Unione dei comuni
Basso campidano

MANUALE PER LA GESTIONE E LA CONSERVAZIONE DOCUMENTALE

SEZIONE I - DISPOSIZIONI GENERALI

Articolo 1 – Ambito di applicazione

Il presente Manuale di Gestione, adottato ai sensi delle regole tecniche contenute nelle Linee Guida sulla formazione, gestione e conservazione dei documenti informatici, emanate dall'AgID ai sensi dell'art. 71 del D. Lgs. 82/05 (d'ora in poi denominate "Linee guida" o "Regole tecniche"), descrive il sistema di gestione documentale e fornisce le istruzioni per la corretta formazione, gestione, tenuta e conservazione della documentazione analogica e digitale. Esso descrive, altresì, il corretto funzionamento del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi dell'Unione dei Comuni Basso Campidano.

Articolo 2 – Area Organizzativa Omogenea e modello di protocollazione adottato

Ai sensi dell'art. 50, comma 4, del DPR 445/00, per Area Organizzativa Omogenea (AOO) si intende un insieme di uffici e di strutture, da considerare ai fini della gestione unica e coordinata dei documenti, che assicuri uniformità di classificazione, archiviazione e comunicazione interna.
All'interno dell'AOO, l'Unità Organizzativa Responsabile (UOR) è un complesso organizzativo di risorse umane e strumentali cui è stata affidata una competenza omogenea nell'ambito della quale i dipendenti assumono la responsabilità nella trattazione di affari, attività e procedimenti amministrativi.
Ai fini della gestione documentale l'Unione dei Comuni (d'ora in poi denominata anche Unione o Ente) è costituito in un'unica AOO. I dati relativi alla suddetta AOO e l'articolazione della stessa nelle varie UOR sono descritti nell'allegato n. 1 al presente manuale di gestione.
L'AOO e le UOR sono indicate, unitamente alle altre informazioni richieste, nell'Indice delle Pubbliche Amministrazioni (IPA). È compito del Referente IPA dell'Ente provvedere all'accreditamento, alla trasmissione delle informazioni richieste dalla legge e all'aggiornamento dei dati nel sito IPA.
Nell'ambito dell'AOO è predisposto un servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi, secondo le modalità previste dall'art. 3 del presente manuale.
Il Sistema di protocollo informatico o Sistema di Gestione Informatica dei Documenti (SGID), utilizzato per la registrazione dei documenti, è unico nell'ambito dell'AOO.
Il modello di protocollazione adottato dall'Unione è decentrato, in quanto la protocollazione in arrivo, in partenza e la registrazione dei protocolli interni sono svolte dagli operatori delle varie Unità Organizzative dell'Ente, ciascuno per la documentazione di propria competenza.
Il Responsabile della gestione documentale (RGD) provvede ad assegnare le abilitazioni all'accesso e all'utilizzo delle funzioni del Sistema di Gestione Informatica dei Documenti dell'Unione; tali abilitazioni sono riportate nell'allegato n. 2 del presente manuale.

Articolo 3 – Servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi

Nell'ambito dell'Unione, ai sensi dell'art. 61, comma 1, del DPR 445/00, è stato istituito un Servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi, funzionalmente inserito nell'Area Amministrativa dell'Ente.
Il Servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi garantisce la corretta gestione, tenuta e tutela dei documenti e vigila sulla corretta applicazione della normativa in materia di gestione documentale durante l'intero ciclo di vita dei documenti medesimi.
Conformemente ai requisiti previsti dal medesimo art. 61, comma 2, del DPR 445/00 e alle Linee guida AgID, è nominato un Responsabile della gestione documentale e un suo vicario per i casi di vacanza, assenza o impedimento del suddetto responsabile.
Conformemente alle medesime Linee guida è, infine, nominato un Responsabile della conservazione.
Al Responsabile della gestione documentale sono affidati i compiti di cui all'art. 61, comma 3, del DPR 445/00 e quelli previsti dalle linee guida AgID; in particolare:

- attribuisce i livelli di autorizzazione degli utenti per l'accesso alle funzioni del Sistema di Gestione Informatica dei Documenti, assegnando profili abilitati alla mera consultazione, all'inserimento o alla modifica delle informazioni, sulla base delle richieste provenienti dal Responsabile di ciascuna UOR;
- garantisce che le operazioni di registrazione, di segnatura di protocollo, di gestione dei documenti e dei flussi documentali, si svolgano nel rispetto della normativa vigente e di quanto indicato nel presente manuale di gestione;
- 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;

- autorizza l'utilizzo del registro di emergenza per le registrazioni di protocollo, nei casi e secondo le modalità previste dall'art. 63 del DPR 445/00;
- autorizza l'annullamento delle registrazioni di protocollo secondo quanto disposto dall'art. 54 del DPR 445/00;
- garantisce il buon funzionamento del Sistema di Gestione Informatica dei Documenti, la formazione e la gestione dell'archivio digitale dell'Ente, nonché la corretta conservazione degli archivi cartacei;
- predispone, d'intesa con il Responsabile della conservazione, il Responsabile per la transizione digitale e acquisito il parere del Responsabile della protezione dei dati personali, il manuale di gestione documentale e il piano di sicurezza (allegato n. 3 del presente manuale) 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 dal manuale di conservazione;
- predispone l'aggiornamento del manuale di gestione, seguendo le modalità di revisione previste dall'articolo 57 del presente manuale;
- cura la pubblicazione del manuale di gestione sul sito internet istituzionale dell'Unione nella sezione "Amministrazione trasparente";
- assicura la corretta produzione del registro giornaliero di protocollo e la sua trasmissione al sistema di conservazione entro la giornata lavorativa successiva, garantendone, inoltre, l'immodificabilità del contenuto;
- predispone il pacchetto di versamento e ne assicura la trasmissione al sistema di conservazione secondo le modalità operative definite nel manuale di conservazione, stabilendo i tempi entro cui i documenti, i fascicoli e le aggregazioni documentali informatiche debbano essere versati in conservazione;
- verifica, infine, il buon esito dell'operazione di versamento, tramite la presa visione del rapporto di versamento prodotto dal sistema di conservazione.

Il Responsabile della conservazione, nei limiti e secondo le modalità previste nel contratto di affidamento del servizio, delega formalmente lo svolgimento del processo di conservazione digitale ad un soggetto conservatore esterno, accreditato dall'Agenzia per l'Italia Digitale (AgID) e fornisce le indicazioni utili alla definizione delle politiche del sistema di conservazione, vigilando periodicamente sull'espletamento dell'attività svolta da parte del soggetto conservatore.
Il Responsabile della Conservazione opera d'intesa con il Responsabile della gestione documentale, il Responsabile per la transizione digitale e il Responsabile della protezione dei dati personali nella predisposizione del manuale di gestione documentale.

Articolo 4 – Sistema di Gestione Informatica dei Documenti

Il Sistema di Gestione Informatica dei Documenti (SGID) è costituito dall'insieme delle risorse di calcolo, degli apparati, delle reti di comunicazione e delle procedure informatiche utilizzati dalle amministrazioni per la gestione dei documenti, come specificato dall'art. 1, comma 1, lett. r), del DPR 445/00.
Il Sistema di Gestione Informatica dei Documenti adottato dall'Unione è integrato funzionalmente con la casella istituzionale di posta elettronica certificata (PEC), eletta a domicilio digitale dell'Ente e con la casella istituzionale di posta elettronica convenzionale.
Conformemente ai disposti dell'articolo 52 del DPR 445/00 e delle Linee guida AgID il Sistema SGID:

- garantisce la "funzionalità minima" del protocollo informatico che, ai sensi dell'art. 56 del DPR 445/00, comprende le operazioni di registrazione, segnatura di protocollo e classificazione dei documenti;
- è dotato delle funzionalità necessarie a garantirne la sicurezza e l'integrità;
- fornisce informazioni sul collegamento esistente tra ciascun documento ricevuto dall'amministrazione e i documenti dalla stessa formati nell'adozione dei provvedimenti finali (fascicolazione);
- consente il reperimento delle informazioni riguardanti i documenti registrati;
- assicura l'univoca identificazione ed autenticazione degli utenti;
- assicura la registrazione delle attività rilevanti ai fini della sicurezza e consente il tracciamento di qualsiasi evento di modifica delle informazioni trattate, individuandone l'autore, la data, l'ora e impedendo che tali registrazioni possano essere modificate senza autorizzazione;
- consente l'accesso al sistema, ai documenti e alle informazioni contenute, in condizioni di sicurezza, mediante la definizione di specifici livelli di abilitazione per gli utenti interessati, nel rispetto della normativa vigente in materia di trattamento dei dati personali;
- rispetta le misure di sicurezza volte a garantire quanto sancito dal D. Lgs. 196/03 e dal Regolamento (UE) 2016/679, in materia di protezione di dati personali, sensibili e giudiziari.

Il Sistema di Gestione Informatica dei Documenti consente inoltre:

- la produzione del registro giornaliero di protocollo conformemente a quanto disposto dall'art. 53, comma 2, del DPR 445/00 e dalle Linee guida;

- la registrazione e la trasmissione tra gli uffici dei documenti amministrativi prodotti internamente con i relativi metadati, permettendo il tracciamento di tutte le attività svolte;
- lo scambio di documenti tra le pubbliche amministrazioni secondo i meccanismi di interoperabilità;
- la produzione del pacchetto di versamento con tutti i metadati previsti dalle Linee guida AgID, al fine del trasferimento dei documenti digitali al soggetto conservatore accreditato AgID di cui l'Unione si serve.

Articolo 5 – Piano di sicurezza

Il manuale di gestione documentale, ai sensi delle Linee guida AgID, contiene il piano di sicurezza informatica relativo alle opportune misure tecniche e organizzative per garantire un livello di sicurezza adeguato al rischio anche in materia di protezione dei dati personali.
Tale piano è predisposto dal Responsabile della gestione documentale, d'intesa con il Responsabile della conservazione, il Responsabile per la transizione digitale e sentito il Responsabile della protezione dei dati personali ed è volto a garantire quanto sancito, in materia di protezione dei dati personali, sensibili e giudiziari, dal D. Lgs. 196/03 e dal Regolamento (UE) 2016/679.
Conformemente a quanto previsto dall'articolo 51, comma 2, del D. Lgs. 82/05, il piano adotta misure di sicurezza tali da ridurre al minimo i rischi di distruzione, perdita, accesso non autorizzato, trattamento non consentito e non conforme alle finalità della raccolta dei dati contenuti all'interno del Sistema; in particolare:

- assicura che le informazioni e i dati siano disponibili, integri e protetti secondo il loro livello di riservatezza;
- garantisce che siano mantenute le caratteristiche di autenticità, integrità, affidabilità, leggibilità e reperibilità dei documenti e dei fascicoli informatici.

SEZIONE II – FORMAZIONE DEI DOCUMENTI

Articolo 6 – Disposizioni generali sulla produzione dei documenti

Ai sensi dell'art. 22, comma 1, lettera d), della L. 241/90 per documento amministrativo si intende ogni rappresentazione, grafica, fotocinematografica, elettromagnetica o di qualunque altra specie, del contenuto di atti, anche interni o non relativi ad uno specifico procedimento, formati dalle pubbliche amministrazioni o, comunque, da queste ultime utilizzati ai fini dell'attività amministrativa (siano essi documenti informatici o analogici).
Ai sensi dell'art. 1, comma 1, lettera p), del D. Lgs. 82/05 per documento informatico si intende la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti. Il documento informatico è, quindi, un file, cioè una sequenza determinata di valori binari indifferente al supporto fisico su cui è memorizzata.
Il documento analogico è, invece, la rappresentazione non informatica, di atti, fatti o dati giuridicamente rilevanti. Qualsiasi documento non informatico (ad es. un documento cartaceo) è, dunque, un documento analogico.
Ai sensi dell'art. 23-ter del D. Lgs. 82/05 per documenti amministrativi informatici si intendono, gli atti formati dalle pubbliche amministrazioni con strumenti informatici, nonché i dati e i documenti informatici detenuti dalle stesse.
L'Unione, nello svolgimento delle proprie attività istituzionali, predispone i propri documenti utilizzando sistemi informativi automatizzati.
I documenti prodotti dall'Unione su supporto informatico, sono prodotti nel rispetto delle regole tecniche emanate ai sensi dell'art. 71 del D. Lgs. 82/05 (Linee Guida AgID), conformemente alle modalità previste dal presente manuale.
Ciascun documento formato dall'Unione, sia esso interno o da trasmettere all'esterno, tratta un unico argomento.

Articolo 7 – Informazioni minime del documento prodotto dall'Unione

Le informazioni minime presenti nei documenti prodotti dall'Unione sono le seguenti:

- denominazione e stemma ufficiale dell'Unione;
- indicazione dell'AOO e dell'ufficio che ha prodotto il documento;
- indirizzo completo comprensivo di numero di telefono, fax e casella istituzionale di posta elettronica certificata (domicilio digitale dell'Ente);
- indicazione di luogo e data di formazione del documento;
- numero e data di protocollo, se soggetto a registrazione;
- oggetto;
- riferimenti ad eventuali documenti precedenti;
- sottoscrizione a cura del Responsabile, o dei responsabili, del procedimento;
- indicazione del destinatario qualora si tratti di documento in uscita.

Articolo 8 – Produzione dei documenti informatici

Il documento informatico presenta le caratteristiche di immodificabilità e integrità in modo tale che forma e contenuto dello stesso non siano alterabili durante le fasi di tenuta, accesso e conservazione.
I documenti informatici sono prodotti dall'Unione mediante una delle seguenti modalità:

- redazione tramite l'utilizzo di appositi strumenti software. In tal caso il documento informatico assume le caratteristiche di immodificabilità e di integrità attraverso uno dei seguenti modi: 1) sottoscrizione con firma digitale/firma elettronica qualificata; 2) trasferimento a soggetti terzi tramite PEC o servizio elettronico di recapito certificato qualificato ai sensi del Regolamento UE n. 910 del 23 luglio 2014; 3) memorizzazione su sistemi di gestione documentale che adottino idonee politiche di sicurezza; 4) versamento ad un sistema di conservazione;
- acquisizione di un documento informatico per via telematica o su supporto informatico o acquisizione della copia per immagine su supporto informatico di un documento analogico ovvero acquisizione della copia informatica di un documento analogico. Nei suddetti casi le caratteristiche di immodificabilità e di integrità sono determinate da: 1) sottoscrizione con firma digitale/firma elettronica qualificata; 2) memorizzazione su sistemi di gestione documentale che adottino idonee politiche di sicurezza; 3) versamento ad un sistema di conservazione;
- memorizzazione su supporto informatico in formato digitale delle informazioni risultanti da transazioni o processi informatici o dalla presentazione di dati attraverso moduli o formulari resi disponibili all'utente. Nei suddetti casi le caratteristiche di immodificabilità e di integrità sono determinate da: 1) apposizione di firma digitale/firma elettronica qualificata; 2) registrazione nei log di sistema dell'esito dell'operazione di formazione del documento informatico, compresa l'applicazione di misure per la protezione dell'integrità delle basi di dati e per la produzione e conservazione dei log di sistema; 3) produzione di una estrazione statica dei dati e il trasferimento della stessa nel sistema di conservazione;
- 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. In tal caso le caratteristiche di immutabilità e di integrità sono determinate con le stesse modalità descritte nel caso precedente.

I documenti informatici prodotti dall'Unione contengono le informazioni minime elencate nel precedente art. 7; il Sistema SGID manterrà il collegamento tra il documento e i dati inseriti in fase di protocollazione, ivi incluso il numero di protocollo assegnato.
I formati elettronici utilizzati dall'Unione per la produzione dei documenti informatici, anche ai fini della conservazione:

- sono conformi a quanto disposto dalle Linee guida AgID;
- sono aperti, completamente documentati e preferibilmente riconosciuti come standard da organismi internazionali;
- sono indipendenti da specifiche piattaforme tecnologiche hardware e software;
- non possono contenere macroistruzioni o codice eseguibile;
- sono ampiamente adottati;
- sono preferibilmente stabili e non soggetti a continue modificazioni nel tempo;
- sono preferibilmente utilizzabili con versioni precedenti e successive dell'applicativo software che li ha prodotti;
- sono privi di meccanismi tecnici di protezione che possano impedirne la replica del contenuto su nuovi supporti o la possibilità di effettuare migrazioni, pregiudicandone la fruibilità nel lungo periodo a causa dell'obsolescenza tecnologica;
- permettono la fruizione anche ad utenti diversamente abili.

I formati elettronici utilizzati dall'Unione sono elencati nell'allegato n. 4 del presente manuale.

Articolo 9 – Sottoscrizione dei documenti informatici

La sottoscrizione dei documenti informatici prodotti dall'Unione avviene in conformità di quanto previsto dal D. Lgs. 82/05 e dalle Regole tecniche emanate ai sensi del medesimo.
Il documento informatico sottoscritto con firma elettronica avanzata, qualificata o digitale, formato nel rispetto delle suddette regole tecniche contenute nelle Linee guida AgID, che garantisca, pertanto, l'identificabilità dell'autore, l'integrità e l'immodificabilità del documento, ha l'efficacia della scrittura privata prevista dall'articolo 2702 del Codice Civile.
Il documento informatico privo di sottoscrizione è una copia informatica e, come tale, forma piena prova dei fatti e delle cose rappresentate, se colui contro il quale è prodotta non ne disconosce la conformità ai fatti o alle cose medesime, secondo quanto disposto dagli artt. 2712 e 2713 del Codice Civile e l'art. 23-quater del D. Lgs. 82/05.

L'associazione a un documento informatico di una firma digitale o di un altro tipo di firma elettronica qualificata basata su un certificato elettronico revocato, scaduto o sospeso equivale a mancata sottoscrizione; tuttavia le firme elettroniche qualificate e digitali, ancorché sia scaduto, revocato o sospeso il relativo certificato qualificato del sottoscrittore, sono valide se alle stesse è associabile un riferimento temporale opponibile ai terzi, prodotto secondo le modalità descritte nell'art. 14 del presente manuale, che collochi la generazione di dette firme rispettivamente in un momento precedente alla scadenza, revoca o sospensione del suddetto certificato.
Il dispositivo per la generazione della firma elettronica qualificata o della firma digitale è usato esclusivamente dal titolare designato dall'Unione; ai sensi della normativa vigente tale utilizzo si presume comunque riconducibile al titolare, salvo che questi dia prova contraria.
Se prodotte sotto forma di documento originale informatico, devono essere sottoscritte a pena di nullità, con firma elettronica qualificata o digitale, le seguenti tipologie documentali:

- Deliberazioni del Consiglio Comunale, della Giunta Comunale e del Commissario Prefettizio;
- Decreti;
- Ordinanze;
- Determinazioni;
- Contratti e atti rogati o autenticati dal Segretario Comunale;
- Circolari;
- Ordini di servizio;
- Mandati di pagamento;
- Reversali;
- Qualsiasi altra tipologia documentale avesse richiesto la firma autografa qualora redatta nella forma di documento originale analogico.

L'utilizzo da parte dell'Unione delle varie tipologie di sottoscrizioni elettroniche avviene nei casi e con le modalità disposte dagli articoli 10, 11, 12 e 13 del presente manuale.

Articolo 10 – Firma elettronica

Per firma elettronica si intende l'insieme dei dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati elettronici e utilizzati dal firmatario per firmare; ovvero i dati elettronici di identificazione informatica del soggetto che compie una determinata operazione.
Come firma elettronica (c.d. firma elettronica "debole") l'Unione adotta la User-Id e la Password per l'accesso al Sistema da parte degli utenti interni.
Ai sensi dell'art. 20, comma 1-bis, del D. Lgs. 82/05, il documento informatico, cui è apposta una firma elettronica "debole" soddisfa il requisito della forma scritta e sul piano probatorio è liberamente valutabile in giudizio, tenuto conto delle sue caratteristiche oggettive di qualità, sicurezza, integrità e immodificabilità.
Le credenziali di identificazione (User-Id e Password) utilizzate per accedere al Sistema di Gestione Informatica dei Documenti dell'Unione costituiscono una firma elettronica "debole" e devono essere utilizzate esclusivamente dal soggetto cui sono state assegnate; tale tipologia di sottoscrizione è abilitata solo nelle comunicazioni e nelle registrazioni dove è sufficiente l'identificazione informatica del soggetto che le esegue.
Per quanto concerne l'identificazione degli utenti esterni, l'Unione provvede all'implementazione del sistema SPID al fine di permettere l'identificazione degli utenti esterni che accedano a servizi erogati direttamente on-line, mediante l'utilizzo del Sistema pubblico dell'Identità digitale di cittadini ed imprese (SPID) e la CIE;

Articolo 11 – Firma elettronica avanzata

Per firma elettronica avanzata si intende un tipo di firma elettronica che è idonea ad identificare il firmatario del documento e garantisce la connessione univoca della firma al firmatario. La firma elettronica avanzata è creata mediante dati che il firmatario può, con un elevato livello di sicurezza, utilizzare sotto il proprio esclusivo controllo ed è collegata ai dati sottoscritti in modo da consentire l'identificazione di ogni successiva modifica di tali dati.
I documenti sottoscritti con firma elettronica avanzata hanno l'efficacia prevista dall'art. 2702 del Codice Civile se la soluzione di firma garantisce:

- l'identificazione del firmatario del documento;
- la connessione univoca della firma al firmatario;
- il controllo esclusivo del firmatario del sistema di generazione della firma, ivi inclusi i dati biometrici eventualmente utilizzati per la generazione della firma medesima;
- la possibilità di verificare che il documento informatico sottoscritto non abbia subito modifiche dopo l'apposizione della firma;
- la possibilità per il firmatario di ottenere evidenza di quanto sottoscritto;
- l'individuazione del soggetto che eroga la soluzione di firma elettronica avanzata;

- l'assenza di qualunque elemento nell'oggetto della sottoscrizione atto a modificarne il contenuto;
- la connessione univoca della firma al documento sottoscritto.

