

La figura sottostante schematizza quanto implementato sul sito principale senza entrare nelle specifiche modalità di replica.

Al fine di garantire i ridondanza e bilanciamento del traffico vengono utilizzati dispositivi di load balancing in grado di distribuire il carico di lavoro su un numero di macchine virtualmente illimitato. Questo meccanismo permette di risolvere oltre a problemi prestazionali con la semplice aggiunta a caldo di nuove macchine, anche problemi relativi ad eventuali guasti delle componenti bilanciate, nonché la manutenzione programmata dei singoli nodi.

copia informatica per consultazione

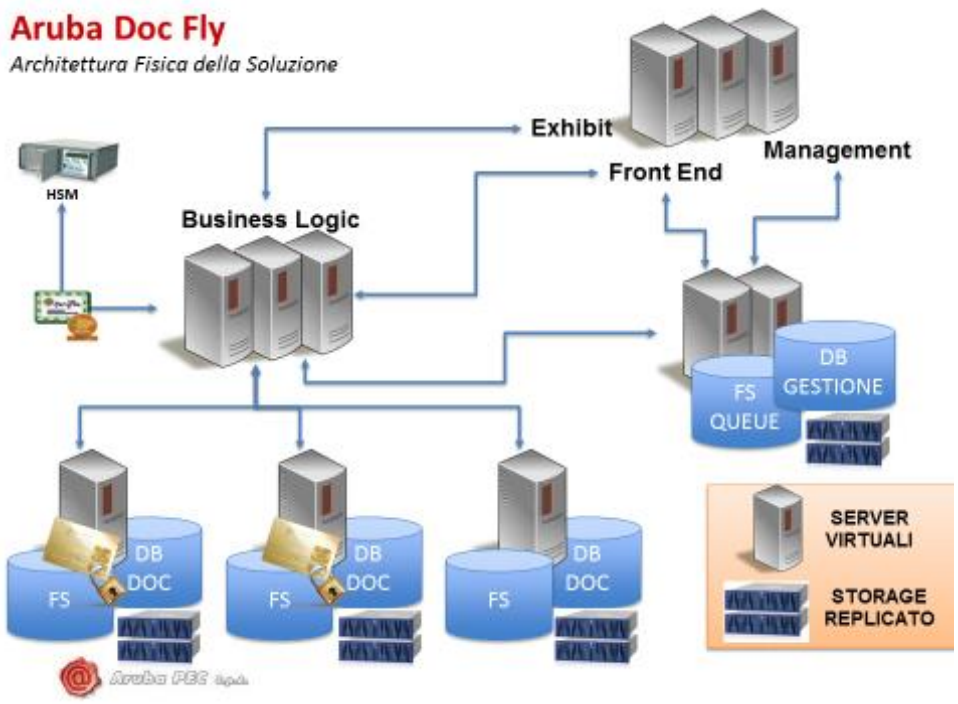


Figura 3: Rappresentazione architettura fisica della soluzione

Torna al sommario

8.5.2 Sito Secondario (DR)

Il sito secondario ospita un'infrastruttura virtuale basata su VMWare sulla quale vengono installati:

- Server di backend corrispondente ad uno dei nodi ridondati dell'ambiente di produzione
- Server DB sincronizzato in maniera sincrona (master-master) con i DB di produzione
- Storage enterprise su cui vengono sincronizzati i dati in maniera asincrona che saranno resi disponibili ai server del sito secondario per ripristinare il servizio
- Collegamenti verso i sistemi esterni di firma e Marcatura temporale (sempre situati nel sito secondario)
- Macchine virtuali replicate dal sito primaro (1 per ciascuna tipologia)

Nello specifico le macchine replicate dal sito primario sono quelle che forniscono i seguenti servizi:

- Frontend Web
- Frontend WS
- Business Logic
- Indicizzazione
- Audit
- Autenticazione

La procedura di switch tra il sito primario ed il secondario è basata tramite il cambio dei puntamenti a livello di DNS.

La figura sottostante schematizza la modalità di replica delle componenti non replicate applicativamente, ad esclusione quindi dei dati archiviati, replicati con doppia scrittura e DB, configurati in Master-Master.

copia informatica per consultazione

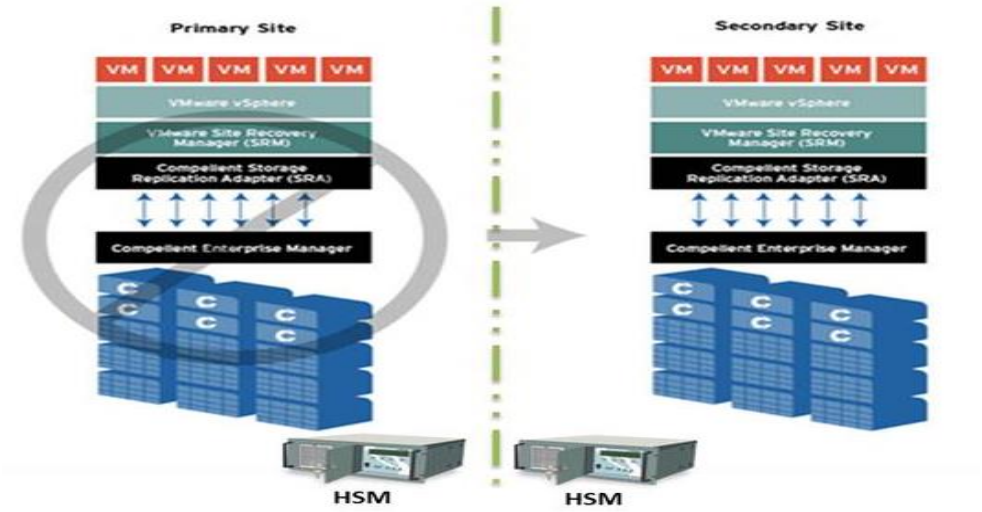


Figura 4 Schema logico della soluzione di Disaster Recovery

In caso di problemi sul sito di Produzione è possibile effettuare la riattivazione del servizio, senza perdita di dati entro 24 ore.

Torna al sommario

8.6 Procedure di gestione e di evoluzione

In linea con quanto previsto dalla circolare n° 65, nell'allegato "REQUISITI DI QUALITÀ E SICUREZZA PER L'ACCREDITAMENTO E LA VIGILANZA, sono descritte le procedure in riferimento a:

- conduzione e manutenzione del sistema di conservazione;
- gestione degli audit-log e loro conservazione;
- monitoraggio del sistema di conservazione:
- change management;
- verifica periodica di conformità a normativa e standard di riferimento

Riguardo i primi tre aspetti, si richiama il documento "MGA_A_38-01 Politica per la gestione dei beni, delle capacità e delle modifiche" I documenti in oggetto descrivono strategie di continuità, considerando tutte le componenti organizzative, operative, del business, tecnologiche, infrastrutturali che contribuiscono all'intero sistema e processo di conservazione.

Torna al sommario

8.6.1 Change management

Qualsiasi operazione di upgrade per evoluzione o bug fixing di una qualsiasi componente del sistema di conservazione Aruba PEC segue una procedura standardizzata atta a operare per garantire il minimo impatto su eventuali fermo servizio e la massima sicurezza possibile riguardo ai dati e documenti a sistema.
Tale procedura si basa sui seguenti assunti:

- ogni componente sviluppata è conservata in opportuno sistema di versionamento del codice
- i file di configurazione di ogni componente sono separati dai compilati in maniera da garantire un accesso più flessibile e veloce al personale addetto
- sono state predisposte apposite macchine di deploy per la compilazione e creazione dei pacchetti delle varie componenti da installare

Ogni aggiornamento del sistema passa da un flusso ben definito che consente contemporaneamente di mantenere stabile e sicura l'intera soluzione in uso dall'esterno e di sviluppare senza ostacoli nuove funzionalità.

copia informatica per consultazione

Tale procedura risulta di particolare importanza anche per garantire l'accesso controllato e limitato a pochi addetti agli ambienti di produzione.

In particolare vengono messi a disposizione 4 ambienti di lavoro: sviluppo, test, collaudo e produzione.
Tutti gli sviluppi vengono condotti e testati nell'ambiente sviluppo che è di uso esclusivo agli sviluppatori per le sue caratteristiche di continua trasformazione.

Qualsiasi altro attore esterno al team di sviluppo non ha nessun accesso a tale ambiente.

Il codice sviluppato viene conservato all'interno di un sistema di versionamento organizzato in maniera da permettere qualora sia necessario l'estrazione di una qualsiasi versione del software. Una volta che un nuovo modulo software è pronto, esso viene registrato nel sistema di versionamento associandogli un tag/versione.

Per operare l'installazione sull'ambiente di test, deputato ai test pre-collaudo, i sorgenti vengono scaricati su un ambiente di deploy, esterno all'ambiente di test stesso, direttamente dal sistema di versionamento, insieme a eventuali script automatici di compilazione, installazione e configurazione.

Sull'ambiente di test il team della QA (Quality Assurance) effettua i test per verificare la corretta implementazione dei moduli rilasciati ed effettua anche i test regressione.

Solo se il processo di testing va a buon fine si procede con il rilascio dei nuovi moduli nell'ambiente di collaudo e produzione con la medesima procedura utilizzata per l'ambiente di test.

Torna al sommario

8.6.2 Verifica periodica di conformità a normativa e standard di riferimento

Aruba, in qualità di conservatore, svolge una verifica periodica della conformità alle normative ed agli standard. di riferimento. A tal proposito, viene effettuata una volta l'anno, una verifica sulla rispondenza ai requisiti di qualità e sicurezza avvalendosi dello strumento di check list, sulla base dell'allegato della circolare n° 65, attraverso il quale viene registrata l'aderenza o meno alla conformità richiesta.

copia informatica per consultazione

9 Monitoraggio e controlli

In questo capitolo si riporta la descrizione delle procedure di monitoraggio della funzionalità del sistema di conservazione e delle verifiche sull'integrità degli archivi con l'evidenza delle soluzioni adottate in caso di anomalie.

9.1 Procedure di monitoraggio

ARUBA assicura la verifica periodica del funzionamento, nel tempo, del sistema di conservazione. Tali verifiche, descritte in "MGA_A_38-01 Politica per la gestione dei beni, delle capacità e delle modifiche", sono riportate in maniera dettagliata all'interno dei documenti "MGA_A_25-03 Layout Logico" e "MGA_A_35-03 Politica di Backup".

Il controllo della buona funzionalità del sistema di conservazione avviene tramite apposite funzionalità di monitoraggio del software. Esse mostrano l'esito delle operazioni automatiche eseguite sul sistema di conservazione come la generazione dei pacchetti di archiviazione, la chiusura dei pacchetti di archiviazione e la verifica dell'integrità degli archivi.

Unitamente all'esito delle predette operazioni vengono controllati anche i log delle operazioni medesime al fine di avere maggiore certezza di quanto effettivamente eseguito dal sistema di conservazione. Tutte queste informazioni sono controllate per ciascun singolo cliente.

Il monitoraggio avviene inoltre anche a livello di processi di elaborazione sul sistema di conservazione. Questo permette di individuare eventuali casi di processi bloccati che potrebbero inficiare il funzionamento del sistema stesso.

Un ultimo controllo del buon funzionamento del sistema può avvenire tramite il monitoraggio delle tracciature che vengono effettuate a livello di database. Tutte le operazioni eseguite determinano infatti la creazione di apposite revisioni che registrano tutte le modifiche intervenute sul sistema permettendo eventualmente di ripristinare i dati a seguito di situazioni anomale.

Torna al sommario

9.2 Verifiche sugli archivi

ARUBA assicura la verifica periodica, **con cadenza non superiore a 36 mesi**, dell'integrità degli archivi e della leggibilità degli stessi; assicura, inoltre, agli organismi competenti previsti dalle norme vigenti l'assistenza e le risorse necessarie per l'espletamento delle attività di verifica e di vigilanza.

Il sistema di conservazione esegue periodicamente ed automaticamente le operazioni di controllo dell'integrità degli archivi. Tali operazioni vengono eseguite solo su una certa percentuale dell'archivio che viene definita nella configurazione del sistema di conservazione.

Il controllo eseguito è di due tipologie:

- **controllo di leggibilità:** consiste nel rendere disponibile attraverso una macchina virtuale un viewer per la visualizzazione dei documenti conservati. Il viewer specifico viene fornito sulla base dell'estensione del documento (mime type) e della versione del formato associato. Il dettaglio di tutte. La lista delle tipologie supportate è definita nella procedura "*Registro dei formati supportati da DocFly2*". Per ogni formato presente nel registro è individuato il relativo programma che ne permette la corretta visualizzazione(viewer). Il registro viene tenuto aggiornato sulla base dei nuovi formati o di quelli che diventano obsoleti. Conseguentemente sono aggiornati i viewer presenti sulla macchina virtuale per la corretta leggibilità dei documenti conservati. Ulteriori dettagli operativi sulla verifica della leggibilità sono disponibili sulla procedura *MGA_A_77-01_Procedura leggibilità documenti in conservazione a norma*.
- **controllo di integrità:** consiste nel ricalcolare l'hash di ciascun oggetto e verificare che corrisponda all'hash memorizzato nel sistema. Questo fornisce una ragionevole certezza dell'integrità degli oggetti dato che la funzione di hash restituisce un valore differente anche a seguito della modifica di un solo bit dell'oggetto.

La combinazione dei due tipi di controllo descritti non fornisce però garanzia di poter visualizzare correttamente

copia informatica per consultazione

il documento e che lo stesso sia effettivamente intellegibile dall'uomo.

Infatti questa garanzia non può essere fornita senza entrare nel merito del documento stesso. La garanzia della corretta visualizzazione del documento è d'altro canto garantita dalla scelta del formato PDF/A per i documenti conservati. Questo formato possiede infatti la caratteristica intrinseca di fornire leggibilità a lungo termine oltre all'ulteriore garanzia di essere basato su specifiche pubbliche (ISO 19005:2005).

Torna al sommario

9.2.1 Pianificazione delle verifiche periodiche da effettuare

La verifica dell'integrità degli archivi viene effettuata sui filesystems in cui i documenti sono replicati, controllando tutti i file presenti in nei PdA conservati.

Viene verificato che i file distribuiti nei filesystems siano identici mediante:

- controllo del nome e della dimensione dei file presenti sui filesystems;
- calcolo dell'hash di ogni singolo file. Il valore viene confrontato con l'hash del corrispondente file censito nell'IPdV del PdA.

Il controllo su ciascun PdA conservato viene effettuato a intervalli temporali. La prima dell'integrità del PdA verifica viene effettuata entro 36 mesi dalla conservazione del PdA. Le successive verifiche vengono effettuate entro 36 mesi dalla conclusione dell'ultima verifica effettuata.

Torna al sommario

9.2.2 Mantenimento della firma per il periodo di conservazione

Il sistema di conservazione si avvale di un fornitore terzo (Certificatore accreditato) per le attività di firma digitale e di marcatura temporale. Questo fornitore garantisce che gli elaboratori che offrono il servizio di marcatura temporale e di firma digitale sono protetti da livelli di protezione logica estremamente elevati. La medesima collocazione fisica del sistema garantisce gli elaboratori dalla possibilità di compromissioni fisiche grazie agli accorgimenti tecnici atti ad impedire accessi non autorizzati da persone e danneggiamenti da eventi accidentali. Non è infatti consentito l'accesso e la permanenza di una sola persona. I locali ove si svolgono le procedure di firma e marca sono dotati di sofisticati impianti di allarme, telecamere, microfoni, rilevatori di movimento (che si attivano soltanto quando nessuna persona vi è presente), al fine di controllare ogni movimento all'interno degli stessi.

Torna al sommario

9.3 Soluzioni adottate in caso di anomalie

In caso di anomalie riscontrate a seguito del monitoraggio delle funzionalità del sistema di conservazione e delle verifiche sull'integrità degli archivi, sono presenti apposite procedure di emergenza (contingency) e piani di Business Continuity da applicare in attesa del ripristino del servizio (così come descritto dal Disaster Recovery Plan del Gruppo Aruba)

Torna al sommario

copia informatica per consultazione

10 Specifiche contrattuali

I documenti costituenti l'impianto contrattuale del servizio di conservazione a norma sono riportati nelle condizioni/accordo di fornitura.

ARUBA, in linea con la normativa vigente, garantisce contratti o accordi scritti che specificano e disciplinano diritti e responsabilità delle Parti, versamento e acquisizione, mantenimento, accesso, ritiro, deposito, diritti e responsabilità di conservazione sui i documenti che tratta, natura economica e di servizio

Ai fini dell'attivazione ed erogazione del servizio di conservazione il Cliente sottoscrive e perfeziona il relativo Contratto. SI tratta del contratto con il quale il Cliente affida ad ARUBA la conservazione digitale dei documenti informatici di cui è titolare nonché dei documenti informatici di titolarità di terzi soggetti dallo stesso prodotti, sottoscritti digitalmente e versati in conservazione in virtù di specifico affidamento a tal fine sottoscritto dai suddetti terzi in favore del Cliente.

Torna al sommario

10.1.1 Nomina di Aruba quale responsabile del servizio di conservazione e del trattamento dei dati

Ai fini dell'erogazione del servizio di conservazione digitale a norma, il Cliente nomina e affida ad ARUBA quale Responsabile del Servizio di Conservazione e Responsabile esterno del trattamento dei dati come previsto dalla vigente normativa in materia di protezione dei dati personali (Regolamento (UE) 2016/679 e D.Lgs. 196/2003 e s.m.i.) e indicato all'art 6 co. 8 delle nuove regole tecniche (DPCM del 3 Dic 2013). Pertanto, i ruoli di Responsabile della conservazione e di Titolare del trattamento sono ricoperti dal Cliente, mentre i ruoli di Responsabile del servizio di conservazione e di Responsabile del trattamento dei dati saranno ricoperti da ARUBA.

Torna al sommario

10.1.2 Scheda di conservazione

Il documento denominato "Scheda di conservazione" costituisce parte integrante e sostanziale del Contratto.

Il Produttore condivide con ARUBA le caratteristiche, le modalità ed i termini di versamento dei documenti informatici da sottoporre a conservazione digitale, approvando espressamente quanto indicato nelle scheda conservazione.

Il contenuto della Scheda di conservazione è volto a precisare:

- le tipologie di documenti da conservare;
- i metadati minimi riferiti ad ogni classe/tipo documento
- eventuali (metadati) extrainfo riferiti ad ogni classe/tipo documento sui quali effettuare specifici controlli;
- i formati da adottare per ogni classe/tipo documento.

Torna al sommario

10.1.3 Elenco Persone

Ai fini dell'affidamento del servizio di conservazione digitale di documenti informatici, il Cliente comunica l'identità delle persone fisiche dallo stesso ufficialmente incaricate di mantenere i rapporti con ARUBA e titolate ad operare in nome e per conto del Produttore medesimo, precisandone funzione e ruolo.

Torna al sommario

10.2 Modello di funzionamento del servizio

L'obiettivo ed il compito di ARUBA è quello di conservare i documenti informatici del Cliente con sistemi coerenti alla normativa regolante la conservazione digitale dei documenti informatici.

In particolare, il servizio di conservazione digitale di ARUBA soddisfa le seguenti funzioni d'uso:

copia informatica per consultazione

- salvaguardia dell'integrità dei documenti informatici conservati mediante apposizione della firma digitale al Pacchetto di Archiviazione. Nel suddetto Pacchetto di Archiviazione è presente, fra l'altro, l'impronta di ogni singolo documento sottoposto a conservazione;
- prolungamento della validità del documento mediante apposizione della marca temporale al Pacchetto di Archiviazione;
- accesso diretto tramite interfaccia Web ai documenti informatici conservati;
- semplicità di invio e versamento dei documenti informatici da sottoporre a conservazione;
- totale sicurezza nella trasmissione dei documenti informatici da sottoporre a conservazione.

Il sistema di conservazione opera secondo un modello organizzativo che garantisce la sua distinzione logica dal sistema di gestione documentale, qualora esistente presso il Cliente.

In particolare, la conservazione è svolta affidando ad ARUBA il ruolo ed i compiti fissati nell'Atto di Affidamento.

A tal fine, ARUBA ed il Cliente hanno adottato il presente *Manuale* ove sono illustrati dettagliatamente l'organizzazione, i soggetti coinvolti ed i ruoli svolti dagli stessi, il modello di funzionamento, la descrizione dei processi, la descrizione delle architetture e delle infrastrutture utilizzate, le misure di sicurezza adottate ed ogni altra informazione utile alla gestione ed alla verifica del funzionamento, nel tempo, del sistema di conservazione.

Pertanto, al fine di attivare il servizio di conservazione digitale dei documenti informatici è necessario che il Cliente abbia sottoscritto il *Contratto* e gli allegati ad esso relativi, all'interno dei quali vengono, fra l'altro, specificati:

a) i contenuti e le caratteristiche generali del Servizio di conservazione digitale;
b) i termini di decorrenza e la durata del Servizio di conservazione digitale;
c) gli eventuali Servizi Estesi erogati su richiesta del Cliente;
d) le responsabilità e gli obblighi del Cliente;
e) le responsabilità e gli obblighi di ARUBA;
f) le modalità di produzione/formazione/emissione/sottoscrizione dei documenti informatici;
g) la descrizione delle tipologie e delle classi dei documenti informatici da sottoporre a conservazione, comprensiva dell'indicazione dei formati gestiti, dei metadati da associare alle diverse tipologie di documenti e delle eventuali eccezioni;
h) la definizione dell'intervallo di conservazione ossia dell'intervallo di tempo intercorrente tra la presa in carico del pacchetto di versamento e la chiusura del Pacchetto di Archiviazione.
i) Le modalità di distribuzione/esibizione dei documenti informatici conservati;

Torna al sommario

10.2.1 Obblighi del Cliente

Il processo di conservazione impone al Cliente l'istituzione di un'organizzazione interna idonea, che garantisca la piena osservanza delle disposizioni normative in tema di gestione documentale[2] e delle procedure da osservare per la corretta produzione/formazione/emissione e sottoscrizione dei documenti informatici destinati alla conservazione digitale in conformità alle regole tecniche di cui all'art. 71 del CAD ed a quanto stabilito dal presente *Manuale* e dal *Contratto*.

A tale scopo, in base alle specifiche necessità, il Cliente deve, sia dal punto di vista dell'impostazione operativa delle attività propedeutiche alla conservazione digitale dei documenti informatici che dal punto di vista della scelta delle risorse coinvolte nel processo, organizzare il lavoro affinché esso venga svolto secondo i principi stabiliti dalla normativa regolante la conservazione digitale dei documenti informatici.

Il Cliente, quindi, all'interno della propria struttura organizzativa, dovrà aver definito:

a) le procedure propedeutiche alla conservazione digitale a lungo termine dei documenti informatici;
b) le funzioni e le attività affidate, con particolare attenzione alla verifica della congruità e continuità dei processi di produzione/formazione/emissione dei documenti informatici destinati alla conservazione digitale a lungo termine;

[2] Si veda, a puro titolo di esempio, il DPR 28.12.2000, n. 445, il DPCM 3.12.2013 sul protocollo informatico, ove applicabili;

copia informatica per consultazione

c) la gestione delle responsabilità derivanti dalle funzioni ed attività affidate;
d) la documentazione delle deleghe ed il relativo mantenimento;
e) le misure organizzative e tecniche idonee ad evitare danno ad altri.

Il Cliente deve attenersi scrupolosamente alle regole previste dal presente *Manuale*, alle prescrizioni previste nel *Contratto* e negli allegati ad esso relativi.

Il Cliente deve altresì prendere visione del presente *Manuale* prima di inoltrare i pacchetti di versamento e/o qualsiasi altra richiesta a ARUBA.

Torna al sommario

10.2.2 Obblighi di ARUBA

ARUBA, come analiticamente descritto nel *Contratto*, limitatamente alle attività ad essa affidate, è responsabile verso il Cliente per l'adempimento degli obblighi discendenti dall'espletamento delle attività previste dalla normativa vigente in materia di conservazione digitale di documenti informatici.

In particolare, ARUBA, ai fini dell'erogazione del Servizio oggetto del *Contratto*, svolge le attività ad essa affidate dal Cliente come in dettaglio riportate nel documento "*Atto di Affidamento*", nei modi e nei termini specificati nel presente *Manuale* e negli allegati ad esso relativi.

Pertanto è obbligo di ARUBA conservare digitalmente i documenti informatici del Cliente allo scopo di assicurare, dalla presa in carico e fino all'eventuale cancellazione, la loro conservazione a norma, garantendone, tramite l'adozione di regole, procedure e tecnologie, le caratteristiche di autenticità, integrità, affidabilità, leggibilità e reperibilità.

Il Sistema di conservazione di ARUBA è in grado di esibire tutti i documenti informatici in esso conservati in qualsiasi momento del periodo di conservazione; a tal fine, ARUBA ha in essere procedure adeguate a soddisfare, senza indebiti ritardi, le richieste di accesso, esibizione o consegna dei documenti conservati, effettuate dai soggetti debitamente autorizzati.

Oltre alla restituzione dei documenti informatici trasferiti e conservati presso ARUBA, viene garantita anche la restituzione delle relative evidenze informatiche che comprovano la corretta conservazione degli stessi, fornendo gli elementi necessari per valutare la loro autenticità e validità giuridica.

Non rientra fra i Servizi offerti da ARUBA la conservazione di documenti analogici.

Torna al sommario

10.2.3 Compiti organizzativi

ARUBA provvede alla realizzazione di una base di dati relativa ai documenti informatici che il Cliente versa in conservazione, gestita secondo i principi di sicurezza illustrati nel presente *Manuale* e nel *Contratto* attuati adottando procedure di tracciabilità tali da garantire la corretta conservazione, l'accessibilità a ogni singolo documento e la sua esibizione.

ARUBA si occupa altresì di definire:

a) le caratteristiche ed i requisiti del sistema di conservazione in funzione della tipologia dei documenti da conservare e organizzare gli stessi in modo da garantire la corretta conservazione e la sicurezza dei dati, anche al fine di poterli prontamente produrre, ove necessario;
b) le procedure di sicurezza e tracciabilità che consentano di risalire in ogni momento alle attività effettuate durante l'esecuzione operativa di conservazione.
c) le procedure informatiche ed organizzative per la corretta tenuta dei supporti su cui vengono memorizzati i documenti informatici oggetto di conservazione.
d) le procedure informatiche ed organizzative atte ad esibire la documentazione conservata, in caso di richieste formulate da chi ne abbia titolo.

copia informatica per consultazione

ARUBA si occupa di redigere e sottoporre a revisione il presente *Manuale*. Il Cliente si dovrà dotare di un proprio Manuale della Conservazione costituito dalla descrizione di componenti, processi ed organizzazione propri, integrato e completato, se ritenuto necessario, dal presente *Manuale*.

Torna al sommario

10.2.4 Compiti di manutenzione e controllo

ARUBA provvede a:

- mantenere un registro cronologico del software dei programmi in uso nelle eventuali diverse versioni succedute nel tempo ed un registro cronologico degli eventi di gestione del sistema di conservazione comprensivo delle risoluzioni adottate per rimuovere eventuali anomalie;
- implementare specifici controlli di sistema per individuare e prevenire l'azione di software che possano alterare i programmi ed i dati;
- verificare la corretta funzionalità del sistema e dei programmi in gestione;
- analizzare e valutare periodicamente la registrazione degli eventi rilevanti ai fini della sicurezza (analisi del log di sistema);
- definire e documentare le procedure di sicurezza da rispettare per l'apposizione del riferimento temporale;
- mantenere e gestire i dispositivi di firma in conformità con le procedure stabilite dal certificatore qualificato che ha rilasciato i relativi certificati;
- verificare la validità delle marche temporali utilizzate dal sistema di conservazione;
- verificare il buon funzionamento del file system

Torna al sommario

10.2.5 Compiti operativi

ARUBA effettua le seguenti attività:

- supervisione dell'intero sistema di conservazione digitale, verificando accuratamente i processi di apposizione delle firme digitali, dei riferimenti temporali e delle marche temporali, in modo che la procedura rispetti la normativa, assicurandosi che tutto il processo si realizzi secondo le procedure descritte nel presente *Manuale*;
- sincronizzazione dell'ora di sistema di tutti i sistemi utilizzati, verifica e controllo della sincronizzazione del clock di sistema per consentire registrazioni accurate e comparabili tra loro;
- mantenimento della documentazione descrittiva del processo di conservazione aggiornata nel corso del tempo;

Torna al sommario

10.2.6 Fasi del processo di conservazione e responsabilità

Il servizio di conservazione digitale dei documenti informatici è erogato e sviluppato per rispondere alle esigenze di qualsiasi soggetto che abbia l'esigenza di conservare documenti informatici come imprese, professionisti, associazioni, Pubblica Amministrazione centrale e locale. Il servizio permette di conservare i documenti informatici del Cliente, garantendone l'integrità e la validità legale nel tempo nonché la loro "esibizione a norma".

Come già fatto osservare, il sistema di conservazione opera secondo i modelli organizzativi esplicitamente concordati con il Cliente e formalizzati nel *Contratto* e negli allegati ad esso relativi che garantiscono la sua distinzione logica dal sistema di gestione documentale del Cliente, qualora esistente.

Pertanto, la conservazione non viene svolta all'interno della struttura organizzativa del Cliente (soggetto titolare dei documenti informatici da conservare), ma è affidata ad ARUBA, che espleterà le attività per le quali ha ricevuto formale affidamento, nei limiti della stessa e per le quali opera in modo autonomo e ne è responsabile.

La sequenza di attività che vanno dalla fase propedeutica alla formazione dei documenti informatici alla fase di conservazione degli stessi è di seguito schematicamente rappresentata:

copia informatica per consultazione

SISTEMI	FASE	DESCRIZIONE E MACRO FASI DEL PROCESSO DI CONSERVAZIONE	ATTIVITÀ A CARICO DI:	
			CLIENTE	ARUBA
Sistema di gestione documentale del Cliente	1	Produzione/formazione/emissione a norma dei documenti informatici e contestuale generazione dei relativi metadati	X	
	2	Produzione del pacchetto di versamento	X	
	3	Deposito in conservazione del pacchetto di versamento e dei relativi documenti informatici completi di metadati	X	
Servizio di Fatturazione Elettronica e PEC	1a	Produzione/formazione/emissione a norma dei documenti informatici e contestuale generazione dei relativi metadati		X
	2a	Produzione del pacchetto di versamento		X
	3a	Deposito in conservazione del pacchetto di versamento e dei relativi documenti informatici completi di metadati		X
Sistema di Firma Digitale	4	Servizio di Firma Automatica e di eventuale apposizione marca temporale, da effettuare sui documenti tributari prima dell'invio al sistema di conservazione.	X	X
Sistema di conservazione digitale dei documenti informatici	5	Acquisizione da parte del sistema di conservazione del pacchetto di versamento prodotto dal Cliente per la sua presa in carico		X
	6	Verifica che il pacchetto di versamento ed i documenti informatici in esso descritti siano coerenti e conformi alle prescrizioni stabilite dal Contratto di servizio		X
	7	Eventuale rifiuto del pacchetto di versamento o dei documenti informatici, nel caso in cui le verifiche di cui alla fase 6 abbiano evidenziato delle anomalie		X
	8	Generazione, in modo automatico, del rapporto di versamento relativo a ciascun pacchetto di versamento		X
	9	Invio al Cliente del rapporto di versamento		X
	10	Preparazione e gestione del Pacchetto di Archiviazione		X
	11	"Chiusura" del Pacchetto di Archiviazione mediante sottoscrizione con firma digitale di ARUBA e apposizione di marca temporale		X
	12	Richieste di esibizione dei documenti informatici conservati	X	
	13	Preparazione del Pacchetto di Distribuzione ai fini dell'esibizione richiesta dall'utente con tutti gli elementi necessari a garantire l'integrità e l'autenticità degli stessi		X
	14	Richiesta del Cliente di duplicati informatici	X	
	15	Produzione di duplicati informatici su richiesta del Cliente		X

Dal prospetto di cui sopra emerge chiaramente come ogni singola fase del processo è propedeutica alle altre.

In ogni caso, prima di dare corso al processo di conservazione, il Cliente e ARUBA dovranno definire, attraverso il perfezionamento del *Contratto* e degli allegati ad esso relativi, come configurare il servizio in base alle specifiche esigenze del Cliente concordando le modalità di gestione e fruizione oltre alla quantità e tipologia di documenti da conservare.

Torna al sommario

copia informatica per consultazione

11 Livelli di servizio (SLA)

I livelli di servizio relativi all'offerta standard, sono riportati nella tabella in basso e rappresentano le metriche di servizio che devono essere rispettate dal conservatore ARUBA nei confronti dei propri clienti/utenti.

CARATTERISTICHE GENERALI DEL SERVIZIO	SPECIFICHE TECNICHE
Disponibilità complessiva del servizio	99,95%
Assistenza	Sistema di ticketing e canale telefonico
Periodo di fatturazione	Annuale
Durata minima contratto	Un anno (eventuali upgrade richiesti in seguito alla stipula del contratto vanno ad allinearsi alla scadenza riportata sul contratto stesso)
Datacenter su cui è attivabile il servizio	DC1-IT (http://datacenter.aruba.it)
FASI ELABORAZIONE PACCHETTI DI VERSAMENTO	**SPECIFICHE TECNICHE**
Presa in carico del PdV (Generazione del Rapporto di versamento)	Entro 48h dal ricevimento dell'ultimo documento contenuto nel pacchetto di versamento
Invio in conservazione del PdA	Entro 72h dalla presa in carico dell'ultimo PdV valido e completo contenuto nel PdA, nel caso in cui tutti i PdV contenuti nel PdA siano validi e completi[3].
RICHIESTA DI ESIBIZIONE	**SPECIFICHE TECNICHE**
Produzione del Pacchetto di Distribuzione	Entro 4h dalla richiesta di produzione del PdD

Torna al sommario

12 Sicurezza del sistema di conservazione

Aruba PEC ed il Gruppo Aruba hanno implementato un Sistema di Gestione della Sicurezza delle Informazioni (SGSI) conforme alla norma ISO 27001. Nell'ambito del Sistema di Conservazione proposto sono adottate misure di sicurezza fisica, logica e organizzativa coerenti con tale SGSI e con la normativa vigente in tema di protezione dei dati personali (Regolamento (UE) 2016/679 e D.lgs. 196/2003 e s.m.i.).Torna al sommario

12.1 Privacy e requisiti di sicurezza dei dati

Aruba PEC tutela la riservatezza dei dati personali e garantisce ad essi la protezione necessaria da ogni evento che possa metterli a rischio di violazione, trattandoli secondo le specifiche previsioni della vigente normativa in materia.