L'invio di dichiarazioni e istanze da una casella di posta elettronica certificata (PEC) eletta a domicilio digitale, ovvero l'inoltro telematico di dichiarazioni e istanze sottoscritte e presentate unitamente alla copia del documento d'identità, sostituiscono nei confronti della Pubblica Amministrazione la firma elettronica avanzata; pertanto i documenti che pervengano all'Unione utilizzando la suddetta modalità, ai sensi dell'art. 65, comma 2, del D. Lgs. 82/05, sono equivalenti a quelli sottoscritti con firma autografa apposta in presenza del dipendente addetto al procedimento.

Articolo 12 – Firma elettronica qualificata

Per firma elettronica qualificata si intende una firma elettronica avanzata generata da un dispositivo per la creazione di una firma elettronica qualificata e basata su un certificato qualificato per firme elettroniche.
La soluzione di firma elettronica qualificata adottata dall'Unione è la firma digitale.

Articolo 13 – Firma digitale

Per firma digitale si intende, ai sensi dell'art. 1, comma 1, lettera s), del D. Lgs. 82/05, quel particolare tipo di firma elettronica qualificata basata su un certificato qualificato e su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consenta al titolare tramite la chiave privata e ad un soggetto terzo 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. Ai sensi dell'art. 24, comma 2, del D. Lgs. 82/05 l'apposizione di firma digitale integra e sostituisce l'apposizione di sigilli, punzoni, timbri, contrassegni e marchi di qualsiasi genere ad ogni fine previsto dalla normativa vigente.
I documenti informatici elencati all'art. 9 del presente manuale, prodotti dall'Unione nello svolgimento della propria attività istituzionale sono sottoscritti dai responsabili del procedimento con firma digitale conforme alla normativa vigente.
La sottoscrizione con firma digitale di documenti informatici prodotti dall'Unione avviene previa conversione dei suddetti documenti in uno dei formati elettronici idonei alla conservazione digitale.
Il titolare del dispositivo di firma digitale:

- assicura la custodia del dispositivo sicuro per la generazione della firma in suo possesso e adotta le misure di sicurezza fornite dal prestatore di servizi di firma elettronica qualificata, al fine di adempiere agli obblighi di cui all'art. 32, comma 1, del D. Lgs. 82/05;
- conserva le informazioni di abilitazione all'uso della chiave privata separatamente dal dispositivo contenente la chiave e segue le indicazioni fornite dal prestatore di servizi di firma elettronica qualificata;
- richiede immediatamente la revoca del certificato qualificato relativo alle chiavi contenute nel dispositivo sicuro per la generazione della firma digitale inutilizzabile o di cui abbia perduto il possesso o il controllo esclusivo;
- salvo quanto previsto dalle disposizioni di legge in materia di firma remota, mantiene in modo esclusivo la conoscenza o la disponibilità di almeno uno dei dati per la creazione della firma elettronica qualificata o digitale;
- richiede immediatamente la revoca del certificato qualificato relativo alle chiavi contenute nel dispositivo sicuro per la generazione della firma digitale qualora abbia il ragionevole dubbio che possa essere usato da altri.

Articolo 14 – Validazione temporale dei documenti sottoscritti con firma digitale

I documenti informatici, sottoscritti con firma elettronica qualificata o con firma digitale, necessitano di un riferimento temporale che attesti il momento in cui la sottoscrizione è stata apposta. Attraverso una validazione temporale, costituita da dati in forma elettronica che collegano altri dati in forma elettronica a una particolare ora e data, si dà evidenza che questi ultimi esistevano in quel momento; in tal modo si attribuisce al suddetto documento una data ed un orario certi opponibili ai terzi.
Detto riferimento temporale viene attribuito al documento per mezzo della generazione e dell'applicazione di una marca temporale elettronica qualificata, rilasciata da un prestatore di servizi fiduciari qualificati, secondo quanto previsto dagli articoli 41 e 42 del Regolamento Europeo 2014/n.910 - EIDAS; costituiscono, altresì, validazione temporale in linea con i requisiti sanciti dal suddetto art. 42:

- il riferimento temporale contenuto nella segnatura di protocollo;
- il riferimento temporale ottenuto attraverso la procedura di conservazione dei documenti in conformità alle norme vigenti, ad opera di un pubblico ufficiale o di una pubblica amministrazione;
- il riferimento temporale ottenuto attraverso l'utilizzo della posta elettronica certificata;
- il riferimento temporale ottenuto attraverso l'utilizzo della marcatura postale elettronica.

Articolo 15 – Copie informatiche di documenti analogici

Le copie su supporto informatico di documenti formati dalla Pubblica Amministrazione in origine su supporto analogico ovvero da essa detenuti hanno, ai sensi dell'articolo 23-ter, comma 3, del D. Lgs. 82/05, il medesimo valore giuridico, ad ogni effetto di legge, degli originali da cui sono tratte, se la loro conformità all'originale è assicurata dal funzionario a ciò delegato nell'ambito dell'ordinamento proprio dell'amministrazione di appartenenza, mediante l'utilizzo della firma digitale o di altra firma elettronica qualificata e nel rispetto di quanto stabilito dalle regole tecniche emanate in materia; in tale caso l'obbligo di conservazione dell'originale del documento è soddisfatto con la conservazione della copia su supporto informatico, salvo il caso di documenti analogici originali unici individuati ai sensi del DPCM 21/03/2013 "Individuazione di particolari tipologie di documenti analogici originali unici"; l'Unione conserva comunque l'originale cartaceo nel proprio archivio.
Le copie per immagine, su supporto informatico, di documenti in origine formati su supporto analogico nonché le copie e gli estratti informatici di documenti originariamente analogici, vengono prodotti dall'Unione utilizzando i formati idonei alla conservazione previsti dalla vigente normativa.
Le suddette copie per immagine sono prodotte per mezzo di processi e strumenti che assicurino il mantenimento di contenuto e forma identici a quelli del documento analogico da cui sono tratte. L'efficacia probatoria delle stesse è la medesima degli originali da cui provengono se la conformità ad essi non è espressamente disconosciuta.
Nell'ambito dell'Unione, le copie per immagine su supporto informatico di documenti originariamente analogici vengono sottoscritti con firma digitale dal pubblico ufficiale preposto a rilasciare le copie.
Laddove richiesta dalla natura dell'attività, l'attestazione di conformità delle copie per immagine su supporto informatico di un documento originariamente analogico, sarà inserita nello stesso documento informatico contenente la copia per immagine; il documento in tal modo prodotto sarà sottoscritto con firma digitale del pubblico ufficiale a ciò autorizzato.
Gli estratti e le copie informatiche, non per immagine, di documenti amministrativi analogici devono garantire, previo raffronto dei documenti, la corrispondenza del contenuto a quello dell'originale. Il pubblico ufficiale preposto al rilascio della copia inserisce la dichiarazione di conformità nel documento contenente la copia informatica, sottoscrivendolo con firma digitale.

Articolo 16 – Copie analogiche di documenti informatici

Ai sensi dell'art. 23 del D. Lgs. 82/05, le copie analogiche di documenti informatici hanno la stessa efficacia probatoria dell'originale da cui sono tratte se la loro conformità all'originale in tutte le sue parti è attestata da un pubblico ufficiale a ciò autorizzato e non è espressamente disconosciuta.
Ai sensi dell'art. 23, comma 2-bis del D. Lgs. 82/05, sulle copie analogiche di documenti informatici può essere apposto un contrassegno elettronico a stampa, tramite il quale è possibile accedere al documento informatico originale, ovvero verificare la corrispondenza allo stesso della copia analogica; tale contrassegno sostituisce a tutti gli effetti di legge la sottoscrizione autografa del pubblico ufficiale e non può essere richiesta la produzione di altra copia analogica con sottoscrizione autografa del medesimo documento informatico.
Ai fini della conservazione l'Unione procede al mantenimento dell'originale informatico.

Articolo 17 – Duplicati e copie informatiche di documenti informatici

Ai sensi dell'art. 23-bis del D. Lgs. 82/05, i duplicati informatici, se prodotti in conformità di quanto previsto dal successivo capoverso, hanno il medesimo valore giuridico, ad ogni effetto di legge, del documento informatico da cui sono tratti.
Il duplicato viene prodotto mediante processi e strumenti che assicurino che il documento informatico ottenuto sullo stesso sistema di memorizzazione, o su un sistema diverso, contenga la stessa sequenza di bit del documento informatico di origine.
Le copie e gli estratti informatici di un documento informatico, prodotti utilizzando i formati previsti nell'allegato n. 4 del presente manuale e mediante processi e strumenti che assicurino la corrispondenza del contenuto della copia o dell'estratto informatico a quello del documento informatico da cui sono tratti, hanno la stessa efficacia probatoria dell'originale, se sottoscritti con firma digitale da parte di chi li ha prodotti, salvo che la conformità all'originale non sia espressamente disconosciuta.
Laddove richiesto dalla natura dell'attività, l'attestazione di conformità della copia o dell'estratto informatico all'originale è inserita nel documento contenente la copia o l'estratto; il documento in tal modo prodotto è sottoscritto con firma digitale da parte del pubblico ufficiale a ciò autorizzato.
Ai fini della conservazione, l'Unione mantiene l'originale informatico.

SEZIONE III – RICEZIONE DEI DOCUMENTI

Articolo 18 – Ricezione di documenti cartacei

I documenti cartacei possono pervenire all'Unione attraverso le seguenti modalità:

- il servizio postale gestito da Poste Italiane Spa o altro gestore autorizzato;
- la consegna diretta, brevi manu, ai vari uffici dell'AOO;
- gli apparecchi telefax.

I documenti ricevuti mediante il servizio postale tradizionale vengono consegnati giornalmente al personale preposto alla protocollazione dei documenti in arrivo.
I documenti consegnati direttamente ai vari uffici della AOO, se soggetti all'obbligo della registrazione di protocollo, vengono presi in carico dal personale che li riceve e da questi fatti pervenire, nell'arco della stessa giornata lavorativa, ai suddetti operatori.
I documenti pervenuti tramite telefax vengono trattati con le stesse modalità degli altri documenti cartacei in arrivo; corre l'obbligo, tuttavia, di sottolineare che, ai sensi dell'art. 47, comma 2, lettera c), del D. Lgs. 82/05 non è ammessa la trasmissione dei documenti a mezzo fax tra le pubbliche amministrazioni.
Qualora all'atto della consegna diretta di un documento cartaceo venga richiesto il rilascio di una ricevuta, l'ufficio a cui è stato presentato il documento rilascia una fotocopia del primo foglio su cui è apposta la sigla dell'addetto a cui tale documento è stato consegnato e un timbro che attesti la data di arrivo. Se la consegna è effettuata direttamente al personale che esegue la protocollazione, l'addetto rilascerà, invece, la ricevuta contenente i dati di protocollo.
La protocollazione dei documenti cartacei in arrivo viene eseguita con le modalità descritte dall'art. 23 del presente manuale, mentre la scansione del documento per l'acquisizione dell'immagine da allegare a detta registrazione avviene secondo le modalità descritte dal successivo art. 40.

Articolo 19 – Ricezione di documenti informatici

Ai sensi dell'art. 45, comma 1, del D. Lgs. 82/05, i documenti trasmessi da chiunque ad una pubblica amministrazione con qualsiasi mezzo telematico o informatico, idoneo ad accertarne la fonte di provenienza, soddisfano il requisito della forma scritta.
Al fine di soddisfare il suddetto requisito, i documenti informatici sono, di norma, acquisiti dal Sistema di Gestione Informatica dei Documenti dell'Unione mediante la casella PEC istituzionale, presso cui è eletto il domicilio digitale dell'Ente;
La posta elettronica certificata garantisce la certezza della provenienza e l'integrità dei documenti ricevuti.
La casella PEC attivata dall'Unione è stata comunicata all'Agenzia per l'Italia digitale (AgID) al fine di essere inserita nell'Indice dei domicili digitali delle Pubbliche Amministrazioni (IPA); l'Unione ha cura di comunicare tempestivamente e almeno con cadenza semestrale le eventuali variazioni.
La suddetta casella di posta elettronica certificata è integrata funzionalmente con il Sistema di Gestione Informatica dei Documenti, in modo tale che si formi una "coda" della corrispondenza in arrivo che permetta la registrazione di protocollo e l'acquisizione sul Sistema di tutti i documenti ricevuti; tale "coda" è resa accessibile al personale abilitato ad eseguire la registrazione di protocollo dei documenti in arrivo.
Qualora i documenti pervenuti tramite PEC siano le ricevute di avvenuta consegna rilasciate dal gestore del servizio di posta elettronica certificata relative a documenti spediti dall'AOO o i messaggi di ritorno generati automaticamente dai sistemi di gestione documentale delle amministrazioni destinatarie di una spedizione, il Sistema procede automaticamente alla loro archiviazione, collegandoli alla registrazione di protocollo cui si riferiscono. Se le ricevute di posta elettronica certificata si riferiscono a situazioni di anomalia come, ad esempio, il mancato recapito di una spedizione, il Sistema notifica l'evento al personale responsabile.
I documenti informatici provenienti da altre pubbliche amministrazioni possono essere recapitati all'Unione sia attraverso la suddetta casella PEC, sia utilizzando i meccanismi di interoperabilità di cui al Sistema Pubblico di Connettività e Cooperazione (SPC), utilizzando le informazioni contenute nella segnatura di protocollo, nel rispetto di quanto previsto dalla normativa vigente.
Qualora si verifichi il caso in cui un documento informatico, soggetto alla registrazione di protocollo, pervenga agli uffici dell'Unione utilizzando una modalità diversa da quelle esposte precedentemente si procede nei seguenti modi:

- nel caso di consegna diretta di un documento memorizzato su un supporto rimovibile o qualora un documento pervenga all'Unione attraverso la casella istituzionale di posta elettronica convenzionale, si procede alla valutazione dello stesso e, accertatane la provenienza, si procede alla protocollazione;
- nel caso in cui un documento pervenga all'Unione attraverso un'altra eventuale casella di posta elettronica convenzionale che dovesse essere attivata, accertatane la provenienza, il documento viene inoltrato alla casella istituzionale di posta elettronica convenzionale di cui sopra al fine di permetterne la protocollazione.

Tali eventualità devono comunque essere disincentivate e costituire un'eccezione rispetto all'utilizzo del canale istituzionale appositamente predisposto che è la posta elettronica certificata.
Per la registrazione di protocollo dei documenti informatici ricevuti dall'Unione si procede secondo le modalità descritte nel successivo art. 24.

SEZIONE IV – REGISTRAZIONE DEI DOCUMENTI

Articolo 20 – Registro di protocollo unico dell'AOO

Il registro di protocollo è lo strumento finalizzato all'identificazione univoca e certa dei documenti indicati nel successivo art. 21 del presente manuale; esso svolge, quindi, una fondamentale funzione giuridico probatoria attestando l'esistenza di un determinato documento all'interno del Sistema di gestione documentale e garantendone l'autenticità.
Il registro di protocollo è un atto pubblico di fede privilegiata e, come tale, fa fede fino a querela di falso, in particolare circa la data e l'effettivo ricevimento o spedizione di un documento determinato, di qualsiasi forma o contenuto; esso è dunque uno strumento idoneo a produrre effetti giuridici tra le parti.
Nell'ambito dell'AOO, secondo quanto disposto dalla vigente normativa in materia, il registro di protocollo è unico e qualsiasi registro di protocollo interno, diverso o alternativo al Sistema di Gestione Informatica dei Documenti, è abolito.

Articolo 21 – Documenti soggetti obbligatoriamente alla registrazione di protocollo

Ai sensi dell'art. 53, comma 5, del DPR 445/00, sono oggetto di registrazione di protocollo obbligatoria i documenti ricevuti e spediti dall'AOO, indipendentemente dalla tipologia di supporto su cui sono formati e tutti i documenti informatici prodotti dall'Ente, anche quelli con valenza esclusivamente interna, ma utilizzati ai fini amministrativi.
Sono esclusi dalla registrazione obbligatoria i documenti elencati nel successivo articolo del presente manuale.

Articolo 22 – Documenti non soggetti all'obbligo della registrazione di protocollo

Ai sensi dell'art. 53, comma 5, del DPR 445/00, sono esclusi dalla registrazione di protocollo le seguenti tipologie di documenti: le gazzette ufficiali, i bollettini ufficiali e i notiziari della pubblica amministrazione, le note di ricezione delle circolari e altre disposizioni, i materiali statistici, gli atti preparatori interni, i giornali, le riviste, i libri, i materiali pubblicitari, gli inviti a manifestazioni e tutti i documenti già soggetti a registrazione particolare dell'Amministrazione.
Ai documenti soggetti a registrazione particolare, siano essi informatici o analogici, viene assegnata una numerazione continua e progressiva per anno, denominata numerazione di repertorio, in base alla tipologia documentale di appartenenza. I repertori formano, pertanto, serie omogenee di documenti uguali per forma e diversi per contenuto; ne sono un esempio la registrazione delle deliberazioni, delle determinazioni, dei contratti, ecc…
La registrazione dei documenti soggetti a registrazione particolare, prodotti su supporto informatico avviene tramite l'assegnazione a ciascun documento di un numero di repertorio informatico, consistente in un codice identificativo univoco e persistente.
I documenti soggetti a registrazione particolare da parte dell'Amministrazione sono indicati nell'allegato n. 5 al presente manuale.
Sono, infine, escluse dalla registrazione di protocollo le comunicazioni scambiate tra i vari uffici dell'AOO che non rivestano alcun valore di natura amministrativa, procedimentale o giuridica (ad es. comunicazioni organizzative di carattere non ufficiale).

Articolo 23 – Registrazione di protocollo

Per ciascuna delle tipologie di documenti descritte al precedente art. 21 viene effettuata una registrazione di protocollo attraverso il Sistema di Gestione Informatica dei Documenti descritto nell'art. 4 del presente manuale. Tale registrazione, ai sensi dell'articolo 53, comma 3, del DPR 445/00, consiste nella memorizzazione dei dati obbligatori riferiti al documento stesso ed è eseguita in un'unica operazione, senza possibilità per l'operatore di inserire le informazioni in più fasi successive.
La numerazione delle registrazioni di protocollo dei documenti dell'Unione è unica e progressiva; corrisponde all'anno solare, chiudendosi il 31 Dicembre di ogni anno e ricominciando da 1 all'inizio dell'anno successivo.

Non è consentita l'identificazione dei documenti mediante l'assegnazione manuale di numeri di protocollo che il Sistema di Gestione Informatica dei Documenti abbia già attribuito ad altri documenti, anche qualora questi ultimi fossero strettamente correlati tra loro.
Ad ogni registrazione di protocollo vengono associati al documento almeno i seguenti dati, conformi a quanto sancito dall'art. 53, comma 1, del DPR 445/00:

- il numero di protocollo, generato automaticamente dal Sistema e registrato in forma non modificabile;
- la data di registrazione, generata automaticamente dal Sistema e registrata in forma non modificabile;
- l'indice di classificazione;
- il mittente o il destinatario del documento, registrati in forma non modificabile;
- l'oggetto del documento, contenente una sintetica ma esaustiva descrizione del contenuto, registrato in forma non modificabile;
- la data e il protocollo del documento ricevuto, se disponibili.

Le registrazioni di protocollo dell'Unione, inoltre, contengono i seguenti dati opzionali:

- l'indicazione della persona o dell'ufficio all'interno della struttura destinataria a cui si presume verrà affidato il trattamento del documento (se trattasi di documento in uscita);
- la data di arrivo per i documenti in entrata (se diversa dalla data di registrazione a protocollo);
- la descrizione sintetica degli allegati;
- il mezzo di ricezione o di spedizione;
- l'ufficio di competenza.

I documenti per cui venga differita la registrazione di protocollo, secondo quanto previsto dall'articolo 30 del presente manuale, devono inoltre riportare gli estremi dell'autorizzazione al differimento dei termini di registrazione.

Articolo 24 – Registrazione di protocollo dei documenti informatici

La registrazione di protocollo dei documenti informatici viene eseguita dopo aver accertato che gli stessi siano leggibili attraverso i sistemi utilizzati dall'Unione; dovranno essere altresì verificate la provenienza e l'integrità dei documenti, nonché il formato utilizzato, se leggibile e conforme a quelli adottati dall'Unione, l'assenza di macroistruzioni o codici eseguibili tali da modificare il contenuto del documento medesimo e la validità temporale dell'eventuale firma digitale.
Qualora gli accertamenti di cui al capoverso precedente dovessero concludersi con un esito negativo:

- laddove sottoscritto con firma digitale scaduta, ovvero senza la presenza di validazione temporale che attesti la validità del certificato di firma al momento della sottoscrizione, il documento sarà comunque oggetto della registrazione di protocollo e verrà acquisito sul Sistema; sarà compito del Responsabile del procedimento incaricato della trattazione eseguire le opportune verifiche e richiedere il documento sottoscritto con firma digitale il cui certificato sia valido, in considerazione di quanto previsto dall'art. 24, comma 4-bis del D. Lgs. 82/05, che stabilisce il principio secondo cui l'apposizione di una sottoscrizione con certificato digitale scaduto equivale alla mancata sottoscrizione del documento;

in tutti gli altri casi:

- verrà notificata al mittente, laddove identificabile, la condizione di eccezione, affinché provveda al rinvio del documento secondo i criteri dettati dall'Unione;
- il documento oggetto di eccezione sarà mantenuto fino alla ricezione del documento corretto o, comunque, quanto necessario ai fini di un controllo successivo e, trascorso tale termine, si procederà alla sua eliminazione.

La registrazione di protocollo dei documenti informatici comporta la memorizzazione sul SGID delle stesse informazioni indicate dal precedente articolo del manuale di gestione aggiungendo, tra i dati obbligatori, l'impronta del documento informatico, costituita dalla sequenza di simboli binari in grado di identificarne univocamente il contenuto, come indicato nell'art. 53, comma 1, lettera f), del DPR 445/00.
Eseguita l'operazione di registrazione, i documenti informatici memorizzati nel Sistema di Gestione Informatica dei Documenti sono immodificabili e collegati logicamente ai rispettivi dati identificativi.
La registrazione di protocollo dei documenti informatici ricevuti per posta elettronica è effettuata in modo tale che, ad ogni messaggio, corrisponda una registrazione, a seguito della quale il Sistema di Gestione Informatica dei Documenti memorizzerà:

- l'intero messaggio;
- il testo del messaggio unitamente ai dati identificativi;
- gli allegati al messaggio insieme ai relativi dati identificativi.

Articolo 25 – Segnatura di protocollo dei documenti cartacei

La segnatura di protocollo è effettuata contemporaneamente all'operazione della registrazione di protocollo; essa consiste nell'apposizione o nell'associazione all'originale del documento, in forma permanente e non

modificabile, delle informazioni riguardanti la registrazione di protocollo per consentire di individuare ciascun documento in modo inequivocabile.
La segnatura di protocollo di un documento cartaceo avviene mediante l'apposizione su di esso di un timbro sul quale siano riportate le seguenti informazioni:

- denominazione e codice identificativo dell'AOO;
- data e numero di protocollo del documento;

Sul documento da segnare potrà, alternativamente, essere apposta un'etichetta adesiva, non rimovibile né modificabile, prodotta dal Sistema di Gestione Informatica dei Documenti all'atto dell'operazione di registrazione di protocollo; su di essa andranno riportati i dati precedentemente specificati.

Articolo 26 – Segnatura di protocollo dei documenti informatici

L'operazione di segnatura di protocollo dei documenti informatici è effettuata contemporaneamente all'operazione di registrazione di protocollo e persegue il fine di favorire l'interoperabilità tra diversi sistemi di gestione documentale, riportando le informazioni archivistiche fondamentali, in modo da facilitare il trattamento dei documenti da parte del ricevente.
I dati, di cui al precedente art. 25, relativi alla segnatura di protocollo, sono apposti sul documento protocollato o sua copia per immagine (acquisita tramite scansione) automaticamente dal Sistema, inoltre i dati di segnatura di protocollo di un documento informatico trasmesso dall'Unione sono associati al documento stesso e contenuti in un file in formato XML il cui schema è conforme alle Linee guida AgID.
Il file XML della segnatura sarà utilizzato al fine di permettere lo scambio di documenti tra le pubbliche amministrazioni in modalità di interoperabilità, secondo quanto previsto per le comunicazioni di documenti amministrativi protocollati tra AOO nelle Linee guida AgID. L'Amministrazione che riceve il suddetto file XML utilizzerà le informazioni in esso contenute per eseguire, eventualmente anche in forma automatizzata, la registrazione di protocollo del documento in entrata e per avviarlo alla Unità Organizzativa Responsabile competente del trattamento.

Articolo 27 – Riservatezza delle registrazioni di protocollo

Il Sistema di Gestione Informatica dei Documenti, conformemente a quanto stabilito nell'art. 4 del presente manuale, consente l'accesso ai documenti e alle informazioni nel rispetto della normativa vigente in materia di riservatezza dei dati personali, per mezzo di uno specifico livello di accesso stabilito per ciascun documento che venga registrato sul Sistema stesso.
Tale livello di riservatezza è attribuito al documento nel momento della sua registrazione sul SGID e serve a determinare, attraverso la creazione di specifiche o predefinite Access Control List (ACL), quali utenti o gruppi di utenti possono avere accesso al documento medesimo.
Di norma, ciascun utente può accedere esclusivamente ai documenti che ha prodotto, che gli sono stati assegnati o di competenza del proprio ufficio e alle informazioni ad essi collegate; viceversa, il Sistema non rende disponibili né visualizza i documenti e i dati delle relative registrazioni di protocollo per cui gli utenti non siano autorizzati.
Le tipologie documentarie riservate e le modalità di trattamento delle stesse, ivi compresi i livelli di riservatezza da associare a ciascuna, sono individuate dal Responsabile della gestione documentale d'intesa con il Responsabile per la protezione dei dati personali, sulla base di quanto previsto dal Regolamento Comunale sulla protezione dei dati.
Secondo i medesimi criteri vengono definiti anche i livelli di riservatezza dei fascicoli informatici; tale operazione viene eseguita al momento dell'apertura degli stessi sul Sistema.
Per quanto concerne le caselle di posta elettronica integrate con il protocollo informatico, il Sistema di Gestione Informatica dei Documenti consente l'accesso a ciascuna di esse, ai fini della registrazione di protocollo, esclusivamente al personale autorizzato sulla base dell'organizzazione dell'Ente.

Articolo 28 – Annullamento o modifica delle registrazioni di protocollo

L'eventuale annullamento delle registrazioni di protocollo deve essere autorizzato dal Responsabile della gestione documentale.
Le informazioni relative alle registrazioni annullate rimangono memorizzate nel Sistema di Gestione Informatica dei Documenti e, conformemente a quanto disposto dall'art. 54 del DPR 445/00, recano una dicitura o un segno in posizione sempre visibile e tale, comunque, da consentire la lettura di tutte le informazioni originarie unitamente alla data, all'identificativo dell'operatore ed agli estremi del provvedimento di autorizzazione.

L'annullamento anche di una sola delle informazioni generate o assegnate automaticamente dal Sistema e registrate in forma immodificabile (la data e il numero di protocollo) comporta l'automatico e contestuale annullamento dell'intera registrazione di protocollo.
L'annullamento anche di un solo campo delle altre informazioni registrate in maniera immodificabile, con particolare riferimento al mittente, al destinatario e all'oggetto, che fosse necessario per correggere eventuali errori intercorsi in sede di immissione di dati, comporta la rinnovazione del campo stesso con i dati corretti e la contestuale memorizzazione, in modo permanente, del valore precedentemente attribuito unitamente alla data, all'ora e all'autore della modifica; tale disposizione si applica per lo stesso campo o per ogni altro che dovesse, in seguito, risultare errato.
Qualora l'annullamento di una registrazione di protocollo riguardi un documento analogico, il documento riporterà, ben visibili, gli estremi del provvedimento di annullamento e sarà conservato nell'Archivio dell'Ente.

Articolo 29 – Registro giornaliero di protocollo

Il Responsabile della gestione documentale provvede alla produzione, in modalità informatica, del registro giornaliero di protocollo costituito dall'elenco delle informazioni, memorizzate in forma statica, immodificabile ed integra, inserite con l'operazione di registrazione di protocollo nell'arco di uno stesso giorno, ivi comprese quelle modificate e annullate in quella medesima data.
Al fine di garantire l'immodificabilità del contenuto, il Responsabile della gestione documentale trasmette il registro giornaliero di protocollo al sistema di conservazione entro la giornata lavorativa successiva; le modalità operative mediante cui avviene tale trasferimento sono descritte nel manuale di conservazione.

Articolo 30 – Differimento dei termini di registrazione

Di norma, le registrazioni di protocollo dei documenti ricevuti dall'Unione sono effettuate entro la giornata lavorativa di ricezione.
Eccezionalmente, in presenza di situazioni che lo rendano necessario, come un imprevisto carico di lavoro che non permetta di effettuare le registrazioni di protocollo nella stessa giornata lavorativa e qualora, a causa di tale condizione, possa venir meno un diritto di terzi, il Responsabile della gestione documentale, per mezzo di provvedimento motivato, può autorizzare il differimento della registrazione di protocollo dei documenti ricevuti, fissando comunque un limite di tempo entro cui le registrazioni dovranno essere effettuate e conferendo valore, nel caso di scadenze predeterminate, alla data di arrivo dei documenti.
Tutte le registrazioni di protocollo che vengono differite devono riportare gli estremi del suddetto provvedimento di autorizzazione.

Articolo 31 – Registro di emergenza

Qualora, per cause tecniche, non sia possibile usufruire del Sistema di Gestione Informatica dei Documenti, il Responsabile della gestione documentale autorizza il personale abilitato alla protocollazione all'effettuazione delle registrazioni di protocollo su un registro, anche cartaceo, di emergenza.
Le informazioni da inserire nel registro di emergenza, ovvero i campi obbligatori da compilare, sono gli stessi previsti dal protocollo generale.
Le modalità con cui vengono eseguite le registrazioni di protocollo sul registro di emergenza sono quelle sancite dall'art. 63 del DPR 445/00, in particolare:

- sul registro di emergenza sono riportate la causa, la data e l'ora di inizio dell'interruzione, nonché la data e l'ora del ripristino della funzionalità del Sistema;
- qualora l'impossibilità di utilizzare la procedura informatica si prolunghi oltre ventiquattro ore, per cause di eccezionale gravità, il Responsabile della gestione documentale può autorizzare l'uso del registro di emergenza per periodi successivi di non più di una settimana. Sul registro di emergenza vanno riportati gli estremi del provvedimento di autorizzazione;
- per ogni giornata di registrazione di emergenza è riportato sul registro di emergenza il numero totale di operazioni registrate;
- la sequenza numerica utilizzata su un registro di emergenza, anche a seguito di successive interruzioni, deve comunque garantire l'identificazione univoca dei documenti registrati nell'ambito del sistema documentale dell'Unione;
- le informazioni relative ai documenti protocollati in emergenza sono inserite nel Sistema di Gestione Informatica dei Documenti al ripristino delle funzionalità dello stesso, prima che sia eseguita qualsiasi ulteriore operazione di registrazione di protocollo. Durante la fase di ripristino, a ciascun documento registrato in emergenza viene attribuito un numero di protocollo del sistema informatico ordinario; si avrà cura, tuttavia, di inserire nel Sistema anche il numero utilizzato in emergenza, in modo che sia mantenuta stabilmente la correlazione tra questo e il numero di protocollo attribuito al ripristino.

SEZIONE V – CLASSIFICAZIONE E FASCICOLAZIONE DEI DOCUMENTI

Articolo 32 – Titolario di classificazione e piano di conservazione dell'archivio

Il titolario di classificazione e il piano di conservazione sono gli strumenti archivistici utilizzati dall'Ente per l'organizzazione, la gestione e la conservazione del proprio archivio.
Il titolario di classificazione consiste in un sistema precostituito di partizioni astratte, ordinate gerarchicamente, definito sulla base dell'organizzazione funzionale dell'Unione ed è lo strumento utilizzato dall'Ente per organizzare in maniera razionale e ordinata la sedimentazione dei documenti del proprio archivio, secondo un ordine logico che rispecchi lo sviluppo storico dell'attività svolta.
Il piano di conservazione (o massimario di selezione), integrato con il titolario suddetto, è lo strumento che stabilisce i criteri e i tempi di selezione del materiale archivistico, al fine di distinguere la documentazione da destinare alla conservazione permanente da quella proposta periodicamente per lo scarto.
Il titolario di classificazione e il piano di conservazione adottati dall'Unione sono allegati al presente manuale.
Qualora, a seguito di modifiche legislative, risulti necessario aggiornare tali strumenti ovvero si presenti la necessità di apportare variazioni o revisioni, queste vengono predisposte dal Responsabile della gestione documentale nel rispetto della normativa vigente e secondo quanto disposto dall'art. 57 del presente manuale di gestione.
L'applicazione del detto titolario e delle sue eventuali modifiche, non è mai retroattiva, in considerazione del fatto che deve essere mantenuto nel tempo il legame dei fascicoli e dei documenti dell'archivio con la struttura del titolario vigente al momento della produzione degli stessi e, dunque, il corretto vincolo archivistico che lega la produzione documentaria dell'Unione all'attività e alle funzioni dello stesso; a tal fine viene garantita la storicizzazione delle variazioni del titolario e la possibilità di ricostruire le diverse voci nel tempo.
Le modifiche del titolario impediscono di aprire nuovi fascicoli nelle partizioni eventualmente eliminate ma non precludono la possibilità di inserire i documenti in fascicoli precedentemente aperti all'interno di tali voci, fino alla chiusura degli stessi.
Le suddette variazioni del titolario di classificazione sono, di norma, introdotte a partire dal 1° gennaio dell'anno successivo.

Articolo 33 – Classificazione dei documenti

La classificazione è l'operazione che viene eseguita a partire dal titolario riportato nell'allegato n. 6 del presente manuale ed è finalizzata ad organizzare logicamente, in relazione alle funzioni dell'Ente, tutti i documenti ricevuti e prodotti dall'Unione , siano essi cartacei o informatici, successivamente alla loro registrazione nel Sistema di Gestione Informatica dei Documenti.
Tale operazione consiste nell'assegnazione a ciascun documento di un codice, detto indice di classificazione che, in base all'oggetto del documento medesimo, lo associa alla voce del titolario relativa alla corrispondente funzione dell'Ente; sulla base dell'indice di classificazione risulta indicata la posizione logica del documento all'interno dell'archivio ed è possibile l'inserimento nel fascicolo appropriato.
A ciascun documento è associato un unico indice di classificazione, anche qualora attenga a più procedimenti, facenti riferimento a fascicoli di classifiche diverse; in tal caso l'indice di classificazione sarà quello relativo alla collocazione che, in base all'oggetto, venga ritenuta prevalente.
La classificazione dei documenti è eseguita dal personale che ne effettua la relativa registrazione al protocollo.
Nel caso siano presenti errori nell'indice di classificazione di un documento in entrata, il personale dell'ufficio che riceve il documento procede a correggere, sul Sistema, la classificazione errata.
Nell'ambito dell'Unione , tutti i soggetti abilitati all'operazione di classificazione devono conoscere e saper correttamente utilizzare il titolario di classificazione; è compito del Responsabile della gestione documentale provvedere affinché detto personale sia adeguatamente formato sul corretto utilizzo dello strumento e debitamente istruito sulle variazioni eventualmente apportate ad esso.

Articolo 34 – Il fascicolo: formazione, identificazione e gestione

Il Sistema di Gestione Informatica dei Documenti consente la formazione di fascicoli cartacei, informatici, ibridi e di aggregazioni documentali informatiche.
Per fascicolo si intende un insieme di documenti, ordinati cronologicamente e classificati in maniera omogenea (salvo alcune eccezioni come nel caso del fascicolo di persona); il fascicolo costituisce l'unità di base, indivisibile, di un archivio.
Si possono distinguere cinque tipologie di fascicolo:

- Affare: conserva i documenti relativi ad una competenza non proceduralizzata né procedimentalizzata. Per gli affari non esiste un termine per la conclusione previsto dalle norme;

- Attività: conserva i documenti relativi ad una competenza proceduralizzata, per la quale esistono documenti vincolanti o attività di aggiornamento procedurale e per la quale non è comunque prevista l'adozione di un provvedimento finale;
- Procedimento amministrativo: conserva una pluralità di documenti che rappresentano azioni amministrative omogenee e destinate a concludersi con un atto finale;
- Persona fisica: conserva i documenti relativi a diversi procedimenti amministrativi, distinti per affare o per attività, ma legati da un vincolo archivistico interno, relativo ad una persona fisica determinata. La chiusura del fascicolo dipende dalla conclusione del rapporto giuridico con l'Ente;
- Persona giuridica: conserva i documenti relativi a una persona giuridica con modalità simili a quelle del fascicolo di persona fisica.

Per fascicolo informatico si intende un'aggregazione strutturata e univocamente identificata di atti, documenti o dati informatici, prodotti e funzionali all'esercizio di una specifica attività, di uno specifico affare, di uno specifico procedimento o riguardanti una stessa persona fisica o giuridica. Nella Pubblica Amministrazione il fascicolo informatico collegato al procedimento amministrativo è creato e gestito secondo le disposizioni stabilite dall'art. 41 del D. Lgs. 82/05.
Per aggregazione documentale informatica si intende, invece, un'aggregazione 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.
Per fascicolo ibrido si intende un fascicolo o un'aggregazione documentale composta al tempo stesso da documenti cartacei e documenti informatici.
Tutti i documenti registrati nel SGID dell'Unione , indipendentemente dal supporto sul quale sono prodotti, sono riuniti in fascicoli sulla base dell'attività, dell'affare, del procedimento amministrativo, della persona fisica o giuridica cui si riferiscono.
L'operazione di fascicolazione consiste nell'inserire ciascun documento nel fascicolo di riferimento, costituito all'interno della corrispondente partizione logica prevista dal titolario di classificazione dell'Unione. Pertanto ciascun documento per cui sia stata eseguita la registrazione di protocollo, a prescindere dal supporto (informatico o analogico) del medesimo, sarà collegato ad un fascicolo informatico presente nel SGID, ovvero, qualora trattasi del primo documento relativo all'affare, all'attività, al procedimento o alla persona fisica/giuridica di riferimento, si procederà, tramite il SGID, all'apertura di un nuovo fascicolo cui, detto documento, e tutti gli altri ad esso collegati successivamente, saranno associati.
La fascicolazione, fondamentale per la gestione e l'uso dell'archivio e per l'esercizio del diritto di accesso, consente di collegare i singoli documenti a quelli precedenti e successivi prodotti o ricevuti dall'Unione nell'ambito di uno stesso procedimento, affare o attività, o relativi alla stessa persona fisica o giuridica, in modo da riflettere il concreto espletamento delle funzioni dell'Ente; tale operazione sarà di tipo logico per i documenti informatici e di tipo fisico per quelli cartacei.
I documenti sono collocati all'interno del fascicolo secondo l'ordine cronologico di registrazione nel Sistema di Gestione Informatica dei Documenti; ogni fascicolo all'interno dell'archivio dell'Unione va ad occupare un posto specifico, definito in base al titolario di classificazione di cui all'allegato n. 6, tale posizione è di natura logica, nel caso di fascicoli informatici, o fisica, nel caso di fascicoli cartacei o per quanto riguarda la parte cartacea dei fascicoli ibridi.
La formazione dei fascicoli è competenza dei responsabili dei procedimenti amministrativi, individuati all'interno dei singoli uffici incaricati della trattazione dei relativi affari o attività.
L'apertura di un nuovo fascicolo o di una nuova aggregazione documentale comporta la registrazione nel Sistema di Gestione Informatica dei Documenti almeno delle seguenti informazioni che li identificano all'interno dell'archivio dell'Unione:

- oggetto del procedimento (denominazione del fascicolo);
- data di apertura;
- indice di classificazione;
- numero del fascicolo (un numero progressivo, immodificabile, attribuito automaticamente dal Sistema al momento dell'apertura nell'ambito della voce di classificazione di appartenenza).

Anche i fascicoli composti esclusivamente da documenti cartacei devono essere formati sul sistema di Gestione Informatica dei Documenti, collegando tra loro le registrazioni di protocollo relative ai documenti cartacei contenuti nel fascicolo e le relative copie per immagine (ottenute tramite scansione); tale operazione è fondamentale al fine di mantenere la corretta numerazione univoca di tutti i fascicoli presenti nell'archivio dell'Ente, a prescindere dal supporto su cui sono formati ed è funzionale alla produzione in modalità informatica, per mezzo del sistema stesso, del repertorio dei fascicoli, che è unico per tutta l'AOO.
Al termine di ciascun procedimento amministrativo, affare o attività ovvero alla cessazione del rapporto con l'Unione della persona fisica o giuridica, si procede alla chiusura del relativo fascicolo, integrando le suddette informazioni con la data di chiusura che fa riferimento alla registrazione nel Sistema dell'ultimo documento prodotto nel corso della trattazione dell'affare medesimo.
Nel caso di fascicoli ibridi, ovvero contenenti anche documenti cartacei, nel Sistema di Gestione Informatica dei Documenti sarà associata a detti fascicoli un'ulteriore informazione, inserita nel campo "note", relativa alla

posizione fisica che questi occupano nell'archivio dell'Ente, al fine di consentire un agile reperimento degli originali cartacei, in modo che l'unità logica del fascicolo medesimo sia salvaguardata e il recupero della documentazione necessaria a svolgere le consuete attività dell'Unione sia quanto più semplice e funzionale possibile. I fascicoli cartacei o le porzioni cartacee dei fascicoli ibridi devono riportare tutte le informazioni già indicate per i fascicoli informatici sul proprio frontespizio.
I fascicoli, qualora se ne avverta l'esigenza ai fini operativi o in considerazione dell'eccessiva mole di documenti contenuti, possono essere al loro interno articolati in sottofascicoli e questi ultimi, a loro volta, in inserti.
Nel caso le esigenze operative imponessero di creare aggregazioni di fascicoli per gestire procedimenti amministrativi particolarmente complessi e articolati, tali collegamenti tra i fascicoli saranno gestiti attraverso l'inserimento nel Sistema di un ulteriore informazione che indichi tale collegamento e permetta di identificare univocamente la "serie" archivistica che si va a costituire.
Ad ogni fascicolo corrisponde nel Sistema di Gestione Informatica dei Documenti uno specifico livello di riservatezza, sulla base di quanto disposto dall'art. 27 del presente manuale, in modo da stabilire quali utenti o gruppi di utenti possano accedere a ciascun fascicolo; tali livelli di riservatezza possono essere diversificati per i documenti contenuti all'interno dello stesso fascicolo, potendo prevedere per essi un livello di riservatezza superiore a quello del fascicolo di cui sono parte.
I fascicoli e le serie documentarie cartacee, relativi a procedimenti, attività o affari conclusi, ovvero a persone fisiche o giuridiche di cui sia cessato il rapporto con l'Unione, sono trasferiti nell'archivio di deposito dell'Unione, secondo quanto disposto dall'art. 67 del DPR 445/00.

SEZIONE VI – GESTIONE DELLA CORRISPONDENZA IN ENTRATA

Articolo 35 – Ricezione

Le modalità operative attraverso le quali vengono trattati i documenti in entrata sono descritte nella sezione III del presente manuale.