Come previsto dal Regolamento dell'Unione Europea n. 2016/679 ("GDPR"), ed in particolare all'art. 13, sono fornite all'utente ("Interessato") tutte le informazioni richieste dalla normativa relative al trattamento dei propri dati personali mediante apposita, specifica e preventiva informativa, resa altresì sempre disponibile all'interno del proprio sito istituzionale. Con specifico riferimento ai compiti affidati con la nomina a Responsabile del trattamento dei dati personali, ARUBA comunica di ottemperare a quanto previsto dalla normativa vigente in materia ed alle prescrizioni di cui all'art. 28 del Regolamento (UE) 2016/679.

In conformità con le proprie politiche di sicurezza delle informazioni e del suo sistema di gestione ISO 27001, ARUBA s'impegna a non divulgare, comunicare o diffondere le informazioni e i dati dei quali verrà a conoscenza durante l'espletamento delle attività. Inoltre si impegna a rispettare, nello svolgimento delle attività oggetto del

[3] La gestione dei PdA non validi o non completi è descritta al paragrafo 7.5.2

copia informatica per consultazione

servizio di conservazione, tutti i principi, contenuti nelle disposizioni normative vigenti, relativi al trattamento dei dati personali e in particolare quelli contenuti nel Regolamento (UE) 2016/679 e garantisce che le informazioni personali, patrimoniali, statistiche, anagrafiche, e/o di qualunque altro genere, di cui verrà a conoscenza in conseguenza dei servizi resi, in qualsiasi modo acquisite, vengano considerati riservati e come tali trattati. Si impegnerà infine a dare istruzioni al proprio personale affinché tutti i dati e le informazioni vengano trattati nel rispetto della normativa di riferimento.

Torna al sommario

12.2 Analisi dei Rischi

Il Gruppo Aruba ha svolto un'analisi dei rischi sul Sistema di Conservazione estesa agli aspetti di sicurezza fisica, logica ed organizzativa, incluso il coinvolgimento di enti esterni (fornitori); l'analisi è riportata nel relativo **Piano della Sicurezza** .

Torna al sommario

12.3 Controllo Accessi

Gli utenti possono accedere – previa identificazione ed autenticazione – solamente alle risorse (es. sistemi, funzionalità, informazioni) per cui sono stati esplicitamente autorizzati in base al ruolo ricoperto. I permessi sono attribuiti alle utenze secondo il principio del "least privilege" e rivisti periodicamente per mitigare il rischio di abuso di privilegi. Ad ogni persona (interna od esterna) viene assegnata un'utenza personale e univoca. Le utenze di gruppo sono usate solo per esigenze particolari ed espressamente autorizzate.

Torna al sommario

12.4 Monitoraggio Eventi e Vulnerabilità di Sicurezza

Nell'ambito del Servizio di Conservazione, viene conservata e periodicamente esaminata una traccia (**audit log**) delle operazioni svolte dagli utenti e dai processi, in modo che tali azioni possano essere documentate ed attribuite a chi le ha eseguite o causate (accountability), anche allo scopo di rilevare eventi di sicurezza, incidenti e vulnerabilità associati ai sistemi coinvolti nel processo di conservazione. Tali log vengono archiviati su supporto permanente e non è permesso agli utenti non autorizzati di accedervi.

Torna al sommario

12.5 Cifratura

Come previsto dal Piano della Sicurezza del Servizio di Conservazione di Aruba PEC, tutte le comunicazioni tra il Sistema e gli utenti (interattivi o applicativi) sono protette col protocollo sicuro TLS e pertanto sono cifrate. Per la cifratura del canale, si utilizzano algoritmi di cifratura con chiavi di lunghezza ≥ 128 bit.

Torna al sommario

copia informatica per consultazione

12.6 Backup

Nell'ambito della gestione operativa del Servizio di Conservazione, sono definite ed applicate procedure di backup finalizzate alla creazione e conservazione di copie di sicurezza dei dati, dei software applicativi, delle loro configurazioni e di ogni altra informazione necessaria per ripristinare il servizio in caso di necessità (per es. a fronte di guasti hardware o incidenti più severi).

I dati vengono scritti e salvati sempre in duplice copia sincrona sui sistemi di storage distribuiti geograficamente con la garanzia dell'effettiva scrittura su entrambi i siti. Sui due storage utilizzati inoltre vengono effettuate copie di sicurezza attraverso meccanismi di snapshot per garantire la massima salvaguardia del dato.

I metadati e i dati utenti sono salvati su istanze dedicate distribuite su due siti geografici distinti e configurate in mirror transazionale in modo da avere una duplicazione non solo del dato ma anche di tutti i metadati necessari alla propria reperibilità e ricerca.

Per quanto riguarda i **documenti**, si fa presente che essi sono sempre conservati in **doppia copia**, ciascuna presso un data center separato (per i documenti, dunque, non vi è una reale distinzione tra copia di produzione e copia di backup).

Torna al sommario

12.7 Isolamento delle componenti critiche

I sistemi utilizzati per il Servizio di Conservazione, da un punto dell'architettura fisica, sono posti all'interno di rack dedicati ai servizi eSecurity di Aruba PEC e isolati dagli altri sistemi del datacenter.

In particolare i server e le componenti software del Sistema di Conservazione sono separati logicamente dagli altri Servizi per mezzo di macchine virtuali ed istanze dedicate.

Per quanto concerne il livello organizzativo, questo è parzialmente separato, coerentemente coi requisiti indicati nel Piano della Sicurezza e nel Manuale della Conservazione.

Torna al sommario

12.8 Sicurezza fisica datacenter del Gruppo Aruba

Nelle due strutture che verranno messe a disposizione per l'erogazione dei servizi viene data grande importanza alla sicurezza degli ambienti e dei dati in essi contenuti. Per questo sono presenti tutta una serie di sistemi che permettono di garantire integrità degli ambienti e dei servizi.

copia informatica per consultazione

Figura 5: Immagine esterna del Datacenter

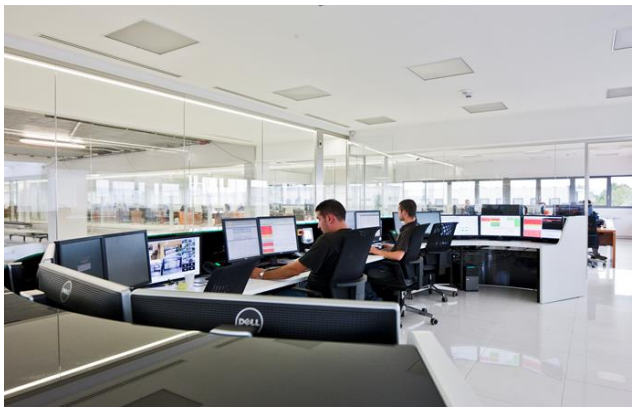


Figura 6: Immagine del Network Operations Center

I datacenter sono situati in un'area classificata come di "basso rischio idrogeologico", inoltre l'edificio è completamente antisismico ed è posto ad un piano rialzato dal livello stradale, in modo da risultare maggiormente protetto alle calamità naturali.

Sia il datacenter primario che quello secondario, sono continuamente monitorati e dotati delle soluzioni di sicurezza più avanzate descritte in seguito.

Torna al sommario

12.8.1 Sicurezza Fisica Data Center Primario

L'edificio primario è situato ad Arezzo in via Gobetti ed è certificato ANSI/TIA 942-A Rating IV (ex Tier). Il datacenter è stato progettato ponendo la massima attenzione alla **sicurezza fisica degli accessi**:

- le **porte esterne** sono di tipo blindato;
- le **finestre** e le **superfici vetrate esterne** a piano terra sono dotate di vetro antiproiettile dello spessore di 21 mm;
- le **griglie per il passaggio dell'aria** necessaria al raffreddamento della sala dati sono protette da sbarre trasversali in acciaio del diametro di 20 mm.

L'**accesso dei visitatori** avviene attraverso una "**bussola**" a due ante rotanti e interbloccate, analoga a quelle normalmente utilizzate negli istituti bancari - anch'essa dotata di vetri anti-proiettile da 21 mm di spessore. Una volta avuto accesso all'interno, è presente una seconda barriera, costituita da varchi motorizzati. Per attraversare tali varchi è necessario essere accreditati alla antistante Reception, con lo scopo di ottenere un badge abilitato. Per la registrazione dei visitatori, è istituito un apposito registro conservato in conformità con quanto previsto dalla **normativa ISO 27001**.

Superata la barriera dei varchi motorizzati, si trova davanti la sala dati principale, delimitata da una parete in vetro antiproiettile da 21 mm. L'accesso, consentito solo al personale abilitato, avviene tramite porte scorrevoli di sicurezza assoggettate al controllo accessi. L'intero stabile è circondato da una resede che lo separa su tutti i lati dalle altre proprietà, e protetto da una recinzione rigida in metallo dell'altezza di 260 cm. La struttura è presidiata e sorvegliata 24x7x365.

Il **data center** è dotato di un **sistema di controllo accessi** esteso a tutti i varchi, sia esterni (ingresso principale, uscite di sicurezza, magazzini, locali tecnici) che interni (sale dati, locali tecnici, uffici). Il riconoscimento è basato su un doppio criterio di autenticazione, mediante l'utilizzo di una tessera di prossimità e la digitazione di un pin.

copia informatica per consultazione

Il sistema di gestione degli accessi prevede la possibilità di abilitare e disabilitare le singole tessere in base alle aree, agli orari ed ad altri parametri, in modo da garantire sia la massima sicurezza degli ambienti che la necessaria fluidità degli accessi. E' possibile generare dettagliati report (per utente, per varco, per data) in modo da ricostruire con la massima precisione - se necessario - i percorsi effettuati da ogni singolo visitatore.

L'edificio è dotato di un **sistema anti-intrusione** che utilizza sensori volumetrici a doppia tecnologia, assieme a sensori a contatti su infissi e sensori di vibrazione sui vetri delle sale dati.

L'impianto è integrato da sistemi evoluti di analisi delle immagini rese disponibili dall'impianto di video-sorveglianza (trattato di seguito). La resede esterna è protetta tramite barriere a raggi infrarossi applicate lungo tutto il perimetro della recinzione esterna. L'impianto anti-intrusione è integrato con il sistema di controllo accessi.

L'**impianto di video-sorveglianza** è costituito da un cospicuo numero di telecamere (oltre 120) posizionate sia all'interno dell'edificio (lungo tutti i punti di passaggio e all'interno dei locali sensibili) che all'esterno (lungo la recinzione, sulla copertura dell'edificio e nella zona dove sono ubicati i gruppi elettrogeni). Le telecamere utilizzate sono di tipologie diverse in base alle diverse esigenze derivanti dai singoli posizionamenti (angolo e distanza di visuale, tipologia di illuminazione, ecc). Le immagini vengono rese disponibili in real-time al personale di presidio mediante appositi monitor presenti all'interno del **NOC**.
Tutte le immagini acquisite vengono immagazzinate tramite videoregistratori digitali, situati in ambienti protetti e conservate per 24H, come previsto dalle vigenti **normative in ambito Privacy**.

Tutto l'edificio è dotato di un **sistema di rilevamento dei fumi** costituito da sensori ottici posizionati in ambiente, sotto al pavimento flottante e sopra il controsoffitto. I sensori sono collegati tra loro in loop e mediante cavo antifiamma, in modo da garantire il loro funzionamento anche in caso di interruzione di un collegamento. Sono stati previsti opportuni sensori in grado di verificare la presenza di fumo all'interno delle condotte per il ricambio dell'aria degli ambienti.

La gestione dell'impianto è demandata ad una centrale a 6 loop, con il compito di rilevare i segnali provenienti dai sensori, attivando gli allarmi ottici e acustici, nonché provvedendo all'attivazione dell'impianto di spegnimento mediante apposite unità di spegnimento. Le aree sensibili e/o a maggiore rischio (2 sale dati, 2 sale tlc, 6 power center, 6 sale trasformatori MT e 2 sale quadri MT) sono dotate di sistema di spegnimento a gas inerte (Azoto).

Il **metodo di spegnimento** è quello della diluizione d'ossigeno, ottenuto mediante una scarica di un'adeguata quantità di azoto in grado di ridurre la percentuale di ossigeno dal 23% presente normalmente in atmosfera al 12% circa, valore che non consente la combustione. Tale scarica non rappresenta un pericolo per la salute delle persone eventualmente ancora presenti nell'ambiente al momento della scarica (comunque annunciata con un anticipo di 60 secondi da allarmi acustici e ottici) e preserva gli apparati consentendo la continuità nell'erogazione dei servizi.

I gruppi elettrogeni di emergenza presenti, posizionati all'esterno, sono dotati di impianti di rilevazione e di spegnimento incendi (ad anidride carbonica) dedicati e autonomi. Tali gruppi sono dotati inoltre di sistema di intercettazione del carburante, in grado di interrompere l'afflusso in caso di incendio. E' inoltre presente la normale dotazione di estintori portatili e carrellati.
I vari locali dell'edificio sono dotati di sensori per il **rilevamento della presenza di liquidi**, posizionati sotto il pavimento flottante. Per quanto riguarda la possibilità di allagamento derivante da rottura delle tubazioni per l'acqua dei servizi igienici (o dalla dimenticanza di rubinetti aperti), è stato previsto un sistema costituito da sensori (flussostati e rilevatori di presenza) e da una logica che, nel caso in cui venga rilevato il flusso di acqua in assenza di persone all'interno dei singoli servizi igienici, provvede all'interruzione dell'erogazione dell'acqua nel medesimo ambiente tramite l'attivazione di una elettrovalvola, eliminando la possibilità di riversamento di acqua a terra.

copia informatica per consultazione

Le eventuali problematiche derivanti da alluvioni sono scongiurate, in quanto la struttura è ubicata in zona pianeggiante ed in posizione rilevata di circa un metro rispetto al piano di campagna. In fase progettuale si è provveduto inoltre a evitare il posizionamento di impianti strategici o di parte di essi a quota inferiore a tale valore: ciò esclude la necessità di sistemi anti-allagamento dotati di pompe idrauliche.

I server dislocati presso il Centro Servizi saranno dotati di meccanismi di sicurezza fisica utili ad impedire il furto locale dei dati. Gli armadi rack sono tutti dotati di sportelli metallici con serratura a chiave e i supporti di memorizzazione contenenti dati sono conservati in luogo sicuro. Gli apparati attivi di rete saranno posizionati in armadi di cablaggio con chiusura a chiave che inibisce l'accesso fisico ai dischi locali e ne impedisce la rimozione.

Tutti gli impianti sopradescritti, assieme agli impianti e sistemi strategici (gruppi elettrogeni, ups, quadri elettrici, condizionamento di potenza) e agli impianti standard (illuminazione, condizionamento uffici) sono supervisionati da un sistema **BMS** (**Building Management System**) a mappe, in grado di gestire tutti gli eventi e gli allarmi, di interpretarli e di assegnare loro le opportune priorità, generando le conseguenti notifiche in modo da ridurre al massimo i tempi di interpretazione e individuazione degli eventi. Il **BMS** - controllato dal personale di presidio del **NOC** (**Network Operation Center**) - è accessibile anche da remoto ed in grado di provvedere alla notifica degli allarmi tramite i consueti canali (e-mail, SMS, ecc).

La pavimentazione flottante è realizzata mediante pannelli in conglomerato ad alta resistenza appoggiate su struttura composta da tubolari in acciaio ed offre adeguate capacità di carico e di resistenza. Al fine di verificare la corrispondenza con i dati del fornitore sono state eseguite prove di carico in laboratorio.

Torna al sommario

12.8.2 Sicurezza fisica Data Center Secondario

La **sicurezza fisica** del **data center** secondario viene garantita attraverso:

- un sistema di video-sorveglianza che utilizza telecamere motorizzate per tenere sotto controllo i punti nevralgici della struttura;
- un sistema di allarme che rileva automaticamente eventuali vibrazioni o aperture non autorizzate di ingressi e di infissi;
- un impianto anti-intrusione – monitorato dal NOC - che utilizza rilevatori di presenza a doppia tecnologia (micro-onde e raggi infrarossi), contatti magnetici e barriere a raggi infrarossi per proteggere le zone in cui gli ambienti sono suddivisi e prevenire l'apertura non autorizzata di ingressi ed infissi;
- sistema di controllo accessi che permette l'accesso al solo personale autorizzato, dotato di badge con tecnologia RFID e codice PIN personale;
- un sistema anti-incendio a gas inerti (non tossici) - connesso a rilevatori di fumo posti sopra e sotto al pavimento flottante – che si attiva automaticamente inondando di gas solo la zona colpita;
- un sistema di rilevazione liquidi che permette di intercettare - dal NOC e tramite appositi allarmi acustici in loco - eventuali fuoriuscite di liquido dagli impianti tecnologici;
- un sistema centrale server per archiviare e consultare (da personale autorizzato tramite accesso protetto) qualsiasi accesso ai locali, che solo avviene attraverso RFID associato a codice numerico.

Anche nel sito secondario, i server saranno dotati di meccanismi di sicurezza fisica utili ad impedire il furto locale dei dati: gli armadi rack sono provvisti di sportelli metallici con serratura a chiave; i supporti di memoria dati sono conservati in un luogo sicuro ed i server sono protetti da un apposito sportello con chiusura a chiave (come inibizione dell'accesso fisico e della rimozione).

Torna al sommario

copia informatica per consultazione

12.8.3 Sicurezza organizzativa comune ai due data center

Aruba garantisce inoltre la sicurezza organizzativa delle strutture, che viene continuamente adeguata in caso di evoluzioni delle normative. Il sistema di registrazione dei log per tutti i servizi erogati è infatti conforme alle normative vigenti ed adeguato in caso di evoluzioni.

A tale proposito viene garantito che:

- i processi attuati per il monitoraggio e la rilevazione di eventuali intrusioni o anomalie sono definiti ed attuati
    - l'accesso alle informazioni riservate dell'Amministrazione viene permesso solo a personale autorizzato, in conformità al Regolamento (UE) 2016/679;

Aruba garantisce che tutti gli apparati necessari all'erogazione dei servizi vengano gestiti solo da personale univocamente individuato e che gli aspetti di sicurezza siano attuati in base a procedure documentate. Le procedure di sistema del Gruppo Aruba, redatte sulla base dello standard ISO27001 per la gestione della sicurezza delle informazioni, garantiscono che siano documentati:

- gli accessi fisici delle persone agli edifici in cui sono situati apparati;
- gli accessi fisici delle persone ai locali contenenti apparati;
- le regole per l'accesso da parte di personale esterno (fornitori, addetti alla manutenzione, visitatori, etc.);
- le modalità di gestione degli strumenti per l'accesso ad eventuali casseforti ed armadi blindati (combinazioni delle casseforti, chiavi degli armadi, etc.);
- le modalità di gestione degli archivi cartacei (regole per la conservazione, modalità di consultazione, eventuale registrazione degli accessi, etc.);
- la gestione di situazioni anomale;
- le modalità di ripristino a seguito di interruzione dell'erogazione di energia elettrica;
- le procedure di backup e di restore;
- le procedure di escalation.

Le **postazioni di lavoro** si trovano in uffici interdetti all'accesso del pubblico. Le postazioni condivise, messe a disposizione della clientela, risiedono su reti e uffici separati (sale riunioni attrezzate), e sono dotate di opportune limitazioni di accesso.

Per l'**accesso alle postazioni di lavoro**, i dipendenti dispongono di token hardware personali protetti da apposito **PIN** associato a credenziali nella forma nome.cognome e password, di tipo strong, conosciute solo dagli stessi. Attraverso l'**Active Directory aziendale** è possibile offrire cambio password con obbligo di password in base a policy standard condivise.

L'accesso ai server viene garantito attraverso le stesse credenziali personali sia per ambienti windows che per ambienti linux. Le password vengono mantenute nella massima riservatezza e non possono essere trascritte.

Torna al sommario

12.8.4 Sicurezza Logica dei sistemi e degli apparati

I protocolli ed i servizi utilizzati per la gestione degli apparati (SNMP, RADIUS, NTP, Log, LDAP) vengono erogati solo verso le reti di management mediante l'utilizzo di ACL (Access Control List). All'interno delle reti dedicate, se il protocollo/servizio lo supporta, è in ogni caso necessario autenticarsi.

Tutti i protocolli previsti per l'accesso ed il controllo dei sistemi sono di tipo sicuro cifrato, prevedendo ssh, https o rdp.

copia informatica per consultazione

All'interno dei singoli apparati i servizi non necessari vengono disattivati e quelli necessari vengono erogati solo verso le interfacce che richiedono che tali servizi vengano resi disponibili.

Le politiche e le conseguenti architetture e configurazioni di rete adottate garantiscono fra l'altro:

- L'impossibilità di effettuare IP spoofing da un qualsiasi utente connesso direttamente alla rete
- L'impossibilità di effettuare attacchi smurf, fraggle, land tramite limitazione nell'accesso agli indirizzi di broadcast e filtraggio dei pacchetti che riportano un indirizzo sorgente palesemente scorretto
- La capacità di reagire tempestivamente a qualsiasi tipo di attacco alle proprie infrastrutture anche tramite la possibilità di configurare in qualsiasi punto della rete qualsiasi regola di filtraggio atta a mitigare il fenomeno evidenziato

Gli enti/gruppi che operano sulla configurazione dei sistemi hanno diverse esigenze in termini di necessità d'accesso alle classi d'apparati. L'autorizzazione all'accesso alla configurazione di un apparato è nominale, non di gruppo. L'accesso ad una specifica classe d'apparati dipende dall'appartenenza dell'utente ad uno specifico gruppo. L'associazione dell'utenza al Gruppo permette di confinare l'accesso degli utenti ai soli apparati la cui gestione è in carico al Gruppo. Sulla base di tale appartenenza, l'utente potrà autenticarsi sull'apparato utilizzando una login ed una password personali nel caso di apparati con tecnologia IP mentre per quanto riguarda apparati di trasporto (SDH e DWDM) l'autenticazione si esegue a livello dei sistemi di gestione. Sono stati inoltre introdotti dei meccanismi di gestione delle password (lunghezza minima, presenza di caratteri numerici, ecc.) di enable e delle password locali in modo da ottenere un bilanciamento tra l'esigenza di avere un adeguato livello di sicurezza e le esigenze di implementazione/gestione delle linee guida.

L'inserimento di un nuovo utente in un gruppo deve essere richiesto dal responsabile del gruppo stesso. La richiesta deve pervenire via e-mail all'apposita casella di posta nel caso della rete IP o all'amministratore di rete nel caso di accesso agli apparati di rete di Trasporto.

Successivamente alla configurazione dell'utente, sarà inviata e-mail di conferma all'utente stesso ed al responsabile del gruppo. La rimozione di un utente da un gruppo deve essere richiesta dal responsabile del gruppo stesso. La richiesta deve pervenire via e-mail all'apposita casella di posta nel caso della rete IP o all'amministratore di rete nel caso di accesso agli apparati di rete di trasporto.

Successivamente alla rimozione dell'utente, sarà inviata e-mail di conferma all'utente stesso ed al responsabile del gruppo. Le password utilizzate dagli utenti dovranno seguire le seguenti regole:

- Non inferiori agli 8 caratteri.
- Non devono essere facilmente identificabili. Nomi propri, nomi di prodotti, nomi di Clienti ecc. sono da evitare
- Devono contenere caratteri misti: minuscole, maiuscole, numeri, spazi, caratteri speciali (@, %, $ ecc.)

L'utente viene invitato a cambiare con regolarità la sua password utente. Nel caso l'utente decidesse di non cambiare la propria password, riceverà quotidianamente, nelle ultime due settimane di validità della stessa, un avviso di richiesta di modifica password.

Torna al sommario

12.9 Piano di Disaster Recovery e Continuità operativa

Aruba ha sviluppato e adotta appositi piani di Disaster Recovery e Business Continuity allo scopo di gestire e mediare i rischi cui può essere soggetta.

Tali documenti definiscono ed elencano le azioni da intraprendere prima, durante e dopo una condizione di emergenza per assicurare il ripristino (Disaster Recovery) e la continuità (Business Continuity) dei servizi erogati.

copia informatica per consultazione

Essi forniscono indicazioni e dove possibile istruzioni passo-passo atte ad assicurare la continuità dei servizi critici di Aruba anche in presenza di eventi indesiderati che possano causare il fermo prolungato dei sistemi informatici.

I Piani di Disaster Recovery sono stati redatti tenendo presente le "Linee Guida per il disaster recovery delle PA" dell'Agenzia per l'Italia Digitale,ed è dunque ispirato al ciclo di Deming (Plan, Do, Check, Act) prevedendo, dopo la fase iniziale di studio/analisi del contesto, il disegno della soluzione tecnologico-organizzativa che meglio risponde alle esigenze di continuità richieste, la realizzazione e il mantenimento della soluzione. Tale piano viene dettagliato maggiormente in fase di setup dell'infrastruttura.

La continuità operativa sarà garantita anche in caso di blocchi prolungati, quali, a titolo esemplificativo:

- distruzione o inaccessibilità di una struttura nella quale sono allocate unità operative o apparecchiature critiche;
- indisponibilità di personale essenziale per il funzionamento dell'azienda;
- interruzione del funzionamento delle infrastrutture (tra cui energia elettrica, reti di telecomunicazione, ecc.);
- alterazione dei dati o indisponibilità dei sistemi a seguito di attacchi perpetrati dall'esterno attraverso reti telematiche;
- danneggiamenti gravi provocati da dipendenti

Torna al sommario

12.9.1 Business Impact Analisys (BIA)

Come prima cosa si valutano gli elementi che più risentirebbero dell'interruzione del servizio, ovvero si valuterà con il cliente quali sono gli aspetti maggiormente critici del servizio offerto.

La BIA valuta normalmente l'impatto di un evento sull'operatività economica, nel caso della conservazione documentale però l'interruzione dei servizi erogati comporta danni non immediatamente "monetizzabili". Le perdite (e dunque l'impatto) saranno valutate assieme al cliente tenendo conto dell'insieme dei seguenti aspetti:

- Aspetti economici
- Aspetti sociali
- Aspetti reputazionali;
- Aspetti normativi.

Torna al sommario

12.9.2 Analisi dei Rischi

In questa fase si identificheranno quali siano gli scenari di rischio che insistono sul patrimonio informativo attraverso i quali si qualificano gli eventi / minacce che presentano maggior probabilità di concretizzarsi (e.g. in funzione dei livelli di vulnerabilità, delle contromisure in essere, dell'appetibilità dei servizi offerti), generando un danno per il cliente. Si individueranno pertanto le possibili cause di indisponibilità quali ad esempio diffusione di virus, interruzione dell'alimentazione elettrica, incendio alla sala CED, etc...

Torna al sommario

copia informatica per consultazione

12.9.3 Classificazione dei Sistemi e delle Risorse

Allo scopo di indirizzare le priorità di ripristino in caso di disastro, nonché realizzare un efficiente utilizzo delle risorse, si ritiene indispensabile classificare i sistemi presenti all'interno delle infrastrutture di ARUBA a seconda della loro criticità in caso di disastro.

Sono stati individuati quattro livelli di criticità, così definiti:

- **Sistemi critici:**
  Sono quei sistemi indispensabili per fornire un minimo ed accettabile livello di servizio in caso di evento disastroso e/o necessari per il funzionamento degli altri sistemi a minore criticità.
- **Sistemi importanti**:
  Sono quei sistemi necessari per garantire un livello standard di servizi, che quindi hanno una significativa importanza operativa.
- **Sistemi semi-importanti:**
  Si tratta di sistemi necessari per le normali operazioni, tuttavia risultano avere una minore importanza operativa rispetto a quelli del punto precedente.
- **Sistemi non-critici:**
  Sono i sistemi che rivestono la minore importanza (quali servizi accessori ecc.) operativa per cui il ripristino non riveste carattere di priorità.

Verrà inoltre fornito l'elenco del personale, il responsabile della Continuità Operativa e le procedure di escalation da utilizzare per dichiarare lo stato di disastro.

Torna al sommario

12.9.4 Modalità tecniche per la Business Continuity ed il Disaster Recovery

Come descritto nell'architettura fisica della soluzione il sistema implementa i seguenti livelli di sicurezza:

1) Il sistema di produzione è completamente ridondato senza alcun Single Point of Failure. Alcune componenti sono per convenienza distribuite sui due Data Center connessi in ambito metropolitano in modo tale da essere totalmente resilienti a qualsiasi guasto HW o SW che possa colpire un singolo nodo fisico o virtuale. Per come è costruito il sistema inoltre l'impatto sulle performance dovuto alla rottura di un singolo componente può essere considerato irrilevante e comunque la configurazione normale ripristinata nel giro di pochi minuti.
2) La presenza di un sito collegato in ambito metropolitano e già parzialmente attivo garantisce la piena operatività della soluzione anche nel caso di fermo del data center principale. Le uniche operazioni necessarie sono la riconfigurazione della rete, per il corretto raggiungimento del sistema, e la riattivazione dei nodi di Front-end ed Application sull'apposita infrastruttura virtuale. Per tutti gli eventi che abbiano impatto sul data center di produzione, che ricordiamo essere certificato **ANSI/TIA 942-A Rating IV (ex Tier)**, la riattivazione del servizio senza perdita di dati è prevista entro 24 ore. Nel caso di attivazione del sito secondario, questa viene eseguita manualmente seguendo apposite procedure, a seguito della dichiarazione di crisi prevista dalle procedure.

Torna al sommario

13 Normative in vigore nei luoghi dove sono conservati i documenti

I documenti informatici sono conservati in Italia; pertanto al sistema di conservazione si rendono applicabili le norme Italiane.

Torna al sommario

copia informatica per consultazione

14 Disposizioni finali

14.1 Nullità o inapplicabilità di clausole

Se una qualsivoglia disposizioni del presente Manuale, o relativa applicazione, risulti per qualsiasi motivo o in qualunque misura nulla o inapplicabile, il resto del presente Manuale (così come l'applicazione della disposizione invalida o inapplicabile ad altre persone o in altre circostanze) rimarrà valido e la disposizione nulla o inapplicabile sarà interpretata nel modo più vicino possibile agli intenti delle parti.

Torna al sommario

14.2 Interpretazione

Salvo disposizioni diverse, questo *Manuale* dovrà essere interpretato in conformità alla correttezza, buona fede ed a quanto ragionevole anche in virtù degli usi commerciali nazionali.

Torna al sommario

14.3 Nessuna rinuncia

In nessun caso eventuali inadempimenti e/o comportamenti del Cliente difformi rispetto al Manuale potranno essere considerati quali deroghe al medesimo o tacita accettazione degli stessi, anche se non contestati da ARUBA. L'eventuale inerzia di ARUBA nell'esercitare o far valere un qualsiasi diritto, clausola o disposizione del Manuale, non costituisce rinuncia a tali diritti o clausole.

Torna al sommario

14.4 Comunicazioni

Qualora ARUBA o il Cliente desiderino o siano tenuti ad effettuare delle comunicazioni, domande o richieste in relazione al presente Manuale, tali comunicazioni dovranno avvenire nelle modalità ed ai riferimenti indicati nel Contratto.

Torna al sommario

14.5 Intestazioni e Appendici e Allegati del presente Manuale Operativo

Le intestazioni, sottotitoli e altri titoli del presente *Manuale* sono utilizzati solo per comodità e riferimento, e non saranno utilizzati nell'interpretazione o applicazione di qualsiasi disposizione ivi contenuta.

Le appendici, gli allegati, comprese le definizioni del presente *Manuale*, sono parte integrante e vincolante del presente *Manuale* a tutti gli effetti.

Torna al sommario

14.6 Modifiche del Manuale di conservazione

ARUBA si riserva il diritto di aggiornare periodicamente il presente *Manuale* in modo estensibile al futuro e non retroattivo. Le modifiche sostituiranno qualsiasi disposizione in conflitto con la versione di riferimento del *Manuale* di conservazione.

Torna al sommario

14.7 Violazioni e altri danni materiali

Il Cliente rappresenta e garantisce che i documenti oggetto di conservazione e le informazioni in essi contenute

copia informatica per consultazione

non interferiscano, danneggino e/o violino diritti di una qualsiasi terza parte di qualunque giurisdizione.

Torna al sommario

14.8 Norme Applicabili

Le attività di conservazione contenute nel presente *Manuale* sono assoggettate alle leggi dell'ordinamento italiano.

Il presente documento informatico è formato nel rispetto delle regole tecniche di cui all'art. 71 del D.Lgs. 7 marzo 2005 n. 82 e s.m.i. (Codice dell'amministrazione digitale) e sottoscritto con firma digitale del Sig. Simone Braccagni

Torna al sommario

copia informatica per consultazione

DECRETO N. 845 DEL 29/09/2022
DEL DIRETTORE GENERALE

OGGETTO: ATTIVAZIONE PROCEDURA PER MANIFESTAZIONE DI INTERESSE AD ATTRIBUZIONE INCARICO QUINQUENNALE DI STRUTTURA COMPLESSA SISTEMI INFORMATIVI AZIENDALI (SIA): ATTRIBUZIONE

copia informatica per consultazione

IL DIRETTORE GENERALE

PREMESSO che:
- in data 29/08/2022 è stato emesso avviso interno (PG 43177) per l'acquisizione delle candidature dei dirigenti del ruolo tecnico, profilo analista, interessati all'affidamento dell'incarico di Struttura Complessa *"Sistemi Informativi Aziendali - SIA";*
- la copertura dell'incarico è stata autorizzata da Regione Lombardia – Direzione Generale Welfare – con nota ns. prot. 50895 del 12/10/2021;

ACQUISITA agli atti una candidatura pervenuta al protocollo aziendale entro i termini di scadenza (12/09/2022) fissato nel bando e verificato il possesso dei requisiti in capo al candidato, ai sensi delle disposizioni dettate dall'art. 70, comma 1, lett. a), del CCNL Personale dell'Area delle Funzioni Locali – Sezione Dirigenti amministrativi, tecnici e professionali delle aziende e degli enti del Servizio sanitario nazionale del 17/12/2020;

RICHIAMATO il verbale redatto in data 27/09/2022 nel quale vengono evidenziate le competenze possedute dal candidato e dato atto del previsto colloquio effettuato con lo stesso, come da scheda allegata allo stesso verbale che ne forma parte integrante, sulle cui basi è da ritenere adeguato allo svolgimento dell'incarico il dirigente indicato nel dispositivo del presente atto;

RITENUTO, pertanto, di procede al conferimento dell'incarico di durata quinquennale, così come previsto dall'art. 71 CCNL cit., a decorrere dal 1° ottobre 2022;

CONFERMATO il valore economico dell'indennità di posizione correlata all'incarico, come precisato dal predetto avviso, coincidente con la retribuzione di posizione fissa prevista per gli incarichi di direzione di struttura complessa dall'art. 89, comma 3, del cit. CCNL, nelle more di una complessiva revisione della graduazione delle funzioni dei dirigenti amministrativi, tecnici e professionali secondo l'assetto previsto nel nuovo POAS;

DATO ATTO che dal presente provvedimento non derivano oneri aggiuntivi per l'Azienda in quanto la retribuzione di posizione connessa agli incarichi, secondo la graduazione vigente in Azienda, trova finanziamento nell'ambito delle risorse disponibili del fondo di posizione;

PRESO ATTO dell'attestazione di regolarità e di legittimità del presente provvedimento espressa da SIMONETTI GIOVANNI Direttore della Struttura RISORSE UMANE, e da BENVENUTI ANTONELLA, responsabile del procedimento;

DATO ATTO che il presente provvedimento non comporta oneri o proventi a carico dell'Azienda;

copia informatica per consultazione

ACQUISITI i pareri del Direttore Amministrativo, del Direttore Sanitario e del Direttore Socio Sanitario;

DECRETA

1. di attribuire - ai sensi dell'art. 71 CCNL Personale dell'Area delle Funzioni Locali – Sezione Dirigenti amministrativi, tecnici e professionali delle aziende e degli enti del Servizio sanitario nazionale del 17/12/2020 - l'incarico di Struttura Complessa *"Sistemi Informativi Aziendali - SIA"* al dirigente sotto identificato, con decorrenza 1° ottobre 2022 e per la durata di cinque anni;

DIREZIONE	DESCRIZIONE	NOMINATIVO	PROFILO
Direzione Generale	SC *Sistemi informativi aziendali- SIA*	Garbossa Paolo	Dirigente analista

2. di dare atto che dal presente provvedimento non derivano oneri aggiuntivi per l'Azienda in quanto la retribuzione di posizione connessa all'incarico trova finanziamento nell'ambito delle risorse disponibili del fondo di posizione (art. 90 cit. CCNL);

3. di pubblicare il presente provvedimento all'Albo on line sul sito istituzionale aziendale, ai sensi dell'art. 32 della L. n. 69/2009 e dell'art. 17 della L.R. 33/2009, nel rispetto del Regolamento UE 2016/679.