Articolo 36 – Gestione della corrispondenza cartacea

La corrispondenza cartacea indirizzata nominativamente al personale dell'Unione viene regolarmente aperta e registrata al protocollo, a meno che sulla busta non sia riportata la dicitura "riservata", "personale", "confidenziale", "S.P.M." et similia. In quest'ultimo caso viene recapitata in busta chiusa al destinatario il quale, dopo averla aperta e preso visione del contenuto, qualora valuti che il documento ricevuto non sia riservato ai sensi della normativa vigente sulla privacy, lo deve riconsegnare celermente al personale preposto per le attività di protocollazione. Qualora invece emerga che il documento sia soggetto a Privacy, il destinatario provvederà ugualmente affinché venga eseguita la registrazione, accertandosi che il documento venga registrato sul Sistema in modo da essere accessibile soltanto dagli incaricati per la gestione del medesimo.
Le lettere anonime devono essere protocollate ed identificate come tali, con la dicitura "mittente sconosciuto" o "mittente anonimo". I documenti anonimi il cui contenuto sia giuridicamente irrilevante o inequivocabilmente da ricondurre a scherzi o situazioni similari, vengono distrutti; se, invece, si ritiene che contengano dati o informazioni rilevanti, dopo la registrazione di protocollo, si provvede ad inviarli agli uffici competenti per ulteriori eventuali determinazioni.
I documenti sottoscritti, di cui non sia identificabile l'autore, vengono protocollati indicando nel campo mittente la dicitura "mittente non identificabile" e sono inoltrati al responsabile competente; quest'ultimo, ricevuto il documento, valuterà la possibilità nonché la necessità di acquisire gli elementi mancanti per perfezionare l'atto, provvedendo altresì affinché venga integrata la registrazione di protocollo.
I documenti ricevuti privi di firma, ma il cui mittente sia comunque identificabile, vengono protocollati e inoltrati al responsabile del procedimento, che valuterà la necessità di acquisire la dovuta sottoscrizione per il perfezionamento degli atti.
La corrispondenza cartacea riportante l'indicazione "offerta", "gara d'appalto", "preventivo" o simili, o dal cui involucro sia possibile evincere che si riferisca alla partecipazione ad una gara, non deve essere aperta, ma protocollata in base agli elementi rilevabili dal plico o dal bando dell'Amministrazione, apponendo numero di protocollo e data di registrazione direttamente sulla busta. Sull'esterno della busta, accanto alla segnatura di protocollo, viene annotato l'orario di arrivo unicamente nei casi in cui il documento venga consegnato brevi manu oltre il limite orario stabilito nel bando o nell'avviso pubblico: la specifica oraria viene pertanto a contrassegnare soltanto le offerte pervenute oltre la prevista scadenza. L'ufficio competente allo svolgimento della procedura di gara provvede alla custodia della busta o dei contenitori così protocollati, sino all'espletamento della gara; lo stesso ufficio, successivamente alla fase di apertura delle buste, riporterà gli estremi di protocollo presenti sulle buste su ogni documento che le stesse contengano.
Qualora l'Unione dovesse ricevere un documento cartaceo di competenza di altro ente, altra AOO, altra persona fisica o giuridica, lo stesso verrà trasmesso a chi di competenza, se individuabile, altrimenti sarà

restituito al mittente. Nel caso in cui un documento della fattispecie sopra indicata venga erroneamente registrato al protocollo, verrà spedito a chi di competenza, oppure restituito al mittente unitamente ad una lettera di trasmissione opportunamente protocollata; il documento erroneamente protocollato sarà soggetto alla procedura di annullamento del protocollo.

Articolo 37 – Gestione della corrispondenza informatica

In tutti i casi in cui la corrispondenza in arrivo dovesse contenere file non leggibili, presentare sottoscrizioni digitali scadute, macroistruzioni o codici eseguibili, ovvero, dovesse essere prodotta utilizzando formati digitali non conformi a quelli adottati dall'Unione, si seguiranno le indicazioni previste dall'art. 24 del presente manuale.
I documenti inerenti acquisti diretti e gare d'appalto acquisiti tramite MEPA o altra piattaforma informatica (es. documenti che formalizzano un OdA o documenti di stipula di RdO, ecc…) saranno scaricati in locale senza essere protocollati, in quanto già dalla piattaforma da cui sono prodotti ricevono una numerazione univoca. Tali documenti sono archiviati e conservati a norma direttamente dalla piattaforma utilizzata.
Le fatture elettroniche destinate all'Unione rispettano i requisiti di formato e contenuto prescritti dal DMEF n. 55 del 03/04/2013 e s.m.i.; tali documenti vengono trasmessi all'Unione attraverso il Sistema di interscambio (SDI) e sono ricevuti tramite casella PEC integrata funzionalmente con il software di protocollo informatico, in modo da poter procedere alla registrazione automatica e all'acquisizione delle stesse sul sistema di gestione informatica dei documenti. La fattura, a seguito della protocollazione e classificazione, è assegnata, tramite integrazione tra il software di protocollo e quello della contabilità, alle UOR interessate ed ai servizi finanziari per la fascicolazione, le verifiche di correttezza e la gestione della medesima. Nel sistema contabile si provvede alla registrazione di ciascuna fattura nel registro delle fatture.
Nel caso delle fatture elettroniche, la data di registrazione di protocollo fa fede quale termine iniziale dei 15 giorni entro cui la fattura va accettata o rifiutata con motivazione (la mancata notifica di rifiuto entro 15 giorni equivale ad accettazione), nonché dei termini previsti per il pagamento della stessa.
Le fatture elettroniche sono obbligatoriamente conservate in modalità digitale.
I certificati di malattia sono acquisiti consultando la banca dati dell'INPS con apposite credenziali rilasciate ai dipendenti incaricati. Ciascun certificato, dopo essere stato visualizzato, viene salvato come file e inserito nel fascicolo personale del dipendente, senza essere soggetti alla registrazione di protocollo.
Per quanto concerne la ricezione, da parte dell'Unione, della corrispondenza in formato elettronico di competenza di altro Ente, altra AOO, altra persona fisica o giuridica, le modalità da seguire, nel trattamento, sono le stesse previste per gli analoghi casi che abbiano ad oggetto la corrispondenza cartacea.

Articolo 38 – Registrazione di protocollo e classificazione

Le operazioni di registrazione di protocollo e di classificazione della corrispondenza in entrata, sia essa cartacea o informatica, vengono eseguite nel rispetto delle regole specificate nelle sezioni IV e V del presente manuale; per eventuali casi particolari si seguiranno le indicazioni previste nell'articolo 36, per quanto attiene la corrispondenza cartacea e 37 per quel che riguarda quella informatica.
I documenti ricevuti via fax, i cui mittenti siano soggetti diversi dalle pubbliche amministrazioni, vengono registrati al protocollo generale; ai sensi dell'art. 45 del D. Lgs. 82/05, infatti, i documenti trasmessi con qualunque mezzo telematico o informatico idoneo ad accertarne la fonte di provenienza soddisfano il requisito della forma scritta e non devono essere seguiti dalla trasmissione dell'originale. Tuttavia, qualora in seguito pervengano gli originali, ad essi saranno attribuiti numero e data di protocollo assegnati ai relativi fax.
Per quanto concerne le comunicazioni tra pubbliche amministrazioni, si ribadisce che, ai sensi dell'art. 47, comma 2, lettera c), del D. Lgs. 82/05, è esclusa la trasmissione dei documenti tramite fax.

Articolo 39 – Assegnazione

L'operazione di assegnazione è finalizzata all'individuazione dell'ufficio o del servizio cui compete la trattazione del relativo affare o procedimento amministrativo, nonché degli eventuali altri uffici interessati per conoscenza.
L'assegnazione dei documenti ricevuti dall'Unione è effettuata dagli operatori che effettuano la registrazione di protocollo, è eseguita attraverso il Sistema di Gestione Informatica dei Documenti ed è effettuata contestualmente alla registrazione di protocollo.
Nel caso di una assegnazione errata, l'ufficio che riceve il documento lo rimanderà indietro all'unità di protocollazione, che procederà ad una nuova assegnazione, correggendo le informazioni inserite nel Sistema di Gestione Informatica dei Documenti.
Il SGID tiene traccia di ogni passaggio, memorizzando per ciascuno di essi l'identificativo dell'operatore che effettua le operazioni sopra descritte, con la data e l'ora di esecuzione.

Articolo 40 – Scansione

I documenti su supporto cartaceo soggetti a registrazione di protocollo, dopo le operazioni di registrazione, classificazione e segnatura, sono digitalizzati in formato immagine attraverso un processo di scansione eseguito in modalità manuale.
Il processo di scansione si articola nelle seguenti fasi:

- acquisizione delle immagini in modo che ad ogni documento, anche composto da più fogli, corrisponda un file unico in un formato idoneo alla conservazione, tra quelli elencati nell'allegato n. 4 del presente manuale;
- verifica della leggibilità e della qualità delle immagini acquisite e della loro esatta corrispondenza con gli originali cartacei;
- collegamento delle rispettive immagini alla relativa registrazione di protocollo;
- memorizzazione delle immagini nel Sistema di Gestione Informatica dei Documenti, in modo non modificabile.

L'operazione di scansione viene eseguita esclusivamente nei casi in cui non vi sia la possibilità di acquisire i documenti direttamente in formato elettronico.
I documenti ricevuti dall'Unione su supporto cartaceo, ancorché digitalizzati, una volta registrati a protocollo, classificati ed assegnati, sono comunque consegnati anche in originale cartaceo all'ufficio competente.
Nel caso di documenti analogici registrati a protocollo, corredati di allegati numerosi e spesso voluminosi (ad es. tavole di allegati progettuali) si procederà alla scansione soltanto dell'istanza o del documento principale e non a quella degli allegati. Sarà cura dell'operatore che esegue la registrazione inserire nel sistema di gestione informatica dei documenti l'indicazione del numero degli allegati ricevuti.

Articolo 41 – Recapito e presa in carico della corrispondenza informatica

I documenti informatici in entrata, una volta protocollati e classificati, sono assegnati agli uffici competenti e resi disponibili attraverso il Sistema di Gestione Informatica dei Documenti; la loro "presa in carico" è pertanto automatica e avviene contestualmente all'assegnazione. Qualora dovesse verificarsi un'assegnazione errata, si procederà secondo quanto descritto nell'art. 39 del presente manuale.

Articolo 42 – Inoltro dei documenti

Nel caso i documenti, già protocollati, classificati e correttamente assegnati, debbano essere trasmessi ad altri operatori, nell'ambito dello svolgimento del procedimento o dell'affare di riferimento, su di essi può essere eseguita, tramite l'apposita funzione di assegnazione del sistema informatico dei documenti, l'operazione di trasmissione.

Articolo 43 – Fascicolazione

Nell'ambito degli uffici cui sono assegnati i documenti in entrata viene eseguita, a cura dei vari Responsabili dei procedimenti amministrativi, l'operazione di fascicolazione così come descritta nella sezione V del presente manuale.

SEZIONE VII – GESTIONE DEI DOCUMENTI INTERNI, DEI FLUSSI DOCUMENTALI E DEI PROCEDIMENTI AMMINISTRATIVI

Articolo 44 – Produzione dei documenti dell'AOO

L'Unione, per quanto riguarda i flussi documentali interni, procede ad una progressiva dematerializzazione, in modo che gli originali di tutti i documenti siano prodotti su supporto digitale.
I documenti informatici, sono formati nel rispetto delle regole definite nella sezione II del presente manuale e, all'interno degli uffici dell'Ente, circolano esclusivamente in modalità digitale.
Le operazioni di registrazione, classificazione e fascicolazione dei documenti interni aventi valenza amministrativa sono eseguite dai vari uffici dell'Ente e sono svolte secondo quanto disposto nelle precedenti sezioni IV e V del presente manuale di gestione.
Non sono soggetti all'obbligo di protocollazione quei documenti, ad uso interno, che non rivestano alcuna utilità amministrativa, giuridica o procedimentale, come previsto dall'art. 22 del presente manuale di gestione.

Articolo 45 – Gestione dei flussi documentali interni

La circolazione dei documenti amministrativi informatici all'interno degli uffici dell'Unione avviene esclusivamente utilizzando le funzionalità del Sistema di Gestione Informatica dei Documenti, tramite l'assegnazione ai vari servizi destinatari o, nel caso si tratti di documenti non soggetti a registrazione (es. semplici comunicazioni di servizio) tramite mail.

Articolo 46 – Gestione dei procedimenti amministrativi

Il Sistema di Gestione Informatica dei Documenti realizza le condizioni operative per una gestione efficace dei flussi documentali dell'Ente anche ai fini dello snellimento delle procedure, della trasparenza e dell'efficacia dell'azione amministrativa ai sensi degli articoli 64 e seguenti del DPR 445/00.
Il Sistema tende a realizzare una gestione integrata dei procedimenti amministrativi, permettendo così agli uffici ed agli utenti di controllare gli stati di avanzamento delle loro pratiche e le responsabilità connesse ai procedimenti stessi e di concorrere all'alimentazione del fascicolo.
Tale gestione avrà il fine di consentire:

- il monitoraggio dei vari step del procedimento, dei sub-procedimenti (identificati nei sottofascicoli), dei possibili percorsi alternativi cui la pratica potrà giungere;
- le comunicazioni interne circa gli stati di avanzamento dei procedimenti amministrativi;
- il controllo dei tempi di svolgimento delle attività connesse al procedimento amministrativo e la segnalazione delle scadenze;
- il tracciamento di ogni operazione effettuata;
- la ricerca e la visualizzazione dello stato di avanzamento delle pratiche attive.

SEZIONE VIII – GESTIONE DELLA CORRISPONDENZA IN USCITA

Articolo 47 – Spedizione dei documenti su supporto cartaceo

La spedizione di documenti prodotti o comunque trattati dall'Unione avviene, di norma, in modalità informatica, secondo le indicazioni definite nell'articolo 48 del presente manuale; l'invio di documenti cartacei avviene esclusivamente nei casi in cui risulti impossibile procedere in modalità digitale.
I documenti da spedire su supporto cartaceo, formati nel rispetto delle modalità definite nella sezione II del presente manuale, una volta registrati, classificati e fascicolati, vengono imbustati e convogliati agli uffici preposti alle operazioni di affrancatura, contabilizzazione delle spese e spedizione.
Nel caso di spedizioni che utilizzino posta raccomandata con ricevuta di ritorno, posta celere, corriere od altro mezzo di spedizione che richieda di allegare altra documentazione alla busta, la relativa modulistica verrà compilata a cura degli uffici mittenti.
La minuta (fotocopia) del documento cartaceo spedito verrà conservata all'interno del relativo fascicolo.
Nel caso in cui l'Ente si trovi ad interagire con utenti sprovvisti di adeguati strumenti informatici o impossibilitati al loro utilizzo si procede, qualora si tratti di documenti originali informatici, alla produzione e alla consegna della copia conforme, in formato analogico, prodotta secondo le modalità previste dall'articolo 16 del presente manuale.

Articolo 48 – Spedizione dei documenti informatici

La spedizione dei documenti informatici, prodotti nel rispetto delle modalità definite nella sezione II del presente manuale, avviene, di norma, per mezzo della casella istituzionale di posta elettronica certificata, integrata con il protocollo informatico, attraverso il Sistema di Gestione Informatica dei Documenti; quest'ultimo, una volta composto il messaggio da spedire, lo inoltra al destinatario o ai destinatari, utilizzando il servizio di PEC dell'Unione.
I documenti informatici vengono trasmessi agli indirizzi di posta elettronica certificata dichiarati dai destinatari ovvero reperibili negli elenchi dei domicili digitali e in indici ed elenchi ufficiali di pubblica consultazione.
La trasmissione di documenti informatici tra pubbliche amministrazioni avviene mediante posta elettronica certificata o mediante i meccanismi di interoperabilità di cui al Sistema Pubblico di Connettività e Cooperazione (SPC), utilizzando le informazioni contenute nella segnatura di protocollo, secondo le modalità espresse dalle Linee guida AgID.
La spedizione di un documento informatico a mezzo PEC viene eseguita dal Sistema al completamento delle operazioni di registrazione di protocollo, conformemente a quanto descritto nelle Sezioni IV e V del presente manuale.
L'integrazione funzionale tra il servizio di posta elettronica certificata e il SGID ovvero i meccanismi di interoperabilità consentono la produzione del messaggio da parte del Sistema stesso e il suo invio in automatico.
Le ricevute rilasciate dai gestori del servizio di posta elettronica certificata e i messaggi di ritorno generati dal SGID del destinatario saranno identificati dal Sistema e da questo automaticamente archiviati, collegandoli alle registrazioni di protocollo dei documenti corrispondenti.
E' onere dell'ufficio che ha effettuato la spedizione la verifica di situazioni di anomalia, ivi incluso il mancato recapito del messaggio stesso.

Al fine di garantire la riservatezza dei dati di cui all'art. 4 del D. Lgs. 196/03 “Codice in materia di protezione dei dati personali” ed al Regolamento UE n. 679 del 27 aprile 2016, 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 regolamento che siano indispensabili per il perseguimento delle finalità per le quali sono acquisite.
In ogni caso, sono osservate le disposizioni contenute nei regolamenti adottati dall’Unione per il trattamento dei dati personali, sensibili e giudiziari anche con strumenti elettronici.

SEZIONE IX – ARCHIVIAZIONE DEI DOCUMENTI

Articolo 49 – Archivio dell’amministrazione

L’archivio dell’Unione consiste nel complesso organico degli atti, cartacei o informatici, prodotti o ricevuti dall’Ente nell’esercizio delle proprie funzioni e per il conseguimento dei propri fini istituzionali.
I documenti facenti parte dell’archivio dell’Unione sono legati tra loro dal vincolo archivistico: nesso che collega in maniera logica la documentazione posta in essere dal soggetto produttore. Essi sono ordinati e conservati in modo coerente e accessibile alla consultazione; l’uso degli atti può essere amministrativo, legale o storico.
L’archivio dell’Ente costituisce un bene culturale ai sensi dell’art. 10, comma 2, lettera b), del D. Lgs. 42/04 “Codice dei beni culturali e del paesaggio”, come tale è inalienabile, non può essere smembrato, danneggiato, distrutto o utilizzato in modo tale da recare pregiudizio alla sua conservazione; è obbligo dell’Unione, ai sensi dell’art. 30, comma 4, del suddetto decreto conservare il proprio archivio nella sua organicità, provvedendo inoltre ad ordinare e inventariare il proprio archivio storico.
Ai sensi dell’art. 21, commi 1 e 2, del D. Lgs. 42/04 le operazioni di spostamento degli archivi non correnti, l’esecuzione di opere e lavori, nonché lo scarto del materiale archivistico sono soggetti all’autorizzazione della Soprintendenza archivistica competente per territorio.
Le responsabilità dell’Unione, connesse alla tutela del proprio patrimonio archivistico, si estendono anche agli archivi digitali depositati presso un conservatore accreditato ai sensi della normativa vigente; in tal senso la competenza per la tutela degli archivi pubblici da parte del Ministero dei beni e delle attività culturali e del turismo si esercita anche sui sistemi di conservazione digitale.
L’archivio in senso proprio costituisce un complesso unitario composto, ai fini della gestione documentale, dall’archivio digitale, dall’archivio ibrido e dall’archivio cartaceo; quest’ultimo, per motivi organizzativi e funzionali, si articola in archivio corrente, archivio di deposito e archivio storico.

Articolo 50 – Archivio corrente

Per archivio corrente si intende l’insieme dei documenti e dei fascicoli prodotti, acquisiti e conservati dall’Unione nell’esercizio delle proprie funzioni, relativi ad attività, affari e procedimenti amministrativi in corso di istruttoria e di trattazione e per i quali sussista un interesse attuale nonché quelli relativi a persona fisica o giuridica che abbia in essere un rapporto con l’Ente.
L’organizzazione dell’archivio deve rispondere a criteri di efficienza ed efficacia al fine di garantire la certezza dell’attività giuridico amministrativa dell’Ente e la conservazione stabile della memoria nel tempo. L’archivio corrente è, quindi, il primo elemento gestionale per il corretto funzionamento del sistema documentale.
L’archivio corrente dell’Unione si forma svolgendo le opportune procedure di registrazione di protocollo, classificazione e fascicolazione secondo le modalità previste nelle sezioni IV e V del presente manuale; tali operazioni permettono la sedimentazione e l’organizzazione dell’archivio in maniera corretta e ordinata, in modo da rendere più semplice il recupero dei documenti.
Ciascun Responsabile di procedimento amministrativo è tenuto alla corretta formazione e gestione dei fascicoli, cartacei, informatici o ibridi, relativi ai procedimenti di propria competenza, fintanto che tali unità archivistiche fanno parte dell’archivio corrente.
I fascicoli e i documenti cartacei e le parti cartacee dei fascicoli ibridi, facenti parte dell’archivio corrente, sono custoditi e conservati a cura dei medesimi Responsabili dei procedimenti amministrativi all’interno degli uffici di ciascuna UOR, fino al versamento nell’archivio di deposito dell’Ente.
I documenti e i fascicoli informatici, facenti parte dell’archivio corrente, sono conservati nel Sistema di gestione informatica dei documenti.

Articolo 51 – Archivio di deposito

L’archivio di deposito è la fase intermedia del processo di tenuta dei documenti cartacei prodotti, ricevuti o gestiti dall’Ente nel corso della propria attività e si colloca temporalmente tra l’archivio corrente e l’archivio storico.

Per archivio di deposito si intende l'insieme dei documenti e dei fascicoli cartacei relativi ad affari e a procedimenti amministrativi conclusi, per i quali non risulti più necessaria una trattazione inerente le attività amministrative correnti, ma che possono rivelarsi ancora utili per finalità amministrative e giuridiche.
Le attività svolte sull'archivio di deposito sono definite dagli art. 67, 68 e 69 del DPR 445/00.
All'inizio di ogni anno, ciascun responsabile di procedimento, verificata la corretta formazione e la completezza, procede al versamento nell'archivio di deposito dell'Ente dei fascicoli relativi a procedimenti amministrativi, attività o affari conclusi, o relativi a persone fisiche o giuridiche che abbiano cessato il loro rapporto con l'Unione.
L'archiviazione e la custodia dei documenti che contengano dati personali o dati sensibili avviene nel rispetto della normativa vigente in materia di protezione e tutela dei dati personali.

Articolo 52 – Procedure di selezione e scarto dei documenti cartacei

Le attività di selezione e scarto della documentazione archivistica sono funzionali ai fini della corretta formazione e conservazione della memoria storica dell'Ente, nonché alla migliore consultabilità dell'archivio. I documenti destinati allo scarto sono genericamente intesi come quelli che hanno perso la loro valenza amministrativa, senza assumere alcuna rilevanza storica, ragione per cui, nell'impossibilità pratica di conservare indiscriminatamente ogni documento, si effettua la selezione.
Le operazioni in oggetto, per quanto attiene alla documentazione cartacea, avvengono nell'archivio di deposito dell'Unione, dove si procede al vaglio del materiale allo scopo di definire quale debba essere scartato e quale, viceversa, sia da destinare alla conservazione permanente nell'archivio storico.
Lo strumento utilizzato per le operazioni di selezione e scarto è il piano di conservazione dell'archivio, allegato al presente manuale, nel quale sono dettagliate per ciascuna tipologia documentaria, le indicazioni relative ai tempi di conservazione.
Le procedure di selezione e scarto sono svolte dal Responsabile della gestione documentale, il quale predispone un elenco di versamento per i documenti e i fascicoli destinati alla conservazione permanente e un elenco di scarto per le unità archivistiche che si intendono eliminare.
L'elenco di scarto viene sottoposto alla Soprintendenza archivistica competente per territorio a cui viene formalmente richiesta l'autorizzazione per poter procedere, trattandosi di intervento soggetto ad autorizzazione ai sensi dell'art. 21 del D. Lgs. 42/04.
Ottenuto il nulla osta si avvia la procedura per l'eliminazione fisica dei documenti, che deve avvenire nel rispetto della normativa vigente, in particolar modo per quanto riguarda la tutela dei dati sensibili e personali; completate dette operazioni, il Responsabile della gestione documentale comunica formalmente alla detta Soprintendenza che lo scarto è avvenuto.
I documenti, i cui affari siano esauriti da almeno quaranta anni, destinati alla conservazione permanente, sono trasferiti, se cartacei, nell'archivio storico dell'Ente, conformemente a quanto previsto dall'art. 69 del DPR 445/00. L'archivio storico deve essere ordinato e inventariato e l'inventario, aggiornato a seguito del versamento del suddetto materiale, deve essere trasmesso alla Soprintendenza archivistica.

Articolo 53 – Archivio storico

Per archivio storico si intende il complesso dei documenti prodotti o acquisiti dall'Ente, relativi ad affari e a procedimenti amministrativi conclusi da oltre quaranta anni e destinati, previa l'effettuazione delle procedure di selezione e scarto, alla conservazione permanente, al fine di garantirne la consultazione al pubblico; ai sensi dell'art. 30, comma 4, del D. Lgs. 42/04, tale documentazione è inventariata e conservata in una sezione separata dell'archivio.
Ai sensi dell'art. 122, comma 1, del suddetto decreto, la documentazione conservata nell'archivio storico è liberamente consultabile, ad eccezione:

- dei documenti dichiarati di carattere riservato, relativi alla politica estera o interna dello Stato, che diventano consultabili cinquanta anni dopo la loro data;
- dei documenti contenenti i dati sensibili nonché i dati relativi a provvedimenti di natura penale espressamente indicati dalla normativa in materia di trattamento dei dati personali, che diventano consultabili quaranta anni dopo la loro data;
- i documenti contenenti dati idonei a rivelare lo stato di salute, la vita sessuale o rapporti riservati di tipo familiare, i quali diventano consultabili settanta anni dopo la loro data.

Articolo 54 – Archivio digitale e sistema di conservazione

L'archivio digitale dell'Unione è costituito da documenti, aggregazioni documentali e fascicoli informatici registrati e gestiti per mezzo del Sistema di Gestione Informatica dei Documenti; tale Sistema rappresenta, dunque, il luogo in cui l'archivio digitale ha sede.

La conservazione a lungo termine e quella permanente dell'archivio digitale dell'Unione è demandata ad un soggetto conservatore accreditato dall'AgID ed avviene nel rispetto di quanto previsto dalle regole tecniche in materia di sistema di conservazione digitale, emanate con Linee guida AgID.
Il trasferimento dei documenti e fascicoli informatici e dei relativi metadati al sistema di conservazione suddetto avviene predisponendo un pacchetto di versamento conforme alle specifiche tecniche descritte nel manuale di conservazione del soggetto conservatore, allegato al presente manuale.
Il suddetto versamento viene eseguito almeno una volta all'anno, ad eccezione del registro giornaliero di protocollo che viene versato in conservazione nel corso della giornata lavorativa successiva a quella di riferimento e dei documenti a rilevanza fiscale e contabile che sono trasferiti al sistema di conservazione nel rispetto delle tempistiche definite dal DMEF 17/06/2014.
Ai documenti che formano il pacchetto di versamento saranno associati dal SGID, ai fini della conservazione digitale, i metadati minimi previsti dalla vigente normativa in materia.

Articolo 55 – Archivio ibrido

Per archivio ibrido si intende il complesso di documenti, fascicoli e aggregazioni documentali, in parte cartacei e in parte digitali, prodotti, acquisiti e conservati dall'Ente nello svolgimento delle proprie attività.
I documenti cartacei facenti parte di fascicoli o aggregazioni documentali ibride saranno oggetto di versamento all'archivio di deposito dell'Unione , secondo le modalità e i tempi previsti dal precedente art. 51; per quanto riguarda, invece, la documentazione digitale e i metadati relativi al fascicolo o all'aggregazione documentale, essi saranno oggetto di trasferimento al sistema di conservazione accreditato secondo quanto previsto dal precedente art. 54.
In ogni caso viene mantenuto il collegamento logico tra la parte cartacea e quella digitale di una stessa unità archivistica; a tal fine, il frontespizio di ciascun fascicolo ibrido, contenente la documentazione cartacea dello stesso, riporterà le informazioni previste dall'art. 34 del presente manuale.

Articolo 56 - Procedure di selezione e scarto dei documenti informatici

Per quanto riguarda lo scarto della documentazione informatica conservata presso una struttura di conservazione accreditata, la procedura avverrà in modo analogo a quanto previsto per i documenti analogici, nel rispetto delle vigenti normative in merito alla tutela dei beni culturali. In particolare, il soggetto conservatore accreditato, che svolge esternamente il servizio di conservazione per conto dell'Ente, comunica al Responsabile della conservazione dell'Unione l'elenco dei pacchetti di archiviazione contenenti i documenti destinati allo scarto. Il Responsabile della conservazione ne prende visione, effettua le verifiche soprattutto in merito al rispetto dei tempi previsti dal piano di conservazione allegato al presente manuale e, appurato che si tratti di documenti per cui sia possibile eseguire lo scarto, ne fornisce comunicazione al Responsabile della gestione documentale, che richiederà formalmente l'autorizzazione alla Soprintendenza archivistica competente per territorio. Ricevuta l'autorizzazione dalla competente Soprintendenza archivistica, il Responsabile della gestione documentale autorizzerà il soggetto conservatore, per mezzo di un atto formale dell'Ente, a procedere all'eliminazione dal Sistema dei pacchetti di archiviazione corrispondenti. Eseguito lo scarto, il conservatore accreditato ne fornirà adeguata documentazione all'Unione il quale, secondo quanto disposto dall'art. 52 del presente manuale, procederà ad informare la Soprintendenza archivistica del completamento delle operazioni.
L'operazione di scarto sarà tracciata nel sistema di conservazione mediante la produzione di metadati che descrivono le informazioni essenziali sullo scarto, inclusi gli estremi della richiesta di nulla osta allo scarto e il conseguente provvedimento di autorizzazione.

SEZIONE X – APPROVAZIONE E AGGIORNAMENTO

Articolo 57 – Approvazione, aggiornamento e pubblicità del manuale

Il presente Manuale è approvato, integrato e modificato con deliberazione della Giunta Comunale; lo stesso è soggetto a revisione ordinaria ogni due anni, su iniziativa del Responsabile della gestione documentale.
In caso di sopravvenienze normative, introduzione di nuove prassi tendenti a migliorare l'azione amministrativa in termini di efficacia, efficienza e trasparenza, evoluzione delle procedure e delle infrastrutture tecnologiche o comunque, ogni qual volta il Responsabile lo riterrà necessario, si potrà procedere a revisione del Manuale anche prima della scadenza sopra prevista.
La modifica o l'aggiornamento di uno o di tutti gli allegati al presente Manuale non comporta la revisione nei modi di cui sopra del Manuale stesso.
Il presente Manuale, secondo quanto previsto dalle Linee guida AgID è pubblicato nel sito internet istituzionale dell'Ente, nella sezione dedicata all'Amministrazione trasparente, ed è capillarmente divulgato in tutti gli uffici e servizi dell'AOO.

GLOSSARIO

- Access Control List (ACL): metodo utilizzato per determinare l'accesso o meno alle risorse del Sistema di Gestione Informatica dei Documenti da parte degli utenti, stabilito sulla base di specifici livelli di riservatezza associati a ciascuna risorsa informatica.
- Accesso: operazione che consente a chi ne ha diritto di prendere visione ed estrarre copia dei documenti informatici.
- Accreditamento: riconoscimento, da parte dell'Agenzia per l'Italia digitale (AgID), 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.
- Agenzia per l'Italia Digitale (AgID): organismo che svolge attività di progettazione e coordinamento delle iniziative strategiche per la più efficace erogazione di servizi in rete della pubblica amministrazione a cittadini e imprese. Elabora gli indirizzi, le regole tecniche e le linee guida per la piena interoperabilità e cooperazione applicativa tra i sistemi informatici della pubblica amministrazione e tra questi e i sistemi dell'Unione Europea, assicura l'uniformità tecnica dei sistemi informativi pubblici destinati a erogare servizi ai cittadini e alle imprese, garantendo livelli omogenei di qualità e fruibilità sul territorio nazionale, nonché la piena integrazione a livello europeo.
- Aggregazione documentale informatica: aggregazione 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, formati, prodotti o comunque acquisiti da un soggetto produttore durante lo svolgimento della propria attività.
- Archivio corrente: complesso dei documenti riferibili ad attività o procedimenti amministrativi in corso di istruttoria e trattazione o da poco conclusi.
- Archivio di deposito: complesso di documenti relativi ad attività o procedimenti conclusi, trasferiti dall'archivio corrente in quanto non più necessari alle attività quotidiane.
- Archivio storico: complesso dei documenti relativi ad affari esauriti da oltre 40 anni e destinati, previe le operazioni di scarto, alla conservazione permanente.
- Archivio ibrido: complesso di documenti, fascicoli e aggregazioni documentali in parte cartacei e in parte digitali.
- Archivio informatico: archivio costituito da documenti informatici, fascicoli informatici nonché aggregazioni documentali informatiche, gestiti e conservati in ambiente informatico.
- Area Organizzativa Omogenea (AOO): 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 DPR 445/00.
- Assegnazione: individuazione, da parte del personale abilitato alla registrazione di protocollo, della UOR di competenza e/o della persona fisica responsabile della trattazione dell'affare o del documento nella fase corrente.
- Autenticità: caratteristica di un documento informatico che garantisce di essere ciò che dichiara di essere, senza aver subito alterazioni o modifiche.
- Casella istituzionale di posta elettronica certificata (PEC): la casella di posta elettronica di una pubblica amministrazione, presso la quale è eletto il domicilio digitale dell'amministrazione medesima.
- Certificati elettronici: gli attestati elettronici che collegano all'identità del titolare i dati utilizzati per verificare le firme elettroniche.
- Certificato qualificato: un certificato di firma elettronica che è rilasciato da un certificatore qualificato ed è conforme ai requisiti di cui all'allegato I del Regolamento (UE) del Parlamento Europeo n. 910/2014.
- Certificatore qualificato o Prestatore di servizi di firma elettronica qualificata: il soggetto che presta servizi di certificazione delle firme elettroniche o che fornisce altri servizi connessi con queste ultime.
- Chiave privata: l'elemento della coppia di chiavi asimmetriche, utilizzato dal soggetto titolare, mediante il quale si appone la firma digitale sul documento informatico.
- Chiave pubblica: l'elemento della coppia di chiavi asimmetriche destinato ad essere reso pubblico, con il quale si verifica la firma digitale apposta sul documento informatico dal titolare delle chiavi asimmetriche.
- Classificazione: attività di organizzazione logica di tutti i documenti secondo il titolario di classificazione, articolato in voci individuate in relazione alle funzioni dell'Ente. Tale operazione consiste nell'assegnazione a ciascun documento, in base all'oggetto, di un indice di classificazione e del numero di repertorio del fascicolo in cui il documento stesso è contenuto.
- Codice eseguibile: insieme di istruzioni o comandi software direttamente elaborabili dai sistemi informatici.

- Codice IPA: il codice univoco che viene assegnato all'Ente al termine del processo di accreditamento all'Indice delle Pubbliche Amministrazioni.
- Conservatore accreditato: soggetto, pubblico o privato, che svolge attività di conservazione, al quale sia stato riconosciuto dall'AgID 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.
- 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 50, comma 4, del DPR 445/2000 nei casi di amministrazioni che abbiano istituito più AOO.
- Copia analogica del documento informatico: documento analogico avente contenuto identico a quello del documento informatico da cui è tratto.
- 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 informatico da cui è tratto, ma avente diversa sequenza di valori binari.
- Dispositivo sicuro per la generazione della firma elettronica qualificata: un dispositivo per la creazione di una firma elettronica che soddisfa i requisiti di cui all'allegato II del Regolamento (UE) del Parlamento Europeo n. 910/2014.
- Documento amministrativo: ogni rappresentazione, comunque formata, del contenuto di atti, anche interni, delle pubbliche amministrazioni o, comunque, utilizzati ai fini dell'attività amministrativa.
- Documento amministrativo informatico: atto formato dalla pubblica amministrazione con strumenti informatici o comunque da essa detenuto, il cui originale sia in formato digitale.
- Documento informatico: il documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti.
- Documento analogico: la rappresentazione non informatica di atti, fatti o dati giuridicamente rilevanti.
- Domicilio digitale: un indirizzo elettronico eletto presso un servizio di posta elettronica certificata (PEC) o un servizio elettronico di recapito certificato qualificato, come definito dal Regolamento (UE) del Parlamento Europeo n. 910/2014.
- Duplicato informatico: il documento informatico ottenuto mediante la memorizzazione, sullo stesso dispositivo o su dispositivi diversi, della medesima sequenza di valori binari del documento originario.
- Evidenza informatica: una sequenza di simboli binari (bit) che può essere elaborata da una procedura informatica.
- Fascicolazione: operazione di riconduzione dei documenti classificati relativi a un medesimo affare o procedimento amministrativo nello stesso fascicolo.
- Fascicolo: insieme di documenti, ordinati cronologicamente, relativi ad un medesimo procedimento amministrativo, a una medesima attività o affare oppure alla medesima persona fisica o giuridica, classificati in maniera omogenea.
- Fascicolo ibrido: fascicolo o aggregazione documentale composta da documenti cartacei e documenti informatici.
- Fascicolo informatico: aggregazione strutturata e univocamente identificata di atti, documenti o dati informatici, prodotti e funzionali all'esercizio di una specifica attività o di uno specifico procedimento.
- Fax Server: software o combinazione di software ed hardware in grado di elaborare, inviare e ricevere documenti informatici; di solito è installato su di una organizzazione di rete locale (LAN).
- Firma digitale: un particolare tipo di firma qualificata basata su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare di firma elettronica tramite la chiave privata e a un soggetto terzo 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.
- Firma elettronica: l'insieme dei dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati elettronici e utilizzati dal firmatario per firmare.
- Firma elettronica avanzata: tipo di firma elettronica che è idonea ad identificare il firmatario del documento e garantisce la connessione univoca della firma al firmatario. La firma elettronica avanzata è creata mediante dati che il firmatario può, con un elevato livello di sicurezza, utilizzare sotto il proprio esclusivo controllo ed è collegata ai dati sottoscritti in modo da consentire l'identificazione di ogni successiva modifica di tali dati.
- Firma elettronica qualificata: una firma elettronica avanzata creata da un dispositivo per la creazione di una firma elettronica qualificata e basata su un certificato qualificato per firme elettroniche.

- Formato elettronico: modalità di rappresentazione della sequenza di bit che costituiscono il documento informatico.
- 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 DPR 445/00.
- Funzionalità minima: la componente del sistema di protocollo informatico che rispetta i requisiti di operazioni ed informazioni minime di cui all'articolo 56 del DPR 445/00.
- Funzione di hash: una funzione matematica che genera, a partire da una evidenza informatica, una 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.
- Gestione dei documenti: insieme delle attività finalizzate alla registrazione di protocollo, alla classificazione, alla fascicolazione, all'assegnazione, al reperimento, alla conservazione e all'accesso dei documenti amministrativi formati o acquisiti dall'AOO.
- Gestore di posta elettronica certificata: il soggetto che presta servizi di trasmissione dei documenti informatici mediante la posta elettronica certificata.
- 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.
- Identificazione informatica: il processo per cui si fa uso di dati di identificazione personale in forma elettronica che rappresentano un'unica persona fisica o giuridica, o un'unica persona fisica che rappresenta una persona giuridica; tali dati consentono, attraverso opportune tecnologie, l'individuazione della persona nei sistemi informativi anche al fine di garantire la sicurezza dell'accesso.
- Immodificabilità: caratteristica che rende il documento informatico non alterabile nella forma e nel contenuto durante l'intero ciclo di gestione e garantisce la staticità ai fini della conservazione del documento stesso.
- Impronta di una sequenza di simboli binari (bit): la sequenza di simboli binari (bit) di lunghezza predefinita generata mediante l'applicazione alla prima di una opportuna funzione di hash.
- Indice delle Pubbliche Amministrazioni (IPA) o Indice degli indirizzi della Pubblica Amministrazione e dei Gestori di Pubblici Servizi: l'Indice delle Pubbliche Amministrazioni consente di reperire le informazioni relative ai domicili digitali e alle strutture organizzative, le cosiddette Aree Organizzative Omogenee (AOO), di tutte le pubbliche amministrazioni locali e centrali. L'Indice è uno strumento di consultazione on-line contenente informazioni dettagliate e certificate. Esso contiene, infatti, la struttura e le competenze degli uffici pubblici con i nominativi dei referenti, l'elenco dei servizi offerti, le informazioni per il loro utilizzo, i numeri di telefono, gli indirizzi di posta elettronica istituzionali afferenti alle AOO e gli indirizzi di posta elettronica certificata attivati dalle Amministrazioni.
- Indice di classificazione: codice alfanumerico assegnato a ciascun documento, per mezzo dell'operazione di classificazione, che identifica le partizioni logiche del titolario cui il documento fa riferimento.
- 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 e la conservazione.
- 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.
- Macroistruzione: istruzione o codice in grado di modificare il contenuto di un documento informatico.
- Manuale di conservazione: strumento organizzativo che 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 utilizzate, le misure di sicurezza adottate e ogni altra informazione utile alla gestione e alla verifica del funzionamento, nel tempo, del sistema di conservazione.
- Manuale di gestione: strumento organizzativo 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.

- Marca temporale: il riferimento temporale che consente la validazione temporale e che dimostra l'esistenza di un'evidenza informatica in un tempo certo.
- Metadati: insieme di dati e informazioni 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 (AIP): pacchetto informativo composto dalla trasformazione di uno o più pacchetti di versamento secondo le modalità riportate nel manuale di conservazione.
- Pacchetto di versamento (SIP): 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, fascicoli informatici, aggregazioni documentali informatiche), oppure anche i soli metadati riferiti agli oggetti da conservare.
- 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.
- Piano generale della sicurezza: documento per la pianificazione delle attività volte alla protezione del sistema e di tutte le possibili azioni finalizzate alla gestione del rischio nell'ambito dell'organizzazione di appartenenza.
- Processo di conservazione: insieme delle attività finalizzate alla conservazione dei documenti informatici.
- Procedimento amministrativo: sequenza di atti e/o fatti tra loro connessi per la definizione di decisioni dell'Amministrazione, nel perseguimento di pubblici interessi, che ha come atto conclusivo la produzione di un atto amministrativo perfetto ed efficace.
- Produttore: persona fisica o giuridica, 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 responsabile della gestione documentale.
- Posta elettronica certificata (PEC): sistema di comunicazione in grado di attestare l'invio e l'avvenuta consegna di un messaggio di posta elettronica e di fornire ricevute opponibili ai terzi.
- 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 di atti e documenti 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.
- Registro particolare: registro informatico di particolari tipologie di atti o documenti; nell'ambito della pubblica amministrazione è previsto ai sensi dell'articolo 53, comma 5, del DPR 445/00.
- Repertorio: registro in cui sono annotati, con numerazione progressiva, i documenti per i quali è prevista la registrazione particolare, alternativa a quella di protocollo. Il complesso dei documenti registrati a repertorio per forma omogenea costituisce una serie.
- Repertorio dei fascicoli: registro in cui sono annotati, con numerazione progressiva, i fascicoli secondo l'ordine cronologico in cui si costituiscono, all'interno delle partizioni gerarchiche del titolario. Il repertorio dei fascicoli è unico nell'ambito di ciascuna AOO ed è collegato al rispettivo registro di protocollo.
- Repertorio informatico: registro informatico che raccoglie i dati registrati direttamente dalle procedure informatiche con cui si formano atti e documenti o indici di atti e documenti secondo un criterio che ne garantisca l'identificazione univoca all'atto della immissione cronologica.
- Responsabile della gestione documentale o responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi (RGD): 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, ai sensi dell'articolo 61 del DPR 445/00, che produce il pacchetto di versamento ed effettua il trasferimento del suo contenuto nel sistema di conservazione.
- Responsabile della conservazione: all'interno di ciascuna pubblica amministrazione, il soggetto responsabile dell'insieme delle attività di gestione del sistema di conservazione, ovvero il soggetto con facoltà di delega e controllo sull'attività di conservazione digitale a norma affidata ad un soggetto esterno, accreditato dall'AgID.
- Responsabile del trattamento dei dati: la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali.