PRESO ATTO dei pareri di

DIRETTORE AMMINISTRATIVO	FERRARI GIUSEPPE
DIRETTORE SANITARIO	MALINGHER ALESSANDRO
DIRETTORE SOCIOSANITARIO	BOSCAINI RENZO

DIRETTORE GENERALE
AZZI MARA
(atto firmato digitalmente ai sensi
delle vigenti disposizioni di legge)

copia informatica per consultazione

Indice

copia informatica per consultazione

Stato delle revisioni					
Rev	**Data**	**Modifica**	**Preparato**	**Verificato**	**Approvato**
0	31/12/2021	Prima emissione	Ing. Paolo Garbossa Ing. Lucio Attolini Dott. Giampietro Barai	Dott. Enrico Burato	Dott.ssa Mara Azzi

copia informatica per consultazione

1. INTRODUZIONE

1.1. Scopo

Questo documento descrive le regole adottate dall'ASST di Mantova per la protezione di sistemi, reti e applicazioni dell'ASST di Mantova a sostegno delle informazioni nel corso di tutto il loro ciclo di vita, dalla progettazione fino alla dismissione. Definisce inoltre ruoli e le responsabilità specifici, preposti all'attuazione delle suddette regole, anche in adempimento delle normative pertinenti.
Questo documento integra le politiche e procedure già definite per la gestione del sistema informativo di ASST di Mantova.

1.2. Ambito di applicazione del documento

Questo documento si applica a tutte le informazioni trattate dall'ASST di Mantova, indipendentemente dagli strumenti utilizzati e dai supporti su cui le informazioni sono memorizzate o trasmesse: non si limita quindi alle informazioni in forma elettronica ma comprende ad esempio anche quelle trattate su supporto cartaceo, etc.
Sono inoltre espressamente inclusi in questo contesto i fornitori e i collaboratori dell'Ente che ne trattano le informazioni o che hanno comunque accesso ad esse.

1.3. Obiettivi per la Sicurezza Informatica

L'ASST di Mantova ha stabilito che l'obiettivo principale per la sicurezza informatica deve essere quello di sostenere la gestione del ciclo di vita dei sistemi, delle reti e delle applicazioni (includendo tra essi anche i sistemi e gli apparati per la sicurezza del patrimonio informativo aziendale) garantendo un adeguato, nel senso di appropriato e uniforme, livello di protezione.
Nel perseguimento di questo obiettivo principale, l'ASST di Mantova ritiene che la sicurezza informatica sia un elemento abilitante per:

- assicurare la disponibilità di sistemi, reti ed applicazioni a supporto delle attività istituzionali, in particolare quelle legate alle attività di prevenzione, diagnosi, cura e riabilitazione del paziente;
- garantire la protezione delle informazioni trattate nell'ambito del sistema informativo, con particolare riferimento ai dati personali e sensibili dei pazienti, in linea con la normativa vigente e nel rispetto della dignità della persona;
- garantire che le attività operative e che le procedure di acquisizione, progettazione, realizzazione e manutenzione dei sistemi, delle reti e delle applicazioni, comprese quelle riconducibili all'ambito dell'ingegneria clinica, siano svolte in accordo con le politiche di sicurezza dell'ASST di Mantova, e con gli standard e le buone pratiche nazionali ed internazionali di sicurezza delle informazioni in conformità con leggi, norme e regolamenti vigenti in materia;
- garantire l'attuazione di adeguate misure tecniche e organizzative su sistemi, reti ed applicazioni, comprese quelle riconducibili all'ambito dell'ingegneria clinica, anche in relazione alle diverse fasi del ciclo di vita, volte a salvaguardare il patrimonio informativo, in particolare rispetto ai rischi derivanti da attacchi intenzionali, errori ed eventi esterni;

copia informatica per consultazione

- integrare la gestione della sicurezza dell'ASST di Mantova nella più generale gestione della sicurezza del Sistema Federato, allineando dove necessario l'organizzazione, le procedure e gli strumenti, anche al fine di realizzare le opportune sinergie;
- assicurare che le decisioni in materia di protezione dei sistemi, delle reti e delle applicazioni, siano prese in accordo con il livello di rischio informatico a cui le informazioni trattate tramite i sistemi, le reti e le applicazioni sono esposte, individuando pertanto il miglior equilibrio possibile tra costi relativi alla sicurezza delle informazioni e livello di protezione atteso;
- garantire, tramite una sempre maggiore integrazione dei processi di *business* con quelli di governo del sistema informatico, una maggiore sensibilità da parte di tutta l'ASST di Mantova rispetto agli obiettivi di sicurezza delle informazioni che devono essere perseguiti.

1.4. Definizioni

Per le definizioni associate ai termini specialistici utilizzati nel presente documento si faccia riferimento al Glossario.

2. RUOLI E RESPONSABILITÀ

Nell'ambito della gestione della sicurezza del sistema informatico, coerentemente con la Politica della Sicurezza delle Informazioni, il Responsabile della Sicurezza delle Informazioni è supportato da:

1. un Responsabile della Sicurezza Informatica e delle Reti;
2. un Responsabile della Sicurezza dei Sistemi RIS-PACS;
3. un Responsabile dell'Ingegneria Clinica;
4. un Responsabile Applicativi e Sistemi.

3. SICUREZZA DEI SISTEMI E DELLE APPLICAZIONI

Il Responsabile della Sicurezza Informatica e delle Reti, in accordo con il Responsabile della Sicurezza delle Informazioni e il Responsabile dell'Ingegneria Clinica, assicura l'adozione delle seguenti misure specifiche al fine di assicurare la continuità dell'operatività e la protezione delle informazioni gestite.
Fatto salvo quando diversamente specificato, il Responsabile Applicativi e Sistemi ha il compito di garantire l'osservanza delle seguenti regole e di riportare al Responsabile della Sicurezza delle Informazioni tutte le eventuali inadempienze. È compito del Responsabile Applicativi e Sistemi identificare e segnalare, laddove necessario, l'esigenza di aggiornare le politiche, le regole e la relativa documentazione in accordo con l'evoluzione tecnologica, i cambiamenti del contesto e dello scenario delle minacce informatiche.

3.1. Gestione della Sicurezza dei Sistemi e delle Applicazioni

Il Responsabile Applicativi e Sistemi, il Responsabile della Fisica sanitaria (per la Sicurezza dei Sistemi RIS-PACS, IOS, ASTRIM) e il Responsabile dell'Ingegneria Clinica, ciascuno per la propria area di competenza, definiscono, documentano e sovrintendono all'implementazione di azioni atte a garantire:

copia informatica per consultazione

- il mantenimento del governo della gestione dei sistemi, anche in caso di outsourcing del servizio o della sua gestione;
- l'individuazione dei soggetti responsabili delle diverse attività, coerentemente con le regole definite;
- l'adozione di misure di sicurezza adeguate alla criticità delle informazioni trattate dai sistemi;
- l'accesso alla rete da parte dei sistemi mediante interfacce e servizi protetti in modo conforme alla classificazione delle informazioni gestite o trasmesse;
- la definizione di livelli di servizio adeguati, anche in termini di sicurezza, alle esigenze delle applicazioni supportate sia per i sistemi gestiti dall'ASST di Mantova che per quelli affidati alla gestione di fornitori esterni;
- la documentazione delle configurazioni attese ed in essere;
- il tracciamento delle operazioni di gestione;
- la definizione, la documentazione e l'attuazione delle misure atte a garantire la disponibilità dei sistemi per attività legate direttamente alla cura dei pazienti, inclusiva della valutazione dell'impatto che un degrado delle performance possa avere sulle attività cliniche.

Il Responsabile Applicativi e Sistemi, il Responsabile della Fisica Sanitaria e il Responsabile dell'Ingegneria Clinica si raccordano altresì con il Responsabile della Struttura Tecnico Patrimoniale per quanto concerne l'attuazione delle misure applicabili di protezione dei sistemi e degli apparati da essi utilizzati, dei centri di elaborazione dati, degli armadi, dei servizi di supporto e delle aree e dei locali designati ad ospitarli.

3.2. Autenticazione e Autorizzazione

In accordo con la PrS07SDI Controllo degli accessi alle informazioni [6], l'accesso a tutti i sistemi e le applicazioni dell'ASST di Mantova prevede obbligatoriamente una procedura di autenticazione e autorizzazione di robustezza adeguate al livello di classificazione delle informazioni trattate.
Particolari misure di autenticazione e autorizzazione sono definite dal Responsabile Applicativi e Sistemi e dal Responsabile dell'Ingegneria Clinica, ciascuno per il proprio ambito di competenza:

- per l'accesso da parte di utenti con particolari privilegi;
- per l'accesso a funzionalità critiche per la sicurezza dei sistemi e delle applicazioni;
- per lo svolgimento di attività di manutenzione e amministrazione dei sistemi, delle applicazioni e dei sistemi atti a garantire la sicurezza dei dati;
- per l'autenticazione e l'autorizzazione di utenze assegnate a sistemi e ad applicazioni (comunicazioni A*pplication-to-Application* e *Machine-to-Machine*).

In particolare, per i sistemi e le applicazioni classificati come ad **Alta Disponibilità** o che trattano dati classificati come **Riservati, Strettamente Riservati e ad Alta Integrità**, le procedure di autenticazione e autorizzazione sono tracciate coerentemente con quanto indicato dalla PrS07SDI Controllo degli accessi alle informazioni [6], e le relative registrazioni sono protette da misure adeguate al livello di classificazione dei sistemi e delle applicazioni che le hanno generate.

copia informatica per consultazione

3.3. Sicurezza dei servizi applicativi e di sistema

Il Responsabile Applicativi e Sistemi, il responsabile del Servizio di Fisica Sanitaria e il Responsabile dell'Ingegneria Clinica ciascuno per il proprio ambito di competenza, assicurano che i servizi di sistema e le applicazioni siano configurati per consentire l'accesso agli utenti ed al personale solo mediante connessioni protette tramite meccanismi di autenticazione e di cifratura delle sessioni di comunicazione, tramite algoritmi e protocolli conformi con gli Indirizzi previsti in "Analisi Protocolli e Algoritmi Crittografici" [17]. Le eccezioni sono adeguatamente documentate, motivate e sottoposte all'approvazione del Responsabile della Sicurezza delle Informazioni, e sono comunque conformi alla normativa vigente, compresa quella emessa da Regione Lombardia nell'ambito del Sistema Federato.
Il Responsabile Applicativi e Sistemi, il responsabile del Servizio di Fisica Sanitaria ed il Responsabile dell'Ingegneria Clinica, ciascuno per il proprio ambito di competenza, assicurano che i servizi di sistema e le applicazioni erogati verso terzi (cittadini, altri Enti, aziende, etc.) prevedano l'autenticazione del servizio mediante l'utilizzo di certificati digitali emessi da autorità di certificazione riconosciute dai browser più comunemente utilizzati o, quando non erogati al cittadino, tramite altri meccanismi di autenticazione concordati con i soggetti terzi, che garantiscano l'autenticazione del server prima della richiesta di credenziali di autenticazione utente.

3.4. Protezione dal malware

Il Responsabile Applicativi e Sistemi, il responsabile del Servizio di Fisica Sanitaria e il Responsabile dell'Ingegneria Clinica nell'ambito delle proprie competenze, assicurano l'adozione di adeguate misure per prevenire, rilevare e contenere la presenza di malware nel sistema informativo, per la sua rimozione e per il ripristino dei sistemi danneggiati. Esse prevedono:

- il ricorso a soluzioni gestite centralmente, per consentire un maggiore controllo sullo stato di aggiornamento dei sistemi di rilevamento e sulle segnalazioni;
- il ricorso ad una strategia di difesa in profondità, che prevede quanto meno:
  - la protezione dei sistemi di posta elettronica contro il malware e le mail indesiderate (SPAM);
  - la protezione locale su tutti i personal computer del personale;
  - la protezione locale su tutti i sistemi server;
  - la protezione di rete tramite Intrusion Detection System/Intrusion Prevention System;
  - la protezione della navigazione degli utenti mediante sistemi centralizzati;
  - l'obbligo, da parte di personale esterno e visitatori occasionali, di disporre di soluzione antivirus aggiornate;
- la verifica quotidiana della presenza di aggiornamenti delle definizioni del malware e la tempestiva installazione degli stessi su tutti i sistemi di protezione;
- la predisposizione di servizi di distribuzione e autorizzazione centralizzata del software per il personale interno ed esterno che opera sui sistemi dell'ASST di Mantova, al fine di contrastare il ricorso all'utilizzo di software proveniente da fonti incontrollate;
- l'obbligo di installazione del software a partire da supporti originali o ottenuto da fonti affidabili, previo opportune verifiche di autenticità.

copia informatica per consultazione

3.5. Rapporti con i fornitori

In accordo con il REGSDI02 Gestione dei rapporti con i Fornitori [2], il Responsabile Applicativi e Sistemi e il Responsabile dell'Ingegneria Clinica, ciascuno per la propria area di competenza, hanno l'incarico di definire e aggiornare i requisiti di sicurezza da includere nell'ambito dei contratti con i fornitori di servizi di gestione del sistema informatico.
Tali requisiti indirizzano in modo particolare:

- l'elenco dei requisiti di sicurezza, coerenti con la classificazione delle informazioni gestite;
- livelli di servizio legati al supporto tecnico ed allo svolgimento delle attività assegnate;
- modalità e tempistiche previste per il rilevamento, la segnalazione, la gestione e la reportistica inerenti agli incidenti di sicurezza;
- clausole e obblighi necessari ad assicurare lo svolgimento delle attività di progettazione, realizzazione, manutenzione ordinaria e straordinaria, aggiornamento e gestione delle catene di fornitura, nel rispetto di adeguati requisiti di sicurezza e qualità.

3.6. Sicurezza delle postazioni di lavoro e dei dispositivi mobili

Il Responsabile Applicativi e Sistemi, definisce un modello di gestione standardizzato per categorie di postazioni di lavoro e dispositivi mobili definite in base a:

- tipologie di dispositivo (es: postazioni desktop, notebook, terminali mobili, tablet, etc.);
- tipologia di utenza (es: personale interno o esterno, operatori ed amministratori di sistema, personale medico, personale di sportello, contabilità, …);
- finalità di utilizzo (gestione sistemistica, elaborazione e analisi dati e documenti, servizi medici, ..);
- appartenenza all'azienda, a fornitori parti o agli utenti (ad esempio, laddove sia tollerato, consentito o incentivato l'uso del c.d. Bring Your Own Device (BYOD));
- altre condizioni o una combinazione delle precedenti.

Il modello di gestione standardizzato è finalizzato ad assicurare:

- la definizione, per le postazioni di lavoro ed i dispositivi mobili afferenti ad ogni categoria, delle misure per assicurare la sicurezza delle procedure operative di gestione in accordo con quanto indicato nella PrS03SDI Gestione delle Informazioni e degli Asset [3];
- il rispetto della PrS03SDI Gestione delle Informazioni e degli Asset [3], in particolare per quanto concerne:
  - la protezione delle informazioni gestite;
  - la catena di custodia e le relative responsabilità;
  - le procedure da adottare per l'assegnazione, la riassegnazione, il rinnovo e la revoca delle postazioni di lavoro e dei dispositivi mobili dell'ASST di Mantova al personale interno e esterno;
  - la gestione del ciclo di vita delle postazioni di lavoro e dei dispositivi mobili;
- le modalità previste per garantire la sicurezza di tali dispositivi in caso di trasporto e uso fuori dalle sedi dell'ASST di Mantova;
- le regole di uso accettabile;

copia informatica per consultazione

- l'autorizzazione esplicita, per categoria, per tipologia di dispositivo o sulla base all'appartenenza organizzativa del personale a cui i dispositivi sono assegnati, per il trattamento di dati classificati come riservati o strettamente riservati;
- l'attivazione dei necessari servizi di gestione tempestiva ed efficace delle anomalie e degli incidenti connessi con l'uso delle postazioni di lavoro e dei dispositivi mobili, in linea con quanto definito in [7]

Il Responsabile Applicativi e Sistemi assicura il rispetto e l'applicazione delle politiche e regole di sicurezza applicabili al modello di gestione delle postazioni di lavoro e dei dispositivi mobili.

3.6.1. Requisiti di Sicurezza particolari per le postazioni di lavoro e i dispositivi mobili

Tutte le postazioni di lavoro ed i dispositivi mobili che l'ASST di Mantova assegna o autorizza all'uso presso le proprie sedi e/o per lo svolgimento di attività lavorative, soddisfano, in aggiunta a quanto già previsto dal presente Documento, i seguenti requisiti di sicurezza delle informazioni:

- prevedono obbligatoriamente l'utilizzo di PIN, password o altro meccanismo di autenticazione, anche locale, per l'accesso al dispositivo, fatte salve regole più restrittive, ed il blocco automatico dello schermo in caso di inutilizzo;
- prevedono l'aggiornamento periodico del software e degli strumenti di sicurezza, inclusi quelli di protezione dal malware, anche quando utilizzati al di fuori delle sedi dell'ASST di Mantova.

In aggiunta, per quanto concerne il trattamento dei dati classificati come **riservati** o **strettamente riservati**, sono previsti i seguenti requisiti particolari:

- le postazioni di lavoro ed i dispositivi mobili utilizzano la cifratura per l'archiviazione dei dati;
- i dispositivi mobili prevedono:
  - funzionalità di blocco e cancellazione remota della memoria mediante strumenti controllati dal Responsabile Applicativi e Sistemi, anche tramite una specifica procedura di emergenza, da attivarsi automaticamente in caso di ripetuti tentativi di accesso errati;
  - il divieto di ricorrere a tecniche di modifica del sistema operativo (*jailbreaking, rooting* etc…), ed il rilevamento di tali modifiche tramite strumento di monitoraggio automatizzato;
  - l'installazione di soluzioni di mobile device management, poste sotto il controllo del Responsabile della Sicurezza dei Sistemi.

3.7. Strumenti per il personale

La diffusione e la disponibilità di servizi di comunicazione istantanea, dei social network, di condivisione delle informazioni attraverso il cloud, nonché l'evoluzione degli strumenti di produttività in mobilità (smartphone, tablet etc.) ed il c.d. *Bring Your Own Device* (BYOD), hanno introdotto innovazioni significative nel modo di lavorare e hanno ampliato la disponibilità di mezzi che semplificano la collaborazione tra le persone. L'ASST di Mantova, anche in applicazione della PrS03SDI Gestione delle Informazioni e degli Asset [3], predispone un insieme di servizi designati

copia informatica per consultazione

appositamente per offrire le funzionalità necessarie al proprio personale per garantirne il massimo livello di produttività nel rispetto delle garanzie di tutela della sicurezza delle informazioni gestite.

L'ASST di Mantova a questo scopo mette a disposizione del personale interno:

- i repository documentali ad accesso condiviso;
- i servizi di posta elettronica ordinaria e posta elettronica certificata tramite accesso web;
- i servizi dedicati alla gestione HR (presenze, cedolino, giustificativi, ecc..);
- la disponibilità di reti wireless dedicate per la connettività ad internet attraverso dispositivi mobili aziendali
- la disponibilità di sistemi cloud aziendali per la condivisione, anche in mobilità di documenti e spazi di lavoro.

Il Responsabile della Sicurezza delle Informazioni, in accordo con il Responsabile della Sicurezza Informatica e delle Reti, assicura che tali strumenti siano realizzati e gestiti in accordo con le politiche di sicurezza dell'ASST di Mantova.

4. SICUREZZA DELLE RETI

Il Responsabile della Sicurezza Informatica e delle Reti, in accordo con il Responsabile della Sicurezza delle Informazioni, assicura l'adozione delle seguenti misure specifiche al fine di assicurare la continuità dei servizi di rete e la protezione delle informazioni trasmesse attraverso di essi.
Fatto salvo quando diversamente specificato, il Responsabile della Sicurezza Informatica e delle Reti ha il compito di garantire l'osservanza delle seguenti regole e di riportare al Responsabile della Sicurezza delle Informazioni le eventuali non conformità. E' compito del Responsabile della Sicurezza Informatica e delle Reti identificare e segnalare l'esigenza di aggiornare le politiche, le regole e la relativa documentazione in accordo con l'evoluzione tecnologica e i cambiamenti del contesto e dello scenario delle minacce informatiche.

4.1. Gestione della Sicurezza della Rete

L'infrastruttura di rete è un componente fondamentale del sistema informativo. La sua protezione è, per l'ASST di Mantova, un aspetto critico nel quadro complessivo della gestione della sicurezza delle informazioni.
Il Responsabile della Sicurezza Informatica e delle Reti definisce, documenta e sovrintende all'implementazione di adeguate procedure atte a garantire:

1. il mantenimento del governo della gestione della sicurezza della rete anche in caso di outsourcing del servizio o della sua gestione;
2. l'individuazione dei soggetti responsabili delle diverse attività, coerentemente con le regole definite;
3. l'adozione di misure di sicurezza adeguate alla criticità delle informazioni in transito sui diversi componenti della rete;
4. la protezione dell'accesso dei sistemi alla rete attraverso modalità di autenticazione e controllo accessi coerenti con la classificazione delle informazioni e dei servizi esposti;

copia informatica per consultazione

5. la definizione di livelli di servizio dei servizi di connettività e delle reti che siano adeguati, anche in termini di sicurezza, alle esigenze dei servizi supportati sia per le reti gestite dall' ASST di Mantova che per quelle affidate alla gestione di fornitori esterni, nonché per la connettività con Internet;
6. la documentazione delle configurazioni attese ed in essere, per garantire la verifica rispetto alle esigenze di comunicazione sicura richieste;
7. il tracciamento delle operazioni di gestione;
8. la definizione, la documentazione e l'attuazione delle misure atte a garantire la disponibilità della connettività e dei servizi di rete per attività legate direttamente alla cura dei pazienti, inclusiva della valutazione dell'impatto che un degrado della connettività possa avere sulle attività cliniche.

Il Responsabile della Sicurezza Informatica e delle Reti si raccorda con il Responsabile della Struttura Tecnico Patrimoniale per quanto concerne l'attuazione delle misure applicabili di protezione dei dispositivi, dei cavi, degli armadi, dei servizi di supporto e delle aree e dei locali designati ad ospitarli.

4.2. Rapporti con i fornitori

In accordo con il REGSDI02 Gestione dei rapporti con i Fornitori [2], il Responsabile della Sicurezza Informatica e delle Reti ha l'incarico di definire e aggiornare i requisiti di sicurezza da includere nell'ambito dei contratti con i fornitori di servizi di connettività e di gestione delle reti.
Tali requisiti indirizzano in modo particolare:

1. l'elenco dei requisiti di sicurezza, coerenti con la classificazione delle informazioni gestite;
2. livelli di servizio legati alla disponibilità della connettività, del supporto tecnico e dello svolgimento delle attività assegnate;
3. modalità e tempistiche previste per il rilevamento, la segnalazione, la gestione e la reportistica inerenti agli incidenti di sicurezza della rete;
4. clausole e obblighi necessari ad assicurare lo svolgimento delle attività di progettazione, realizzazione, manutenzione ordinaria e straordinaria, aggiornamento e gestione delle catene di fornitura, nel rispetto di adeguati requisiti di sicurezza e qualità.

4.3. Segregazione tra le reti

L'ASST di Mantova adotta la segregazione fra le reti come misura imprescindibile per garantire il controllo del traffico e quindi la sicurezza della rete. Le modalità e le tecnologie adottate sono stabilite sulla base della classificazione delle informazioni trattate.
A tale scopo, il Responsabile della Sicurezza Informatica e delle Reti assicura la separazione fisica almeno tra le seguenti reti:

1. la rete interna, intesa come l'insieme dei sistemi (server, postazioni di lavoro, apparati di rete, ecc..) presenti negli ambienti interni e tra loro interconnessi;
2. Internet;
3. la DMZ per i servizi che l'Ente offre all'esterno;

copia informatica per consultazione

4. la Extranet del Sistema Federato, anche in coerenza con la normativa emessa da Regione Lombardia;
5. le reti di ambienti esterni all'Ente;
6. una sottorete dedicata agli accessi VPN;
7. sottoreti dedicate a sistemi esposti a rischi specifici (reti di radiologia, radioterapia, medicina nucleare);
8. le reti utilizzate per attività e servizi direttamente connesse alla cura dei pazienti (reti degli elettromedicali);
9. le reti delle diverse sedi;
10. le reti degli ambienti di sviluppo e test;
11. le reti per i servizi di supporto (controllo accessi, IoT, videosorveglianza, ecc..)

Sono inoltre separate, con meccanismi da definire in relazione alla classificazione delle informazioni trattate:

1. la rete di fonia, anche in modalità VoIP;
2. la rete delle Postazioni di Lavoro;
3. le reti dedicate all'utilizzo da parte di personale esterno, ospiti e consulenti, le quali devono consentire esclusivamente l'accesso a internet;
4. le sottoreti utilizzate dai sistemi che trattano dati classificati come riservati o strettamente riservati, ad alta disponibilità o ad alta integrità;

La comunicazione fra le suddette reti, quando necessaria, deve essere mediata da firewall, configurati e gestiti in accordo con gli Indirizzi per la Configurazione dei Firewall [10].

4.4. Accessi di rete per la gestione del sistema informatico

L'ASST di Mantova utilizza una rete dedicata per la gestione del sistema informativo di produzione (rete di management), la quale è segregata rispetto al resto della rete dell'Ente, ed alla quale è eventualmente connessa mediante firewall.
Le connessioni per attività di gestione sistemistica agli apparati di rete, ai sistemi ed alle interfacce di amministrazione delle applicazioni comprese le connessioni per modifiche alla configurazione, manutenzione, aggiornamenti o per il monitoraggio, sono cifrate a livello applicativo (SSH, TLS).
Le suddette connessioni avvengono da postazioni preventivamente identificate e autorizzate.

4.5. Reti wireless

La predisposizione, l'attivazione e l'utilizzo di reti wireless aziendali è consentito presso le aree ed i locali dell'ASST di Mantova solo previa autorizzazione espressa del Responsabile della Sicurezza Informatica e delle Reti, ed è subordinata all'implementazione di misure atte a garantire:

1. l'identificazione puntuale dei servizi di rete accessibili mediante reti wireless;
2. l'identificazione delle categorie di utenti e di operatori autorizzati ad accedere;
3. l'autenticazione dei dispositivi e dei sistemi alle reti wireless in modalità definite in relazione alla tipologia di utenza, di servizi ed alla classificazione delle informazioni trattate;

copia informatica per consultazione

4. la protezione dei dati trasmessi attraverso reti wireless. In particolare, i canali di comunicazione wireless devono essere sempre protetti mediante meccanismi di cifratura aventi caratteristiche di comprovata robustezza;
5. l'aggiornamento periodico delle configurazioni e delle componenti tecnologiche, al fine di assicurare che l'obsolescenza, errori o cattive pratiche nella gestione possano portare ad un'esposizione a rischi non necessaria.

L'uso di reti wireless non è consentito per l'accesso diretto ai sistemi server, alle interfacce di configurazione degli apparati di rete cablata ed ai sistemi di sicurezza della rete.
La gestione di reti wireless deve comunque rientrare nell'ambito della gestione strutturata da parte del Responsabile della Sicurezza Informatica e delle Reti, anche quando si tratti di reti dedicate ad ambiti ristretti e specifici.
Sono vietate le connessioni di apparati e sistemi contemporaneamente alla rete dell'ASST di Mantova e ad altre reti, ad esempio mediante l'attivazione di servizi di tethering su dispositivi mobili o accedendo a reti wireless non appartenenti all'ASST di Mantova. Tale divieto è riportato all'interno del Regolamento Informatico.

4.6. Accesso remoto alla rete

L'accesso alla rete interna dell'ASST di Mantova, intesa come l'insieme dei sistemi (server, postazioni di lavoro e apparati, compresi quelli di rete e medicali) è consentito al personale, interno o esterno, preventivamente autorizzato, nelle modalità previste dalla PrS07SDI Controllo degli accessi alle informazioni [6] e nel rispetto dei seguenti criteri:

- gli utenti sono preventivamente autenticati;
- ciascun utente è autorizzato all'accesso ai soli servizi di rete, sistemi ed applicazioni necessari per lo svolgimento delle attività lavorative, tramite una procedura di autorizzazione;
- il canale di comunicazione è cifrato (es: utilizzo di VPN, IPSEC, TLS);
- le connessioni sono attestate su una rete dedicata;
- le modalità di abilitazione e le procedure di controllo accessi sono definite nel rispetto dei criteri definiti nella PrS07SDI Controllo degli accessi alle informazioni.

Il Responsabile della Sicurezza Informatica e delle Reti assicura che l'accesso da parte di personale esterno per attività di amministrazione e manutenzione sia effettuato mediante VPN attestata su apposita sottorete dedicata agli accessi tramite VPN. Gli accessi devono avvenire dalla rete del fornitore, da indirizzi IP preventivamente concordati. Eventuali eccezioni devono essere specificamente autorizzate da parte del Responsabile della Sicurezza Informatica e delle Reti, e devono prevedere adeguati controlli compensativi.

4.7. Continuità dei servizi di rete

L'ASST di Mantova, oltre a quanto previsto dalla PrS06SDI Gestione degli Incidenti per garantire la Continuità Operativa [7] assicura la disponibilità dei servizi di rete e dei collegamenti con internet mediante soluzioni ridondate. A questo scopo, il Responsabile della Sicurezza Informatica e delle

copia informatica per consultazione

Reti definisce i requisiti di disponibilità della rete in base ai requisiti di disponibilità dei servizi supportati e la classificazione di disponibilità delle informazioni trattate.
In particolare, tutti gli apparati di rete, i collegamenti utilizzati ed i sistemi di protezione (es: firewall) da cui dipende la connettività ad applicazioni classificate ad Alta Disponibilità, sono implementati nel rispetto dei requisiti di alta affidabilità previsti per la connettività supportata.

5. PROGETTAZIONE, SVILUPPO E MANUTENZIONE DEL SISTEMA INFORMATICO

Deve essere garantito che i requisiti di sicurezza delle informazioni siano definiti e gestiti correttamente durante l'intero ciclo di vita del sistema informatico. Il Responsabile della Sicurezza Informatica e delle Reti ed il Responsabile dell'Ingegneria Clinica, per le rispettive aree di competenza, devono quindi assicurare che:

1. le iniziative di progettazione, realizzazione ed evoluzione del sistema informatico siano svolte in accordo con gli obiettivi ed i principi di sicurezza definiti nella POL1SDI Politica di Sicurezza delle Informazioni [1]. Tali iniziative comprendono quelle relative all'ingegneria clinica, per quanto riguarda il trattamento di informazioni e l'interfacciamento con il sistema informatico;
2. il Responsabile della Sicurezza delle Informazioni sia coinvolto nella definizione dell'organizzazione, delle procedure e degli strumenti per la gestione del sistema informatico, al fine di garantire la necessaria integrazione degli aspetti di sicurezza ICT per le informazioni e per i servizi erogati;
3. la pianificazione delle iniziative di progettazione, realizzazione ed evoluzione del sistema informatico comprendano un'adeguata allocazione di risorse per fare fronte alle esigenze di sicurezza, anche nel corso dell'esercizio di quanto realizzato.

In accordo con questo Documento, il Responsabile della Sicurezza delle Informazioni si raccorda con il Responsabile Applicativi e Sistemi e il Responsabile della Sicurezza Informatica e delle Reti, con i Responsabili di Progetto e con il Responsabile della Struttura Tecnico Patrimoniale, per garantire l'attuazione delle misure di sicurezza nell'ambito della gestione del sistema informatico e delle relative procedure operative, anche nel rispetto degli obiettivi più generali definiti nell'ambito del sistema di sicurezza federato.

5.1. Sicurezza delle procedure di progettazione, sviluppo e collaudo

Deve essere garantito che i requisiti di sicurezza delle informazioni siano definiti e gestiti correttamente nelle attività di progettazione, sviluppo e collaudo relative al sistema informativo. La Direzione Strategica dell'ASST di Mantova, quando opportuno attraverso gli sponsor dei progetti, assicura l'allocazione delle risorse necessarie per garantire che i nuovi progetti approvati possano soddisfare i requisiti di sicurezza previsti dalle politiche aziendali. Il Responsabile della Sicurezza Informatica e delle Reti ed il Responsabile dell'Ingegneria Clinica, per le rispettive aree di competenza e con il supporto del Responsabile della Sicurezza delle Informazioni, devono inoltre assicurare che, in applicazione del principio di security-by-design definito dalla POL1SDI Politica di Sicurezza delle Informazioni [1], la sicurezza delle informazioni sia indirizzata in tutte le attività di progettazione o di acquisizione relative al sistema informativo aventi come scopo:

copia informatica per consultazione

1. il perseguimento di nuovi obiettivi;
2. l'introduzione di nuovi servizi e funzionalità;
3. lo svolgimento di nuove attività precedentemente non previste;
4. l'attuazione di cambiamenti rilevanti su sistemi, reti, applicazioni e processi operativi ICT, apparati elettromedicali e sistemi di supporto, che abbiano impatti significativi sui processi, sulle procedure operative, sull'assetto organizzativo, o sulle tecnologie e gli strumenti ICT.