- Responsabile della transizione al digitale (RTD): soggetto al quale, in ottemperanza all'art. 17 del D. Lgs. 82/05, compete la definizione delle soluzioni tecnologiche ed organizzative in attuazione delle disposizioni in materia di transizione al digitale e del piano triennale dell'informatica per la Pubblica Amministrazione.
- Riferimento temporale: evidenza informatica, contenente la data e l'ora, con riferimento al Tempo Universale Coordinato (UTC), che viene associata ad uno o più documenti informatici.
- Scarto: operazione con cui si eliminano, secondo quanto previsto dalla normativa vigente, i documenti ritenuti privi di valore amministrativo e di interesse storico culturale.
- Segnatura di Protocollo: l'apposizione o l'associazione, all'originale del documento, in forma permanente e non modificabile delle informazioni riguardanti il documento stesso.
- Serie archivistica: aggregazione di unità archivistiche con caratteristiche omogenee in relazione alla natura o alla forma delle unità archivistiche medesime, ovvero in funzione dell'oggetto, della materia e delle funzioni del produttore.
- Servizio in rete o on-line: qualsiasi servizio di una amministrazione pubblica fruibile a distanza per via elettronica.
- Sistema di conservazione: sistema di conservazione a norma dei documenti informatici di un soggetto conservatore accreditato presso AgID.
- Sistema di Gestione Informatica dei Documenti (SGID): nell'ambito della pubblica amministrazione è il sistema di cui all'articolo 52 del DPR 445/00; per i privati è il sistema che consente la tenuta di un documento informatico.
- Sistema pubblico di connettività e cooperazione (SPC): l'insieme di infrastrutture tecnologiche e di regole tecniche, per lo sviluppo, la condivisione, l'integrazione e la diffusione del patrimonio informativo e dei dati della pubblica amministrazione, necessarie per assicurare l'interoperabilità di base ed evoluta e la cooperazione applicativa dei sistemi informatici e dei flussi informativi, garantendo la sicurezza, la riservatezza delle informazioni, nonché la salvaguardia e l'autonomia del patrimonio informativo di ciascuna pubblica amministrazione.
- Sistema pubblico per la gestione dell'identità digitale di cittadini e imprese (SPID): sistema costituito come insieme aperto di soggetti pubblici e privati che, previo accreditamento da parte dell'Agenzia per l'Italia digitale, gestiscono i servizi di registrazione e di messa a disposizione delle credenziali e degli strumenti di accesso in rete nei riguardi di cittadini e imprese per conto delle pubbliche amministrazioni, in qualità di erogatori di servizi in rete, ovvero, direttamente su richiesta degli interessati.
- Staticità: caratteristica che garantisce l'assenza nel documento informatico 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 del documento medesimo.
- Titolare di firma elettronica: la persona fisica cui è attribuita la firma elettronica e che ha accesso ai dispositivi per la sua creazione nonché alle applicazioni per la sua apposizione.
- Titolario o sistema di classificazione: sistema precostituito di partizioni astratte che permette di organizzare tutti i documenti secondo un ordinamento logico con riferimento alle funzioni e alle attività dell'amministrazione interessata.
- Unità Organizzativa Responsabile (UOR): l'Unità Organizzativa Responsabile è un sottoinsieme di una AOO, cioè un complesso di risorse umane e strumentali cui è affidata una competenza omogenea.
- 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: dati in forma elettronica che collegano altri dati in forma elettronica a una particolare ora e data, così da provare che questi ultimi esistevano in quel momento.

ELENCO DEGLI ALLEGATI

1. Area Organizzativa Omogenea dell'Unione
2. Abilitazioni all'utilizzo delle funzionalità del sistema di gestione informatica dei documenti (SGID)
3. Piano di sicurezza del Sistema di gestione informatica dei documenti
4. Formati elettronici adottati dall'Unione
5. Documenti soggetti a registrazione particolare da parte dell'Unione
6. Titolario di classificazione
7. Piano di conservazione dell'archivio
8. Manuale di conservazione conservatore accreditato AgID affidatario del servizio di Conservazione digitale.

ALLEGATO N. 1
AREA ORGANIZZATIVA OMOGENEA (AOO) DELL'UNIONE

L'art. 50, comma 4, del DPR 445/00 stabilisce che all'interno di ciascuna amministrazione siano create delle Aree Organizzative Omogenee, in modo da assicurare criteri uniformi di classificazione e archiviazione, nonché di comunicazione interna delle stesse.
L'art. 61 del DPR 445/00 stabilisce, altresì, che si costituisca per ciascuna AOO un Servizio responsabile della tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi. Al detto Servizio deve essere preposto un dirigente ovvero funzionario, in possesso di idonei requisiti professionali o di professionalità tecnico-archivistica.
Le Linee guida AgID sul documento informatico ribadiscono l'obbligo di individuare le suddette Aree Organizzative Omogenee e di nominare, al loro interno, un Responsabile della gestione documentale nonché un suo vicario per casi di vacanza, assenza o impedimento un Responsabile della conservazione.

In base alle succitate disposizioni normative, l'Unione dei Comuni Basso Campidano:

- è costituito in un'unica Area Organizzativa Omogenea;
- la denominazione ufficiale dell'AOO all'IPA è Unione dei Comuni Basso Campidano;
- il codice identificativo dell'Ente presso l'IPA è udcbc;
- il codice identificativo dell'AOO presso l'IPA è AAB9634.

Nell'ambito dell'AOO è stato istituito un Servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi, funzionalmente inserito nell'Area Amministrativa dell'Ente.
Nell'ambito della stessa AOO sono stati individuati un Responsabile della gestione documentale, un vicario per i casi di vacanza, assenza o impedimento del suddetto responsabile e un Responsabile della conservazione.

ALLEGATO N. 2
ABILITAZIONI ALL'UTILIZZO DELLE FUNZIONALITÀ DEL SISTEMA DI GESTIONE INFORMATICA DEI DOCUMENTI

I livelli di autorizzazione di accesso alle funzioni del Sistema di Gestione Informatica dei Documenti sono stabiliti dal Responsabile della gestione documentale; gli utenti accedono alle suddette funzionalità previa identificazione per mezzo di User-Id e Password secondo quanto stabilito dall'art. 10 del presente manuale.
All'interno dell'Unione l'utilizzo delle varie funzionalità è dettagliato per mezzo del seguente schema:

FUNZIONALITÀ ABILITATE	ABILITAZIONI
Definizione delle liste di controllo degli accessi (ACL)	Il Responsabile della gestione documentale
Registrazione di protocollo dei documenti in arrivo	Tutti gli operatori dell'Ente
Registrazione di protocollo dei documenti in partenza	Tutti gli operatori dell'Ente
Registrazione di protocollo dei documenti interni	Tutti gli operatori dell'Ente
Classificazione dei documenti	Operatore che esegue la registrazione di protocollo
Correzione/modifica della classificazione	Tutti gli operatori dell'Ente

ALLEGATO N. 3
PIANO DI SICUREZZA DEL SISTEMA DI GESTIONE INFORMATICA DEI DOCUMENTI

Premessa
Il presente piano di sicurezza, adottato ai sensi delle Linee guida AgID sul documento informatico, descrive le politiche adottate dall'Unione affinché:

- i documenti e le informazioni trattati dall'Ente siano resi disponibili, integri e riservati;
- i dati personali comuni, sensibili e/o giudiziari vengano custoditi in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

A tali fini le Linee guida AgID individuano i requisiti minimi di sicurezza dei sistemi di protocollo informatico a cui il presente piano si conforma.
Il piano di sicurezza, in base ai rischi cui sono esposti i dati (personali e non) e/o i documenti trattati, definisce:

- le politiche generali e particolari di sicurezza da adottare all'interno dell'Unione ;
- le modalità di accesso al Sistema di Gestione Informatica dei Documenti;
- gli interventi operativi adottati sotto il profilo organizzativo, procedurale e tecnico, al fine di garantire le misure di sicurezza necessarie alla tutela del patrimonio documentale dell'Ente e alla tutela e garanzia dei dati personali, sensibili o giudiziari;
- la formazione degli addetti;
- le modalità con le quali deve essere effettuato il monitoraggio periodico dell'efficacia e dell'efficienza delle misure di sicurezza.

Tale piano di sicurezza è soggetto a revisione con cadenza almeno biennale; a seguito di particolari esigenze, determinate da sopravvenienze normative o evoluzioni tecnologiche, potrà essere modificato anticipatamente.

Elementi di rischio cui sono soggetti i documenti informatici e i dati contenuti nel Sistema di Gestione Informatica dei Documenti
I principali elementi di rischio cui sono soggetti i documenti informatici e i dati trattati con l'ausilio delle tecnologie informatiche sono essenzialmente riconducibili alle seguenti tipologie:

- accesso non autorizzato, sia esso inteso come accesso al SGID o come accesso ai documenti, dati e unità archivistiche in esso contenuti;
- cancellazione o manomissione dei documenti e dei dati, includendo a tale proposito tutti i dati presenti sul Sistema di Gestione Informatica dei Documenti;
- perdita dei documenti e dei dati contenuti nel Sistema;
- trattamento illecito, eccedente rispetto allo scopo o comunque non in linea con la normativa vigente, dei dati personali.

Per prevenire tali rischi e le conseguenze da essi derivanti, l'Unione adotta gli accorgimenti e le politiche per la sicurezza di seguito descritte.

Procedure comportamentali degli operatori ai fini della protezione dei documenti informatici e dei dati in essi contenuti
Le postazioni di lavoro, da tavolo e portatili, o gli strumenti comunque funzionalmente assimilabili, di proprietà dell'Unione a vario titolo messi a disposizione del personale, sono strumenti di lavoro e il loro utilizzo è finalizzato allo svolgimento delle attività professionali e istituzionali dell'Ente.
Ogni operatore adotta comportamenti corretti, tali da preservare il buon funzionamento degli strumenti e da ridurre i rischi per la sicurezza dei sistemi informativi.
Gli operatori cui sono affidati i dispositivi informatici di proprietà dell'Unione sono tenuti ad avere le seguenti accortezze:

- l'accesso alle singole postazioni di lavoro avviene previa autenticazione dell'operatore tramite apposite credenziali di accesso personali, modificate con cadenza periodica e impostate secondo i criteri di default di Active Directory di Windows;
- qualora nei dispositivi e nelle postazioni di lavoro siano memorizzati dati personali, sensibili o giudiziari, l'operatore che li utilizza deve porre in atto comportamenti idonei a garantire la protezione di detti dati;
- ciascun operatore è tenuto a segnalare immediatamente ai referenti informatici ogni sospetto utilizzo non autorizzato, violazione della sicurezza o malfunzionamento relativo ai dispositivi informatici a lui assegnati;
- al momento della cessazione del rapporto di lavoro, ciascun operatore deve restituire all'Unione qualsiasi risorsa informatica a lui assegnata e mettere a disposizione ogni informazione di interesse istituzionale;

- non è consentito installare programmi non inerenti all'attività lavorativa;
- non è consentito copiare dati la cui titolarità sia dell'Unione su dispositivi esterni personali.

Ai fini della vigilanza nell'utilizzo degli strumenti informatici assegnati, ciascun operatore ha l'obbligo di impedire ad altri l'utilizzo non autorizzato della propria apparecchiatura informatica.
Le stazioni di lavoro, da tavolo e portatili, o gli strumenti comunque funzionalmente assimilabili, messi a disposizione del personale, non devono essere lasciati incustoditi. L'operatore è tenuto a bloccare o a spegnere il personal computer in caso di sospensione o termine dell'attività lavorativa e, comunque sempre, al termine dell'orario di servizio.

Accesso al Sistema di Gestione Informatica dei Documenti e ai documenti e dati in esso contenuti da parte di utenti interni all'AOO
L'accesso al Sistema di Gestione Informatica dei Documenti, da parte degli utenti interni all'AOO, avviene attraverso l'utilizzo di credenziali di autenticazione; i profili di abilitazione alle funzionalità del Sistema stesso sono attribuiti a ciascun utente sulla base di quanto stabilito dall'allegato n. 2 al presente manuale. L'accesso ai documenti e ai dati presenti sul Sistema è definito in base al livello di riservatezza degli stessi.
Le credenziali di autenticazione consistono in un codice (User-Id), per l'identificazione dell'incaricato, associato ad una parola chiave riservata (Password), conosciuta solamente dal medesimo; tali credenziali vengono verificate in tempo reale da un apposito sistema di identificazione, il quale consente l'accesso ai soggetti abilitati e traccia tutti gli accessi di ciascun utente, memorizzando, ai fini di controllo, l'User-Id corrispondente, ma non la Password dello stesso.
Agli incaricati è prescritto di adottare le necessarie cautele volte ad assicurare la segretezza della password; quest'ultima è composta di almeno 8 caratteri (di cui almeno una lettera maiuscola, una lettera minuscola, un numero ed un simbolo non alfanumerico) e non contiene riferimenti agevolmente riconducibili al titolare. La password è modificata dall'incaricato al suo primo utilizzo e, successivamente, con cadenza quadrimestrale o semestrale a seconda degli operatori;
Le credenziali di autenticazione non utilizzate da almeno sei mesi vengono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica; tali credenziali sono altresì disattivate anche nel caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali. I profili di accesso associati alle credenziali disattivate non vengono riattivati neppure successivamente.
Qualora il titolare delle credenziali di autenticazione dimenticasse la propria password si procederà all'assegnazione di una nuova chiave di accesso.
Le credenziali di accesso sono strettamente personali e ogni attività non regolare effettuata e riconducibile alle stesse è imputata al titolare delle credenziali medesime.

Accesso al trattamento di dati personali sensibili o giudiziari e politiche di sicurezza espressamente previste
L'accesso ai documenti contenenti dati personali, sensibili o giudiziari e ai dati medesimi avviene per mezzo dell'individuazione di specifici profili di autorizzazione, stabiliti sulla base del livello di riservatezza di ciascun documento, fascicolo, sottofascicolo o inserto, secondo quanto stabilito dall'art. 27 del presente manuale; tali profili, per ciascun incaricato o per classi omogenee di incaricati, sono individuati e configurati anteriormente all'inizio del trattamento.
Periodicamente, e comunque con cadenza almeno annuale, è verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione.
Gli incaricati del trattamento di dati personali, sensibili o giudiziari, come precedentemente indicato, non possono lasciare incustodita e accessibile la propria postazione di lavoro durante il trattamento degli stessi.
Per quanto riguarda l'accesso al Sistema di Gestione Informatica dei Documenti, le credenziali di autenticazione di ciascun operatore vengono consegnate dai medesimi in busta chiusa e sigillata al Responsabile della propria UOR; in caso di prolungata assenza o impedimento del soggetto incaricato del trattamento dei dati personali, sensibili o giudiziari e, qualora si renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema, il Responsabile della UOR è autorizzato ad utilizzare le credenziali contenute nella suddetta busta per procedere al trattamento, comunicandolo al titolare. Il soggetto titolare delle credenziali provvederà, al momento del proprio rientro in servizio, alla sostituzione della password, provvedendo all'inserimento della stessa in altra busta sigillata da consegnare nuovamente al suddetto Responsabile.

Trattamento dei dati personali, sensibili o giudiziari senza l'ausilio di strumenti elettronici
Analogamente al trattamento dei medesimi dati svolto per mezzo di strumenti elettronici, sarà verificato il sussistere delle condizioni per l'accesso e il trattamento dei suddetti dati, da parte di ciascun utente o gruppo di utenti, con cadenza almeno annuale.

I documenti, sono controllati e custoditi dagli incaricati del trattamento per tutto il tempo di svolgimento dei relativi compiti; nell'arco di tale periodo gli incaricati medesimi si assicureranno che a tali documenti non accedano persone prive di autorizzazione.
L'accesso agli archivi contenenti dati sensibili o giudiziari è consentito solo previa autorizzazione; le persone ammesse sono identificate e registrate.

Formazione dei documenti
I documenti informatici dell'Unione sono prodotti utilizzando i formati previsti dall'allegato n. 4 del presente manuale.
L'apposizione della firma digitale, volta a garantire l'attribuzione certa della titolarità del documento e la sua integrità, avviene previa conversione in un formato, tra quelli previsti dalle Linee guida AgID, che garantisca la leggibilità, l'interscambiabilità, la non alterabilità, l'immutabilità nel tempo del contenuto e della struttura del documento medesimo (ad esempio il PDF/A); l'acquisizione mediante scansione dei documenti analogici avverrà in uno dei formati aventi le medesime caratteristiche.
L'apposizione della firma digitale o di altre eventuali sottoscrizioni elettroniche, nonché la validazione temporale del documento sottoscritto digitalmente avvengono in conformità di quanto sancito dalla vigente normativa in materia.

Sicurezza delle registrazioni di protocollo
L'accesso al registro di protocollo al fine di effettuare le registrazioni o di apportare modifiche è consentito soltanto al personale abilitato.
Di norma i dipendenti che operano nell'ambito dei vari uffici dell'Ente sono abilitati ad accedere esclusivamente ai dati di protocollo dei documenti da essi prodotti, ad essi assegnati o, comunque, di competenza del proprio ufficio di riferimento.
Ogni registrazione di protocollo viene memorizzata dal Sistema di Gestione Informatica dei Documenti, unitamente all'identificativo univoco dell'autore che l'ha eseguita e alla data e all'ora della stessa.
Eventuali modifiche, autorizzate ai sensi dell'art. 28 del presente manuale, vengono registrate per mezzo di log di sistema che mantengono traccia dell'autore, della modifica effettuata, nonché della data e dell'ora; il Sistema mantiene leggibile la precedente versione dei dati di protocollo, permettendo, in tal modo, la completa ricostruzione cronologica di ogni registrazione.
Il Sistema non consente la modifica del numero e della data di protocollo; in tal caso l'unica possibile modifica è l'annullamento della registrazione stessa di cui, analogamente al caso precedente, il Sistema manterrà traccia. L'annullamento di una registrazione di protocollo deve sempre essere accompagnato da autorizzazione del Responsabile della gestione documentale.
L'impronta digitale del documento informatico, associata alla registrazione di protocollo del medesimo è generata utilizzando una funzione di hash, conforme a quanto previsto dalla normativa vigente.
Al fine di garantire l'immodificabilità delle registrazioni di protocollo, il Sistema permette, al termine della giornata lavorativa, la produzione del registro giornaliero delle registrazioni di protocollo, in formato digitale; tale registro, formato nel rispetto di quanto previsto nel manuale di conservazione, sarà trasferito nell'arco della giornata lavorativa successiva, alla struttura di conservazione accreditata di cui l'Unione si serve, secondo quanto previsto dall'articolo 3 del presente manuale.

Gestione dei documenti e sicurezza logica del Sistema
I documenti informatici, una volta registrati sul Sistema di Gestione Informatica dei Documenti, risultano immodificabili e non eliminabili; l'accesso ad essi, da parte degli utenti interni all'AOO, avviene soltanto attraverso il Sistema medesimo, previa la suddetta procedura di identificazione informatica e nel rispetto dei profili di autorizzazione di ciascun utente.
Il Sistema consente l'effettuazione di qualsiasi operazione su di esso o sui dati, documenti, fascicoli e aggregazioni documentali in esso contenuti, esclusivamente agli utenti abilitati per lo svolgimento di ciascuna attività; il Sistema effettua, inoltre, il tracciamento di qualsiasi evento di modifica delle informazioni trattate e di tutte le attività rilevanti ai fini della sicurezza svolte su di esso da ciascun utente, in modo da garantirne l'identificazione; tali registrazioni (log di sistema) sono protette al fine di non consentire modifiche non autorizzate. I dati registrati nei file di log sono raccolti, memorizzati e conservati dal sistema informatico in conformità alla normativa vigente. Le informazioni contenute nei file di log possono essere messe a disposizione dell'autorità giudiziaria, la quale può richiedere la non cancellazione e la conservazione di tali file per un periodo più lungo di quanto disposto dalla legge.
Il Sistema e tutti i documenti e dati in esso contenuti sono protetti contro i rischi di intrusione non autorizzata e contro l'azione di programmi informatici.
Ai fini di ridurre la vulnerabilità dei sistemi informativi, il sistema operativo utilizzato dall'AOO e il Sistema di Gestione Informatica dei Documenti, vengono tenuti costantemente aggiornati, per mezzo dell'istallazione degli aggiornamenti periodici che i fornitori rendono disponibili.

Backup e ripristino dell'accesso ai dati
Il Backup dei dati contenuti nel Sistema di Gestione Informatica dei Documenti viene eseguito quotidianamente.
Il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici avviene nel rispetto dei tempi previsti dalla vigente normativa in materia.
I supporti riscrivibili contenenti dati sensibili o giudiziari, possono venire cancellati e riutilizzati esclusivamente nel caso in cui le informazioni in essi contenute non siano intelligibili e in alcun modo ricostruibili.
Qualora dati sensibili e giudiziari vengano memorizzati su supporti rimovibili non riscrivibili, una volta che sia cessato lo scopo per cui tali dati sono stati memorizzati, i supporti vengono distrutti.

Trasmissione e interscambio dei documenti
La trasmissione e l'interscambio di documenti e fascicoli informatici all'interno dell'AOO avviene esclusivamente per mezzo del Sistema di Gestione Informatica dei Documenti; nessun'altra modalità è consentita, al fine di evitare la dispersione e la circolazione incontrollata di documenti e dati.
La trasmissione di documenti informatici al di fuori dell'Ente avviene tramite PEC o mediante i meccanismi dell'interoperabilità di cui al Sistema Pubblico di Connettività e Cooperazione (SPC), utilizzando le informazioni contenute nella segnatura di protocollo.
Le informazioni relative alla segnatura di protocollo sono strutturate in un file XML conforme alle specifiche contenute nelle Linee guida AgID relative alla produzione, gestione e conservazione del documento informatico.

Conservazione dei documenti
I documenti informatici registrati sul SGID sono affidati per la conservazione digitale ad un soggetto conservatore accreditato dall'AgID, che svolge tale attività in conformità a quanto sancito dalle regole tecniche contenute nelle Linee guida AgID. Il trasferimento in conservazione avviene mediante la produzione di pacchetti di versamento, basati su uno schema XML conforme a quanto previsto nel manuale di conservazione del consevatore.

Disaster recovery e continuità operativa
L'Unione si è dotato di sistema di disaster recovery, in grado di garantire il ritorno alla normale operatività in caso di eventi calamitosi, prevedendo il ripristino dei dati dalle copie in cloud, nel rispetto dei tempi previsti dalla vigente normativa in materia.

Accesso di Utenti esterni al Sistema
L'esercizio del diritto di accesso da parte di utenti esterni al Sistema viene effettuato nel rispetto di quanto sancito dalla legge 241/90 e s.m.i., dal D. Lgs. 196/03 e s.m.i. e dal Regolamento Europeo sulla Protezione dei Dati n. 679 del 2016.
Qualora l'utente esterno decida di esercitare il proprio diritto di accesso rivolgendosi direttamente all'URP o ad altro sportello allo scopo predisposto, la consultazione deve avvenire in modo che siano resi visibili soltanto dati o notizie che riguardino il soggetto interessato ed adottando gli opportuni accorgimenti (ad es. il posizionamento del monitor) volti ad evitare la diffusione di informazioni di carattere personale.

Piani formativi del personale
Ai fini di una corretta gestione dell'intero ciclo dei documenti informatici, dalla formazione degli stessi fino alla loro trasmissione al sistema di conservazione, l'Unione predispone le apposite attività formative per il personale, con particolare riferimento ai seguenti temi:
- utilizzo applicativi software per la gestione dei documenti informatici;
- utilizzo del Sistema di Gestione Informatica dei Documenti;
- politiche e aspetti organizzativi previsti nel manuale di gestione;
- legislazione e tematiche relative al documento informatico, alla gestione documentale e alla conservazione digitale a norma;
- fascicolazione dei documenti informatici;
- gestione dei fascicoli informatici;

Monitoraggio periodico del funzionamento del Sistema
Il Responsabile della gestione documentale dell'Ente effettua periodiche verifiche sul corretto funzionamento del Sistema di Gestione Informatica dei Documenti, valutando a tal fine, anche per mezzo di controlli a campione, il corretto svolgimento delle operazioni inerenti la gestione documentale. I log di sistema sono comunque conservati e protetti in modo da consentire successive verifiche che dovessero risultare necessarie sullo svolgimento di tutte le operazioni rilevanti al fine della sicurezza dei dati, effettuate sul sistema.

Misure di tutela e garanzia
Qualora l'Ente adotti misure minime di sicurezza avvalendosi di soggetti esterni alla propria struttura, per provvedere all'esecuzione, riceverà dall'installatore una descrizione scritta dell'intervento che ne attesti la conformità ai criteri di protezione dei dati sensibili, personali e giudiziari previsti dalla normativa.

ALLEGATO N. 4
FORMATI ELETTRONICI ADOTTATI

Al fine di produrre e gestire documenti informatici che siano conformi alla normativa vigente e compatibili con un processo conservativo a lungo termine, l'Unione utilizza i formati elettronici individuati dalla normativa vigente come idonei alla conservazione digitale. Nell'utilizzo dei formati più comuni, l'Ente segue le indicazioni di seguito riportate:

- I documenti informatici prodotti dall'Ente, per poter essere acquisiti nel Sistema di Gestione Informatica dei Documenti, devono essere prodotti o convertiti in uno dei formati previsti dalle Linee guida AgID; tale conversione avviene preferibilmente nel formato PDF/A ma possono essere memorizzati nel Sistema anche documenti prodotti utilizzando gli altri formati individuati dalla normativa, fatti salvi i casi di seguito descritti;
- i documenti informatici prodotti dall'Ente, al fine di essere sottoscritti con firma digitale, vengono migrati in PDF/A prima di essere sottoscritti e registrati nel Sistema, non fanno eccezione eventuali elaborati grafici dell'Ufficio Tecnico, prodotti originariamente con formati diversi, ad es. DXF e DWF; gli elaborati eventualmente prodotti tramite i formati DWG o SVG, invece, poiché trattasi di formato idoneo alla conservazione, possono essere firmati senza che siano stati preventivamente convertiti;
- per l'acquisizione in formato digitale di documenti, nativamente prodotti in formato cartaceo, mediante l'attività di scansione, l'Ente può utilizzare i formati PDF/A, TIF/TIFF e JPG/JPEG;
- per l'acquisizione di file immagine l'Ente può utilizzare i formati PNG, TIF/TIFF e JPG/JPEG;
- per l'acquisizione di documenti sottoscritti con firma digitale o altra sottoscrizione elettronica inviati all'AOO da parte di utenti esterni, l'Unione richiede l'utilizzo preferibilmente del formato PDF/A; costituiscono eccezione le fatture elettroniche le quali sono in formato XML;
- per la produzione di distinte di mandati e reversali informatici viene utilizzato il formato XML conforme allo standard OPI, previsto dalla vigente normativa conformemente alle regole del SIOPE+;
- per l'acquisizione sul sistema di documenti che non necessitano di firma digitale o altra sottoscrizione elettronica l'Unione accetta, a seconda delle finalità per cui i documenti sono utilizzati, tutti i formati previsti dalla vigente normativa in materia, adatti ai fini della conservazione digitale; in tal caso possono essere utilizzati anche i formati ODF, OOXML (es. DOCX o XLSX) e TXT;
- ai fini della conservazione dei messaggi di posta elettronica lo standard a cui fare riferimento è RFC 2822/MIME, mentre per quanto riguarda il formato degli allegati al suddetto messaggio si utilizzeranno, a seconda della tipologia del documento trattato e delle esigenze, i formati elettronici precedentemente indicati;
- al fine della pubblicazione di documenti sul proprio sito istituzionale l'Ente utilizza il formato PDF/A;
- per la produzione del registro giornaliero di protocollo da inviare al conservatore accreditato l'Ente utilizza il formato PDF/A;
- per la produzione di archivi di file compressi l'Ente utilizza il forato ZIP; tenendo presente che i formati dei file contenuti nella cartella .zip seguano le indicazioni previste nel presente allegato.

Per quanto riguarda la scelta di formati compressi si deve valutare sempre quanto segue: i formati compressi consentono la riduzione della dimensione del file, permettendo di risparmiare spazio ai fini della memorizzazione dello stesso. La compressione può essere di tipo lossless o lossy: il primo tipo consente di comprimere il file senza la perdita di informazioni, evitando la riduzione di qualità e permettendo il recupero integrale della qualità del file originario non compresso, il secondo tipo di compressione, invece, comporta la perdita di alcune informazioni, causando una diminuzione della qualità del file al momento della sua rappresentazione, non più recuperabili, esso permette però di ottenere dimensioni più ridotte rispetto ad una compressione di tipo lossless.
Ai fini di un processo di conservazione a lungo termine sono sempre da preferire, laddove sia necessaria la compressione del file, formati con compressione di tipo lossless.

ALLEGATO N. 5
DOCUMENTI SOGGETTI A REGISTRAZIONE PARTICOLARE

L'Unione individua le seguenti tipologie di documenti come soggette a registrazione particolare, secondo quanto disposto dall'articolo 22 del presente manuale di gestione:

- Deliberazioni dell'Assemblea;
- Deliberazioni della Giunta;
- Decreti del Presidente;
- Ordinanze del Presidente;
- Atti rogati o autenticati dal Segretario Comunale;
- Ordinanze dei responsabili;
- Determinazioni dei responsabili;
- Mandati di pagamento;
- Reversali;
- Fatture;
- Atti di liquidazione;
- Autorizzazioni edilizie;

I suddetti documenti soggetti a registrazione particolare sono registrati con una propria numerazione, attribuita sulla base di appositi repertori.

ALLEGATO N. 6
TITOLARIO

Titolo I. Amministrazione generale

1. Legislazione e circolari esplicative
2. Denominazione, territorio e confini, circoscrizioni di decentramento, toponomastica
3. Statuto
4. Regolamenti
5. Stemma, gonfalone, sigillo
6. Archivio generale
7. Sistema informativo
8. Informazioni e relazioni con il pubblico
9. Politica del personale; ordinamento degli uffici e dei servizi
10. Relazioni con le organizzazioni sindacali e di rappresentanza del personale
11. Controlli interni ed esterni
12. Editoria e attività informativo-promozionale interna ed esterna
13. Cerimoniale, attività di rappresentanza; onorificenze e riconoscimenti
14. Interventi di carattere politico e umanitario; rapporti istituzionali
15. Forme associative e partecipative per l'esercizio di funzioni e servizi e adesione dell'Unione ad Associazioni
16. Area e città metropolitana
17. Associazionismo e partecipazione

Titolo II. Organi di governo, gestione, controllo, consulenza e garanzia

1. Sindaco
2. Vice-Sindaco
3. Consiglio
4. Presidente del Consiglio
5. Conferenza dei capigruppo e Commissioni del Consiglio
6. Gruppi consiliari
7. Giunta
8. Commissario prefettizio e straordinario
9. Segretario e Vice-segretario
10. Direttore generale e dirigenza
11. Revisori dei conti
12. Difensore civico
13. Commissario/ad acta
14. Organi di controllo interni
15. Organi consultivi
16. Consigli circoscrizionali
17. Presidente dei Consigli circoscrizionali
18. Organi esecutivi circoscrizionali
19. Commissioni dei Consigli circoscrizionali
20. Segretari delle circoscrizioni
21. Commissario /ad acta/ delle circoscrizioni
22. Conferenza dei Presidenti di quartiere

Titolo III. Risorse umane

1. Concorsi, selezioni, colloqui
2. Assunzioni e cessazioni
3. Comandi e distacchi; mobilità
4. Attribuzione di funzioni, ordini di servizio e missioni
5. Inquadramenti e applicazione contratti collettivi di lavoro
6. Retribuzioni e compensi
7. Trattamento fiscale, contributivo e assicurativo
8. Tutela della salute e sicurezza sul luogo di lavoro
9. Dichiarazioni di infermità ed equo indennizzo
10. Indennità premio di servizio e trattamento di fine rapporto, quiescenza
11. Servizi al personale su richiesta
12. Orario di lavoro, presenze e assenze
13. Giudizi, responsabilità e provvedimenti disciplinari
14. Formazione e aggiornamento professionale
15. Collaboratori esterni

Titolo IV. Risorse finanziarie e patrimoniali
1. Bilancio preventivo e Piano esecutivo di gestione (PEG)
2. Gestione del bilancio e del PEG (con eventuali variazioni)
3. Gestione delle entrate: accertamento, riscossione, versamento
4. Gestione della spesa: impegno, liquidazioni, ordinanze e pagamento
5. Partecipazioni finanziarie
6. Rendiconto della gestione; adempimenti e verifiche contabili
7. Adempimenti fiscali, contributivi e assicurativi
8. Beni immobili
9. Beni mobili
10. Economato
11. Oggetti smarriti e recuperati
12. Tesoreria
13. Concessionari ed altri incaricati della riscossione delle entrate
14. Pubblicità e pubbliche affissioni

Titolo V. Affari legali
1. Contenzioso
2. Responsabilità civile e patrimoniale verso terzi; assicurazioni
3. Pareri e consulenze

Titolo VI. Pianificazione e gestione del territorio
1. Urbanistica: piano regolatore generale e varianti
2. Urbanistica: strumenti di attuazione del Piano regolatore generale
3. Edilizia privata
4. Edilizia pubblica
5. Opere pubbliche
6. Catasto
7. Viabilità
8. Servizio idrico integrato, luce, gas, trasporti pubblici, gestione dei rifiuti e altri servizi
9. Ambiente: autorizzazioni, monitoraggio e controllo
10. Protezione civile ed emergenze

Titolo VII. Servizi alla persona
1. Diritto allo studio e servizi
2. Asili nido e scuola materna
3. Promozione e sostegno delle istituzioni di istruzione e della loro attività
4. Orientamento professionale; educazione degli adulti; mediazione culturale
5. Istituti culturali (Musei, biblioteche, teatri, Scuola comunale di musica, etc.)
6. Attività ed eventi culturali
7. Attività ed eventi sportivi
8. Pianificazione e accordi strategici con enti pubblici e privati e con il volontariato sociale
9. Prevenzione, recupero e reintegrazione dei soggetti a rischio
10. Informazione, consulenza ed educazione civica
11. Tutela e curatela di incapaci
12. Assistenza diretta e indiretta, benefici economici
13. Attività ricreativa e di socializzazione
14. Politiche per la casa
15. Politiche per il sociale

Titolo VIII. Attività economiche
1. Agricoltura e pesca
2. Artigianato
3. Industria
4. Commercio
5. Fiere e mercati
6. Esercizi turistici e strutture ricettive
7. Promozione e servizi

Titolo IX. Polizia locale e sicurezza pubblica
1. Prevenzione ed educazione stradale
2. Polizia stradale
3. Informative
4. Sicurezza e ordine pubblico

Titolo X. Tutela della salute
1. Salute e igiene pubblica
2. Trattamenti Sanitari Obbligatori
3. Farmacie
4. Zooprofilassi veterinaria
5. Randagismo animale e ricoveri

Titolo XI. Servizi demografici
1. Stato civile
2. Anagrafe e certificazioni
3. Censimenti
4. Polizia mortuaria e cimiteri

Titolo XII. Elezioni e iniziative popolari
1. Albi elettorali
2. Liste elettorali
3. Elezioni
4. Referendum
5. Istanze, petizioni e iniziative popolari

Titolo XIII. Affari militari
1. Leva e servizio civile sostitutivo
2. Ruoli matricolari
3. Caserme, alloggi e servitù militari
4. Requisizioni per utilità militari

Titolo XIV. Oggetti diversi
1. Oggetti diversi

Titolo I. Amministrazione generale

Classi	Tipologie documentarie	Conservazione	Note
1. Legislazione e circolari esplicative			
	Pareri chiesti dal Comune su leggi specifiche	Permanente	
	Circolari pervenute: repertorio annuale	Permanente	
	Circolari emanate dal Comune: repertorio annuale	Permanente	
2. Denominazione, territorio e confini, circoscrizioni di decentramento, toponomastica			
	Denominazione del Comune	Permanente	
	Attribuzione del titolo di città	Permanente	
	Confini del Comune	Permanente	
	Costituzione delle circosccrizioni	Permanente	
	Verbali e deliberazioni della Commissione comunale per la toponomastica: repertorio annuale	Permanente	
3. Statuto			
	Redazione, modifiche e interpretazioni dello statuto	Permanente, dopo sfoltimento del materiale informativo relativo ad altri Comuni	
4. Regolamenti			
	Regolamenti emessi dal Comune: repertorio annuale	Permanente	
	Redazione dei regolamenti: un fasc. per ciascun affare	Permanente, previo sfoltimento dei documenti di carattere transitorio	Tenere un solo esemplare, scartare gli altri
5. Stemma, gonfalone, sigillo			
	Definizione, modifica, riconoscimento dello stemma	Permanente	
	Definizione, modifica, riconoscimento del gonfalone	Permanente	
	Definizione, modifica, riconoscimento del sigillo	Permanente	
	Concessione del patrocinio gratuito e del connesso uso dello stemma del Comune: fasc. annuale per attività	Permanente	Perché documenta attività che si svolgono nel territorio

6. Archivio generale			
	Registro di protocollo	Permanente	
	Repertorio dei fascicoli	Permanente	
	Organizzazione del servizio e dell'attività ordinaria (aggiornamento del manuale di gestione con titolario e piano di conservazione, selezione periodica, riordino, inventariazione, spostamenti e versamenti di materiale, depositi e comodati):	Permanente	
	Interventi straordinari (ad esempio, traslochi, restauri, gestione servizi esterni, scelta del software di gestione)	Permanente	
	Richieste di accesso per fini amministrativi	1 anno dalla ricollocazione del materiale	
	Richieste di informazioni archivistiche e richieste per motivi di studio	Permanente	
	Richieste di pubblicazione all'albo pretorio	1 anno	
	Registro dell'Albo pretorio	20 anni	
	Richieste di notifica presso la casa comunale (con allegati)	2 anni	
	Registro delle notifiche	20 anni	
	Registri delle spedizioni e delle spese postali	1 anno	
	Ordinanze del Sindaco: repertorio	Permanente	
	Decreti del Sindaco: repertorio	Permanente	
	Ordinanze dei dirigenti: repertorio	Permanente	
	Determinazioni dei dirigenti: repertorio	Permanente	
	Deliberazioni del Consiglio comunale: repertorio	Permanente	
	Deliberazioni della Giunta comunale: repertorio	Permanente	
	Verbali delle adunanze del Consiglio comunale: repertorio	Permanente	
	Verbali delle adunanze della Giunta comunale: repertorio	Permanente	
	Verbali degli altri organi collegiali del Comune: repertorio	Permanente	
	Verbali delle adunanze dei Consigli circoscrizionali: un repertorio annuale per ciascuna circoscrizione	Permanente	
	Deliberazioni dei Consigli circoscrizionali: un repertorio annuale per ciascuna circoscrizione	Permanente	
	Verbali delle adunanze degli Esecutivi circoscrizionali: un repertorio annuale per ciascuna circoscrizione	Permanente	
	Deliberazioni degli Esecutivi circoscrizionali: un repertorio annuale per ciascuna circoscrizione	Permanente	
	Verbali degli organi collegiali delle circoscrizioni: un repertorio annuale per ciascuna circoscrizione	Permanente	
	Registro dell'Albo della circoscrizione: un repertorio annuale per ciascuna circoscrizione	Permanente	

	Contratti e convenzioni: repertorio	Permanente	20 anni per un'eventuale serie separata di contratti di scarsa rilevanza
	Contratti e convenzioni delle circoscrizioni: un repertorio per ciascuna circoscrizione	Permanente	20 anni per un'eventuale serie separata di contratti di scarsa rilevanza
	Atti rogati dal segretario comunale (contratti e atti unilaterali in forma pubblica amministrativa)	Permanente	
7. Sistema informativo			
	Organizzazione del sistema	Permanente	
	Statistiche	Permanente, dopo l'eliminazione dei materiali preparatori	
8. Informazioni e relazioni con il pubblico			
	Iniziative specifiche dell'URP: un fasc. per ciascun affare	Permanente, dopo sfoltimento del carteggio di carattere transitorio e strumentale	
	Reclami dei cittadini (comunque pervenuti)	Permanente	
	Atti del Difensore civico	Permanente	
	Bandi e avvisi a stampa	Permanente	
	Materiali preparatori per il sito Web	Permanente	
9. Politica del personale; ordinamento degli uffici e dei servizi			
	Attribuzione di competenze agli uffici	Permanente	
	Organigramma: un fasc. per ciascuna definizione dell'organigramma	Permanente	
	Organizzazione degli uffici: un fasc. per ciascun affare	Permanente	
	Orari di apertura degli uffici comunali e degli altri uffici e attività insistenti sul territorio comunale	Permanente	
	Materiale preparatorio per le deliberazioni in materia di politica del personale	10 anni	

10. Relazioni con le organizzazioni sindacali e di rappresentanza del personale			
	Rapporti di carattere generale	Permanente	
	Costituzione delle rappresentanze del personale	Permanente	
	Verbali della Delegazione trattante per la contrattazione integrativa decentrata	Permanente	
11. Controlli esterni			
	Controlli	Permanente	
12. Editoria e attività informativo-promozionale interna ed esterna			
	Pubblicazioni istituzionali del Comune (libri, riviste, inserzioni o altro)	Permanente	
	Pubblicazioni istituzionali del Comune (materiali preparatori)	2 anni	
	Comunicati stampa	Permanente	
13. Cerimoniale, attività di rappresentanza; onorificenze e riconoscimenti			
	Iniziative specifiche: un fasc. per ciascuna iniziativa	Permanente	
	Onorificenze (concesse e ricevute): un fasc. per ciascun evento	Permanente	
	Concessione dell'uso del sigillo: un fasc. annuale	Permanente	
14. Interventi di carattere politico e umanitario; rapporti istituzionali			
	Iniziative specifiche (ad esempio, adesione a movimenti di opinione): un fasc. per ciascun affare	Permanente	
	Gemellaggi	Permanente	
	Promozione di comitati: un fasc. per ciascun affare	Permanente	