Essi dovranno anche tenere conto di eventuali altre politiche definite, non di sicurezza, ad esempio relativamente al ciclo di vita del software. A tale scopo, le attività di progettazione o di acquisizione relative al sistema informativo sono articolate nelle fasi di:

1. definizione dei requisiti;
2. progettazione;
3. sviluppo;
4. test e collaudo;
5. rilascio in produzione.

All'interno di tali fasi sono definiti milestone e attività specifiche relative alla sicurezza, la cui esecuzione, operativamente in carico al Responsabile di Progetto, si svolge sotto la responsabilità del Responsabile della Sicurezza Informatica e delle Reti e del Responsabile dell'Ingegneria Clinica, per le rispettive aree di competenza e con il supporto del Responsabile della Sicurezza delle Informazioni. Queste attività comprendono:

- la definizione di Referenti per la Sicurezza delle Informazioni per gli asset che coincidono con il personale SIA rilevanti all'interno del progetto, in linea con il PrS03SDI Gestione delle Informazioni e degli Asset [3]; in particolare, il Responsabile di Progetto ricopre il ruolo di Referente della Sicurezza delle Informazioni di tutti i nuovi asset in ambiente di sviluppo e test, per tutta la durata del progetto. Il Responsabile della Sicurezza Informatica e delle Reti accerta che la designazione del Referente della Sicurezza delle Informazioni di tutti i nuovi asset avvenga prima del passaggio in produzione e/o dell'attuazione di nuove procedure o cambiamenti organizzativi, ed ha il compito di supportare la risoluzione di eventuali conflitti in accordo con le Direzioni coinvolte;
- nell'ambito della fase di definizione dei requisiti, la determinazione degli obiettivi di integrità, disponibilità, riservatezza e di conformità alle normative vigenti ed agli standard nazionali ed internazionali di sicurezza, nonché dei livelli di assurance previsti; la definizione dei requisiti è svolta sulla base delle indicazioni fornite dagli utenti e dallo sponsor del progetto, e non solo sulla base di valutazioni tecniche in carico alle strutture di gestione del sistema informativo; i requisiti devono tenere conto inoltre delle esigenze di sicurezza complessive del Sistema Federato, sulla base delle indicazioni e delle specifiche fornite al riguardo da Regione Lombardia;
- in fase di progettazione:
  - la formalizzazione delle specifiche di dettaglio relativamente alle misure di sicurezza atte a soddisfare tutti i suddetti obiettivi. In caso di acquisizioni, tali requisiti sono esplicitamente inclusi nella documentazione contrattuale;

copia informatica per consultazione

- specificatamente per quanto concerne la realizzazione di nuovi sistemi o applicazioni, la definizione di una architettura hardware e software che preveda l'utilizzo di risorse adeguate a sopperire a condizioni di erogazione al limite dei requisiti di funzionamento previsti, e la valutazione degli impatti di capacity sull'infrastruttura esistente;
- la redazione della lista di verifiche di sicurezza per il controllo della presenza e dell'efficacia di tutte le misure di sicurezza definite dalle specifiche di dettaglio o dalla documentazione contrattuale;

- il superamento delle verifiche di sicurezza prima del passaggio in produzione e/o dell'attuazione di nuove procedure o cambiamenti organizzativi. In caso di acquisizioni, il superamento di tali verifiche costituisce uno dei criteri di accettazione della fornitura; le verifiche devono comprendere la validazione da parte degli utenti e dello sponsor del progetto, anche relativamente agli aspetti di usabilità delle funzionalità di sicurezza;
- l'integrazione, nell'ambito della documentazione di progetto, di tutti gli aspetti di sicurezza relativi al progetto stesso;
- la predisposizione di sessioni di formazione e sensibilizzazione del personale riguardo ai nuovi incarichi e responsabilità;
- l'aggiornamento tempestivo di tutte le procedure operative e dei processi afferenti alle funzioni organizzative coinvolte;
- in caso di acquisizioni, nei casi previsti dal REGSDI02 Gestione dei rapporti con i Fornitori [2], la consegna di tutti i codici sorgente, tracciati record e documentazione di progetto da parte dei fornitori;
- la definizione, in fase di rilascio, di adeguate istruzioni operative per la manutenzione ordinaria, per il monitoraggio e per la risoluzione rapida ed efficace degli errori e delle eccezioni che possono coinvolgere in ambiente di produzione la soluzione realizzata.

5.1.1. Misure ed accorgimenti per lo sviluppo sicuro di software e per l'integrazione sicura dei sistemi

Il Responsabile della Sicurezza Informatica e delle Reti ed il Responsabile dell'Ingegneria Clinica, per le rispettive aree di competenza e con il supporto del Responsabile della Sicurezza delle Informazioni integrano nell'ambito della propria Procedura di Gestione del Ciclo di Vita dei Sistemi e delle Applicazioni apposite misure per lo sviluppo sicuro del software e per l'integrazione sicura dei sistemi informativi. Esse prevedono:

- la protezione logica e fisica dell'ambiente e dei dati usati per lo sviluppo e, in particolare:
  - i controlli di accesso logico e fisico alla documentazione tecnica, al codice sorgente ed alle configurazioni, nonché il loro corretto "*versioning*";
  - il mantenimento delle copie e/o dei supporti originali del software utilizzato;
- la ricerca e l'eliminazione di vulnerabilità nel codice sorgente eventualmente sviluppato, tramite opportune tecniche di sviluppo sicuro e di analisi del codice;
- la limitazione delle modifiche (c.d. "personalizzazioni") dei pacchetti software (in particolare i prodotti acquisiti da fornitori esterni) ai soli casi strettamente necessari, provvedendo altresì a controllare e documentare tutti i cambiamenti;

copia informatica per consultazione

- l'estensione dell'obbligo di osservanza delle suddette misure ai fornitori, indipendentemente dalle sedi e dai sistemi ove siano svolte le attività commissionate (locali/sistemi dell'ASST di Mantova, dei fornitori o di sub-fornitori);
- l'adozione di buone pratiche riconosciute nell'intero ciclo di vita dei sistemi.

Per ciascun sistema o applicazione, il Responsabile della Sicurezza Informatica e delle Reti, con il supporto del Responsabile dell'Ingegneria Clinica per la rispettiva area di competenza, documenta e mantiene aggiornato un censimento delle diverse tipologie di informazioni trattate. L'individuazione e la classificazione delle informazioni sono in carico all'utente o, per i progetti per i quali non sia ancora individuato, allo sponsor del progetto. È invece in carico al Responsabile di Progetto la documentazione ed implementazione, in funzione della classificazione delle informazioni stesse:

- dei requisiti normativi, statutari, contrattuali e di business, compresi quelli definiti nell'ambito del Sistema Federato;
- delle regole di sicurezza applicabili ad ogni sistema, all'applicazione ed ai dati trattati, compresa la definizione dei profili e dei criteri di accesso, in linea con le politiche e regole di controllo accessi. Tali profili comprendono quelli necessari per la gestione e manutenzione dei sistemi, dei database e delle applicazioni;
- dei requisiti di non ripudiabilità e autenticità che devono essere garantiti, anche in opposizione a terzi in caso di contenziosi o di violazioni normative;
- delle regole di *retention*, in conformità con i requisiti normativi pertinenti;
- della frequenza e delle modalità opportune di svolgimento della verifica di sicurezza;
- degli ulteriori requisiti di sicurezza definiti nell'ambito delle politiche e regolamenti dell'ASST di Mantova, come ad esempio le modalità di backup, i requisiti relativi alla continuità operativa ecc.

Le misure individuate sono implementate nel rispetto del principio della difesa in profondità, assicurando pertanto che le informazioni siano protette sia agendo sulle componenti applicative, che sui servizi middleware, di database e tramite misure adeguate sui sistemi e sulle reti coinvolti.

5.1.2. Separazione degli ambienti e protezione dei dati di test

L'ASST di Mantova prevede la separazione degli ambienti di sviluppo (tipicamente presso le software house), test e produzione, prevede cioè che siano tre ambienti separati, per migliorare l'efficacia delle misure di sicurezza e per ridurre il rischio di accesso o cambiamenti non autorizzati all'ambiente di produzione. A tale scopo, il Responsabile della Sicurezza Informatica e delle Reti, con il supporto del Responsabile dell'Ingegneria Clinica per la rispettiva area di competenza, sentito il Responsabile della Sicurezza delle Informazioni:

- garantisce la separazione logica e fisica degli ambienti di sviluppo, test e produzione;
- definisce le regole necessarie per il passaggio di software/componenti hardware dallo sviluppo, al test, alla produzione riducendo il rischio di problemi e/o di accesso o cambiamenti non autorizzati all'ambiente di produzione;

copia informatica per consultazione

- non consente l'utilizzo di strumenti di sviluppo in ambiente di produzione;
- limita i privilegi e l'accesso ai sistemi ed apparati di produzione da parte del personale che svolge attività di sviluppo e test prevedendo gruppi separati per le attività di amministrazione e configurazione di reti, sistemi e applicazioni nei tre ambienti;
- vieta l'utilizzo di dati reali in ambienti di sviluppo.

5.1.3. Sicurezza delle informazioni nella gestione dei progetti

La responsabilità di assicurare che i progetti siano realizzati in conformità con il presente documento è attribuito dall'ASST di Mantova Responsabili di Progetto incaricati ai i quali devono assicurare che ogni attività progettuale o di acquisizione sia condotta indirizzando gli aspetti di sicurezza delle informazioni, dalla definizione degli obiettivi/requisiti fino alla completa attuazione.
I Responsabili di Progetto devono in particolare assicurare:

1. l'individuazione o la raccolta dei requisiti utente per gli aspetti di sicurezza delle informazioni, sulla base delle indicazioni fornite dai soggetti interessati e/o competenti, quali gli utenti, la Struttura Complessa Avvocatura, la Struttura Complessa Risorse Umane, ecc.
2. l'individuazione dei livelli di *assurance* per i requisiti sopra indicati, secondo criteri analoghi e sulla base della criticità del progetto;
3. la documentazione, in tutte le fasi del progetto, delle modalità di gestione di tali requisiti, ed in particolare di implementazione in linea con i principi di *security-by-design* e *privacy-by design*;
4. l'adozione di misure di sicurezza per l'ambiente di sviluppo adeguate ai requisiti di sicurezza e *assurance* individuati;
5. l'adozione di tecniche di sviluppo sicuro adeguate ai requisiti di sicurezza ed *assurance* individuati;
6. l'effettuazione di test specifici per i requisiti di sicurezza;
7. l'adozione di una metodologia di valutazione del rischio a supporto delle valutazioni e scelte sopra indicate.

L'ASST di Mantova adotta adeguati piani di formazione ed aggiornamento per i Responsabili di Progetto e alloca le adeguate risorse per garantire il raggiungimento degli obiettivi. A questo scopo, il Responsabile della Sicurezza Informatica, il responsabile del Servizio di Fisica Sanitaria e delle Reti ed il Responsabile dell'Ingegneria Clinica, per le rispettive aree di competenza e con il supporto del Responsabile della Sicurezza delle Informazioni, individuano le esigenze di formazione e si coordinano con l'Area Formazione, ricerca e Innovazione per l'erogazione della formazione necessaria.

5.2. Sicurezza nella gestione dei cambiamenti

Il Responsabile della Sicurezza Informatica e delle Reti, il Responsabile Sistemi RIS-PACS ed il Responsabile dell'Ingegneria Clinica, ciascuno per le rispettive aree di competenza e con il supporto del Responsabile della Sicurezza delle Informazioni, prevedono opportuni controlli di sicurezza nell'ambito delle procedure di gestione dei cambiamenti al sistema informatico ed ai suoi

copia informatica per consultazione

processi di gestione, al fine di minimizzare il potenziale impatto dei cambiamenti stessi sull'operatività, sulla sicurezza delle informazioni e sull'erogazione dei servizi informatici. Sono al di fuori dell'ambito di questo documento le attività relative alla gestione di eventi riconducibili al *Disaster Recovery*, oggetto di specifiche politiche. Sono altresì da ritenersi fuori ambito tutte le attività sistemistiche svolte di routine, quali ad esempio:

1. attività di gestione di utenti e gruppi di utenze, gestione password, modifica di permessi di accesso;
2. attività di modifica su sistemi in ambiente di sviluppo.

Il Responsabile della Sicurezza Informatica e delle Reti, il responsabile del Servizio di Fisica Sanitaria ed il Responsabile dell'Ingegneria Clinica, per le rispettive aree di competenza e con il supporto del Responsabile della Sicurezza delle Informazioni prevedono, all'interno del processo di gestione dei cambiamenti, una valutazione dell'impatto potenziale del cambiamento sul sistema informatico e sulla sua sicurezza.
La valutazione tiene conto della classificazione delle informazioni trattate dai componenti interessati. I cambiamenti sono classificati secondo le seguenti categorie:

1. modifiche evolutive;
2. modifiche correttive;
3. nuovi servizi;
4. progetti infrastrutturali;
5. cambiamenti critici, ovvero i cambiamenti il cui impatto potenziale è tale da poter provocare disservizi rilevanti in sistemi classificati come critici ai fini della continuità operativa;
6. cambiamenti in emergenza, ovvero quelli effettuati per la risoluzione urgente di un incidente o disservizio.

Nell'ambito della procedura di gestione dei cambiamenti, gli aspetti di sicurezza sono gestiti coerentemente con la tipologia di cambiamento e con la valutazione di impatto effettuata.
Sono affrontati in particolare:

1. il processo autorizzativo;
2. la documentazione, in particolare la predisposizione o l'aggiornamento di:
   - classificazione delle informazioni trattate;
   - requisiti di capacità e disponibilità, con particolare riferimento a quelli di continuità operativa;
   - tempi e modalità di *backup*, e tempi di *retention* per le diverse tipologie di informazioni trattate;
   - configurazioni;
   - istruzioni operative per la gestione;
   - profili autorizzativi, in coerenza con la PG02SDI Controllo degli Accessi.
3. la possibilità di gestire eventuali problemi in fase di introduzione del cambiamento, definendo dei piani di rientro, al fine di poter avviare il ripristino dei software/sistemi impattati in uno stato funzionante e di garantire la continuità dei servizi nel caso in cui il cambiamento non vada a buon fine, anche ripristinando lo stato precedente (*rollback*). La

copia informatica per consultazione

procedura di gestione dei cambiamenti identifica i soggetti che hanno la responsabilità, caso per caso, di stabilirne le condizioni di attuazione.

I cambiamenti sono programmati in accordo con l'utenza dei servizi, limitando al minimo i possibili disservizi. Tutti i cambiamenti sono formalmente approvati da un responsabile, posto al livello gerarchico adeguato in relazione all'impatto stimato del cambiamento. L'approvazione avviene da parte del Responsabile della Sicurezza Informatica e delle Reti, del responsabile del Servizio di Fisica Sanitaria e del Responsabile dell'Ingegneria Clinica, per le rispettive aree di competenza, previa verifica del rispetto dei requisiti di sicurezza previsti da questo documento, o da soggetti da questi delegati. Per i cambiamenti critici, l'approvazione avviene anche da parte della Direzione Strategica.

Tutte le attività svolte nell'ambito della gestione dei cambiamenti devono essere tracciate, a cura del Responsabile di Progetto, mediante adeguati sistemi di monitoraggio per consentire di ricostruire l'insieme delle operazioni svolte, e al fine di supportare l'identificazione dei problemi e delle loro cause, nonché l'attuazione eventuale delle procedure di rientro.
Il Responsabile di Progetto assicura la mitigazione del potenziale impatto dei cambiamenti critici sull'operatività e sull'erogazione dei servizi informatici, in coerenza con la PG03SDI Gestione degli incidenti per garantire la Continuità Operativa.
La gestione di cambiamenti critici prevede, in aggiunta a quanto già sopra indicato:

1. l'approvazione del relativo progetto da parte del Responsabile della Sicurezza delle Informazioni o, in alternativa, l'acquisizione del relativo parere;
2. la revisione del Piano di Continuità Operativa e delle procedure di *disaster recovery*, per quanto impattato dai componenti del sistema informatico interessati dal cambiamento;
3. per cambiamenti critici a componenti infrastrutturali, il riesame dei controlli applicativi e delle procedure a garanzia dell'integrità, per assicurare che non siano stati compromessi.

5.2.1. Cambiamenti in emergenza

I cambiamenti in emergenza sono effettuati per la gestione/risoluzione di incidenti, attraverso apposite procedure che bilanciano adeguatamente gli obiettivi di urgenza con quelli di protezione dell'operatività e della sicurezza del sistema informatico.
I criteri per avviare la procedura di gestione in emergenza, i tempi di attivazione, nonché i responsabili che possono autorizzare tale attivazione, sono definiti nell'ambito del PrS06SDI Gestione degli incidenti per garantire la Continuità Operativa [7] e delle relative procedure.
In particolare, rispetto all'approccio ordinario, sulla base di criteri emergenziali possono prevedere:

- la possibilità di ricorrere all'approvazione in assunzione di responsabilità da parte del Responsabile della Sicurezza Informatica e delle Reti, del Responsabile dell'Ingegneria Clinica o del Responsabile della Sicurezza delle Informazioni sentiti quando possibile il Responsabile Applicativi e Sistemi, in assenza di altri referenti;
- l'esecuzione delle attività in assenza di adeguato preavviso, ricorrendo alla sospensione di altri cambiamenti pianificati.

copia informatica per consultazione

La procedura di emergenza prevede comunque, al termine dell'emergenza, le attività di validazione e allineamento della documentazione necessarie per riportare l'intervento nelle modalità di gestione ordinaria delle modifiche, nonché l'estensione del tracciamento, includendo i nominativi del personale che ha svolto le singole attività.

5.3. Sicurezza delle procedure operative di gestione

Il Responsabile della Sicurezza Informatica e delle Reti e il Responsabile dell'Ingegneria Clinica, per le rispettive aree di competenza, sentito il Responsabile della Sicurezza delle Informazioni, assicurano l'integrazione, nell'ambito della gestione dei sistemi, delle reti e delle applicazioni, apposite misure volte a garantire che le attività di installazione, configurazione, aggiornamento manutenzione e risoluzione dei problemi siano svolte nel rispetto degli obiettivi di sicurezza delle informazioni.

5.3.1. Installazione, configurazione e aggiornamento

Il Responsabile della Sicurezza Informatica e delle Reti e il Responsabile dell'Ingegneria Clinica, per le rispettive aree di competenza, sentito il Responsabile della Sicurezza delle Informazioni, adottano appropriate misure di sicurezza nell'ambito delle attività operative di installazione, configurazione e aggiornamento dei sistemi informatici, degli apparati di rete e degli applicativi (includendo tra essi anche i sistemi atti a proteggere il patrimonio aziendale, come firewall, servizi di logging ecc.), a valle della loro acquisizione, sviluppo o modifica, con l'obiettivo di rispettare e mantenere nel tempo il livello di sicurezza atteso. Tali misure prevedono:

- la formalizzazione e l'applicazione delle istruzioni operative per la sicurezza nelle attività di installazione, configurazione e aggiornamento dei sistemi, degli apparati di rete e degli applicativi;
- la definizione e l'aggiornamento di istruzioni operative per l'installazione, l'aggiornamento e la configurazione sicura dei sistemi, apparati di rete e software in accordo con le linee guida e gli indirizzi tecnici applicabili emanati dalla Regione Lombardia (in particolare, Indirizzi tecnici per l'Hardening,[12] e Indirizzi per il Patching [11]]). Tali istruzioni identificano le attività che è necessario svolgere sui diversi sistemi operativi, apparati di rete e componenti software (middleware, applicazioni e basi di dati) utilizzati presso l'ASST di Mantova;
- la tracciabilità delle operazioni di gestione svolte da parte del personale, interno o esterno.

È vietata l'installazione e l'utilizzo di software di cui l'ASST di Mantova non disponga di licenza a sé stesso intitolata, o ottenuta nell'ambito di un contratto di fornitura da parte di terzi.
E' inoltre vietata l'installazione di software da parte del personale non specificamente incaricato.
Eventuali eccezioni devono essere specificamente autorizzate dal Responsabile della Sicurezza Informatica e delle Reti, anche per categorie di utenza, sentito il parere del Responsabile della Sicurezza delle Informazioni.

copia informatica per consultazione

5.3.2. Manutenzione ordinaria, monitoraggio e gestione dei problemi

Il Responsabile della Sicurezza Informatica e delle Reti, il Responsabile del servizio di Fisica Sanitaria e il Responsabile dell'Ingegneria Clinica, per le rispettive aree di competenza, e sentito il Responsabile della Sicurezza delle Informazioni, verificano l'osservanza, nell'ambito della gestione quotidiana dei sistemi, delle reti e delle applicazioni, delle istruzioni operative di manutenzione definite in fase di rilascio in ambiente di produzione. Laddove tali istruzioni operative non siano disponibili, definiscono procedure periodiche di controllo per verificare la presenza di errori, potenziali malfunzionamenti, o il superamento o l'approssimarsi del limite di utilizzo delle risorse disponibili. Individuano inoltre, in tali casi, un insieme di operazioni di manutenzione da svolgersi periodicamente, atte a ridurre il rischio di malfunzionamenti, errori e disservizi.
Il Responsabile della Sicurezza Informatica e delle Reti, con il supporto del Responsabile dell'Ingegneria Clinica e sentito il Responsabile della Sicurezza delle Informazioni, definisce e attua una procedura di monitoraggio dei sistemi, delle reti e delle applicazioni, comprese quelle riconducibili all'ambito dell'Ingegneria Clinica, con l'obiettivo di assicurare il rilevamento tempestivo di anomalie, errori e malfunzionamenti, ed in osservanza delle istruzioni operative definite in fase di rilascio in ambiente di produzione.

5.3.3. Supporto tecnico effettuato all'esterno

Il Responsabile della Sicurezza Informatica e delle Reti, in accordo con il Responsabile dell'Ingegneria Clinica, e sentito il Responsabile della Sicurezza delle Informazioni, assicura che le procedure operative prevedano l'adozione di specifiche misure di protezione degli asset e dei supporti fisici laddove un sistema, elementi dell'infrastruttura di rete o componenti di essi debbano essere trasportati all'esterno dell'organizzazione, per lo svolgimento di attività di manutenzione correttiva e riparazione, e comunque in tutti i casi sia necessario trasferirli.
Tali misure sono definite dalla PrS03SDI Gestione delle Informazioni e degli Asset [3] in accordo con il REGSDI02 Gestione dei rapporti con i Fornitori [4]. Della loro attuazione sono incaricati il Responsabile Applicativi e Sistemi o il Responsabile della Sicurezza Informatica e delle Reti, per competenza, in accordo con il Referente della Sicurezza delle applicazioni interessate.

5.3.4. Gestione delle Vulnerabilità Tecniche

Il Responsabile della Sicurezza delle Informazioni individua fonti tempestive, affidabili e complete sulle vulnerabilità dei prodotti e servizi software che utilizza e sulle modalità e strumenti di eliminazione o mitigazione.
Nella stipula di contratti di fornitura di prodotti e servizi software, il Responsabile della Sicurezza Informatica e delle Reti ed il Responsabile dell'Ingegneria Clinica assicurano, ciascuno per la propria area di competenza ed in accordo con il REGSDI02 Gestione dei rapporti con i Fornitori [2], la disponibilità di questo tipo di fonti, secondo livelli di servizio basati sulla classificazione delle informazioni gestite. Essi definiscono inoltre ed assicurano l'implementazione di una procedura di eliminazione o mitigazione delle vulnerabilità tecniche conforme con gli Indirizzi per il *patching* dei sistemi [11] secondo priorità definite sulla base della criticità delle componenti coinvolte e delle relative vulnerabilità.

copia informatica per consultazione

Tutte le attività sono gestite come incidenti di sicurezza, e come tali essere tracciate e gestite secondo gravità, prevedendo nella fase di *patching* vera e propria l'esecuzione della procedura di gestione dei cambiamenti o dei cambiamenti in emergenza.

5.3.5. Backup e ripristino delle informazioni

Il Responsabile della Sicurezza Informatica e delle Reti assicura, con il supporto del Responsabile dell'Ingegneria Clinica per la rispettiva area di competenza, e sentito il Responsabile della Sicurezza delle Informazioni, che i backup ed il ripristino delle informazioni siano effettuati secondo specifiche procedure definite in accordo con la PrS03SDI Gestione delle Informazioni e degli Asset [3].
Tali procedure garantiscono per ciascun sistema, applicazione o database:

- la definizione degli obiettivi di salvaguardia dei dati (Recovery Point Objective - **RPO**) e, in caso di trattamento di informazioni classificate in alta disponibilità, i tempi di ripristino (Recovery Time Objective - **RTO**), in accordo con il PrS06SDI Gestione degli incidenti per garantire la Continuità Operativa [7].
- la creazione e conservazione protetta di copie di Backup in accordo con gli obiettivi di disponibilità e i tempi di ripristino definiti;
- la creazione di copie di backup relative ai componenti software utilizzati (firmware o sistema operativo, middleware, servizi di database, componenti applicative, utilità e strumenti installati sul sistema stesso), all'ultima versione installata;
- il ripristino dei sistemi in accordo con gli obiettivi definiti;
- il ripristino delle componenti di sistema operativo ed i servizi (middleware, software applicativo, utilità di sistema etc…) dei singoli sistemi;
- il ripristino delle configurazioni software di ciascun sistema fino all'ultima modifica apportata;
- il ripristino delle informazioni gestite da ogni applicazione in accordo con il valore di RPO definito;
- la verifica che le procedure di backup siano state svolte in modo corretto e che i dati salvati siano integri ed utilizzabili per le procedure di recovery tramite l'esecuzione periodica di esercitazioni e test delle complete procedure di ripristino;
- la protezione dell'integrità e della confidenzialità dei dati di backup mediante idonee misure di sicurezza fisica e logica, in accordo con la classificazione delle informazioni, e quindi dei sistemi e delle applicazioni cui essi fanno riferimento;
- la protezione della disponibilità dei dati di backup mediante la loro conservazione presso siti alternativi.

5.3.6. Gestione dei Log

Il Responsabile della Sicurezza Informatica e delle Reti, con il supporto del Responsabile dell'Ingegneria Clinica e del Responsabile della Fisica Sanitaria per la rispettiva area di competenza, sentito il Responsabile della Sicurezza delle Informazioni e in conformità con il "Provvedimento sugli amministratori di sistema" del Garante per la Protezione dei dati Personali

copia informatica per consultazione

(rif.[19]), implementa una Procedura di Gestione dei Log di Sistema e Applicativi [13] che definisce:

- le modalità previste per la generazione, la raccolta, la conservazione e l'analisi dei log degli eventi rilevanti per la sicurezza del sistema informativo;
- le informazioni significative per la sicurezza che devono essere tracciate nei suddetti log ed i tempi previsti per la *retention* degli stessi e delle relative copie di backup, in accordo con le normative vigenti;
- i criteri per assicurare la protezione dei log dalla modifica, dall'accesso non autorizzato, anche da parte di personale interno, e dalla cancellazione o perdita, coerentemente con la classificazione delle informazioni ivi memorizzate;
- misure particolari per la registrazione delle operazioni svolte dagli amministratori e dagli operatori di sistema, in conformità con il "Provvedimento sugli amministratori di sistema" del Garante per la Protezione dei dati Personali (rif.[19]).

5.3.7. Capacity Management

Il Responsabile della Sicurezza Informatica e delle Reti, con il supporto del Responsabile dell'Ingegneria Clinica, il Responsabile della Fisica Sanitaria per la rispettiva area di competenza e sentito il Responsabile della Sicurezza delle Informazioni, assicura l'operatività dei sistemi, reti ed applicazioni tramite la gestione delle risorse informatiche attuata attraverso una procedura di Capacity Management, che prevede:

- la raccolta, da parte delle procedure di monitoraggio, delle informazioni statistiche relative all'uso delle risorse da parte dei sistemi, delle reti e delle applicazioni, ed il calcolo dei relativi trend evolutivi in base all'analisi storica degli stessi;
- l'attivazione, nell'ambito dei sistemi automatizzati a supporto delle procedure di monitoraggio, di appositi allarmi al superamento di soglie critiche relative all'utilizzo delle risorse;
- la valutazione almeno annuale, in sede di Comitato per la Sicurezza delle Informazioni, dei trend evolutivi per individuare i requisiti futuri di capacità, per pianificare il fabbisogno di risorse;

In particolare, per quanto concerne i sistemi e le applicazioni classificati ad *Alta Disponibilità*:

- l'individuazione delle interdipendenze funzionali e tecniche tra sistemi, reti e applicazioni, per determinare gli eventuali impatti derivanti dal superamento dei requisiti di *capacity*, anche per effetto di cambiamenti;
- l'acquisto o la definizione di opportuni livelli di servizio (SLA) nei contratti con i fornitori, per garantire la disponibilità tempestiva di parti di ricambio, servizi di supporto, componenti e risorse aggiuntive rispetto a quelle normalmente utilizzati;
- la definizione di opportuni margini in termini di risorse computazionali e di connettività, disponibili o acquisibili al bisogno in tempi brevi, al fine di tutelare la disponibilità dei servizi da picchi di carico.

copia informatica per consultazione

5.3.8. Gestione delle chiavi crittografiche

Il Responsabile della Sicurezza delle Informazioni, con il supporto del Responsabile dell'Ingegneria Clinica per la rispettiva area di competenza, assicura la protezione delle chiavi crittografiche utilizzate per la cifratura, la firma elettronica e l'autenticazione sui sistemi, sulle reti e sulle applicazioni, mediante misure di efficacia equivalente o superiore alle informazioni che esse proteggono, e mediante l'attuazione della appropriata procedura di gestione per tutto il loro ciclo di vita.
Tale procedura assicura l'individuazione dei Responsabili delle Chiavi di Cifratura nei vari ambiti di gestione.
In particolare, tale ruolo è assegnato a:

- il Responsabile Applicativi e Sistemi e al Responsabile della Sicurezza Informatica e delle Reti, ciascuno nel proprio ambito di competenza;
- i Referenti della Sicurezza di ciascuna applicazione, per le chiavi utilizzate per l'attuazione di funzionalità e servizi di natura applicativa o per la protezione delle informazioni gestite dall'applicazione stessa;
- la definizione di apposite misure di sicurezza nell'ambito dello svolgimento delle operazioni di creazione, distribuzione, archiviazione, rinnovo e distruzione delle chiavi;
- per ciascun ambito, la definizione degli algoritmi e delle lunghezze minime delle chiavi utilizzate e il periodo di tempo massimo durante il quale saranno valide, in accordo con gli Indirizzi Tecnici relativi ad "Analisi protocolli e algoritmi crittografici" [17];
- la definizione di misure atte ad assicurare la protezione delle chiavi dall'accesso non autorizzato;
- la definizione delle misure a garanzia dell'integrità e della disponibilità delle chiavi di cifratura durante il ciclo di vita;
- la documentazione e l'aggiornamento periodico della lunghezza delle chiavi in congiunzione a ogni algoritmo, metodo e strumento utilizzati dall'ASST di Mantova, in accordo con gli Indirizzi Tecnici relativi ad "Analisi protocolli e algoritmi crittografici" [17];
- l'accesso in emergenza alle chiavi, in assenza del relativo Responsabile, previa autorizzazione del Responsabile della Sicurezza delle Informazioni, il quale presiede all'accesso e dispone il tracciamento tutte le operazioni svolte.

Misure particolari per l'utilizzo di strumenti crittografici per i quali la lunghezza e il tempo di validità delle chiavi sono già regolati al di là della sua possibilità d'intervento o da normative vigenti.

Il Responsabile della Sicurezza delle Informazioni dispone la duplicazione di tutte le chiavi crittografiche la cui disponibilità è requisito per l'accesso ad informazioni o servizi non altrimenti accessibili, e la loro conservazione in almeno due siti fisici differenti al fine di evitare il rischio di smarrimento delle stesse e le conseguenti ricadute che questo potrebbe avere sulla sicurezza delle informazioni da esso gestite.

copia informatica per consultazione

5.3.9. Gestione degli Incidenti

Il Responsabile della Sicurezza Informatica e delle Reti, con il supporto del Responsabile dell'Ingegneria Clinica e il Responsabile della Fisica Sanitaria per la rispettiva area di competenza e sentito il Responsabile della Sicurezza delle Informazioni, assicura, tramite l'attuazione della procedura di Risposta agli Incidenti, il rilevamento tempestivo, la gestione, la mitigazione e la risoluzione degli incidenti sui sistemi, sulle reti e sulle applicazioni, al fine di ridurne i potenziali impatti negativi sulle attività operative o sulla sicurezza delle informazioni.
La procedura assicura:

1. la disponibilità di canali di segnalazione degli incidenti, anche raccordandosi con le procedure di monitoraggio;
2. la tracciatura degli incidenti, garantendo anche che in ogni momento siano in carico a qualcuno che ne debba gestire la risoluzione;
3. procedure di escalation che coinvolgano tempestivamente i diversi soggetti interessati o dalla cui valutazione o autorizzazione dipenda la risoluzione dell'incidente;
4. la valutazione, al termine dell'incidente, di eventuali attività da svolgere per eliminare le vulnerabilità che hanno causato l'incidente o per migliorare il processo di gestione.

5.3.10. Gestione della Continuità

Il Responsabile della Sicurezza Informatica e delle Reti assicura, con il supporto del Responsabile dell'Ingegneria Clinica e il Responsabile della Fisica Sanitaria per la rispettiva area di competenza, la continuità di sistemi, reti e applicazioni e dell'operatività aziendale tramite l'attuazione della PrS06SDI Gestione degli incidenti per garantire la Continuità Operativa definita in [7].

5.3.11. Dismissione

Il Responsabile della Sicurezza Informatica e delle Reti, con il supporto del Responsabile dell'Ingegneria Clinica e il Responsabile della Fisica Sanitaria per la rispettiva area di competenza, e sentito il Responsabile della Sicurezza delle Informazioni assicura che la dismissione dei sistemi, dei componenti delle reti e di tutti i componenti dell'infrastruttura informatica, sia effettuata nel rispetto di procedure operative definite in accordo con le disposizioni definite dalla PrS03SDI Gestione delle Informazioni e degli Asset [3], in particolare per quanto concerne i supporti di memorizzazione contenenti le informazioni gestite dalle applicazioni e le configurazioni dei sistemi e dei componenti di rete.

Il Responsabile Applicativi e Sistemi e il Responsabile della Sicurezza Informatica e delle Reti, ciascuno per competenza, assicurano la definizione e l'osservanza di specifiche istruzioni operative da parte del personale impiegato.

5.3.12. Diffusione

La Struttura Complessa Qualità, Accreditamento e Risk Management rende conoscibili ed accessibili con semplicità, da parte del personale interno o esterno, le politiche, regole, procedure e istruzioni operative di sicurezza, anche attraverso ordini di servizio, consegnati al personale interessato in forma cartacea o elettronica, o messe a disposizione su intranet o strumenti

copia informatica per consultazione

analoghi. Tali procedure e istruzioni operative sono parte dell'attività di formazione sulla sicurezza delle informazioni erogata al personale interessato.

5.3.13. Sicurezza degli strumenti di gestione

Il Responsabile della Sicurezza Informatica e delle Reti, con il supporto del Responsabile dell'Ingegneria Clinica e il Responsabile della Fisica Sanitaria per la rispettiva area di competenza e sentito il Responsabile della Sicurezza delle Informazioni, assicura l'adozione di specifiche misure di sicurezza per i servizi e le interfacce riservate alla gestione ed alla manutenzione dei sistemi, delle reti e delle applicazioni, in particolare nei casi in cui essi consentano di aggirare controlli applicativi e di sistema previsti.
Anche in ottemperanza con i requisiti normativi applicabili, tali misure prevedono:

1. l'identificazione e la documentazione di tutti i servizi e delle interfacce di gestione disponibili sui sistemi;
2. l'identificazione di tutto il personale interno ed esterno che è autorizzato ad utilizzarli;
3. il tracciamento degli accessi, dei tentativi di accesso errati, delle operazioni svolte (con relativo esito) durante le sessioni di lavoro.

6. RIFERIMENTI

6.1.1. Normativa interna dell'ASST di Mantova

[1] POL1SDI Politica di Sicurezza delle Informazioni;
[2] REGSDI02 Gestione dei rapporti con i Fornitori;
[3] PrS03SDI Gestione delle Informazioni e degli Asset;
[4] PrS07SDI Controllo degli accessi alle informazioni;
[5] PrS06SDI Gestione degli incidenti per garantire la Continuità Operativa;
[6] PrS01SDI Gestione delle Utenze e dei Privilegi;

6.1.2. Normativa interna di Regione Lombardia

6.1.2.1. Linee Guida e Indirizzi Tecnici

[7] Glossario – Sicurezza delle Informazioni Collana degli Indirizzi Tecnici per la sicurezza dell'informazione – Regione Lombardia/Lombardia Informatica:
[8] Indirizzi per la Configurazione dei Firewall
[9] Indirizzi per il Patching dei sistemi
[10] Indirizzi per l'Hardening dei Sistemi
[11] Indirizzi per la sicurezza dei file di LOG
[12] Indirizzi per la sicurezza delle basi di dati
[13] Codice JAVA sicuro
[14] Indirizzi per l'Autenticazione
[15] Analisi protocolli e algoritmi crittografici

6.1.3. Normative Nazionali

[16] Garante per la protezione dei dati personali – Linee guida in materia di trattamento di dati personali, contenuti anche in atti e documenti amministrativi, effettuato per finalità di

copia informatica per consultazione

pubblicità e trasparenza sul web da soggetti pubblici e da altri enti obbligati; G.U. n.134 del 12 giugno 2014

[17] Garante per la protezione dei dati personali - Provvedimento 27 nov. 2008 recante prescrizioni ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni di amministratore di sistema e proroga dei termini per il loro adempimento - 25 giugno 2009;

[18] Garante per la protezione dei dati personali – Linee guida in materia di trattamento di dati personali per finalità di pubblicazione e diffusione nei siti web esclusivamente dedicati alla salute; G.U. n.42 del 20 febbraio 2012

[19] Garante per la protezione dei dati personali – Linee guida in materia di trattamento di dati per lo svolgimento di indagini di customer satisfaction in ambito sanitario; G.U. n.120 del 25 maggio 2011

[20] Garante per la protezione dei dati personali – Linee guida in materia di trattamento di dati personali contenuti anche in atti e documenti amministrativi, effettuato da soggetti pubblici per finalità di pubblicazione e diffusione sul web; G.U. n.64 del 19 marzo 2011

[21] Garante per la protezione dei dati personali – Linee guida in tema di referti on line; G.U. n.288 dell'11 dicembre 2009

[22] Garante per la protezione dei dati personali – Linee guida per i trattamenti di dati personali nell'ambito delle sperimentazioni cliniche di medicinali; G.U. n.190 del 14 agosto 2008

[23] DECRETO-LEGGE 18 ottobre 2012, n. 179: "Ulteriori misure urgenti per la crescita del Paese", come convertito dalla LEGGE 17 dicembre 2012, n. 221, art. 12, 13, 13 bis.

[24] D.lgs. 196/03 – Codice in materia di protezione dei dati personali – Allegato A.3: "Codice di deontologia e di buona condotta per i trattamenti di dati personali a scopi statistici e di ricerca scientifica effettuati nell'ambito del Sistema statistico nazionale"

6.1.4. Altri riferimenti

[25] Garante per la protezione dei dati personali – Provvedimenti - Trattamento non consentito di dati sanitari raccolti tramite apparecchiature diagnostiche - 10 aprile 2014;

[26] Garante per la protezione dei dati personali – Provvedimenti - Trattamento di dati tramite il dossier sanitario aziendale - 3 luglio 2014;

[27] Garante per la protezione dei dati personali – Provvedimenti - Informazioni sulle convinzioni religiose dei pazienti: i casi in cui possono essere raccolte durante il ricovero – 12 novembre 2014

copia informatica per consultazione

DECRETO N. 213 DEL 19/02/2021
DEL DIRETTORE GENERALE

OGGETTO: NOMINA DEL RESPONSABILE DELLA TRANSIZIONE DIGITALE (RTD) DELL'ASST DI MANTOVA

Riproduzione cartacea del documento informatico sottoscritto digitalmente da
RAFFAELLO STRADONI il 19/02/2021 13:58:32 ai sensi dell'art. 20 e 23 del D.lgs 82/2005

copia informatica per consultazione

IL DIRETTORE GENERALE

PREMESSO che negli ultimi anni sono state introdotte importanti disposizioni in materia di digitalizzazione della pubblica amministrazione per dare completa attuazione alle regole stabilite dal D.Lgs. 82/2005 "Codice dell'amministrazione digitale";

VISTA la L. 7 agosto 2015 n. 124 *"Deleghe al Governo in materia di riorganizzazione delle amministrazioni pubbliche"*, che contiene importanti deleghe legislative in materia di digitalizzazione volte a modificare ed integrare il CAD con l'intento di rendere effettivi i diritti digitali di cittadini e imprese nei confronti delle amministrazioni pubbliche, garantendo, anche attraverso le tecnologie dell'informazione e delle comunicazioni, il diritto di accedere a tutti i dati , i documenti e i servizi di loro interesse in modalità digitale e assicurando la semplificazione nell'accesso ai servizi stessi;

CONSIDERATO che, in attuazione di detta delega, il Governo ha emanato il Decreto Legislativo n. 179 del 2016, recante *"Modifiche ed integrazioni al Codice dell'amministrazione digitale",* e successivamente il Decreto Legislativo n. 217 del 2017, contenente *"disposizioni integrative e correttive" ,* provvedimenti che hanno, tra le altre cose, modificato in maniera sensibile l'impianto dell'articolo 17 del CAD;

ATTESO che il novellato art. 17 comma 1 del D.Lgs. 82/2005 stabilisce che ciascuna pubblica amministrazione è tenuta ad affidare ad un unico ufficio dirigenziale, fermo restando il numero complessivo degli uffici, la "*transizione alla modalità operativa digitale e i conseguenti processi di riorganizzazione finalizzati alla realizzazione di un'amministrazione digitale e aperta, di servizi facilmente utilizzabili e di qualità, attraverso una maggiore efficienza ed economicità*", nominando un Responsabile per la Transizione al Digitale (RTD);

VISTA, altresì, la Circolare del Ministro per la Pubblica Amministrazione n. 3 del 1° ottobre 2018 che approfondisce le caratteristiche della figura del Responsabile della Transizione Digitale;

DATO ATTO che al Responsabile della transizione competono tutti i poteri di impulso e coordinamento finalizzati alla piena transizione verso la modalità operativa digitale e, inoltre, al suo ufficio sono espressamente attribuiti, dall'articolo 17 del CAD, i seguenti compiti:

a) coordinamento strategico dello sviluppo dei sistemi informativi, di telecomunicazione e fonia, in modo da assicurare anche la coerenza con gli standard tecnici e organizzativi comuni;
b) indirizzo e coordinamento dello sviluppo dei servizi, sia interni che esterni, forniti dai sistemi informativi di telecomunicazione e fonia dell'amministrazione;
c) indirizzo, pianificazione, coordinamento e monitoraggio della sicurezza informatica relativamente ai dati, ai sistemi e alle infrastrutture anche in relazione al sistema pubblico di connettività, nel rispetto delle regole tecniche di cui all'articolo 51, comma 1;
d) accesso dei soggetti disabili agli strumenti informatici e promozione dell'accessibilità anche in attuazione di quanto previsto dalla L. 9 gennaio 2004 n.

Riproduzione cartacea del documento informatico sottoscritto digitalmente da
RAFFAELLO STRADONI il 19/02/2021 13:58:32 ai sensi dell'art. 20 e 23 del D.lgs 82/2005

copia informatica per consultazione

4;
e) analisi periodica della coerenza tra l'organizzazione dell'amministrazione e l'utilizzo delle tecnologie dell'informazione e della comunicazione, al fine di migliorare la soddisfazione dell'utenza e la qualità dei servizi nonché di ridurre i tempi e i costi dell'azione amministrativa;
f) cooperazione alla revisione della riorganizzazione dell'amministrazione ai fini di cui alla lettera e);
g) indirizzo, coordinamento e monitoraggio della pianificazione prevista per lo sviluppo e la gestione dei sistemi informativi di telecomunicazione e fonia;
h) progettazione e coordinamento delle iniziative rilevanti ai fini di una più efficace erogazione di servizi in rete a cittadini e imprese mediante gli strumenti della cooperazione applicativa tra pubbliche amministrazioni, ivi inclusa la predisposizione e l'attuazione di accordi di servizio tra amministrazioni per la realizzazione e compartecipazione dei sistemi informativi cooperativi;
i) promozione delle iniziative attinenti l'attuazione delle direttive impartite dal Presidente del Consiglio dei Ministri o dal Ministro delegato per l'innovazione e le tecnologie;
j) pianificazione e coordinamento del processo di diffusione, all'interno dell'amministrazione, dei sistemi di identità e domicilio digitale, posta elettronica, protocollo informatico, firma digitale o firma elettronica qualificata e mandato informatico, e delle norme in materia di accessibilità e fruibilità nonché del processo di integrazione e interoperabilità tra i sistemi e servizi dell'amministrazione e quello di cui all'articolo 64-bis.
j-bis) pianificazione e coordinamento degli acquisti di soluzioni e sistemi informatici, telematici e di telecomunicazione al fine di garantirne la compatibilità con gli obiettivi di attuazione dell'agenda digitale e, in particolare, con quelli stabiliti nel piano triennale di cui all'articolo 16, comma 1, lettera b).

CONSIDERATO che il RTD, in ragione della trasversalità della sua figura all'interno dell'organizzazione e per poter agire su tutti gli uffici e aree aziendali, ha poteri di impulso e coordinamento nei confronti di tutti gli altri dirigenti nell'attuazione di tutte le iniziative dell'amministrazione legate al digitale, anche per quanto riguarda pareri e verifiche, nonché nella realizzazione degli atti preparatori e di attuazione delle pianificazioni e programmazioni previste dal Piano Triennale;

CONSIDERATO inoltre che il RTD rappresenta il punto di contatto dell'Azienda verso l'esterno con diversi interlocutori, quali le altre pubbliche amministrazioni, l'Agenzia per l'Italia Digitale, il Difensore Civico per il digitale ed i cittadini e imprese, per i quali diviene un punto di riferimento rispetto ai servizi online e ai diritti digitali;

ATTESO che, nel rispetto della propria autonomia organizzativa, le pubbliche amministrazioni diverse dalle amministrazioni dello Stato devono individuare l'ufficio per il digitale di cui all'art. 17 del D.Lgs 82/2005 tra quelli di livello dirigenziale;

RILEVATO che il Responsabile del citato ufficio per il digitale deve essere dotato di adeguate competenze tecnologiche, di informatica giuridica e manageriale e deve rispondere, con riferimento ai compiti relativi alla transizione alla modalità digitale, direttamente all'organo di vertice;

copia informatica per consultazione

RITENUTO di individuare, quale Responsabile aziendale della transizione al digitale, l'Ing. Paolo Garbossa, dirigente presso la Struttura Complessa Sistemi Informativi Aziendali, appurato che lo stesso è in possesso delle adeguate competenze tecnologiche, di informatica giuridica e manageriali necessarie a ricoprire l'incarico;

PRESO ATTO dell'attestazione di regolarità e di legittimità del presente provvedimento espressa da ALBINI GIUSEPPE Direttore della Struttura Affari generali e Controlli interni , e da CASARI ANTONELLA, responsabile del procedimento;

DATO ATTO che il presente provvedimento non comporta oneri o proventi a carico dell'Azienda;

ACQUISITI i pareri del Direttore Amministrativo, del Direttore Sanitario e del Direttore Socio Sanitario;

DECRETA

1. di nominare, ai sensi dell'art.17del D.Lgs.82/2005, l'ing. Paolo Garbossa, dirigente della Struttura Complessa Sistemi Informativi Aziendali, quale Responsabile per la Transizione Digitale dell'Azienda Socio Sanitaria Territoriale di Mantova, con decorrenza dalla data di approvazione del presente atto;

2. di incaricare il Responsabile per la Transizione Digitale, affinché ponga in essere le azioni conseguenti alla sua nomina e previste dalla normativa di settore;

3. di precisare che tale incarico è differenziato ed aggiuntivo rispetto al ruolo ricoperto nella struttura di appartenenza e che tale incarico non comporta oneri a carico dell'ASST;

4. di pubblicare il presente provvedimento all'Albo on line sul sito istituzionale aziendale, ai sensi dell'art. 32 della legge n. 69/2009 e dell'art. 17 della L.R. 33/2009, nel rispetto del Regolamento UE 2016/679.

PRESO ATTO dei pareri di

DIRETTORE AMMINISTRATIVO	FERRARI GIUSEPPE
DIRETTORE SANITARIO	BELLOMETTI SIMONA AURELIA
DIRETTORE SOCIOSANITARIO	BOSCAINI RENZO

DIRETTORE GENERALE

STRADONI RAFFAELLO

(atto firmato digitalmente ai sensi
delle vigenti disposizioni di legge)

copia informatica per consultazione

ASST Mantova

Manuale di Conservazione

Redatto dal Responsabile della Conservazione dell'Azienda Socio Sanitaria Territoriale di Mantova

Azione	**Data**	**Nominativo**	**Funzione**
Redazione		Paolo Garbossa	Responsabile delle conservazione Responsabile della transizione digitale
Verifica		Piero Canino	Responsabile della gestione documentale
Approvazione		Mara Azzi	Direttore Generale

Registro delle versioni

N°Ver/Rev/Bozza	**Data emissione**	**Modifiche apportate**	**Osservazioni**
Rev 0	06/10/2022		

copia informatica per consultazione

Indice

copia informatica per consultazione

copia informatica per consultazione

copia informatica per consultazione

1 Scopo e Ambito del Documento

Il presente Manuale di Conservazione (d'ora in poi Manuale) descrive il processo di Conservazione dei documenti digitali dell'Azienda Socio Sanitaria Territoriale Mantova (d'ora in poi ASST), che sottopone a conservazione digitale alcune tipologie documentali, affidando il processo di conservazione in outsourcing ai conservatori ai sensi dell'art. 44-bis del CAD (art. 5, comma 3).
Nella tabella successiva sono indicati i dati identificativi dell'ASST.

Ragione Sociale	Azienda Socio Sanitaria Territoriale Mantova
Partita Iva	02481840201
Codice Fiscale	02481840201
Sede	Strada Lago Paiolo, 10 - 46100 Mantova
AOO	Vedi Tabella successiva
Codice univoco AOO	
Codice IPA	asstm
Indirizzo PEC	protocollogenerale@pec.asst-mantova.it
Telefono	

Codice	AOO	PEC
A23285C	Struttura Complessa Affari Generali e Controlli Interni	protocollogenerale@pec.asst-mantova.it
A85808E	Area amministrativa fabbisogni di personale	reclutamento@pec.asst-mantova.it
A34F9EE	Protocollo Fatture elettroniche in ingresso	ragioneria@pec.asst-mantova.it
A514405	Protocollo Fatture elettroniche in uscita	fatture@pec.asst-mantova.it
A3219D2	Sistemi Informativi Aziendali	sia@pec.asst-mantova.it

In linea con quanto indicato nelle Linee Guida AgID sulla formazione, gestione e conservazione dei documenti informatici, il documento illustra l'organizzazione, i soggetti coinvolti e i ruoli svolti dagli stessi, il modello di funzionamento, le procedure, la descrizione dei processi, la descrizione delle architetture e delle infrastrutture utilizzate, le misure di sicurezza adottate e ogni altra informazione utile alla gestione e alla verifica del funzionamento nel tempo, del sistema di conservazione.
In particolare, nel presente Manuale sono riportati:

- i dati dei soggetti che nel tempo hanno assunto la responsabilità del servizio di conservazione, descrivendo in modo puntuale, in caso di affidamento, i soggetti, le funzioni e gli ambiti oggetto dell'affidamento stesso;
- la struttura organizzativa comprensiva delle funzioni, delle responsabilità e degli obblighi dei diversi soggetti che intervengono nel processo di conservazione;
- la descrizione delle tipologie dei documenti informatici sottoponibili a conservazione, comprensiva dell'indicazione dei formati gestiti, dei metadati da associare alle diverse tipologie di documenti e delle eventuali eccezioni;
- la descrizione delle modalità di presa in carico di uno o più pacchetti di versamento, comprensiva della predisposizione del rapporto di versamento e della descrizione dei controlli effettuati su ciascuno specifico formato adottato;

copia informatica per consultazione

- la descrizione del processo di conservazione e del trattamento dei pacchetti di archiviazione;
- la modalità di svolgimento del processo di esibizione e di esportazione dal sistema di conservazione con la produzione del pacchetto di distribuzione;
- la descrizione del sistema di conservazione, comprensivo di tutte le componenti tecnologiche, fisiche e logiche, opportunamente documentate e delle procedure di gestione e di evoluzione delle medesime;
- la descrizione delle procedure di monitoraggio della funzionalità del sistema di conservazione e delle verifiche sull'integrità degli archivi con l'evidenza delle soluzioni adottate in caso di anomalie;
- la descrizione delle procedure per la produzione di duplicati o copie;
- i tempi entro i quali le diverse tipologie di documenti informatici devono essere oggetto di scarto/cancellazione;
- le modalità con cui viene richiesta la presenza di un pubblico ufficiale, indicando anche quali sono i casi per i quali è previsto il suo intervento;
- le normative in vigore nei luoghi dove sono conservati i documenti.

Il presente Manuale integra, per le parti specifiche di competenza dell'ASST, il Manuale di conservazione del conservatore, tale Manuale è allegato al presente documento.
Sono comunque individuati e pubblicati nel presente Manuale i tempi di versamento, le tipologie documentali trattate, i metadati, le modalità di trasmissione dei PdV e le tempistiche di selezione e scarto dei propri documenti informatici.
Al presente Manuale sono inoltre allegati i documenti riportati di seguito, che entrano più nel dettaglio dei diversi aspetti del Sistema di Conservazione e costituiscono parti integranti e sostanziali del Manuale di conservazione:

- **Specificità di contratto**: È il disciplinare tecnico che contiene le specifiche forniture del servizio di Conservazione per i produttori dei documenti. È parte integrante del contratto di servizi sottoscritto tra le parti e del Manuale di Conservazione, contenente i requisiti essenziali del Servizio, le relative specifiche tecnico-funzionali e procedurali per le varie fase del sevizio (attivazione, versamento, conservazione, post-produzione, distribuzione) oltre ai livelli di Servizio (SLA); tale documento è redatto in fase di analisi, prima del primo processo di Conservazione. Ogni variazione delle modalità di erogazione del Servizio, dovuta a richieste dell'ASST o a evoluzioni del Sistema di Conservazione, comporta la necessità di aggiornare le Specificità del Contratto.
- **Piano di sicurezza:** È il documento che analizza il contesto in cui l'ASST opera riportando i fattori interni ed esterni che lo influenzano ed evidenzia le principali criticità legate alla gestione della sicurezza delle informazioni gestite. In esso è descritto anche il dettaglio del processo di Gestione degli incidenti/malfunzionamenti.
- **Manuale del conservatore**
- **Titolario di classificazione e Piano di conservazione (Massimario di scarto)**
- **Atto di affidamento**

Come previsto dalle Linee Guida sulla formazione, gestione e conservazione dei documenti informatici, pubblicate da AgID il 9 settembre 2020, il Manuale è adottato con provvedimento formale e pubblicato sul sito istituzionale dell'ASST nell'area "Amministrazione trasparente" prevista dall'art. 9 del d.lgs. 33/2013.

Torna al sommario

copia informatica per consultazione

2 Terminologia (Glossario dei Termini e degli Acronimi)

Di seguito si riporta la tabella contenente in ordine alfabetico il Glossario dei termini e degli Acronimi ritenuti di particolare importanza.

Glossario dei termini	
Accesso	Operazione che consente a chi ne ha diritto di prendere visione dei documenti informatici conservati
Aggregazione documentale informatica	Raccolta di documenti informatici o di fascicoli informatici, riuniti per caratteristiche omogenee, in relazione alla natura e alla forma dei documenti o in relazione all'oggetto e alla materia o in relazione alle funzioni dell'ente
Archivio	Complesso organico di documenti, di fascicoli e di aggregazioni documentali di qualunque natura e formato, prodotti o comunque acquisiti da un soggetto produttore durante lo svolgimento dell'attività
Archivio informatico	Archivio intestato dal Soggetto Produttore al Titolare nel quale sono conservati costituito da documenti informatici, fascicoli informatici nonché aggregazioni documentali informatiche gestiti e conservati in ambiente informatico e di cui il medesimo è giuridicamente responsabile
Area organizzativa omogenea	Un insieme di funzioni e di strutture, individuate dalla amministrazione, che opera su tematiche omogenee e che presenta esigenze di gestione della documentazione in modo unitario e coordinato ai sensi dell'articolo 50, comma 4, del D.P.R. 28 dicembre 2000, n.445 e s.m.i.
Autenticità	Caratteristica di un documento informatico che garantisce di essere ciò che dichiara di essere, senza aver subito alterazioni o modifiche. L'autenticità può essere valutata analizzando l'identità del sottoscrittore e l'integrità del documento informatico
Base di dati	Collezione di dati registrati e correlati tra loro
Ciclo di gestione	Arco temporale di esistenza del documento informatico, del fascicolo informatico, dell'aggregazione documentale informatica o dell'archivio informatico dalla sua formazione alla sua eliminazione o conservazione nel tempo
Classificazione	Attività di organizzazione logica di tutti i documenti secondo uno schema articolato in voci individuate attraverso specifici metadati
Codice o CAD	Decreto legislativo 7 marzo 2005, n. 82 e successive modificazioni e integrazioni
Conservazione	Insieme delle attività finalizzate a definire ed attuare le politiche complessive del sistema di conservazione e a governarne la gestione in relazione al modello organizzativo adottato e descritto nel Manuale di conservazione
Destinatario	Identifica il soggetto/sistema al quale il documento informatico è indirizzato.
Documento analogico	La rappresentazione non informatica di atti, fatti o dati giuridicamente rilevanti.
Documento analogico originale	Documento analogico che può essere unico oppure non unico se, in questo secondo caso, sia possibile risalire al suo contenuto attraverso altre scritture o documenti di cui sia obbligatoria

copia informatica per consultazione

	la conservazione, anche se in possesso di terzi.
Documento informatico	La rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti.
Esibizione	Operazione che consente di visualizzare un documento conservato e di ottenerne copia
Evidenza informatica	Una sequenza di simboli binari (bit) che può essere elaborata da una procedura informatica.
Fascicolo informatico	Raccolta, individuata con identificativo univoco, di atti, documenti e dati informatici, da chiunque formati, del procedimento amministrativo.
Firma digitale	Un particolare tipo di firma elettronica avanzata basata su un certificato qualificato e su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici.
Firmatario delegato	Responsabile del servizio di conservazione o Persona formalmente delegata ad apporre la propria firma digitale sui Pacchetto di Archiviazione
Formato	Modalità di rappresentazione del documento informatico mediante codifica binaria; comunemente è identificato attraverso l'estensione del file e/o il tipo MIME.
Funzione di hash	Una funzione matematica che genera, a partire da una evidenza informatica, una sequenza di bit (impronta) in modo tale che risulti di fatto impossibile, a partire da questa, ricostruire l'evidenza informatica originaria e generare impronte uguali a partire da evidenze informatiche differenti.
Identificativo univoco	Sequenza di caratteri alfanumerici associata in modo univoco e persistente al documento informatico, al fascicolo informatico, all'aggregazione documentale informatica, in modo da consentirne l'individuazione.
Indice del Pacchetto di Versamento (IPdV)	Indice che contiene le informazioni relative al pacchetto di versamento in formato xml.
Impronta	La sequenza di simboli binari (bit) di lunghezza predefinita generata mediante l'applicazione alla prima di una opportuna funzione di hash.
Insieme minimo di metadati del documento informatico	Complesso dei metadati da associare al documento informatico per identificarne provenienza e natura e per garantirne la tenuta.
Integrità	Insieme delle caratteristiche di un documento informatico che ne dichiarano la qualità di essere completo ed inalterato.
Interoperabilità	Capacità di un sistema informatico di interagire con altri sistemi informatici analoghi sulla base di requisiti minimi condivisi.
Leggibilità	Insieme delle caratteristiche in base alle quali le informazioni contenute nei documenti

copia informatica per consultazione

	informatici sono fruibili durante l'intero ciclo di gestione dei documenti.
Log di sistema	Registrazione cronologica delle operazioni eseguite su di un sistema informatico per finalità di controllo e verifica degli accessi, oppure di registro e tracciatura dei cambiamenti che le transazioni introducono in una base di dati.
Memorizzazione	Processo di trasposizione su un qualsiasi idoneo supporto, attraverso un processo di elaborazione, di documenti analogici o informatici.
Marca temporale	Evidenza informatica che consente di rendere opponibile a terzi un riferimento temporale; la marca temporale prova l'esistenza in un certo momento di una determinata informazione, sotto forma di struttura dati firmata da una Time Stamping Authority.
Metadati	Insieme di dati associati a un documento informatico, o a un fascicolo informatico, o ad un'aggregazione documentale informatica per identificarlo e descriverne il contesto, il contenuto e la struttura, nonché per permetterne la gestione nel tempo nel sistema di conservazione.
Pacchetto di Archiviazione	Pacchetto informativo composto dalla trasformazione di uno o più pacchetti di versamento secondo le specifiche e le modalità riportate nel Manuale di conservazione.
Pacchetto di Distribuzione	Pacchetto informativo inviato dal sistema di conservazione all'utente in risposta ad una sua richiesta.
Pacchetto di invio documenti	Pacchetto informativo utilizzato per inviare i documenti fisici al sistema di conservazione a seguito dell'avvenuta accettazione di un pacchetto di versamento.
Pacchetto di versamento	Pacchetto informativo inviato dal produttore al sistema di conservazione secondo un formato predefinito e concordato descritto nel Manuale di conservazione;
Pacchetto informativo	Contenitore che racchiude uno o più oggetti da conservare (documenti informatici, documenti amministrativi informatici, documenti informatici rilevanti ai fini tributari, fascicoli informatici, aggregazioni documentali informatiche), oppure anche i soli metadati riferiti agli oggetti da conservare.
Piano di conservazione	Strumento, integrato con il sistema di classificazione per la definizione dei criteri di organizzazione dell'archivio, di selezione periodica e di conservazione ai sensi dell'articolo 68 del D.P.R. 28 dicembre 2000, n. 445 e s.m.i.
Presa in carico	Accettazione da parte del sistema di conservazione di un pacchetto di versamento in quanto conforme alle modalità previste dal Manuale di conservazione;
Processo di conservazione	Insieme delle attività finalizzate alla conservazione dei documenti informatici;
Produttore del pdv	E' il soggetto che in proprio o attraverso le persone fisiche da egli stesso incaricate produce il Pacchetto di versamento ed è responsabile del trasferimento del suo contenuto nel sistema di conservazione; nel caso della Pubblica Amministrazione è identificato nella figura del responsabile della gestione documentale.
Rapporto di versamento	Documento informatico che attesta l'avvenuta presa in carico da parte del sistema di conservazione dei pacchetti di versamento inviati dal produttore.
Responsabile della	Dirigente o funzionario, comunque in possesso di idonei requisiti professionali o di

copia informatica per consultazione

gestione documentale	professionalità tecnico archivistica, preposto al servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi.
Responsabile della sicurezza	Soggetto al quale compete la definizione delle soluzioni tecniche ed organizzative in attuazione delle disposizioni in materia di sicurezza.
Riferimento temporale	Informazione contenente la data e l'ora con riferimento al Tempo Universale Coordinato (UTC), della cui apposizione è responsabile il soggetto che forma il documento.
Scarto	Operazione con cui si eliminano, secondo quanto previsto dalla normativa vigente, i documenti ritenuti privi di valore amministrativo e di interesse culturale.
Scheda/e di conservazione	Elenco dei documenti informatici sottoposti a conservazione con il Contratto.
Sistema di classificazione	Strumento che permette di organizzare tutti i documenti secondo un ordinamento logico
Sistema di conservazione	Insieme di hardware, software, politiche, procedure, linee guida, regolamenti interni, infrastrutture fisiche e organizzative, volto ad assicurare la conservazione elettronica dei documenti per il periodo di tempo specificato nel Contratto. Detto sistema tratta i documenti informatici in conservazione in pacchetti informativi che si distinguono in pacchetti di versamento, pacchetti di archiviazione e pacchetti di distribuzione;
Sistema di gestione informatica dei documenti	Nell'ambito della pubblica amministrazione è il sistema di cui all'articolo 52 del D.P.R. 28 dicembre 2000, n. 445 e s.m.i..
Staticità	Caratteristica che indica l'assenza di tutti gli elementi dinamici, quali macroistruzioni, riferimenti esterni o codici eseguibili, e l'assenza delle informazioni di ausilio alla redazione, quali annotazioni, revisioni, segnalibri, gestite dal prodotto software utilizzato per la redazione;
Testo unico	Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, e successive modificazioni.
Utente	Persona, ente o sistema che interagisce con i servizi di un sistema di gestione informatica dei documenti e/o di un sistema per la conservazione dei documenti informatici, al fine di fruire delle informazioni di interesse.
Validazione temporale	Il risultato della procedura informatica con cui si attribuiscono, ad uno o più documenti informatici, una data ed un orario opponibili ai terzi
Versamento agli archivi di stato	Operazione con cui il responsabile della conservazione di un'amministrazione statale effettua l'invio agli Archivi di Stato o all'Archivio Centrale dello Stato della documentazione destinata ad essere ivi conservata ai sensi della normativa vigente in materia di beni culturali.

Glossario degli Acronimi	
AgID	Agenzia per l'Italia Digitale
CAD	Decreto legislativo 7 marzo 2005, n. 82, e successive modificazioni - "Codice

copia informatica per consultazione

	dell'amministrazione digitale”;
CA - Certification Authority	Soggetto autorizzato dall’Agenzia per l’Italia Digitale che garantisce l’identità dei soggetti che utilizzano la firma digitale;
C.M.	Circolare Ministeriale;
D.LGS.	Decreto Legislativo;
D.M.	Decreto Ministeriale;
D.P.C.M.	Decreto del Presidente del Consiglio dei Ministri;
D.P.R.	Decreto Presidente della Repubblica;
ETSI	European Telecommunications Standards Institute
FTP server	programma che permette di accettare connessioni in entrata e di comunicare con un Client attraverso il protocollo FTP
HTTP (Hypertext Transfer Protocol)	Protocollo di trasmissione, che permette lo scambio di file (testi, immagini grafiche, suoni, video e altri documenti multimediali) su World Wide Web;
HTTPS (Secure Hypertext Transfer Protocol)	Protocollo di trasmissione, sviluppato da Netscape Communications Corporation, per la cifratura e decifratura dei dati trasmessi durante la consultazione di siti e pagine Internet. Corrisponde ad un’estensione del protocollo Internet standard HTTP (Hypertext Transfer Protocol), attraverso il protocollo SSL;
ICT - Information and Communication Technology	Tecnologia dell'Informazione e delle Telecomunicazioni. Il dipartimento che gestisce i sistemi informatici e telematici;
ISO – International Organization for Standardization	Organizzazione internazionale per la standardizzazione, costituita da organismi nazionali provenienti da più di 75 paesi. Ha stabilito numerosi standard nell’area dei sistemi informativi. L’ANSI (American National Standards Institute) è uno dei principali organismi appartenenti all’ISO;
MEF	Ministero dell'Economia e delle Finanze;
OAIS	ISO 14721:2012; Space Data information transfer system
PdV	Pacchetto di Versamento
PdA	Pacchetto di Archiviazione
PdD	Pacchetto di Distribuzione
PU	Pubblico Ufficiale
PIN – Personal Identification Number	Codice di sicurezza riservato che permette l’identificazione del soggetto abbinato ad un dispositivo fisico. Permette ad esempio l’attivazione delle funzioni del dispositivo di firma;
SSL – Secure Socket	Protocollo standard per la gestione di transazioni sicure su Internet, basato sull’utilizzo di

copia informatica per consultazione

Layer	algoritmi crittografici a chiave pubblica;
TUDA	DPR 28 dicembre 2000, n. 445, e successive modificazioni - “Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa”;
URL – Uniform Resource Locator	Sistema standard di nomenclatura specificante un sito, dominio o altro oggetto (file, gruppo di discussione, ecc.) su Internet. La prima parte dell’URL (http, ftp, file, telnet, news) specifica il protocollo di accesso all’oggetto;
XML	Extensible Markup language;

Torna al sommario

copia informatica per consultazione

3 Normativa e Standard di riferimento

3.1 Normativa di riferimento

Alla data odierna l'elenco dei principali riferimenti normativi italiani in materia, ordinati secondo il criterio della gerarchia delle fonti, è costituito da:

- **Codice Civile** [Libro Quinto Del lavoro, Titolo II Del lavoro nell'impresa, Capo III Delle imprese commerciali e delle altre imprese soggette a registrazione, Sezione III Disposizioni particolari per le imprese commerciali, Paragrafo 2 Delle scritture contabili], articolo 2215 bis - Documentazione informatica.
- **Legge del 7 agosto 1990, n. 241 e s.m.i.** – Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi.
- **Decreto del Presidente della Repubblica del 28 dicembre 2000, n. 445 e s.m.i.** – Testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa.
- **Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 (GDPR)** relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).
- **Decreto Legislativo 10 agosto 2018, n. 101** che ha dettato disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016.
- **Decreto Legislativo del 30 giugno 2003, n. 196 e s.m.i.** – Codice in materia di protezione dei dati personali.
- **Decreto Legislativo del 22 gennaio 2004, n. 42 e s.m.i.** – Codice dei Beni Culturali e del Paesaggio.
- **Decreto Legislativo del 7 marzo 2005 n. 82 e s.m.i –** Codice dell'amministrazione digitale (CAD).
- **Decreto del Presidente del Consiglio dei Ministri del 22 febbraio 2013 –** Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma3, lettera b), 35, comma 2, 36, comma 2, e 71.[20] Manuale di conservazione
- **Decreto del Ministero dell'Economia e delle Finanze del 17 giugno 2014 -** Modalità di assolvimento degli obblighi fiscali relativi ai documenti informatici ed alla loro riproduzione su diversi tipi di supporto - articolo 21, comma 5, del decreto legislativo n. 82/2005.
- **Circolare AgID del 9 aprile 2018, n. 2 –** Criteri per la qualificazione dei Cloud Service Provider per la PA
- **Circolare AgID del 9 aprile 2018, n. 3 –** Criteri per la qualificazione di servizi SaaS per il Cloud della PA
- **Linee Guida sulla formazione, gestione e conservazione dei documenti informatici, pubblicate da AgID il 9 settembre 2020** e relativi allegati
- **Circolare AgID n. 2/2021 del 29 marzo 2021**, recante integrazioni alla circolare AgID n. 2 del 9 aprile 2018 «Criteri per la qualificazione dei Cloud Service Provider per la PA» e alla circolare AgID n. 3 del 9 aprile 2018 «Criteri per la qualificazione di servizi SaaS per il Cloud della PA».

Torna al sommario

copia informatica per consultazione

3.2 Standard di riferimento

Di seguito sono riportati i principali standard e specifiche tecniche di riferimento nell'ambito conservazione di documenti informatici e documenti amministrativi informatici.
Dove non sono indicate una versione e/o una data specifica, si intende fare riferimento alla più recente versione disponibile del documento citato:

- **UNI 11386** - Standard SInCRO - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali.
- **ISO 14721** - OAIS (Open Archival Information System), Sistema informativo aperto per l'archiviazione.
- **ISO 15836** - Information and documentation - The Dublin Core metadata element set, Sistema di metadata del Dublin Core
- ISO/TR 18492 - Long-term preservation of electronic document-based information.
- **ISO 20652** - Space data and information transfer systems - Producer-Archive interface - Methodology abstract standard.
- **ISO 20104** - Space data and information transfer systems — Producer-Archive Interface Specification (PAIS).
- **ISO/CD TR 26102** - Requirements for long-term preservation of electronic records.
- **SIARD** Software Independent Archiving of Relational Databases 2.0
- **Ministère de la culture et de la communication,** Service interministériel des Archives de France, Standard d'échange de donnéès pour l'archivage. Transfert – Communication – Élimination – Restitution - Modification, ver. 2.1, 2018
- **METS** - Metadata Encoding and Transmission Standard
- **PREMIS** – PREservation Metadata: Implementation Strategies.
- **EAD (3)/ISAD (G)**
- **EAC (CPF)/ISAAR (CPF)/NIERA (CPF)**
- **SCONS2/EAG/ISDIAH**
- **ISO 16363** - Space data and information transfer systems -- Audit and certification of trustworthy digital repositories
- **ISO 16919** - Space data and information trans:fer systems -- Requirements for bodies providing audit and certification of candidate trustworthy digital repositories
- **ISO 17068** - Information and documentation -- Trusted third party repository for digital records
- **ISO/IEC 27001** - Information technology - Security techniques - Information security management systems – Requirements, Requisiti di un ISMS (Information Security Management System);
- **ISO/IEC 27017** - Information technology -- Security techniques -- Code of practice for information security controls based on ISO/IEC 27002 for cloud services;
- **ISO/IEC 27018** - Information technology -- Security techniques -- Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors;
- **ETSI TS 101 533-1 V1.2.1** - Technical Specification, Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part 1: Requirements for Implementation and Management, Requisiti per realizzare e gestire sistemi sicuri e affidabili per la conservazione elettronica delle informazioni;

copia informatica per consultazione

- **ETSI TR 101 533-2 V1.2.1** - Technical Report, Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part 2: Guidelines for Assessors, Linee guida per valutare sistemi sicuri e affidabili per la conservazione elettronica delle informazioni.

Torna al sommario

copia informatica per consultazione

4 Ruoli e Responsabilità

In linea con quanto indicato dalle Linee Guida sulla formazione, gestione e conservazione dei documenti informatici, pubblicate da AgID, l'ASST individua i seguenti ruoli principali nel processo di conservazione:

Titolare dell'oggetto della conservazione: struttura organizzativa che ha la titolarità dei documenti da conservare.

Produttore dei PdV: assicura la trasmissione del pacchetto di versamento al sistema di conservazione, secondo le modalità operative definite nel manuale; provvede a generare e trasmettere al sistema di conservazione i pacchetti di versamento nelle modalità e con i formati concordati con il conservatore e nel manuale; provvede a verificare il buon esito della operazione di trasferimento al sistema di conservazione tramite la presa visione del rapporto di versamento prodotto dal sistema di conservazione stesso.

Utente abilitato: può richiedere al sistema di conservazione l'accesso ai documenti per acquisire le informazioni di interesse nei limiti previsti dalla legge e nelle modalità previste dal manuale.

Responsabile della conservazione: Il responsabile della conservazione opera secondo quanto previsto dall'art. 44, comma 1-quater, del CAD (L'art. 44, comma 1-quater, del CAD prevede che: "Il responsabile della conservazione, che opera d'intesa con il responsabile del trattamento dei dati personali, con il responsabile della sicurezza e con il responsabile dei sistemi informativi, può affidare, ai sensi dell'articolo 34, comma 1-bis, lettera b), la conservazione dei documenti informatici ad altri soggetti, pubblici o privati, che offrono idonee garanzie organizzative, e tecnologiche e di protezione dei dati personali. Il responsabile della conservazione della pubblica amministrazione, che opera d'intesa, oltre che con i responsabili di cui al comma 1-bis, anche con il responsabile della gestione documentale, effettua la conservazione dei documenti informatici secondo quanto previsto all'articolo 34, comma 1-bis".). Il responsabile della conservazione definisce e attua le politiche complessive del sistema di conservazione e ne governa la gestione con piena responsabilità ed autonomia.

In particolare, il responsabile della conservazione dell'ASST si occupa delle seguenti attività:

- definisce le politiche di conservazione, in conformità alla normativa vigente e tenuto conto degli standard internazionali;
- sottoscrive il rapporto di versamento, secondo le modalità previste dal manuale;
- assicura la presenza di un pubblico ufficiale, nei casi in cui sia richiesto il suo intervento, garantendo allo stesso l'assistenza e le risorse necessarie per l'espletamento delle attività al medesimo attribuite;
- provvede per le amministrazioni statali centrali e periferiche a versare i documenti informatici, le aggregazioni informatiche e gli archivi informatici, nonché gli strumenti che ne garantiscono la consultazione, rispettivamente all'Archivio centrale dello Stato e agli archivi di Stato territorialmente competenti, secondo le tempistiche fissate dall'art. 41, comma 1, del Codice dei beni culturali;
- predispone il manuale di conservazione e ne cura l'aggiornamento periodico in presenza di cambiamenti normativi, organizzativi, procedurali o tecnologici rilevanti.

Il Responsabile della conservazione ha delegato al responsabile del servizio di conservazione del conservatore le seguenti funzioni e attività specificate nell'Atto di Affidamento:

- definisce le caratteristiche e i requisiti del sistema di conservazione in funzione della tipologia dei documenti da conservare individuati nel Capitolato tecnico alla

copia informatica per consultazione

Gara 06/2017/LI, della quale tiene evidenza, in conformità alla normativa vigente, al Manuale di Conservazione ed alle Specificità di Contratto, la definizione degli aspetti tecnico-operativi nonché le modalità di trasferimento da parte dell'ASST dei documenti informatici versati in conservazione;

- gestisce il processo di conservazione garantendo nel tempo la conformità alla normativa vigente;
- genera il rapporto di versamento, secondo le modalità previste dal Manuale di Conservazione del conservatore;
- genera e sottoscrive il pacchetto di distribuzione con Firma Digitale nei casi previsti dal Manuale di Conservazione del conservatore;
- effettua il monitoraggio della corretta funzionalità del sistema di conservazione;
- assicura la verifica periodica, con cadenza non superiore ai cinque anni, dell'integrità degli archivi e della leggibilità degli stessi;
- adotta misure per rilevare tempestivamente l'eventuale degrado dei sistemi di memorizzazione e delle registrazioni, al fine di garantire la conservazione e l'accesso ai documenti informatici, e, ove necessario, per ripristinare la corretta funzionalità; il conservatore adotta analoghe misure con riguardo all'obsolescenza dei formati;
- provvede alla duplicazione o copia dei documenti informatici in relazione all'evolversi del contesto tecnologico, secondo quanto previsto dal Manuale di Conservazione del conservatore;
- adotta le misure necessarie per la sicurezza fisica e logica del sistema di conservazione come previsto dalle Linee Guida sulla formazione, gestione e conservazione dei documenti informatici;
- richiede la presenza di un pubblico ufficiale, nei casi in cui sia richiesto il suo intervento, garantendo allo stesso l'assistenza per l'espletamento delle attività al medesimo attribuite;
- assicura agli organismi competenti previsti dalle norme vigenti l'assistenza e le risorse necessarie per l'espletamento delle attività di verifica e di vigilanza;
- in presenza di cambiamenti normativi, organizzativi, procedurali o tecnologici rilevanti, cura l'aggiornamento periodico del Manuale di Conservazione del conservatore.

Rimane in ogni caso inteso che la responsabilità giuridica generale sui processi di conservazione, non essendo delegabile, rimane in capo al responsabile della conservazione dell'ASST, chiamato altresì a svolgere le necessarie attività di verifica e controllo in ossequio alle norme vigenti sui servizi affidati in outsourcing dalle PA.

Conservatore: persona fisica o la persona giuridica (il conservatore può anche essere un soggetto esterno alla PA) che si occupa della conservazione.

La tabella successiva riassume i ruoli previsti.

Ruolo	**Dettaglio**
Titolare dell'oggetto della conservazione	Azienda Socio-Sanitaria Territoriale Mantova
Soggetto Produttore del PdV	Per il soggetto produttore del PdV si fa riferimento al decreto del

copia informatica per consultazione

	direttore generale n.1496 del 28/12/2021
Utente abilitato	Gli utenti abilitati sono indicati all'interno delle specificità di contratto allegate al presente documento.
Responsabile della conservazione	Per il Responsabile della Conservazione si fa riferimento al decreto del direttore generale n. 549 del 23/06/2022
Conservatore (Responsabile del servizio di conservazione)	Per il conservatore si fa riferimento all'Atto di Affidamento allegato al presente documento.

Torna al sommario

4.1 Profili professionali responsabili del Conservatore

Il processo di conservazione prevede inoltre le seguenti figure responsabili:

- Responsabile del servizio di conservazione;
- Responsabile della funzione archivistica di conservazione;
- Responsabile del trattamento dei dati personali, ora Responsabile della protezione dei dati personali (DPO)
- Responsabile della sicurezza dei sistemi per la conservazione;
- Responsabile dei sistemi informativi per la conservazione;
- Responsabile dello sviluppo e della manutenzione del sistema di conservazione

Per le attività associate a ciascuna delle figure elencate fare riferimento alla tabella sotto.
Per i nominativi e relativi dati dei soggetti che nel tempo hanno assunto particolari funzioni e responsabilità con riferimento al sistema di conservazione, si rimanda al Manuale di conservazione del conservatore.

Ruoli	**Attività di competenza**
Responsabile del servizio di conservazione	Le attività affidate dal Responsabile della conservazione con l'Atto di Affidamento e indicate sopra.
Responsabile Sicurezza dei sistemi per la conservazione	Rispetto e monitoraggio dei requisiti di sicurezza del sistema di conservazione stabiliti dagli standard, dalle normative e dalle politiche e procedure interne di sicurezza; segnalazione delle eventuali difformità al Responsabile del servizio di conservazione e individuazione e pianificazione delle necessarie azioni correttive.
Responsabile funzione archivistica di conservazione	Definizione e gestione del processo di conservazione, incluse le modalità di trasferimento da parte del produttore, di acquisizione, verifica di integrità e descrizione archivistica dei documenti e delle aggregazioni documentali trasferiti, di esibizione, di accesso e fruizione del patrimonio documentario e informativo conservato; definizione del set di metadati di conservazione dei documenti e dei fascicoli informatici; monitoraggio del processo di conservazione e analisi archivistica per lo sviluppo di nuove funzionalità del sistema di conservazione; collaborazione col Produttore ai fini del trasferimento in conservazione, della selezione e della gestione dei rapporti con il Ministero dei beni e delle attività culturali per quanto di competenza.
Responsabile trattamento dati personali	Garanzia del rispetto delle vigenti disposizioni in materia di trattamento dei dati personali; garanzia che il trattamento dei dati affidati dal Produttore avverrà nel rispetto delle istruzioni impartite dal titolare del trattamento dei

copia informatica per consultazione

	dati personali, con garanzia di sicurezza e di riservatezza. In particolare tenuto a: a) informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal Regolamento UE 2016/679 nonché da altre disposizioni relative alla protezione dei dati; b) sorvegliare l'osservanza del Regolamento UE 2016/679, di altre disposizioni relative alla protezione dei dati nonché delle politiche del titolare del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo; c) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35 del Regolamento UE 2016/679; d) cooperare con l'autorità di controllo; e e) fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36 del Regolamento UE 2016/679, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione. Nell'eseguire i propri compiti il responsabile della protezione dei dati considera debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo.
Responsabile sistemi informativi per la conservazione	Gestione dell'esercizio delle componenti hardware e software del sistema di conservazione; monitoraggio del mantenimento dei livelli di servizio (SLA) concordati con il fornitore; segnalazione delle eventuali difformità degli SLA al Responsabile del servizio di conservazione e individuazione e pianificazione delle necessarie azioni correttive; pianificazione dello sviluppo delle infrastrutture tecnologiche del sistema di conservazione; controllo e verifica dei livelli di servizio erogati da terzi con segnalazione delle eventuali difformità al Responsabile del servizio di conservazione.
Responsabile sviluppo e manutenzione del sistema di conservazione	Coordinamento dello sviluppo e manutenzione delle componenti hardware e software del sistema di conservazione; pianificazione e monitoraggio dei progetti di sviluppo del sistema di conservazione; monitoraggio degli SLA relativi alla manutenzione del sistema di conservazione; interfaccia col Produttore relativamente alle modalità di trasferimento dei documenti e fascicoli informatici in merito ai formati elettronici da utilizzare, all'evoluzione tecnologica hardware e software, alle eventuali migrazioni verso nuove piattaforme tecnologiche; gestione dello sviluppo di siti web e portali connessi al servizio di conservazione.

Torna al sommario

5 Struttura organizzativa per il Servizio di Conservazione

In questo capitolo sono indicate le strutture organizzative coinvolte nel servizio di conservazione, comprese le responsabilità che intervengono nelle principali funzioni che riguardano il servizio di conservazione.

5.1 Strutture Organizzative

Il Produttore è il titolare delle unità documentarie informatiche poste in conservazione e, attraverso il proprio Responsabile della conservazione, definisce e attua le politiche complessive del Sistema di conservazione governandone la gestione con piena responsabilità ed autonomia, in relazione al modello organizzativo adottato affida al Conservatore la gestione del servizio di conservazione secondo quanto previsto dalla normativa in materia.

copia informatica per consultazione

La scelta adottata dall'ASST è quella del modello in outsourcing per la fornitura del servizio di conservazione tramite adesione a gara regionale 6/2017/LI.
Il Sistema di conservazione garantisce l'autenticità, l'integrità, l'affidabilità, la leggibilità e la reperibilità degli oggetti conservati dal momento della loro presa in carico dal Produttore, fino all'eventuale scarto indipendentemente dall'evolversi del contesto tecnologico e organizzativo.
Il ruolo del conservatore come Responsabile del sistema di conservazione è definito nel testo del contratto esecutivo sottoscritto fra l'ASST e il conservatore in cui si dichiara che, nel rispetto delle norme di legge, è individuato come Responsabile del sistema di conservazione degli oggetti informatici trasferiti in base al contratto stesso.
In quanto soggetto responsabile, il conservatore si occupa delle politiche complessive del Sistema di conservazione e ne determina l'ambito di sviluppo e le competenze. A tal fine provvede alla pianificazione strategica, alla ricerca dei finanziamenti, alla revisione periodica dei risultati conseguiti e ad ogni altra attività gestionale mirata a coordinare lo sviluppo del Sistema.
Nella Tabella successiva sono dettagliate le funzioni e le responsabilità in capo a ciascun soggetto coinvolto nel processo di conservazione.

Funzioni/Responsabilità del processo di Conservazione	**Responsabile della Conservazione**	**Responsabile della Gestione Documentale**	**Conservatore**
Creazione del Pacchetto di Versamento (PdV)		X	
Trasferimento del PdV al sistema di conservazione		X	
Acquisizione e presa in carico del PdV			X
Verifiche sul PdV			X
Accettazione del PdV e generazione del Rapporto di Versamento (RdV) di presa in carico			X
Sottoscrizione del RdV con FD, FEQ o FEA			X
Rifiuto del PdV e comunicazione delle anomalie			X
Presa visione del RdV		X	
Presa visione delle anomalie a seguito del rifiuto del PdV		X	

copia informatica per consultazione

Preparazione, gestione e Sottoscrizione con FD, FEQ o FEA del Pacchetto di Archiviazione			X
Richiesta del Pacchetto di Distribuzione ai fini dell'esibizione	X		
Preparazione, gestione e Sottoscrizione con FD, FEQ o FEA del Pacchetto di Distribuzione ai fini dell'esibizione			X
Produzione di duplicati e copie informatiche ed eventuale intervento del pubblico ufficiale nei casi previsti			X
Predisposizione elenco pacchetti di archiviazione da scartare			X
Richiesta alla soprintendenza di autorizzazione allo scarto	X		
Scarto dei pacchetti di archiviazione			X
Predisposizione di misure a garanzia dell'interoperabilità e trasferibilità ad altri conservatori			X
Audit Log			X
Verifica a campione dei PDV conservati	X		

Torna al sommario

6 Oggetti sottoposti a conservazione

In questo capitolo sono descritte le tipologie degli oggetti e dei pacchetti in essi contenuti sottoposti a conservazione.

6.1 Oggetti conservati

Nel paragrafo sono elencate e descritte le tipologie di documenti sottoposti a conservazione e le relative politiche di conservazione. Per ciascuna tipologia sono elencati e descritti i relativi formati (comprensivi della relativa versione) dei file utilizzati.
Si rimanda agli allegati "Specificità del contratto" per i metadati associati a ciascuna tipologia di documento e per le modalità adottate per garantire la leggibilità dei formati gestiti, i

copia informatica per consultazione

visualizzatori relativi ai formati gestiti e le modalità con cui il sistema di conservazione ne garantisce la leggibilità nel tempo.
Le tipologie di documento oggetto di conservazione per il servizio erogato dal conservatore per l'ASST sono:

- **Documenti amministrativi informatici:** sono la "rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti" come definito dal Codice dell'Amministrazione Digitale costituenti atti amministrativi con rilevanza interna al procedimento amministrativo;
- **Documenti clinici**: possono contenere informazioni su osservazioni cliniche dirette, quali rivelazioni di anamnesi, segni vitali o sintomi, osservazioni indirette, derivanti, ad esempio da diagnostica strumentale, esami di laboratorio o rappresentazione iconografica di resoconti radiologici, oppure opinioni mediche quali valutazioni di osservazioni cliniche, consulti e consulenze, obiettivi da raggiungere o piani diagnostico terapeutici, azioni di natura clinico-sanitaria atte a generare osservazioni cliniche ed opinioni mediche.

La Tabella successiva riassume le classi documentali gestite dal conservatore.

Classi documentali	**Tipologia**
Fatture PA Attive	Documento Informatico
Fatture PA Passive	Documento Informatico
Notifiche SDI Fatture PA Attive	Documento Informatico
Notifiche SDI Fatture PA Passive	Documento Informatico
Delibere	Documento Informatico
Determine	Documento Informatico
Repertori	Documento Informatico
Documenti Protocollati	Documento Informatico
Cedolini, Cartellini e CU Risorse umane	Documento Informatico
LOG di trasmissione di Cedolini e CU Risorse umane	Documento Informatico
Ricevute Telematiche RT	Documento Informatico
Richiesta Pagamento Telematico RPT	Documento Informatico
SINTEL 5/10/20 anni e illimitati	Documento Informatico
Ricette Dematerializzate Erogate	Documento Clinico
Ricette Dematerializzate Erogate Annullate	Documento Clinico
Ricette Dematerializzate Prescritte	Documento Clinico
Ricette Dematerializzate Prescritte Annullate	Documento Clinico
Lettere di Dimissione	Documento Clinico
Referti Ambulatoriali	Documento Clinico
Referti di Documenti Clinici Generici	Documento Clinico
Referti Anatomia Patologica	Documento Clinico
Referti di Laboratorio	Documento Clinico
Referti di Radiologia	Documento Clinico
Verbali di Pronto Soccorso	Documento Clinico
Verbali Operatori	Documento Clinico
DICOM	Documento Clinico

Per ciascuna classe documentale sono riportati di seguito i dettagli.

Torna al sommario

copia informatica per consultazione

copia informatica per consultazione

6.1.1 Fatture PA Attive

Classe documentale	Fatture PA Attive
Livello 1	DAE2
Descrizione	Fatture Attive verso la PA
Sistema Alimentante	Hub Regionale
Fornitore del sistema alimentante	Aria
Formato	XML, P7M
Frequenza di versamento	Annuale
Tempo entro il quale trasferire i documenti al sistema di conservazione	Entro l'anno successivo la data di competenza
Tempo di scarto	10 anni
Codice prontuario di scarto	5. Risorse finanziarie e gestione contabile .03 Gestione entrate-uscite

Torna al sommario

6.1.2 Fatture PA Passive

Classe documentale	Fatture PA Passive
Livello 1	DAE2
Descrizione	Fatture Passive da PA e fornitori
Sistema Alimentante	Hub Regionale
Fornitore del sistema alimentante	Aria
Formato	XML, P7M
Frequenza di versamento	Annuale
Tempo entro il quale trasferire i documenti al sistema di conservazione	Entro l'anno successivo la data di competenza
Tempo di scarto	10 anni
Codice prontuario di scarto	5. Risorse finanziarie e gestione contabile .03 Gestione entrate-uscite

Torna al sommario

6.1.3 Notifiche SDI Fatture PA Attive

Classe documentale	Notifiche SDI Fatture PA Attive

copia informatica per consultazione

Livello 1	DAE2
Descrizione	Notifiche SDI relative a Fatture Attive verso la PA
Sistema Alimentante	Hub Regionale
Fornitore del sistema alimentante	Aria
Formato	XML, P7M
Frequenza di versamento	Annuale
Tempo entro il quale trasferire i documenti al sistema di conservazione	Entro due anni successivi la data di competenza
Tempo di scarto	10 anni
Codice prontuario di scarto	5. Risorse finanziarie e gestione contabile .03 Gestione entrate-uscite

Torna al sommario

6.1.4 Notifiche SDI Fatture PA Passive

Classe documentale	Notifiche SDI Fatture PA Passive
Livello 1	DAE2
Descrizione	Notifiche SDI relative a Fatture Passive da PA e fornitori
Sistema Alimentante	Hub Regionale
Fornitore del sistema alimentante	Aria
Formato	XML, P7M
Frequenza di versamento	Annuale
Tempo entro il quale trasferire i documenti al sistema di conservazione	Entro due anni successivi la data di competenza
Tempo di scarto	10 anni
Codice prontuario di scarto	5. Risorse finanziarie e gestione contabile .03 Gestione entrate-uscite

Torna al sommario

6.1.5 Delibere

Classe documentale	Delibere
Livello 1	DAE
Descrizione	Atti di direzione - Delibere

copia informatica per consultazione

Sistema Alimentante	Sfera
Fornitore del sistema alimentante	Data Processing
Formato	PDF, P7M, M7M, TSD
Frequenza di versamento	Giornaliera
Tempo entro il quale trasferire i documenti al sistema di conservazione	l termine del periodo di pubblicazione sull'albo pretorio (15gg)
Tempo di scarto	Illimitato
Codice prontuario di scarto	.01

Torna al sommario

6.1.6 Determine

Classe documentale	Determine
Livello 1	DAE
Descrizione	Atti di direzione - Determine
Sistema Alimentante	Sfera
Fornitore del sistema alimentante	Data Processing
Formato	PDF, P7M, M7M, TSD
Frequenza di versamento	Giornaliera
Tempo entro il quale trasferire i documenti al sistema di conservazione	l termine del periodo di pubblicazione sull'albo pretorio (15gg)
Tempo di scarto	Illimitato
Codice prontuario di scarto	.01

Torna al sommario

6.1.7 Repertori

Classe documentale	Repertori
Livello 1	DAE
Descrizione	Registri giornalieri di protocollo
Sistema Alimentante	Prisma

copia informatica per consultazione

Fornitore del sistema alimentante	Data Processing
Formato	PDF, PDF/A, P7M
Frequenza di versamento	Giornaliera
Tempo entro il quale trasferire i documenti al sistema di conservazione	Entro 3 giorni
Tempo di scarto	Illimitato
Codice prontuario di scarto	.01

Torna al sommario

6.1.8 Documenti Protocollati

Classe documentale	Documenti Protocollati
Livello 1	DAE
Descrizione	Documenti protocollati
Sistema Alimentante	Prisma
Fornitore del sistema alimentante	Data Processing
Formato	BMP, CSV, dat, Word DOC, Word DOCX, EML, emz, GIF, HTM, HTML, jpe, JPEG, JPG, LDIF, LOG, msg, M7M, ODB, ODG, ODP, ODS, ODT, OTT, PDF, PNG, PPS, PPSX, PPT, PPTX, PROPERTIES, P7M, P7S, rar, RTF, TIF, TIFF, TSD, TSR, TXT, WFM, XLS, xlsb, XLSX, XML, ZIP, 7z
Frequenza di versamento	Dopo 30 giorni da protocollazione
Tempo entro il quale trasferire i documenti al sistema di conservazione	30gg.
Tempo di scarto	Illimitato
Codice prontuario di scarto	.01

Torna al sommario

6.1.9 Cedolini, Cartellini e CU Risorse umane

Classe documentale	Cedolini, Cartellini e CU Risorse umane
Livello 1	DAE
Descrizione	Cedolini, Cartellini, CU Risorse umane
Sistema Alimentante	Sigma / GPI
Fornitore del sistema alimentante	Aria

copia informatica per consultazione

Formato	PDF
Frequenza di versamento	Mensile
Tempo entro il quale trasferire i documenti al sistema di conservazione	30gg. per i cedolini 120gg per i cartellini Annuale per i CU
Tempo di scarto	10 anni
Codice prontuario di scarto	1.4.06 TITOLO 1 – Area Amministrativa 4. Risorse Umane .06 Retribuzioni e compensi

Torna al sommario

6.1.10 Ricevute telematiche RT

Classe documentale	RT
Livello 1	DAE
Descrizione	Ricevute Telematiche
Sistema Alimentante	MyPay
Fornitore del sistema alimentante	Aria
Formato	xml, p7m, pdf
Frequenza di versamento	Ogni tre ore
Tempo entro il quale trasferire i documenti al sistema di conservazione	in giornata (al netto dei documenti pregressi)
Tempo di scarto	10 anni
Codice prontuario di scarto	1.5.03 TITOLO 1 - Area Amministrativa 5. Risorse finanziarie e gestione contabile .03 Gestione entrate-uscite

Torna al sommario

6.1.11 Richiesta di pagamento telematico - RPT

Classe documentale	RPT
Livello 1	DAE
Descrizione	Richiesta di Pagamento Telematico
Sistema Alimentante	MyPay
Fornitore del sistema alimentante	Aria

copia informatica per consultazione

Formato	xml, p7m, pdf
Frequenza di versamento	Ogni tre ore
Tempo entro il quale trasferire i documenti al sistema di conservazione	in giornata (al netto dei documenti pregressi)
Tempo di scarto	10 anni
Codice prontuario di scarto	1.5.03 TITOLO 1 - Area Amministrativa 5. Risorse finanziarie e gestione contabile .03 Gestione entrate-uscite

Torna al sommario

6.1.12 SINTEL 5/10/20 anni e illimitati

Classe documentale	SINTEL 5/10/20 anni e illimitati
Livello 1	DAE
Descrizione	Documentazione presente nella piattaforma SINTEL: 1. Documentazione di gara caricata dagli utenti della Stazione Appaltante 2. Tutti i report generati in automatico da Sintel (di proposta di aggiudicazione, di aggiudicazione, verbale della commissione,..) o su richiesta della SA (report intermedi) (per le procedure multilotto sia a livello multilotto che a livello di singolo lotto) 3. Verbali della commissione giudicatrice caricati durante il percorso di valutazione delle offerte 4. Documentazione relativa alle offerte "valide" pervenute nell'ambito della procedura (tutti gli allegati ed il documento di offerta che costituiscono ogni singola offerta sottomessa dal singolo operatore economico) (per le procedure multilotto sia a livello multilotto che a livello di singolo lotto) 5. Documentazione relativa alle offerte "non valide" (in stato "sostituita", "offerta ritirata",..) cifrate. 6. Documentazione relativa alle "Comunicazioni di procedura" effettuate attraverso la funzionalità "Comunicazioni di procedura" (1 documento per ciascuna coppia mittente / destinatario) con riferimento ad eventuali allegati1

copia informatica per consultazione

	7. Allegati alle comunicazioni di procedura 8. Documento "report messaggi PEC" (relativo a tutti i messaggi PEC che sono stati inviati da Sintel nell'ambito della procedura). 9. Eventuale file opzionale "password.txt.zip" 10. Documento di indice del fascicolo in formato XML
Sistema Alimentante	Sintel
Fornitore del sistema alimentante	Aria
Formato	.pdf, .p7m,.m7m (Documento di offerta) Scelto dal fornitore (allegati)
Frequenza di versamento	Al momento della creazione.
Tempo entro il quale trasferire i documenti al sistema di conservazione	Al momento della creazione
Tempo di scarto	5/10/20 o illimitato
Codice prontuario di scarto	1.6.03 Titolo 1 – Area Amministrativa 6. Gestione e organizzazione del patrimonio. .03 Acquisizione e gestione di beni mobili / generi di consumo e di servizi

6.1.13 Ricette Dematerializzate Erogate

Classe documentale	Ricette Dematerializzate Erogate
Livello 1	RD
Descrizione	Ricette elettroniche dematerializzate erogate
Sistema Alimentante	Hub Regionale
Fornitore del sistema alimentante	Aria
Formato	ZIP, XML
Frequenza di versamento	Al momento della creazione del documento
Tempo entro il quale trasferire i documenti al sistema di conservazione	Al momento della creazione del documento
Tempo di scarto	10 anni
Codice prontuario di scarto	3.4.01 TITOLO 3 - Area Ospedaliera 4. Assistenza ambulatoriale .01 Prestazioni ambulatoriali- Prescrizione – proposta - ricetta per richieste di prestazioni sanitarie

copia informatica per consultazione

Torna al sommario

6.1.14 Ricette Dematerializzate Erogate Annullate

Classe documentale	Ricette Dematerializzate Erogate Annullate
Livello 1	RD
Descrizione	Ricette elettroniche dematerializzate erogate e annullate
Sistema Alimentante	Hub Regionale
Fornitore del sistema alimentante	Aria
Formato	ZIP, XML
Frequenza di versamento	Al momento della creazione del documento
Tempo entro il quale trasferire i documenti al sistema di conservazione	Al momento della creazione del documento
Tempo di scarto	10 anni
Codice prontuario di scarto	3.4.01 TITOLO 3 - Area Ospedaliera 4. Assistenza ambulatoriale .01 Prestazioni ambulatoriali- Prescrizione – proposta - ricetta per richieste di prestazioni sanitarie

Torna al sommario

6.1.15 Ricette Dematerializzate Prescritte

Classe documentale	Ricette Dematerializzate Prescritte
Livello 1	RD
Descrizione	Ricette elettroniche dematerializzate prescritte
Sistema Alimentante	Hub Regionale PRR - Dataprocessing
Fornitore del sistema alimentante	Aria
Formato	ZIP, XML
Frequenza di versamento	Al momento della creazione del documento
Tempo entro il quale trasferire i documenti al sistema di conservazione	Al momento della creazione del documento
Tempo di scarto	10 anni
Codice prontuario di scarto	3.4.01 TITOLO 3 - Area Ospedaliera 4. Assistenza ambulatoriale .01 Prestazioni ambulatoriali- Prescrizione – proposta - ricetta per richieste di prestazioni sanitarie

copia informatica per consultazione

Torna al sommario

6.1.16 Ricette Dematerializzate Prescritte Annullate

Classe documentale	Ricette Dematerializzate Prescritte Annullate
Livello 1	RD
Descrizione	Ricette elettroniche dematerializzate prescritte e annullate
Sistema Alimentante	Hub Regionale PRR - Dataprocessing
Fornitore del sistema alimentante	Aria
Formato	ZIP, XML
Frequenza di versamento	Al momento della creazione del documento
Tempo entro il quale trasferire i documenti al sistema di conservazione	Al momento della creazione del documento
Tempo di scarto	10 anni
Codice prontuario di scarto	3.4.01 TITOLO 3 - Area Ospedaliera 4. Assistenza ambulatoriale .01 Prestazioni ambulatoriali- Prescrizione – proposta - ricetta per richieste di prestazioni sanitarie

Torna al sommario

6.1.17 Lettere di Dimissione

Classe documentale	Lettere di Dimissione
Livello 1	DCE
Descrizione	Lettere di dimissioni - Documento Clinico Elettronico
Sistema Alimentante	Repository Aziendali Galileo
Fornitore del sistema alimentante	Dedalus
Formato	M7M e P7M
Frequenza di versamento	Al momento della creazione del documento
Tempo entro il quale trasferire i documenti al sistema di conservazione	Entro la giornata
Tempo di scarto	Illimitato
Codice prontuario di scarto	3.3.02 Massimario del Sistema Sociosanitario lombardo già Sistema Sanitario e Sociosanitario di Regione Lombardia

Torna al sommario

copia informatica per consultazione

6.1.18 Referti di Documenti Clinici Generici

Classe documentale	Referti di Documenti Clinici Generici
Livello 1	DCE
Descrizione	Referti di Documenti Clinici Generici- Documenti
Sistema Alimentante	Repository Aziendali Galileo
Fornitore del sistema alimentante	Dedalus
Formato	M7M e P7M
Frequenza di versamento	Al momento della creazione del documento
Tempo entro il quale trasferire i documenti al sistema di conservazione	Entro la giornata
Tempo di scarto	Illimitato
Codice prontuario di scarto	Massimario del Sistema Sociosanitario lombardo già Sistema Sanitario e Sociosanitario di Regione Lombardia

Torna al sommario

6.1.19 Referti Ambulatoriali

Classe documentale	Referti Ambulatoriali
Livello 1	DCE
Descrizione	Referti Ambulatoriali - Documento Clinico Elettronico
Sistema Alimentante	Repository Aziendali Galileo
Fornitore del sistema alimentante	Dedalus
Formato	M7M e P7M
Frequenza di versamento	Al momento della creazione del documento
Tempo entro il quale trasferire i documenti al sistema di conservazione	Entro la giornata
Tempo di scarto	M7m 30 anni, P7M 10 anni
Codice prontuario di scarto	3.4.01 Massimario del Sistema Sociosanitario lombardo già Sistema Sanitario e Sociosanitario di Regione Lombardia

Torna al sommario

copia informatica per consultazione

6.1.20 Referti Anatomia Patologica

Classe documentale	Referti Anatomia Patologica
Livello 1	DCE
Descrizione	Referti Anatomia Patologica - Documento Clinico Elettronico
Sistema Alimentante	Repository Aziendali Galileo
Fornitore del sistema alimentante	Dedalus
Formato	M7M e P7M
Frequenza di versamento	Al momento della creazione del documento
Tempo entro il quale trasferire i documenti al sistema di conservazione	Entro la giornata
Tempo di scarto	5 anni
Codice prontuario di scarto	2.3.04 Massimario del Sistema Sociosanitario lombardo già Sistema Sanitario e Sociosanitario di Regione Lombardia

Torna al sommario

6.1.21 Referti di Laboratorio

Classe documentale	Referti di Laboratorio
Livello 1	DCE
Descrizione	Referti di Laboratorio - Documento Clinico Elettronico
Sistema Alimentante	Repository Aziendali Galileo
Fornitore del sistema alimentante	Dedalus
Formato	M7M e P7M
Frequenza di versamento	Al momento della creazione del documento
Tempo entro il quale trasferire i documenti al sistema di conservazione	Entro la giornata
Tempo di scarto	5 anni
Codice prontuario di scarto	3.4.01 Massimario del Sistema Sociosanitario lombardo già Sistema Sanitario e Sociosanitario di Regione Lombardia

Torna al sommario

copia informatica per consultazione

6.1.22 Referti di Radiologia

Classe documentale	Referti di Radiologia
Livello 1	DCE
Descrizione	Referti di Radiologia Documento Clinico Elettronico
Sistema Alimentante	Repository Aziendali Galileo
Fornitore del sistema alimentante	Dedalus
Formato	M7M e P7M
Frequenza di versamento	Al momento della creazione del documento
Tempo entro il quale trasferire i documenti al sistema di conservazione	Entro la giornata
Tempo di scarto	Illimitato
Codice prontuario di scarto	3.4.01 Massimario del Sistema Sociosanitario lombardo già Sistema Sanitario e Sociosanitario di Regione Lombardia

Torna al sommario

6.1.23 Verbali di Pronto Soccorso

Classe documentale	Verbali di Pronto Soccorso
Livello 1	DCE
Descrizione	Verbali di Pronto Soccorso - Documento Clinico Elettronico
Sistema Alimentante	Repository Aziendali Galileo
Fornitore del sistema alimentante	Dedalus
Formato	M7M e P7M
Frequenza di versamento	Al momento della creazione del documento
Tempo entro il quale trasferire i documenti al sistema di conservazione	Entro la giornata
Tempo di scarto	Illimitato
Codice prontuario di scarto	3.2.02 Massimario del Sistema Sociosanitario lombardo già Sistema Sanitario e Sociosanitario di Regione Lombardia

Torna al sommario

copia informatica per consultazione

6.1.24 Verbali Operatori

Classe documentale	Verbali di Sala Operatoria
Livello 1	DCE
Descrizione	Documenti Clinici Elettronici (Verbali di Sala Operatoria)
Sistema Alimentante	Repository Aziendali Galileo
Fornitore del sistema alimentante	Dedalus
Formato	M7M e P7M
Frequenza di versamento	Al momento della creazione del documento
Tempo entro il quale trasferire i documenti al sistema di conservazione	Entro la giornata
Tempo di scarto	Illimitato
Codice prontuario di scarto	3.02 Massimario del Sistema Sociosanitario lombardo già Sistema Sanitario e Sociosanitario di Regione Lombardia

Torna al sommario

6.1.25 DICOM

Classe documentale	DICOM
Livello 1	DICOM
Descrizione	Studi diagnostici, detenuti dall'ES, costituiti da insiemi di oggetti conformi allo standard DICOM
Sistema Alimentante	PACS
Fornitore del sistema alimentante	Siemens/Kodak
Formato	DICOM 3.0
Frequenza di versamento	Settimanale
Tempo entro il quale trasferire i documenti al sistema di conservazione	15 giorni
Tempo di scarto	Illimitato
Codice prontuario di scarto	3.02 Titolario e Massimario Regione Lombardia

Torna al sommario

6.2 Metadati minimi dei documenti conservati

Le successive tabelle illustrano i metadati minimi obbligatori relativi al documento informatico, documento amministrativo informatico e aggregazioni documentali informatiche,

copia informatica per consultazione

ovvero sono elencate le informazioni che ne caratterizzano l'identificazione certa del documento. Tali informazioni (metadati) sono organizzate in file xml, associate indissolubilmente al documento secondo quanto disposto dalle regole tecniche attualmente in vigore. I metadati minimi obbligatori, ed eventuali informazioni aggiuntive a corredo del documento, sono indicati nelle Specificità di Contratto a cui si fa riferimento.

Documento Informatico				
Metadato	**Descrizione**	**Campi/ Sottocampi**	**Valori Ammessi**	**Tipo dato**
IdDoc	Identificativo univoco e persistente associato in modo univoco e permanente al documento informatico in modo da consentirne l'identificazione. Inoltre, rappresenta le informazioni necessarie per verificare l'integrità del documento. L'impronta è generata impiegando la funzione di hash, come da definizione nell'Allegato 6 delle Linee Guida nella tabella 1 del paragrafo 2.2 "Regole di processamento". Il metadato è costituito da: • Impronta: sottocampo in cui viene memorizzato l'hash del documento • Algoritmo: sottocampo nel quale deve essere indicata la tipologia dell'algoritmo applicato riportati nell'Allegato 6 delle Linee Guida nella tabella 1 del paragrafo 2.2 "Regole di processamento" • Identificativo: come da sistema di identificazione formalmente definito	Impronta crittografica del documento		
		Impronta	Rappresenta l'hash del documento	Alfanumerico
		Algoritmo	Rappresenta l'algoritmo applicato	Alfanumerico
		Identificativo	Come da sistema di identificazione formalmente definito	Alfanumerico
Modalità formazione documento	Indica la modalità di generazione del documento informatico. Sono previste le seguenti modalità secondo quanto riportato nelle Linee guida: a) creazione tramite l'utilizzo di strumenti software che assicurino la produzione di documenti nei formati previsti nell'Allegato 2 delle Linee Guida; b) acquisizione di un documento informatico per via telematica o su supporto informatico, acquisizione della copia per immagine su supporto informatico di un documento analogico, acquisizione della copia informatica di un documento analogico; c) memorizzazione su supporto informatico in formato digitale delle informazioni risultanti da transazioni o processi informatici o dalla presentazione telematica di dati attraverso moduli o formulari resi disponibili all'utente; d) generazione o raggruppamento anche in via automatica di un insieme di dati o registrazioni, provenienti da una o più banche dati, anche appartenenti a più soggetti interoperanti, secondo una struttura logica predeterminata e memorizzata in forma statica		a, b, c, d	Alfanumerico
Tipologia documentale	Metadato testuale libero per indicare le tipologie documentali trattate		Es. Fatture, Delibere, Determine, etc	Alfanumerico
Dati di Registrazione	Metadato che comprende i dati di registrazione del documento sia nel caso di documento protocollato che non protocollato. Si intende per registrazione l'operazione che, in senso lato, associa ad	Tipologia di flusso	U = In Uscita; E = In Entrata; I = Interno	Alfanumerico
		Tipo Registro	Nessuno, Protocollo Ordinario/Protocollo Emergenza, Repertorio/Registro	Alfanumerico

copia informatica per consultazione

	un documento una data e un numero. In tale ottica, quindi potrebbe non essere identificabile uno specifico registro, ma sono sempre identificabili una data di registrazione e un numero di registrazione del documento. Sono previsti i seguenti campi: • Tipologia di flusso: indica se si tratta di un documento in uscita, in entrata o interno. • Tipo registro: indica il sistema di registrazione adottato: protocollo ordinario/protocollo emergenza, o Repertorio/Registro. • Data: è la data associata al documento all'atto della registrazione • Numero documento: Numero identificativo del documento nel caso di documento non protocollato (ad esempio, numero fattura), numero di protocollo nel caso di documento protocollato. • Codice Registro: Identificativo del registro nel caso in cui il tipo registro sia protocollo ordinario/ protocollo emergenza, o Repertorio/Registro.	Data di Registrazione	nel caso di documento non protocollato: • Data di registrazione del Documento/Ora di registrazione del Documento nel caso di documento protocollato: • Data di registrazione di protocollo/Ora di protocollazione del Documento	DateTime
		Numero Documento	nel caso di documento non protocollato: • Numero di registrazione del documento nel caso di documento protocollato: • Numero di protocollo	Alfanumerico
		Codice Registro	Codice identificativo del registro in cui il documento viene registrato	Alfanumerico
Soggetti	Indica il metadato che consente di individuare le informazioni relative a tutti i soggetti coinvolti e competenti sul documento a vario titolo e definiti dal campo Ruolo. Sono definiti quindi i seguenti attributi: • Ruolo: consente di indicare, a seconda delle necessità, l'autore del documento, il mittente, il destinatario, l'assegnatario. Al fine di rendere i dati di registrazione univoci deve essere sempre indicato il Soggetto che effettua la registrazione del documento (tipicamente l'Organizzazione che protocolla). Obbligatorio inoltre indicare almeno l'autore o il mittente. Nel caso di documento protocollato deve essere obbligatoriamente indicato il mittente. • Per "Operatore" si intende il soggetto autorizzato ad apportare modifiche/integrazioni al documento, la cui definizione si renderà obbligatoria nel caso in cui venga compilato il metadato "Tracciature modifiche documento". • Tipo soggetto: consente di tipizzare i soggetti come persone fisiche, giuridiche, amministrazioni pubbliche (italiane ed estere). Il Tipo Soggetto = SW è indicabile solo se si è indicato il ruolo = "Produttore". Per ogni Tipo Soggetto sono indicati i metadati di riferimento. Il metadato ha una struttura ricorsiva.	Ruolo	• Assegnatario • Autore • Destinatario • Mittente • Operatore • Produttore • RGD (Responsabile della Gestione Documentale) • RSP (Responsabile del Servizio di Protocollo) • Soggetto che effettua la registrazione	Alfanumerico
		Tipo soggetto	Se Ruolo = Assegnatario • AS Se Ruolo = Soggetto che effettua la registrazione • PF per Persona Fisica • PG per Organizzazione Se Ruolo = Mittente o Destinatario o Altro • PF per Persona Fisica • PG per Organizzazione • PAI per le Amministrazioni Pubbliche italiane (valido solo come mittente nei flussi in entrata, come destinatario nei flussi in uscita) • PAE per le Amministrazioni Pubbliche estere (valido solo come mittente nei flussi in entrata, come destinatario nei flussi in uscita) Se Ruolo = Autore • PF per Persona Fisica • PG per Organizzazione • PAI per le Amministrazioni Pubbliche italiane (valido solo nei flussi in entrata) • PAE per le Amministrazioni Pubbliche estere (valido solo nei flussi in entrata) Se Ruolo = Operatore o Responsabile della Gestione Documentale o Responsabile del Servizio Protocollo • PF per Persona Fisica Se Ruolo = Produttore • SW per i documenti prodotti automaticamente	Alfanumerico
		PF	Cognome	Alfanumerico
			Nome	Alfanumerico

copia informatica per consultazione

		PG	Denominazione Organizzazione	Alfanumerico
		PAI	Denominazione Amministrazione\ Codice IPA	Alfanumerico
		PAE	Denominazione Amministrazione	Alfanumerico
		AS	Denominazione Amministrazione\ Codice IPA	Alfanumerico
			Denominazione Amministrazione AOO \ Codice IPA AOO	Alfanumerico
			Denominazione Amministrazione UOR \ Codice IPA UOR	Alfanumerico
		SW	Denominazione Sistema	Alfanumerico
Chiave descrittiva	Metadato funzionale volto a riassumere il contenuto del documento o comunque a chiarirne la natura. È costituito da seguenti campi: • Oggetto: testo libero; • Parole Chiave: da compilare facoltativamente attingendo da thesauri o da vocabolari controllati, per evitare ambiguità terminologiche e avere la possibilità di utilizzare il metadato come chiave di ricerca del documento. Il metadato è ricorsivo fino ad un massimo di 5 occorrenze.	Oggetto	Testo Libero	Alfanumerico
Allegati	Indica il numero di allegati al documento e, nell'eventualità che il numero di allegati indicati sia maggiore di zero, devono essere compilati, in modalità ricorsiva, i dati: • IdDoc: Identificativo del documento relativo all'allegato • Descrizione: Titolo dell'allegato	Numero allegati	Inserire un numero intero compreso tra 0 e 9999	Numerico
		Indice allegati	Da indicare per ogni allegato se Numero allegati > 0	Alfanumerico
		IdDoc	Identificativo del documento relativo all'allegato	
		Descrizione	Testo libero	Alfanumerico
Riservato	Rappresenta il livello di sicurezza di accesso al documento: • Vero: se il documento è considerato riservato • Falso: se il documento non è considerato riservato Consente di gestire gli accessi al documento al solo personale autorizzato.		• Vero: se il documento è considerato riservato • Falso: se il documento non è considerato riservato	Boolean
Identificativo del formato	Indica il formato del documento e la versione del software utilizzato per la creazione del documento stesso. É costituito dai seguenti campi: • Formato: secondo quanto previsto dall'Allegato 2 delle Linee Guida. • Prodotto software: Prodotto software utilizzato per la creazione del documento e relativa versione, suddiviso a sua volta in tre sottocampi: o Nome prodotto o Versione prodotto o Produttore	Formato	Previsti dall'Allegato 2 delle Linee guida	Alfanumerico
		Prodotto software	Prodotto software utilizzato per la creazione del documento e relativa versione	
		Nome prodotto		Alfanumerico
		Versione prodotto		Alfanumerico
		Produttore		Alfanumerico
Verifica	Check di controllo presenza Firma elettronica, Sigillo, Marcatura temporale e Conformità copie immagine nelle modalità di formazione del documento informatico previste nelle Linee Guida.	Firmato Digitalmente	• Vero • Falso	Boolean
		Sigillato Elettronicamente	• Vero • Falso	Boolean
		Marcatura Temporale	• Vero • Falso	Boolean
		Conformità copie immagine su supporto informatico	• Vero • Falso	Boolean

copia informatica per consultazione

Aggregazione documentale	Identificativo univoco dell'Aggregazione come definito nella tabella dedicata alle aggregazioni documentali. Metadato ricorsivo.		Identificativo del fascicolo o della serie.	Alfanumerico
Documento Primario	Identificativo univoco e persistente del Documento primario.		IdDoc del documento primario	
Nome del documento\file	Nome del documento\file così come riconosciuto all'esterno.			Alfanumerico
Versione del documento	Versione del documento		Indicare la versione del documento	Alfanumerico
Tracciature modifiche documento	Metadato volto a tracciare la presenza di operazioni di modifica effettuate sul documento e la data in cui esse sono state effettuate. L'autore delle modifiche è tracciato nel metadato "Soggetti" con il ruolo "Operatore".	Tipo modifica	• Annullamento • Rettifica • Integrazione • Annotazione	Alfanumerico
		Soggetto autore della modifica	Come da ruolo = Operatore definito nel metadato Soggetti	Alfanumerico
		Data modifica/Ora modifica		Date/Time
		IdDoc versione precedente	Identificativo documento versione precedente	

Documento Amministrativo informatico				
Metadato	**Dettaglio**	**Campi/ Sottocampi**	**Valori Ammessi**	**Tipo dato**
IdDoc	Identificativo univoco e persistente associato in modo univoco e permanente al documento amministrativo informatico in modo da consentirne l'identificazione. Inoltre, rappresenta le informazioni necessarie per verificare l'integrità del documento. Il metadato è costituito dai campi: • Impronta crittografica del documento: a sua volta suddiviso in: o Impronta: sottocampo in cui viene memorizzato l'hash del documento o Algoritmo: sottocampo nel quale deve essere indicata la tipologia dell'algoritmo applicato secondo quanto riportato nell'Allegato 6 delle Linee Guida nella tabella 1 del paragrafo 2.2 "Regole di processamento" • Identificativo: come da sistema di identificazione formalmente definito • Segnatura: segnatura di protocollo, da indicare obbligatoriamente nel caso di documento amministrativo protocollato, a sua volta strutturato come da Allegato 6 delle Linee Guida.	Impronta crittografica del documento		
		Impronta	Rappresenta l'hash del documento	Binary
		Algoritmo	Rappresenta l'algoritmo applicato Default = SHA-256	Alfanumerico
		Identificativo	Come da sistema di identificazione formalmente definito	Alfanumerico
		Segnatura	Segnatura del protocollo	Alfanumerico

copia informatica per consultazione

Modalità di formazione	Indica la modalità di generazione del documento amministrativo informatico. Sono previste le seguenti modalità secondo quanto riportato nelle Linee guida: a) creazione tramite l'utilizzo di strumenti software che assicurino la produzione di documenti nei formati previsti nell'Allegato 2 delle Linee Guida; b) acquisizione di un documento informatico per via telematica o su supporto informatico, acquisizione della copia per immagine su supporto informatico di un documento analogico, acquisizione della copia informatica di un documento analogico; c) memorizzazione su supporto informatico in formato digitale delle informazioni risultanti da transazioni o processi informatici o dalla presentazione telematica di dati attraverso moduli o formulari resi disponibili all'utente; d) generazione o raggruppamento anche in via automatica di un insieme di dati o registrazioni, provenienti da una o più banche dati, anche appartenenti a più soggetti interoperanti, secondo una struttura logica predeterminata e memorizzata in forma statica.		Indicare a) creazione tramite l'utilizzo di strumenti software che assicurino la produzione di documenti nei formati previsti nell'Allegato 2 delle Linee; b) acquisizione di un documento informatico per via telematica o su supporto informatico, acquisizione della copia per immagine su supporto informatico di un documento analogico, acquisizione della copia informatica di un documento analogico; c) memorizzazione su supporto informatico in formato digitale delle informazioni risultanti da transazioni o processi informatici o dalla presentazione telematica di dati attraverso moduli o formulari resi disponibili all'utente; d) generazione o raggruppamento anche in via automatica di un insieme di dati o registrazioni, provenienti da una o più banche dati, anche appartenenti a più soggetti interoperanti, secondo una struttura logica predeterminata e memorizzata in forma statica	Alfanumerico
Tipologia documentale	Metadato funzionale che indica la tipologia del documento tra quelle trattate per lo svolgimento delle attività.		Metadato testuale libero per indicare le tipologie documentali trattate (ad esempio, fatture, delibere, determine, etc)	Alfanumerico
Dati di registrazione	Sono previsti i seguenti campi: • Tipologia di flusso: indica se si tratta di un documento in uscita, in entrata o interno. Per documento interno si intende un documento scambiato tra le diverse UOR afferenti alla stessa AOO • Tipo registro: indica il sistema di registrazione adottato: protocollo ordinario/protocollo emergenza, o Repertorio/Registro. • Data: è la data associata al documento all'atto della registrazione • Numero documento: Numero identificativo del documento nel caso di documento non protocollato (ad esempio, numero fattura), numero di protocollo nel caso di documento protocollato. • Codice Registro: Identificativo del registro in cui il documento viene registrato.	Tipologia di flusso	• "U" = In uscita • "E" = In entrata • "I" = Interno Per documenti interni si intende i documenti scambiati all'interno della medesima AOO	Alfanumerico
		Tipo registro	• Protocollo Ordinario /Protocollo Emergenza • Repertorio/Registro	Alfanumerico
		Data registrazione	nel caso di documento non protocollato: • Data di registrazione del Documento/Ora di registrazione del Documento nel caso di documento protocollato: • Data di registrazione di protocollo/Ora di protocollazione del Documento	Date/Time
		Numero Documento	nel caso di documento non protocollato: • Numero di registrazione del documento nel caso di documento protocollato: • Numero di protocollo	Alfanumerico
		Codice Registro	Codice identificativo del registro in cui il documento viene registrato.	Alfanumerico

copia informatica per consultazione

Soggetti	Indica il metadato che consente di individuare le informazioni relative a tutti i Soggetti coinvolti e competenti sul documento a vario titolo e definiti dal campo Ruolo. Sono definiti quindi i seguenti attributi: • Ruolo: consente di indicare, a seconda delle necessità, l'autore del documento, il mittente, il destinatario, l'assegnatario. Al fine di rendere i dati di registrazione univoci deve essere sempre indicata l'Amministrazione che effettua la registrazione del documento. Obbligatorio inoltre indicare almeno l'autore o il mittente. Nel caso di documento protocollato deve essere obbligatoriamente indicato il mittente. Per "Operatore" si intende il soggetto autorizzato ad apportare modifiche/integrazioni al documento, la cui definizione si renderà obbligatoria nel caso in cui venga compilato il metadato "Tracciature modifiche documento". Nel caso di ruolo Assegnatario si prevede l'indicazione della UOR di riferimento con l'indicazione, a completamento, della persona fisica. Nel caso di ruolo RUP le informazioni relative alla persona fisica e alla UOR di appartenenza diventano obbligatorie. • Tipo soggetto: consente di tipizzare i soggetti come persone fisiche, giuridiche, amministrazioni pubbliche (italiane ed estere). Il Tipo Soggetto = SW è indicabile solo se si è indicato il ruolo = "Produttore". Per ogni Tipo Soggetto sono indicati i metadati di riferimento. Il metadato ha una struttura ricorsiva.	Ruolo	• Amministrazione che effettua la registrazione • Assegnatario • Autore • Destinatario • Mittente • Operatore • Produttore • RGD (Responsabile della Gestione Documentale) • RSP (Responsabile del Servizio di Protocollo) • RUP	Alfanumerico
		Tipo soggetto	Se Ruolo = Assegnatario ü AS Se Ruolo = Amministrazione che effettua la registrazione ü PAI per le Amministrazioni Pubbliche italiane Se Ruolo = Mittente o Destinatario ü PF per Persona Fisica ü PG per Organizzazione ü PAI per le Amministrazioni Pubbliche Italiane ü PAE per le Amministrazioni Pubbliche Estere Se Ruolo = Autore ü PF per Persona Fisica ü PG per Organizzazione (valido solo nei flussi in entrata) ü PAI per le Amministrazioni Pubbliche italiane ü PAE per le Amministrazioni Pubbliche Estere (valido solo nei flussi in entrata) Se Operatore o Responsabile della Gestione Documentale o Responsabile del Servizio Protocollo ü PF per Persona Fisica Se Ruolo = RUP ü RUP Se Ruolo = Produttore ü SW per i documenti prodotti automaticamente	Alfanumerico
		PF	Cognome	Alfanumerico
			Nome	Alfanumerico
		PG	Denominazione Organizzazione	Alfanumerico
		PAI	Denominazione Amministrazione\ Codice IPA	Alfanumerico
			Denominazione Amministrazione AOO \ Codice IPA AOO	Alfanumerico
			Indirizzi Digitali Di Riferimento	Alfanumerico
		PAE	Denominazione Amministrazione	Alfanumerico
			Indirizzi Digitali Di Riferimento	Alfanumerico
		AS	Denominazione Amministrazione\ Codice IPA	Alfanumerico
			Denominazione Amministrazione AOO \ Codice IPA AOO	Alfanumerico
			Denominazione Amministrazione UOR \ Codice IPA UOR	Alfanumerico
			Indirizzi Digitali Di Riferimento	Alfanumerico
		RUP	Nome	Alfanumerico
			Codice Fiscale	Alfanumerico

copia informatica per consultazione

			Denominazione Amministrazione AOO \ Codice IPA AOO	Alfanumerico
			Denominazione Amministrazione UOR \ Codice IPA UOR	Alfanumerico
			Indirizzi Digitali Di Riferimento	Alfanumerico
		SW	Denominazione Sistema	Alfanumerico
Chiave descrittiva	Metadato funzionale volto a riassumere il contenuto del documento o comunque a chiarirne la natura. È costituito da seguenti campi: • Oggetto: testo libero; • Parole Chiave: da compilare facoltativamente attingendo da thesauri o da vocabolari controllati, per evitare ambiguità terminologiche e avere la possibilità di utilizzare il metadato come chiave di ricerca del documento. Il metadato è ricorsivo fino ad un massimo di 5 occorrenze.	Oggetto	Testo libero	Alfanumerico
Allegati	Indica il numero di allegati al documento e, nell'eventualità che il numero di allegati indicati sia maggiore di zero, devono essere compilati, in modalità ricorsiva, i dati: • IdDoc: Identificativo del documento relativo all'allegato • Descrizione: Titolo dell'allegato	Numero allegati	Inserire un numero intero compreso tra 0 e 9999	Numerico
		Indice allegati	Da indicare per ogni allegato se Numero allegati > 0	
		IdDoc	Identificativo del documento relativo all'allegato	Alfanumerico
		Descrizione	Testo libero	Alfanumerico
Classificazione	Classificazione del documento secondo il Piano di classificazione utilizzato, da indicare sia nel caso di documento protocollato che nel caso di documento non protocollato: • Indice di classificazione: Codifica del documento secondo il Piano di classificazione utilizzato • Descrizione: Descrizione per esteso dell'Indice di classificazione indicato. • Piano di classificazione: riportare l'URI di pubblicazione del Piano di classificazione	Indice di classificazione	Codifica del documento secondo il Piano di classificazione utilizzato	Alfanumerico
		Descrizione	Descrizione per esteso dell'Indice di classificazione indicato.	Alfanumerico
Riservato	Rappresenta il livello di sicurezza di accesso al documento: • Vero: se il documento è considerato riservato • Falso: se il documento non è considerato riservato Consente di gestire gli accessi al documento al solo personale autorizzato.		• Vero: se il documento è considerato riservato • Falso: se il documento non è considerato riservato	Boolean
Identificativo del formato	Indica il formato del documento e la versione del software utilizzato per la creazione del documento stesso. É costituito dai seguenti campi: • Formato: secondo quanto previsto dall'Allegato 2 delle Linee Guida. • Prodotto software: Prodotto software utilizzato per la creazione del documento e relativa versione, suddiviso a sua volta in tre sottocampi: o Nome prodotto o Versione prodotto o Produttore	Formato	Previsti dall'Allegato 2 delle Linee guida	Alfanumerico
		Prodotto software	Prodotto software utilizzato per la creazione del documento e relativa versione	
		Nome prodotto		Alfanumerico
		Versione prodotto		Alfanumerico
		Produttore		Alfanumerico
Verifica	Check di controllo presenza Firma elettronica, Sigillo, Marcatura temporale e Conformità copie immagine nelle modalità di formazione del documento informatico previste nelle Linee Guida.	Firmato Digitalmente	• Vero • Falso	Boolean
		Sigillato Elettronicamente	• Vero • Falso	Boolean
		Marcatura Temporale	• Vero • Falso	Boolean

copia informatica per consultazione

		Conformità copie immagine su supporto informatico	• Vero • Falso	Boolean
Aggregazione documentale	Identificativo univoco dell'Aggregazione come definito nella tabella dedicata alle aggregazioni documentali. Metadato ricorsivo.		Identificativo del fascicolo o della serie.	Alfanumerico
Documento Primario	Identificativo univoco e persistente del Documento primario.		IdDoc del documento primario	
Nome del documento\file	Nome del documento\file così come riconosciuto all'esterno.			Alfanumerico
Versione del documento	Versione del documento		Indicare la versione del documento	Alfanumerico
Tracciature modifiche documento	Metadato volto a tracciare la presenza di operazioni di modifica effettuate sul documento e la data in cui esse sono state effettuate. L'autore delle modifiche è tracciato nel metadato "Soggetti" con il ruolo "Operatore".	Tipo modifica	• Annullamento • Rettifica • Integrazione • Annotazione	Alfanumerico
		Soggetto autore della modifica	Come da ruolo = Operatore definito nel metadato Soggetti	Alfanumerico
		Data modifica/Ora modifica		Date/Time
		IdDoc versione precedente	Identificativo documento versione precedente	

Aggregazioni documentali Informatiche				
Metadato	**Dettaglio**	**Campi/ Sottocampi**	**Valori Ammessi**	**Tipo dato**
Identificativo dell' Aggregazione	L' Identificativo dell'Aggregazione documentale è una sequenza di caratteri alfanumerici associata in modo univoco all'aggregazione documentale informatica in modo da consentirne l'identificazione, indica se si tratta di un Fascicolo o di una Serie Documentale o di una Serie di Fascicoli. Il fascicolo è una aggregazione documentale informatica strutturata e univocamente identificata contenente atti, documenti o dati informatici prodotti e funzionali all'esercizio di una attività o allo svolgimento di uno specifico procedimento. Le serie documentarie sono costituite da documenti singoli accorpati per ragioni funzionali in base alla tipologia di riferimento. Le serie di fascicoli sono costituite da fascicoli accorpati per ragioni funzionali in base alla classe di riferimento o alla tipologia di fascicoli.	TipoAggregazione	Indicare: • Fascicolo • Serie Documentale • Serie Di Fascicoli	Alfanumerico
		IdAggregazione	Come da sistema di identificazione formalmente definito.	Alfanumerico

copia informatica per consultazione

Tipologia fascicolo	I fascicoli sono organizzati per: • affare: conserva i documenti relativi a una competenza non proceduralizzata, ma che nella consuetudine amministrativa la PA deve concretamente portare a buon fine. Il fascicolo per affare ha una data di apertura e una durata circoscritta. • attività: comprende i documenti prodotti nello svolgimento di un'attività amministrativa semplice che implica risposte obbligate o meri adempimenti, per la quale quindi non è prevista l'adozione di un provvedimento finale. Ha in genere durata annuale. • persona fisica: comprende tutti i documenti, anche con classifiche diverse, che si riferiscono a una persona fisica. Quasi sempre i fascicoli intestati alle persone restano correnti per molti anni, costituendo serie aperte. • persona giuridica: comprende tutti i documenti, anche con classifiche diverse, che si riferiscono a una persona giuridica. Quasi sempre i fascicoli intestati alle persone restano correnti per molti anni, costituendo serie aperte • procedimento amministrativo: conserva una pluralità di documenti che rappresentano azioni amministrative omogenee e destinate a concludersi con un provvedimento amministrativo.	NON Applicabile	Solo in caso di TipoAggregazione = 'Fascicolo' Tipologia del fascicolo: • affare • attività • persona fisica • persona giuridica • procedimento amministrativo	Alfanumerico
Soggetti	Indica il metadato che consente di individuare le informazioni relative a tutti i Soggetti che, a vario titolo, sono coinvolti nella costituzione dell'aggregazione. Sono definiti quindi i seguenti attributi: • Ruolo: o Amministrazione titolare o Amministrazioni partecipanti o Assegnatario o Soggetto intestatario persona fisica o Soggetto intestatario persona giuridica o RUP: da indicare solo in caso di TipoAggregazione = 'Fascicolo' • Tipo soggetto: consente di tipizzare i soggetti come persone fisiche, giuridiche, amministrazioni pubbliche (italiane ed estere) in funzione del Ruolo. Per ogni tipo soggetto sono indicati i metadati di riferimento. Nel caso in cui sia stato definito un Ruolo=RUP è obbligatorio indicare anche l'UOR	Ruolo	• Amministrazione che effettua la registrazione • Assegnatario • Autore • Destinatario • Mittente • Operatore • Produttore • RGD (Responsabile della Gestione Documentale) • RSP (Responsabile del Servizio di Protocollo) • RUP	Alfanumerico

copia informatica per consultazione

	corrispondente.	Tipo soggetto	Se Ruolo = Amministrazione titolare ü PAI per le Amministrazioni Pubbliche italiane Se Ruolo = Amministrazioni partecipanti ü PAI per le Amministrazioni Pubbliche italiane ü PAE per le Amministrazioni Pubbliche estere Se Ruolo = Assegnatario ü AS Se Ruolo = Soggetto intestatario persona giuridica • PG per Organizzazione • PAI per le Amministrazioni Pubbliche Italiane • PAE per le Amministrazioni Pubbliche estere Se Ruolo = Soggetto intestatario persona fisica ü PF per Persona Fisica Se Ruolo = RUP ü RUP	Alfanumerico
		PF	Cognome	Alfanumerico
			Nome	Alfanumerico
		PG	Denominazione Organizzazione	Alfanumerico
		PAI	Denominazione Amministrazione\ Codice IPA	Alfanumerico
			Denominazione Amministrazione AOO \ Codice IPA AOO	Alfanumerico
			Indirizzi Digitali Di Riferimento	Alfanumerico
		PAE	Denominazione Amministrazione	Alfanumerico
			Indirizzi Digitali Di Riferimento	Alfanumerico
		AS	Denominazione Amministrazione\ Codice IPA	Alfanumerico
			Denominazione Amministrazione AOO \ Codice IPA AOO	Alfanumerico
			Denominazione Amministrazione UOR \ Codice IPA UOR	Alfanumerico
			Indirizzi Digitali Di Riferimento	Alfanumerico
		RUP	Cognome	Alfanumerico
			Nome	Alfanumerico
			Denominazione Amministrazione\ Codice IPA	Alfanumerico
			Denominazione Amministrazione AOO \ Codice IPA AOO	Alfanumerico
			Denominazione Amministrazione UOR \ Codice IPA UOR	Alfanumerico
			Indirizzi Digitali Di Riferimento	Alfanumerico
Assegnazione	Indica il metadato che consente di individuare le informazioni relative all'assegnazione per conoscenza o per competenza. I Soggetti indicati in questo metadato devono essere stati dichiarati nel metadato Soggetti. Sono definiti quindi i seguenti attributi: • Tipo assegnazione • Soggetto assegnatario • Data inizio assegnazione • Data fine assegnazione Il metadato ha una struttura ricorsiva.	Tipo assegnazione	• Per competenza • Per conoscenza	Alfanumerico
		Soggetto Assegnatario	Come da Ruolo = Assegnatario definito del metadato Soggetti.	Alfanumerico
		Data inizio assegnazione / Ora inizio assegnazione	Data inizio assegnazione	Date/Time
Data Apertura	Data di apertura dell'aggregazione documentale		Data di apertura dell'aggregazione documentale	Date
Classificazione	Classificazione dell'aggregazione: • Indice di classificazione: Codifica del documento secondo il Piano di classificazione utilizzato • Descrizione: Descrizione per esteso	Indice di classificazione	Codifica secondo il Piano di classificazione utilizzato	Alfanumerico
		Descrizione	Descrizione per esteso dell'Indice di classificazione indicato.	Alfanumerico

copia informatica per consultazione

	dell'Indice di classificazione indicato. • Piano di classificazione: se presente, riportare eventualmente l'URI di pubblicazione del Piano di classificazione			
Progressivo	Progressivo numerico calcolato nell'ambito della chiave della classificazione o in ordine cronologico nell'ambito dell'anno			Numerico
Chiave descrittiva	Metadato funzionale volto a chiarire la natura del fascicolo o della serie. È costituito da seguenti campi: • Oggetto: testo libero; • Parole Chiave: da compilare facoltativamente attingendo da thesauri o da vocabolari controllati, per evitare ambiguità terminologiche e avere la possibilità di utilizzare il metadato come chiave di ricerca. Il metadato è ricorsivo fino ad un massimo di 5 occorrenze.	Oggetto	Testo libero	Alfanumerico
DataChiusura	Data di chiusura dell'aggregazione documentale		Data di chiusura dell'aggregazione documentale	Date
Procedimento Amministrativo	Metadato funzionale volto ad indicare il procedimento a cui il fascicolo afferisce, nonché lo stato di avanzamento e le relative fasi. Il campo "Fase", a sua volta costituito da "Tipo Fase": • Preparatoria • Istruttoria • Consultiva • Decisoria o deliberativa • Integrazione dell'efficacia e da "Data inizio fase" e "Data fine fase" deve considerarsi dinamico, destinato ad essere aggiornato con lo stato di avanzamento dell'iter del procedimento\processo.	Materia\ Argomento\ Struttura	Indicare la materia o l'argomento o la struttura per la quale sono stati catalogati i procedimenti amministrativi	Alfanumerico
		Procedimento	Denominazione del Procedimento	Alfanumerico
		Catalogo procedimenti	URI di pubblicazione del catalogo	Alfanumerico
		Fasi	A sua volta suddiviso, in una struttura ricorsiva:	
		Tipo Fase	• Preparatoria • Istruttoria • Consultiva • Decisoria o deliberativa • Integrazione dell'efficacia	Alfanumerico
		Data inizio fase	Secondo le regole indicate per i documenti informatici o i documenti ammnistrativi informatici	Date
Indice documenti	Elenco degli identificativi dei documenti contenuti nell'aggregazione, definiti secondo le regole indicate per i documenti informatici o i documenti amministrativi informatici. Metadato ricorsivo	Tipo documento	• documento amministrativo informatico • documento informatico	
		IdDoc		
Posizione fisica Aggregazione Documentale	Posizione fisica dell'aggregazione. Nel caso di fascicoli ibridi indica la posizione della componente cartacea del fascicolo.		Testo libero	Alfanumerico

Torna al sommario

6.3 Pacchetti informativi

6.3.1 Pacchetto di versamento

In questo paragrafo è fornita la struttura dati dei pacchetti di versamento gestiti.
In particolare, un pacchetto di versamento (PdV) è composto dalle seguenti parti:

- documento/i stesso oggetto della conservazione;
- file di metadati relativo ai documenti da conservare;
- Indice del Pacchetto di Versamento (IPdV), cioè un'evidenza informatica (file .xml), che descrive il versamento stesso e i documenti che ne fanno parte attraverso l'uso di metadati.

copia informatica per consultazione

In linea con gli standard, l'indice del pacchetto di versamento si caratterizza per le seguenti sezioni:

- **Area di identificazione del PDV**: in cui è obbligatorio l'indicazione del pdvid ovvero l'identificativo univoco del PDV.
- **Area di identificazione dei documenti costituenti il pacchetto:** composta dai seguenti elementi:
    - metadati obbligatori
    - metadati extra-info

Per ogni documento da versare, sono necessari i seguenti dati per l'identificazione del documento:

- nome file
- algoritmo di hashing per la generazione dell'impronta
- impronta del documento

Inoltre, poiché il sistema di conservazione controlla la tipologia di documento per valutarne l'aderenza alle condizioni espresse in fase di contratto, è indicato il MIME type del documento.
Per rimanere poi aderenti alla norma vigente è anche indicato un identificativo univoco dei singoli documenti del pacchetto e la data di chiusura degli stessi.
L'ultima parte dell'Indice contiene un insieme di metadati extra-info, così come definiti in fase contrattuale col Conservatore e indicati nelle specificità di contratto.

Torna al sommario

6.3.2 Pacchetto di Archiviazione

Per la descrizione della struttura dati del pacchetto di archiviazione completa delle ulteriori strutture collegate ai diversi elementi "MoreInfo" previsti dallo standard SInCRO, si rimanda al manuale di conservazione del Conservatore.

Torna al sommario

6.3.3 Pacchetto di distribuzione

Per la descrizione delle tipologie di pacchetto di distribuzione gestite e relativa struttura dati, si rimanda al manuale della conservazione del Conservatore.

Torna al sommario

copia informatica per consultazione

7 Processo di conservazione

Il processo di conservazione consta di più fasi di seguito elencate:

Funzioni/Responsabilità del processo di Formazione	**ASST**	**Conservatore**
Creazione del Pacchetto di Versamento (PdV)	X	
Trasferimento del PdV al sistema di conservazione	X	
Acquisizione e presa in carico del PdV		X
Verifiche sul PdV		X
Accettazione del PdV e generazione del Rapporto di Versamento (RdV) di presa in carico		X
Sottoscrizione del RdV con FD, FEQ o FEA		X
Rifiuto del PdV e comunicazione delle anomalie		X
Presa visione del RdV	X	
Presa visione delle anomalie a seguito del rifiuto del PdV	X	
Preparazione, gestione e Sottoscrizione con FD, FEQ o FEA del Pacchetto di Archiviazione		X
Richiesta del Pacchetto di Distribuzione ai fini dell'esibizione	X	
Preparazione, gestione e Sottoscrizione con FD, FEQ o FEA del Pacchetto di Distribuzione ai fini dell'esibizione		X
Produzione di duplicati e copie informatiche ed eventuale intervento del pubblico ufficiale nei casi previsti		X
Predisposizione elenco pacchetti di archiviazione da scartare		X
Richiesta alla soprintendenza di autorizzazione allo scarto	X	
Scarto dei pacchetti di archiviazione		X
Predisposizione di misure a garanzia dell'interoperabilità e trasferibilità ad altri		X

copia informatica per consultazione

conservatori		
Audit Log		X

Per la descrizione delle fasi del processo di conservazione in carico al Conservatore si rimanda al Manuale di conservazione del conservatore.
Nei paragrafi successivi sono altresì descritte le fasi inerenti il processo di conservazione in carico all'ASST.

Torna al sommario

7.1 Creazione del PdV e trasferimento al sistema di conservazione

L'operazione di creazione dei Pacchetti di Versamento (PdV) consiste nella messa a disposizione del sistema di conservazione dei documenti oggetto di conservazione e dei relativi metadati in formato idoneo e definito.

L'ASST ha la possibilità di creare e trasferire al sistema di conservazione un PdV tramite almeno una delle seguenti modalità:

- **Web Services:** la creazione del pacchetto è effettuata dal sistema alimentante tramite appositi Web Services che mettono a disposizione il/i documento/i corredato/i dei relativi metadati formato csv/json. Nel caso di invio di più documenti questi sono inseriti all'interno di un archivio zip.
- **Manuale:** l'ASST può creare il PdV direttamente dal sistema di conservazione tramite due procedure
  - Manuale guidata
  - Manuale non guidata

  Con il caricamento guidato è possibile versare un documento alla volta mentre nell'altro caso è possibile versare più documenti inseriti all'interno di uno zip e il file di indice in formato csv o json.

L'ASST può inoltre usufruire dell'utilizzo del Flyadapter. Il FlyAdapter fornisce un frontend locale che permette di rendere il collegamento tra sistema alimentante e componente centrale del sistema di conservazione (CSC) più efficace e performante svolgendo un ruolo "home-based services" direttamente nelle architetture dell'ASST. In particolare tale modalità prevede il versamento tramite rete locale dell'ASST direttamente sul Flyadapter che poi successivamente provvede in modo asincrono a versare sul CSC. Il vantaggio significativo è rappresentato dalla possibilità di avere un servizio Always-on che non dipenda da elementi terzi quali connettività ed accesso internet che potrebbero rendere l'accesso intermittente da parte dell'ASST con conseguente ritardo nello svolgimento delle funzioni da parte del personale.

Il sistema di conservazione prende in carico un PdV solo dopo che tutte le sue parti (IPdV e relativi documenti) sono correttamente ricevute e superano con esito positivo i relativi controlli.
L'operazione è sancita dalla generazione di un Rapporto di Versamento (RdV) relativo a ciascun pacchetto di versamento effettuato, cioè un documento informatico in formato .xml marcato temporalmente e firmato dal responsabile del servizio di conservazione. In caso di riscontro di eventuali anomalie, il pacchetto di versamento viene rifiutato.

copia informatica per consultazione

La produzione del Rapporto di Versamento (RdV) rappresenta formalmente la presa in carico del Pacchetto di Versamento (PdV) da parte del sistema di conservazione e la trasformazione di quest'ultimo in pacchetto di archiviazione, cioè un documento informatico che attesta il caricamento dei documenti in un determinato momento e la loro conservazione a norma di legge.

Inoltre, i sistemi alimentanti dei documenti amministrativi (Data Processing) e documenti clinici elettronici (Repository aziendale Galileo) acquisiscono il flag di ritorno a seguito della conservazione e la possibilità di inviare nuovamente eventuali documenti in errore.

La tabella successiva indica le modalità di creazione del PdV e Trasferimento al sistema di conservazione per ciascuna classe documentale.

Classi documentali	**Sistema alimentante**	**Modalità di creazione del PDV (Automatica / Manuale)**	**Modalità di trasferimento (Attiva/ Passiva)**	**Utilizzo del FlyAdapter (Si/No)**	**Modalità di acquisizione del pacchetto di versamento**
Fatture PA Attive	Hub Regionale	Automatica	Passiva	Si (Adapter EDK)	Web Services SOAP , Interfacce RESTful
Fatture PA Passive	Hub Regionale	Automatica	Passiva	Si (Adapter EDK)	Web Services SOAP , Interfacce RESTful
Notifiche SDI Fatture PA Attive	Hub Regionale	Automatica	Passiva	Si (Adapter EDK)	Web Services SOAP , Interfacce RESTful
Notifiche SDI Fatture PA Passive	Hub Regionale	Automatica	Passiva	Si (Adapter EDK)	Web Services SOAP , Interfacce RESTful
Delibere	Sfera	Automatica	Passiva	Si	Web Services SOAP, Interfacce RESTful
Determine	Sfera	Automatica	Passiva	Si	Web Services SOAP, Interfacce RESTful
Repertori	Prisma	Automatica	Passiva	Si	Web Services SOAP, Interfacce RESTful
Documenti Protocollati	Prisma	Automatica	Passiva	Si	Web Services SOAP, Interfacce RESTful
Cedolini	Sigma / GPI	Automatica	Passiva	Si	Web Services SOAP, Interfacce RESTful
Ricevute Telematiche RT	MyPay	Automatica	Passiva	Si	Web Services SOAP
Richiesta Pagamento Telematico RPT	MyPay	Automatica	Passiva	Si	Web Services SOAP
SINTEL 5/10/20 anni e illimitati	Sintel	Automatica	Passiva	Si	--
Aria	Hub Regionale	Automatica	Attiva	Si	Web Services SOAP, Interfacce RESTful
.pdf, .p7m,.m7m (Documento di offerta) Scelto dal fornitore (allegati)	Hub Regionale	Automatica	Attiva	Si	Web Services SOAP, Interfacce RESTful

copia informatica per consultazione

Al momento della creazione.	Hub Regionale	Automatica	Attiva	Si	Web Services SOAP, Interfacce RESTful
Al momento della creazione	Hub Regionale	Automatica	Attiva	Si	Web Services SOAP, Interfacce RESTful
5/10/20 o illimitato	Repository Aziendale Galileo	Automatica	Passiva	Si	HL7
1.6.03 Titolo 1 – Area Amministrativa 6. Gestione e organizzazione del patrimonio. .03 Acquisizione e gestione di beni mobili / generi di consumo e di servizi	Repository Aziendale Galileo	Automatica	Passiva	Si	HL7
Referti Ambulatoriali	Repository Aziendale Galileo	Automatica	Passiva	Si	HL7
Referti Anatomia Patologica	Repository Aziendale Galileo	Automatica	Passiva	Si	HL7
Referti di Laboratorio	Repository Aziendale Galileo	Automatica	Passiva	Si	HL7
Referti di Radiologia	Repository Aziendale Galileo	Automatica	Passiva	Si	HL7
Verbali di Pronto Soccorso	Repository Aziendale Galileo	Automatica	Passiva	Si	HL7
Verbali Operatori	Repository Aziendale Galileo	Automatica	Passiva	Si	HL7
DICOM	PACS - Siemens	Automatica	Attiva	Si	DICOM 3.0

Torna al sommario

copia informatica per consultazione

7.2 Presa visione del RdV

Il Rapporto di Versamento è un documento informatico che attesta l'avvenuta presa in carico da parte del sistema di conservazione dei pacchetti di versamento inviati dal produttore.
Il rapporto di versamento è strutturato secondo lo standard UNI-SInCRO e ha ad oggetto:

- I riferimenti al versamento a cui fa riferimento;
- Il riferimento temporale relativo alla sua creazione secondo l'orario di sistema;
- Tutte le informazioni contenute nel file indice del PdV;
- L'indicazione di tutte le verifiche effettuate e l'esito puntuale delle stesse.

Il rapporto, firmato digitalmente in modo da autenticarne la provenienza e l'integrità, è messo a disposizione dell'ASST sul sistema di conservazione.
I rapporti di versamento sono conservati a norma nel sistema di conservazione, associati logicamente al pacchetto di archiviazione cui si riferiscono, come registrazioni ufficiali che attestano la presa in carico.

Il sistema di conservazione invia giornalmente una mail all'indirizzo PEC conservazione@pec.asst-mantova.it contenenti la reportistica relativa all'archivio Sanitario Amministrativo, in cui viene indicato per ognuna delle classi documentali il numero di PdV ricevuti, quanti hanno dato esito positivo e quanti negativo.

Inoltre, per le classi documentali Delibere, Determine, Repertori e Documenti Protocollati viene registrato l'esito del RdV sul sistema alimentante di Data Processing mentre per le classi DCE viene registrato l'esito del RdV sul Repository Aziendale Galileo.

L'esito dell'invio in conservazione del PdV è inoltre monitorabile accedendo nella sezione dedicata del sistema di conservazione.

Torna al sommario

7.3 Presa visione delle anomalie a seguito del rifiuto del PdV

Nel caso si verifichino errori o anomalie relative ai documenti inviati in un pacchetto di versamento, il sistema di Conservazione mette in evidenza il problema ed il tipo di errore. Nel caso in cui il documento risulti non conforme ai controlli sopra indicati, viene messo in uno stato di "scarto"/"errore di validazione". La presenza di errori di validazione impedisce la chiusura del pacchetto di versamento e, pertanto, i documenti verranno scartati e riversati nuovamente sul Sistema una volta risolta l'anomalia.

Torna al sommario

7.4 Richiesta del Pacchetto di Distribuzione ai fini dell'esibizione

Nel rispetto degli obblighi previsti in materia di esibizione documentale della normativa vigente, il sistema di conservazione garantisce la possibilità ai soggetti autorizzati all'accesso diretto, anche da remoto, al documento informatico conservato, attraverso la produzione di un pacchetto di distribuzione.

Un utente autorizzato può interrogare il sistema per ricevere in uscita uno specifico Pacchetto di Distribuzione. L'utente utilizzerà le funzionalità di richiesta di esibizione di un documento o

copia informatica per consultazione

di un insieme di documenti, per ottenerne una replica esatta secondo i fini previsti dalla norma.

Per le modalità di produzione del Pacchetto di Distribuzione si fa riferimento al manuale d'uso del sistema di conservazione.

Torna al sommario

7.5 Richiesta alla soprintendenza di autorizzazione allo scarto

7.5.1 Dichiarazioni d'intenti e scopo

Questa procedura ha lo scopo di fornire istruzioni ai servizi e alle unità operative dell'ASST di Mantova per lo scarto della documentazione cartacea secondo le indicazioni di Regione Lombardia e della Soprintendenza Archivistica della Lombardia.
Lo scarto è l'operazione con cui vengono eliminati quei documenti che hanno esaurito la loro validità giuridica o amministrativa e che, allo stesso tempo, non sono considerati di rilevanza storica tale da renderne opportuna la conservazione illimitata.
La periodica eliminazione di tali documenti è funzionale a una ordinata gestione dell'archivio e permette di garantire la conservazione ottimale di quanto si ritiene investito di valore permanente, evitando l'accumulo di masse ingenti di documentazione effimera.

7.5.2 Campo di applicazione

Questa procedura si applica a tutte le strutture, i servizi e le unità operative dell'ASST.

7.5.3 Glossario

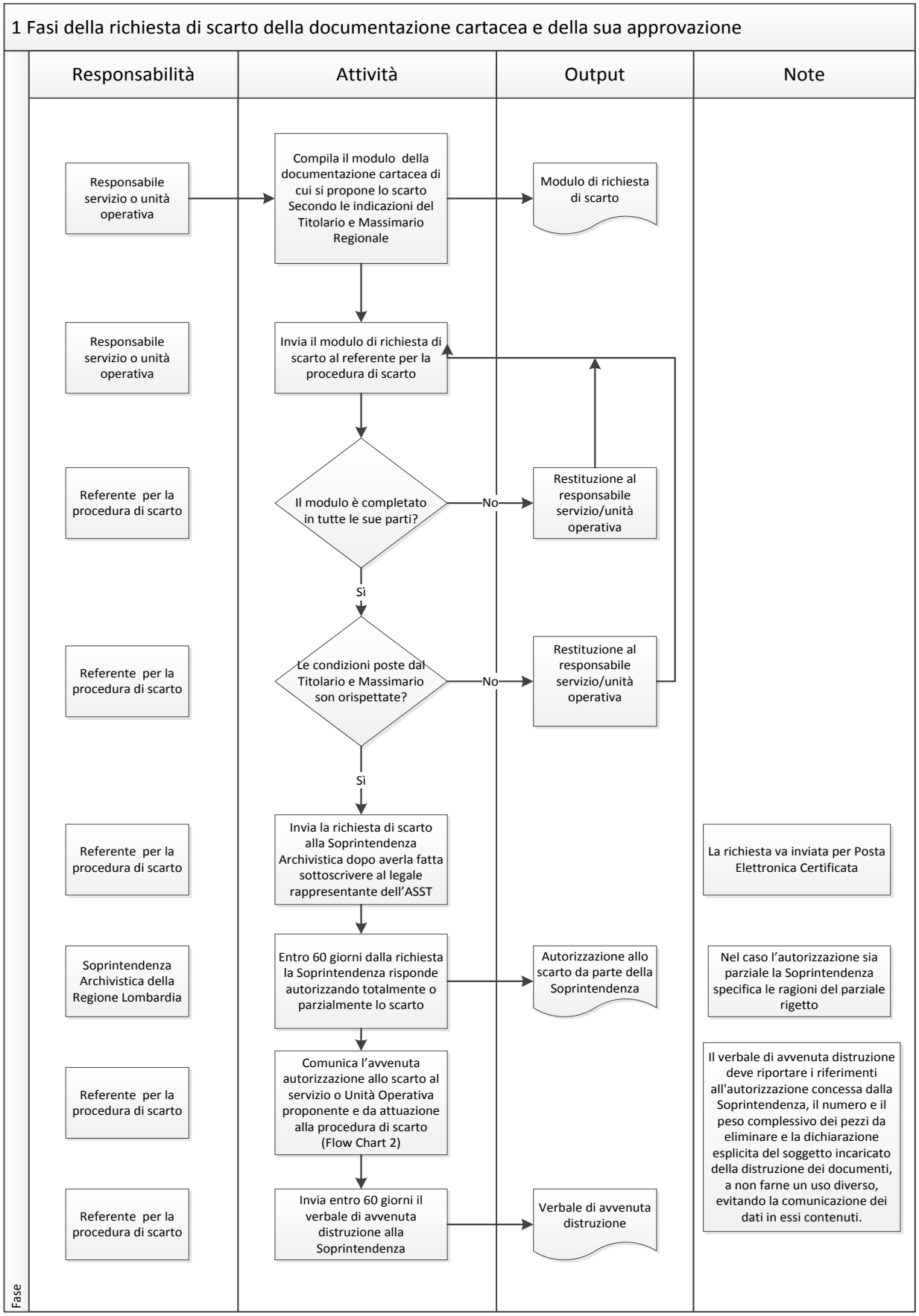
Dati personali	Qualunque informazione relativa a persona fisica, identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale.
Dati sensibili	Qualunque informazione idonea a rilevare l'origine etnica , le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni o organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali a rilevare lo stato di salute e la vita sessuale.
Interessato	Qualunque persona fisica a cui si riferiscono i dati personali
Massimario di selezione/scarto	Strumento che consente di coordinare razionalmente lo scarto legale dei documenti. Il massimario riprende l'organizzazione del Titolario e indica quali documenti conservare e quali destinare alla distruzione
Referto/Documento principale	Documento analogico o digitale relativo ad una prestazione sanitaria, rilasciato dal professionista sanitario, a cui possono essere allegate una o più registrazioni
Referente aziendale per la procedura di scarto	È il responsabile del procedimento amministrativo di scarto dei documenti e rappresenta l'interlocutore unico tra l'ASST di Mantova e la Soprintendenza Archivistica della Lombardia. Il suo compito è coordinare ogni fase della procedura di eliminazione dei documenti a livello aziendale con il supporto dei referenti locali.
Referente locale per la procedura di scarto	operatore che coordina, presso il presidio ospedaliero o il servizio territoriale di appartenenza, la procedura di scarto collaborando con il referente aziendale e il responsale del Servizio/Unità Operativa che propone lo scarto.
Soprintendenza archivistica	è un organo periferico del Ministero dei beni e delle attività culturali e del turismo. Suo compito primario è la tutela e vigilanza degli archivi degli enti

copia informatica per consultazione

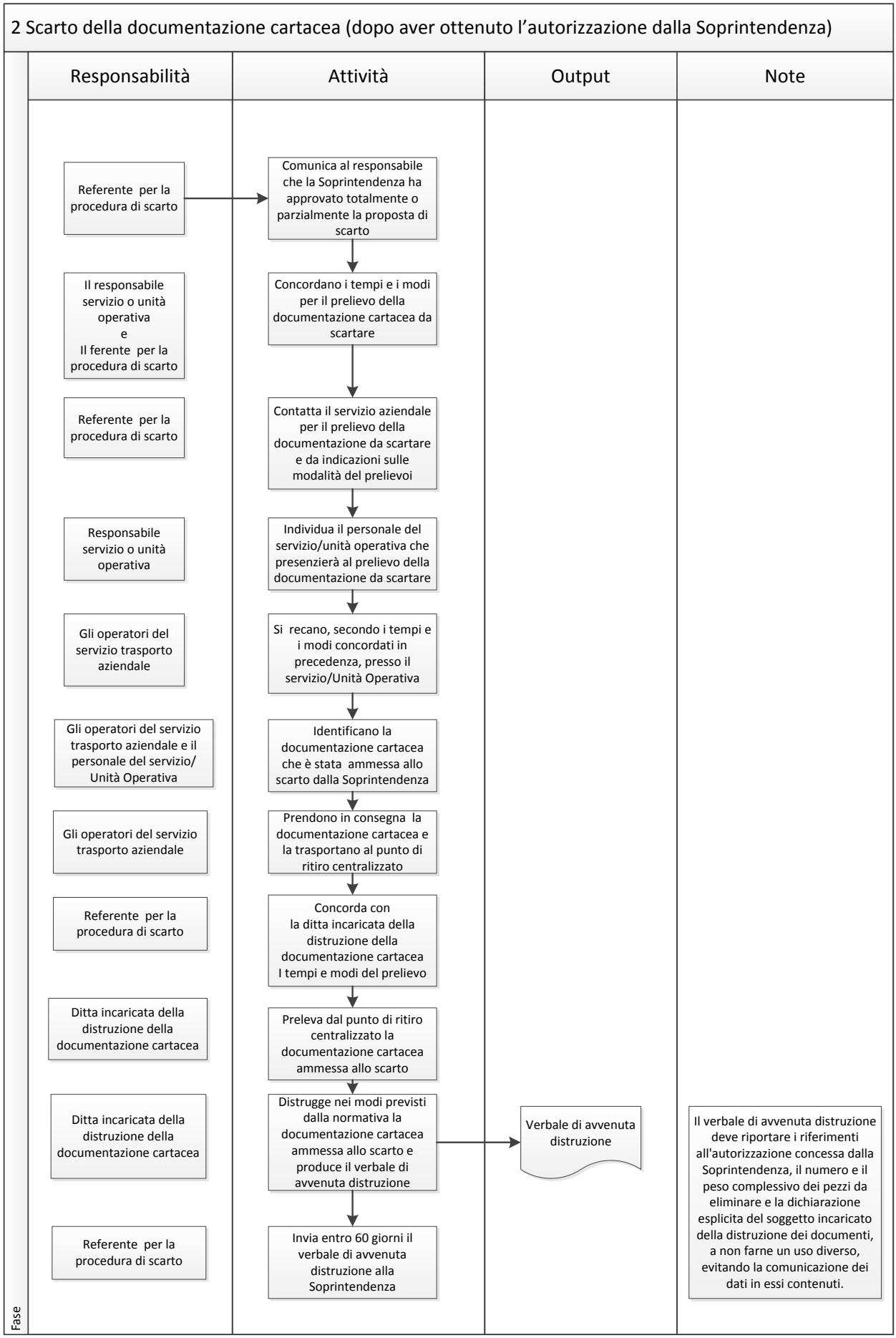
	pubblici territoriali e non, come pure degli archivi o singoli documenti di proprietà privata che siano di particolare interesse storico.
Tempo di conservazione	Intervallo temporale minimo con obbligo di mantenimento in conservazione dei documenti in coerenza con quanto previsto dal massimario di scarto.
Titolario/Quadro di classificazione	Strumento che permette di classificare tutti i documenti secondo un ordinamento logico con riferimento alle funzioni e alle attività dell'amministrazione sanitaria interessata.
Trasporto della documentazione cartacea (addetti al)	Operatori dell'Ufficio Tecnico – Polo Territoriale e/o operatori della ditta appaltatrice

copia informatica per consultazione

7.5.4 Diagrammi di flusso



copia informatica per consultazione



copia informatica per consultazione

7.5.5 Descrizione delle attività

7.5.6 Premessa – la procedura di autorizzazione allo scarto.

L'eliminazione di documenti di archivi pubblici o degli archivi privati per i quali sia intervenuta la dichiarazione di interesse culturale ai sensi del d.lgs. 22 gen. 2004, n. 42,"Codice dei beni culturali e del paesaggio" è soggetta alla preventiva e vincolante autorizzazione della Soprintendenza archivistica, secondo quanto disposto dall'art. 21 del Codice dei beni culturali e del paesaggio relativo agli "interventi soggetti ad autorizzazione" che alla lettera d) include tra tali interventi anche l'operazione di scarto dei documenti d'archivio.

7.5.7 Fasi del procedimento di scarto.

1) Il responsabile del Servizio/Unità Operativa o suo delegato deve elencare utilizzando l'apposito modulo, allegato a questa procedura, la documentazione che propone per lo scarto.
   Tale elenco deve contenere almeno i seguenti dati:
   - classificazione dei documenti di cui si propone lo scarto;
   - descrizione degli atti;
   - estremi cronologici;
   - numero dei pezzi: faldoni, registri, scatole etc.;
   - peso approssimativo;
   - eventuali osservazioni che aiutino a comprendere la motivazione dello scarto.

   In calce alla tabella dovrà anche essere indicata la stima della consistenza in metri lineari, del numero complessivo dei pezzi e del peso complessivo della documentazione di cui si propone lo scarto.
2) L'elenco, sottoscritto dal responsabile del Servizio/Unità Operativa dovrà essere inviato al Referente locale per la procedura di scarto, che dopo averlo controllato lo invierà al Referente aziendale.
3) Il Referente aziendale per la procedura di scarto trasmetterà la richiesta alla Soprintendenza archivistica via PEC con allegata una nota firmata dal Direttore Amministrativo dell'ASST di Mantova o suo delegato.
4) La Soprintendenza ha l'obbligo di concludere il procedimento, entro 60 giorni dalla ricezione della richiesta, fatte salve le richieste di maggiori informazioni sulla proposta di scarto che interrompono il termine del procedimento. L'autorizzazione allo scarto può essere totale o parziale. In questo caso nella risposta della Soprintendenza saranno motivate le ragioni di esclusione dallo scarto dei documenti indicati.
5) Dopo avere ottenuto l'autorizzazione della Soprintendenza archivistica, l'ente che ha proposto lo scarto, dovrà consegnare ad una organizzazione che ne garantisca in modo certo la distruzione, con particolare attenzione ai documenti contenenti dati sensibili.
6) Il verbale di avvenuta distruzione degli atti dovrà riportare i riferimenti all'autorizzazione concessa dalla Soprintendenza, il numero e il peso complessivo dei pezzi da eliminare e la dichiarazione esplicita del soggetto incaricato della distruzione dei documenti, a non farne un uso diverso, evitando la comunicazione dei dati in essi contenuti.
7) Copia del verbale di avvenuta distruzione degli atti, dovrà essere trasmesso alla Soprintendenza archivistica entro 60 giorni, per la conclusione del procedimento.

copia informatica per consultazione

7.5.8 Le unità di misura archivistiche.

Il peso di un metro lineare d'archivio varia a seconda delle dimensioni e della densità dei documenti (1 metro lineare di grossi registri pesa più di 1 metro lineare di piccoli fascicoli).
È tuttavia possibile fornire delle equivalenze medie tra metri lineari, peso e volume degli archivi considerati:

- 1 metro lineare d'archivio = da 35 a 80 kg (media 50 kg)
- 1 metro lineare d'archivio = da 0,06 a 0,12 m^3 (media 0,08 m^3)
- 1 kg d'archivio = da 0,010 a 0,040 ml. (media 0,025 ml .)
- 1 kg d'archivio = da 0,0008 a 0,0030 m^3 (media 0,0016 m^3)
- 1 tonnellata d'archivio = da 10 a 40 ml. (media 25 ml.)
- 1 tonnellata d'archivio = da 0,8 a 3,0 m^3 (media 1, 6 m^3)
- 1 m3 d'archivio = da 8 a 16 ml. (media 12 ml.)
- 1 m^3 d'archivio = da 400 a 800 kg (media 600 kg)

A supporto delle operazioni di stima della quantità in Kg., si riporta la tabella di equivalenza tra metri lineari, peso e volume dei documenti cartacei d'archivio:

Unità di misura archivistica		
1 metro lineare d'archivio	Da 35 a 80 kg (media 50kg)	Da 0,06 a 0,12 m^3 (media 0,08 m^3)
1 kg. d'archivio	Da 0,010 a 0,040 m. (media 0,025 m.)	Da 0,0008 a 0,0030 m^3 (media 0,016)
1 tonnellata d'archivio	Da 10 a 40 m. (media 25 m.)	Da 0,8 a 3,0 m^3 (media 1,6 m^3)
1 m^3 d'archivio	Da 8 a 16 m. (media 12 m.)	Da 400 a 800 kg (media 600 kg)

7.5.9 Riferimenti legislativi e normativi.

- d.p.r. 28 dicembre 2000, n. 445, "*Testo unico sulla documentazione amministrativa*"
- d.p.r. 8 gennaio 2001, n. 37, "*Regolamento di semplificazione dei procedimenti di costituzione e rinnovo delle Commissioni di sorveglianza sugli archivi e per lo scarto dei documenti degli uffici dello Stato (n. 42, allegato 1, della L. n. 50/1999)*"
- d.lgs. 22 gen. 2004, n. 42 "*Codice dei beni culturali e del paesaggio*"
- lettera circolare n. 5/2007 dalla Direzione generale per gli archivi - Ministero per i beni e le attività culturali
- Titolario e Massimario del Sistema Sanitario e Sociosanitario di Regione Lombardia versione 3 approvato con Decreto della Regione Lombardia 17 dicembre 2015, n.11466

Torna al sommario

8 Procedure per la produzione di duplicati o copie

Si rimanda al Manuale di conservazione del conservatore.

copia informatica per consultazione

Torna al sommario

9 Intervento del Pubblico Ufficiale

Si rimanda al Manuale di conservazione del conservatore.

Torna al sommario

10 Sistema di conservazione

Il sistema di conservazione adottato è quello del conservatore. Per la sua descrizione si rimanda al Manuale di conservazione del conservatore.

10.1 Componenti Logiche

Si rimanda al Manuale di conservazione del conservatore.

Torna al sommario

10.2 Componenti Tecnologiche

Si rimanda al Manuale di conservazione del conservatore.

Torna al sommario

10.3 Componenti Fisiche

Si rimanda al Manuale di conservazione del conservatore.

Torna al sommario

10.4 Procedure di gestione e di evoluzione

Si rimanda al Manuale di conservazione del conservatore.

Torna al sommario

11 Monitoraggio e Controlli

I monitoraggi e i controlli sul sistema di conservazione sono operati dal conservatore e descritti nel Manuale di conservazione del conservatore.

11.1 Procedure di monitoraggio

Si rimanda al Manuale di conservazione del conservatore.

Torna al sommario

copia informatica per consultazione

11.2 Verifiche sugli archivi

Si rimanda al Manuale di conservazione del conservatore.

Torna al sommario

11.3 Soluzioni adottate in caso di anomalie

Si rimanda al Manuale di conservazione del conservatore.

Torna al sommario

copia informatica per consultazione