15. Forme associative e partecipative per l'esercizio di funzioni e servizi e adesione del Comune ad Associazioni			
	Costituzione di enti controllati dal Comune (comprensivo della nomina dei rappresentanti e dei verbali inviati per approvazione)	Permanente, previo sfoltimento del carteggio di carattere transitorio	
	Partecipazione del Comune a enti e associazioni (comprensivo della nomina dei rappresentanti)	Permanente, previo sfoltimento del carteggio di carattere transitorio	
16. Area e città metropolitana			
	Costituzione e rapporti istituzionali	Permanente	
17. Associazionismo e partecipazione			
	Politica di incoraggiamento e appoggio alle associazioni	Permanente	
	Albo dell'associazionismo: elenco delle associazioni accreditate	Permanente	
	Fascicoli delle associazioni che chiedono l'iscrizione all'albo	Permanente	

Titolo II. Organi di governo, gestione, controllo, consulenza e garanzia

Classi	Tipologie documentarie	Conservazione	Note
1. Sindaco			
	Fasc. personale che dura quanto il mandato	Permanente	
2. Vice-sindaco			
	Fasc. personale che dura quanto il mandato	Permanente	
3. Consiglio			
	Fasc. personali: un fasc. per ogni consigliere che dura quanto dura il mandato	Permanente	
	Convocazioni del Consiglio e OdG	1 anno	Purché riportati nei verbali
	Interrogazioni e mozioni consiliari	Permanente	dopo sfoltimento
	Bollettino della situazione patrimoniale dei titolari di cariche elettive e di cariche direttive	Permanente	
4. Presidente del Consiglio			
	Fasc. personale che dura quanto il mandato	Permanente	
5. Conferenza dei capigruppo e Commissioni del Consiglio			
	Verbali della Conferenza	Permanente	
	Verbali delle Commissioni	Permanente	
6. Gruppi consiliari			
	Accreditamento presso il Consiglio	Permanente	Scartare i materiali prodotti o raccolti dai Gruppi
7. Giunta			
	Nomine, revoche e dimissioni degli assessori	Permanente	
	Convocazioni della Giunta e OdG	1 anno	Purché riportati nei verbali

8. Commissario prefettizio e straordinario			
	Fasc. personale	Permanente	
9. Segretario e Vice-segretario			
	Fasc. personale (nomina, etc.) per la durata dell'incarico	Permanente	
10. Direttore generale e dirigenza			
	Fasc. personale	Permanente	
11. Revisori dei conti			
	Fasc. personale	Permanente	
12. Difensore civico			
	Fasc. personale	Permanente	
13. Commissario *ad acta*			
	Fasc. personale	Permanente	
14. Organi di controllo interni			
	Un fasc. per ogni organo	Permanente	
15. Organi consultivi			
	Un fasc. per ogni organo	Permanente	
16. Consigli circoscrizionali			
	Fasc. personali: un fasc. per ogni consigliere che dura quanto dura il mandato	Permanente	
	Convocazioni del Consiglio e OdG	1 anno	Purché riportati nei verbali
	Interrogazioni consiliari	Permanente	
17. Presidenti dei Consigli circoscrizionali			
	Fasc. personale che dura quanto il mandato	Permanente	

18. Organi esecutivi circoscrizionali			
	Nomine e dimissioni dei componenti	Permanente	
	Convocazioni e OdG delle riunioni	1 anno	Purché riportati nei verbali
19. Commissioni dei Consigli circoscrizionali			
	Un fasc. per ogni commissione	Permanente	
20. Segretari delle circoscrizioni			
	Fasc. personale (nomina, etc.) per la durata dell'incarico	Permanente	
21. Commissario *ad acta* delle circoscrizioni			
	Fasc. personale	Permanente	
22. Conferenza dei Presidenti di quartiere			
	Verbali della Conferenza	Permanente	

Titolo III. Risorse umane

Classi	Tipologie documentarie	Conservazione	Note
	Fascicoli personali dei dipendenti e assimilati (quindi anche collaboratori a contratto o a progetto)	Permanente previo sfoltimento da eseguire seguendo la tempistica prevista per le singole classi	
1. Concorsi, selezioni, colloqui			
	Criteri generali e normativa per il reclutamento del personale: un fasc. con eventuali sottofascicoli	Permanente	
	Procedimenti per il reclutamento del personale: un fasc. per ciascun procedimento (fasc. per affare), con i seguenti sottofascicoli: - Bando e manifesto - Domande - Allegati alle domande (ove previsti dal bando) - Verbali - Prove d'esame - Copie bando restituite al Comune	Permanente 1 anno dopo la scadenza dei termini per i ricorsi da restituire dopo la scadenza dei termini per i ricorsi permanente 1 anno dopo la scadenza dei termini per i ricorsi 1 anno dopo la scadenza dei termini per i ricorsi	Agli interessati
	Curricula inviati per richieste di assunzione	2 anni	
	Domande di assunzione pervenute senza indizione di concorso o selezione	1 anno	
2. Assunzioni e cessazioni			
	Criteri generali e normativa per le assunzioni e cessazioni	Permanente	
	Determinazioni di assunzione e cessazione dei singoli inserite nei singoli fascicoli personali	Permanente	

3. Comandi e distacchi; mobilità			
	Criteri generali e normativa per comandi, distacchi, mobilità	Permanente	
	Determinazioni di comandi, distacchi e mobilità inserite nei singoli fascicoli personali	Permanente	
4. Attribuzione di funzioni, ordini di servizio e missioni			
	Criteri generali e normativa per le attribuzioni di funzioni, ordini di servizio e missioni	Permanente	
	Determinazioni di attribuzione di funzioni inserite nei singoli fascicoli personali	Permanente	
	Determinazioni di missioni inserite nei singoli fascicoli personali	10 anni	
	Determinazioni di ordini di servizio inserite nei singoli fascicoli personali	Permanente	
	Ordini di servizio collettivi	Permanente	
	Autorizzazione allo svolgimento di incarichi esterni	2 anni	
5. Inquadramenti e applicazione contratti collettivi di lavoro			
	Criteri generali e normativa per gli inquadramenti e le applicazione dei contratti collettivi di lavoro	Permanente	
	Determinazione dei ruoli e contratti collettivi	Permanente	NB i contratti con il singolo confluiscono nel fasc. personale
	Determinazioni relative ai singoli	Permanente	
6. Retribuzioni e compensi			
	Criteri generali e normativa per le retribuzioni e compensi	Permanente	
	Anagrafe delle prestazioni: schede	5 anni	
	Determinazioni inserite nei singoli fascicoli personali	5 anni dalla cessazione dal servizio	
	Ruoli degli stipendi: base di dati/ tabulati	Permanente	
	Provvedimenti giudiziari di requisizione dello stipendio	5 anni	
7. Trattamento fiscale, contributivo e assicurativo			
	Criteri generali e normativa per gli adempimenti fiscali, contributivi e assicurativi	Permanente	
	Trattamento assicurativo inserito nei singoli fascicoli personali	5 anni dalla chiusura del fascicolo	

	Trattamento contributivo inserito nei singoli fascicoli personali	5 anni dalla chiusura del fascicolo	
	Trattamento fiscale inserito nei singoli fascicoli personali	5 anni dalla chiusura del fascicolo	
	Assicurazione obbligatoria inserita nei singoli fascicoli personali	5 anni dalla chiusura del fascicolo	
8. Tutela della salute e sicurezza sul luogo di lavoro			
	Criteri generali e normativa per la tutela della salute e sicurezza sul luogo di lavoro	Permanente	
	Rilevazione dei rischi, ai sensi della 626/94: un fasc. per sede	Tenere l'ultima e scartare la precedente	
	Prevenzione infortuni	Permanente	
	Registro infortuni	Permanente	Per L. 626/94
	Verbali delle rappresentanze dei lavoratori per la sicurezza	Permanente	
	Denuncia di infortunio e pratica relativa, con referti, inserita nei singoli fascicoli personali	Permanente	
	Fascicoli relativi alle visite mediche ordinarie (medicina del lavoro)	10 anni	
9. Dichiarazioni di infermità ed equo indennizzo			
	Criteri generali e normativa per le dichiarazioni di infermità	Permanente	
	Dichiarazioni di infermità e calcolo dell'indennizzo inserite nel singolo fascicolo personale	Permanente	
10. Indennità premio di servizio e trattamento di fine rapporto, quiescenza			
	Criteri generali e normativa per il trattamento di fine rapporto	Permanente	
	Trattamento pensionistico e di fine rapporto inserito nel singolo fascicolo personale	Permanente	
11. Servizi al personale su richiesta			
	Criteri generali e normativa per i servizi su richiesta	Permanente	
	Domande di servizi su richiesta (mensa, asili nido, colonie estive, soggiorni climatici, etc.)	2 anni	

12. Orario di lavoro, presenze e assenze			
	Criteri generali e normativa per le assenze	Permanente	
	Domande e dichiarazioni dei dipendenti sull'orario inserite nel singolo fascicolo personale: - 150 ore - permessi d'uscita per motivi personali - permessi per allattamento - permessi per donazione sangue - permessi per motivi sindacali - opzione per orario particolare e part-time	 2 anni 2 anni 2 anni 2 anni 2 anni Permanente	
	Domande e dichiarazioni dei dipendenti sulle assenze (con allegati) inserite nel singolo fascicolo personale: - congedo ordinario - congedo straordinario per motivi di salute - congedo straordinario per motivi personali e familiari - aspettativa per infermità - aspettativa per mandato parlamentare o altre cariche elettive - aspettativa obbligatoria per maternità e puerperio - aspettativa facoltativa per maternità e puerperio - aspettativa per motivi di famiglia - aspettativa sindacale - certificati medici	 2 anni 2 anni Alla cessazione dal servizio Permanente Permanente Permanente Permanente Permanente Permanente Alla cessazione dal servizio	
	Referti delle visite di controllo inseriti nel singolo fascicolo personale	Alla cessazione dal servizio	
	Fogli firma; cartellini marcatempo; tabulati elettronici di rilevazione presenze	2 anni	In assenza di pendenze disciplinari o giudiziarie
	Rilevazioni delle assenze per sciopero: - singole schede - prospetti riassuntivi	 1 anno dopo la redazione dei prospetti riassuntivi Permanente	
13. Giudizi, responsabilità e provvedimenti disciplinari			
	Criteri generali e normativa per i provvedimenti disciplinari	Permanente	
	Provvedimenti disciplinari inseriti nel singolo fascicolo personale	Permanente	

14. Formazione e aggiornamento professionale			
	Criteri generali e normativa per la formazione e l'aggiornamento professionale	Permanente	
	Organizzazione di corsi di formazione e aggiornamento: un fasc. per ciascun corso	Permanente previo sfoltimento dopo 5 anni	
	Domande/Invio dei dipendenti a corsi inseriti nel singolo fascicolo personale	Permanente previo sfoltimento dopo 5 anni	
15. Collaboratori esterni			
	Criteri generali e normativa per il trattamento dei collaboratori esterni	Permanente	
	Elenco degli incarichi conferiti: repertorio	Permanente	

Titolo IV. Risorse finanziarie e patrimoniali

Classi	Tipologie documentarie	Conservazione	Note
2. Bilancio preventivo e Piano esecutivo di gestione (PEG)			
	Bilancio preventivo e allegati, tra cui Relazione previsionale e programmatica	Permanente	
	PEG: articolato in fascicoli: un fasc. per ogni obiettivo	Permanente, previo sfoltimento	
	Carteggio prodotto dai differenti uffici del Comune per questioni afferenti alla formazione del bilancio e del PEG	10 anni	
2. Gestione del bilancio e del PEG (con eventuali variazioni)			
	Gestione del bilancio: un fasc. per ciascuna variazione	Permanente, previo sfoltimento	
3. Gestione delle entrate: accertamen-to, riscossione, versamento			
	Fascicoli personali dei contribuenti comunali: un fasc. per ciascun contribuente per ciascun tipo di imposte (ICI, TARSU, TOSAP, etc.), con eventuali sottofascicoli (variazioni, ricorsi, etc.)	10 dopo la cancellazione del contribuente dai ruoli	
	Ruolo ICI: base di dati/ stampe	10 anni	Prevedere una stampa periodica
	Ruolo imposta comunale sulla pubblicità: base di dati	10 anni	Prevedere una stampa periodica
	Ruolo diritti sulle pubbliche affissioni: base di dati	10 anni	Prevedere una stampa periodica
	Ruolo TARSU: base di dati	10 anni	Prevedere una stampa periodica
	Ruolo COSAP: base di dati	10 anni	Prevedere una stampa periodica
	Contratti di mutuo: un fasc. per ciascun mutuo	5 anni dall'estinzione del mutuo	
	Proventi da affitti e locazioni: un fasc. annuale per ciascun immobile locato	5 anni dal termine del contratto	
	Diritti di segreteria: registrini annuali o pagamenti virtuali	5 anni	

	Matrici dei bollettari delle entrate: registri annuali	5 anni	
	Ricevute dei versamenti in banca delle somme riscosse nelle differenti UOR per diritti di segreteria	5 anni	
	Fatture emesse: repertorio annuale	10 anni	
	Reversali	5 anni	
	Bollettari vari	5 anni	
	Ricevute di pagamenti vari	5 anni	
4. Gestione della spesa: impegno, liquidazione, ordinazione e pagamento			
	Impegni di spesa (determinazioni dei dirigenti delle UOR): copie inviate dalle UOR alla Ragioneria: repertorio annuale	2 anni	
	Fatture ricevute: repertorio annuale	10 anni	
	Atti di liquidazione con allegati trasmessi da ciascuna UOR: repertorio annuale	2 anni	
	Mandati di pagamento con allegati emessi dalla Ragioneria e inviati alla Tesoreria: repertorio annuale	10 anni dall'approvazione del bilancio	Purché registrati in scritture contabili di sintesi
	Eventuali copie di mandati	2 anni	
5. Partecipazioni finanziarie			
	Gestione delle partecipazioni finanziarie: un fasc. per ciascuna partecipazione	Permanente, previo sfoltimento	
6. Rendiconto della gestione; adempimenti e verifiche contabili			
	Rendiconto della gestione, articolato in Conto del bilancio, Conto del patrimonio e Conto economico	Permanente	
7. Adempimenti fiscali, contributivi e assicurativi			
	Mod. 770	10 anni	Più se si ritiene opportuno
	Ricevute dei versamenti (IVA, IRPEF, etc.)	10 anni	
	Pagamento dei premi dei contratti assicurativi	5 anni dall'estinzione del contratto	

8. Beni immobili			
	Inventario dei beni immobili: registro o base di dati perenne	Permanente	
	Fascicoli dei beni immobili: un fasc. per ciascun bene immobile, articolato nei seguenti sottofascicoli, relativi ad attività specifiche, che possono anche essere di competenza di UOR diverse: - acquisizione - manutenzione ordinaria - gestione - uso - alienazione e dismissione	 Permanente 20 anni 5 anni 5 anni Permanente	
	Concessioni di occupazione di spazi e aree pubbliche: repertorio	Permanente	
	Concessioni di beni del demanio statale: repertorio	Permanente	
	Concessioni cimiteriali: repertorio	Permanente	
	Fascicoli personali dei concessionari: un fasc. per ciascun concessionario	5 anni dalla cessazione del rapporto	
9. Beni mobili			
	Inventari dei beni mobili: uno per consegnatario	Permanente	
	Fascicoli dei beni mobili: un fasc. per ciascun bene mobile, articolato nei seguenti sottofascicoli, relativi ad attività specifiche, che possono anche essere di competenza di UOR diverse: - acquisizione - manutenzione - concessione in uso - alienazione e altre forme di dismissione	 5 anni dalla dismissione 5 anni dalla dismissione 5 anni dalla dismissione 5 anni dalla dismissione	
10. Economato			
	Acquisizione di beni e servizi: un fasc. per ciascun acquisto	5 anni dalla dismissione del bene	
	Elenco dei fornitori: repertorio (in forma di base di dati)	Permanente	
11. Oggetti smarriti e recuperati			
	Verbali di rinvenimento: serie annuale repertoriata	2 anni	
	Ricevute di riconsegna ai proprietari: serie annuale repertoriata	2 anni	
	Vendita o devoluzione: un fasc. periodico (per attività)	2 anni	

12. Tesoreria			
	Giornale di cassa	Permanente	
	Mandati quietanzati, che vengono inviati in Ragioneria: repertorio periodico (mese/anno)	10 anni	
13. Concessionari ed altri incaricati della riscossione delle entrate			
	Concessionari: un fasc. per ciascuno dei concessionari	10 anni dalla cessazione del rapporto	
14. Pubblicità e pubbliche affissioni			
	Autorizzazioni alla pubblicità stabile: repertorio annuale	5 anni dalla scadenza dell'autorizzazione	Salvo non si rilevi qualche necessità particolare di conservazione a campione
	Autorizzazioni alla pubblicità circoscritta: repertorio annuale	5 anni dalla scadenza dell'autorizzazione	
	Richieste di affissione (con allegati da affiggere): un fasc. per richiesta	5 anni dalla scadenza dell'autorizzazione	

Titolo V. Affari legali

Classi	Tipologie documentarie	Conservazione	Note
1. Contenzioso			
	Fascicoli di causa	Permanente	Concentrare quelli presso gli studi professionali esterni
2. Responsabilità civile e patrimoniale verso terzi; assicurazioni			
	Contratti assicurativi	2 anni dalla scadenza	
	Richieste e pratiche di risarcimento	10 anni	
3. Pareri e consulenze			
	Pareri e consulenze	Permanente	

Titolo VI. Pianificazione e gestione del territorio

Classi	Tipologie documentarie	Conservazione	Note
1. Urbanistica: piano regolatore generale e varianti			
	PGR	Permanente	Possono essere eliminate le copie degli elaborati non più occorrenti agli uffici ed il carteggio transitorio
	Pareri su piani sovracomunali	Permanente	Dopo sfoltimento
	Certificati di destinazione urbanistica	1 anno dopo la scadenza	
	Varianti al PRG	Permanente	Possono essere eliminate le copie degli elaborati non più occorrenti agli uffici ed il carteggio transitorio
2. Urbanistica: strumenti di attuazione del piano regolatore generale			
	Piani particolareggiati del PRG	Permanente	Possono essere eliminate le copie degli elaborati non più occorrenti agli uffici ed il carteggio transitorio
	Piani di lottizzazione	Permanente	Possono essere eliminate le copie degli elaborati non più occorrenti agli uffici ed il carteggio transitorio
	Piani di edilizia economica e popolare – PEEP	Permanente	Possono essere eliminate le copie degli elaborati non più occorrenti agli uffici ed il carteggio transitorio
	Piano particolareggiato infrastrutture stradali - PPIS	Permanente	Possono essere eliminate le copie degli elaborati non più occorrenti agli uffici ed il carteggio transitorio
	Piano di riqualificazione urbana – PRU	Permanente	Possono essere eliminate le copie degli elaborati non più occorrenti agli uffici ed il

			carteggio transitorio
	Piano insediamenti produttivi - PIP	Permanente	Possono essere eliminate le copie degli elaborati non più occorrenti agli uffici ed il carteggio transitorio
	Programma integrato di riqualificazione	Permanente	Possono essere eliminate le copie degli elaborati non più occorrenti agli uffici ed il carteggio transitorio
	programma di riqualificazione urbana e di sviluppo sostenibile del territorio	Permanente	Possono essere eliminate le copie degli elaborati non più occorrenti agli uffici ed il carteggio transitorio
3. Edilizia privata			
	Autorizzazioni edilizie: repertorio	Permanente	
	Fascicoli dei richiedenti le autorizzazioni: un fasc. per ciascuna autorizzazione	Permanente	Possono essere eliminate le copie degli elaborati non più occorrenti agli uffici ed il carteggio transitorio
	Accertamento e repressione degli abusi	Permanente	Possono essere eliminate le copie degli elaborati non più occorrenti agli uffici ed il carteggio transitorio
	Denunce e relazioni finali delle opere in cemento armato	Fino a quando esiste l'edificio	
4. Edilizia pubblica			
	Costruzione di edilizia popolare	Permanente	Possono essere eliminate le copie degli elaborati non più occorrenti agli uffici ed il carteggio transitorio
5. Opere pubbliche			
	Realizzazione di opere pubbliche	Permanente	Possono essere eliminate le copie degli elaborati non più occorrenti agli uffici ed il carteggio transitorio
	Manutenzione ordinaria	5 anni	Salvo necessità particolari
	Manutenzione straordinaria	20 anni	Salvo necessità particolari

6. Catasto			
	Catasto terreni: mappe	Permanente	
	Catasto terreni: registri	Permanente	
	Catasto terreni: indice alfabetico dei possessori	Permanente	
	Catasto terreni: estratti catastali	Permanente	
	Catasto terreni: denunce di variazione (volture)	Permanente	
	Catasto fabbricati: mappe	Permanente	
	Catasto fabbricati: registri	Permanente	
	Catasto fabbricati: indice alfabetico dei possessori	Permanente	
	Catasto fabbricati: estratti catastali	Permanente	
	Catasto terreni: denunce di variazione (volture)	Permanente	
	Richieste di visure e certificazioni	1 anno	
7. Viabilità			
	Piano Urbano del Traffico:un fasc. per ciascun affare	Permanente con sfoltimento	
	Piano Urbano della Mobilità: un fasc. per ciascun affare	Permanente con sfoltimento	
	Autorizzazioni in deroga: serie annuale repertoriata	2 anni	
8. Servizio idrico integrato, luce, gas, trasporti pubblici, gestione dei rifiuti e altri servizi			
	Approvvigionamento idrico (organizzazione e funzionamento)	Permanente con sfoltimento	
	Fascicoli relativi alle irregolarità	10 anni	
	Iniziative a favore dell'ambiente	Permanente con sfoltimento	
	Distribuzione dell'acqua: contratti con gli utenti	2 anni dalla cessazione del rapporto	Purché in assenza di contenzioso
	Produzione di energia elettrica o altre fonti energetiche (organizzazione e funzionamento)	Permanente con sfoltimento	
	Distribuzione di energia elettrica o altre fonti energetiche: contratti con gli utenti:	2 anni dalla cessazione del rapporto	Purché in assenza di contenzioso
	Trasporti pubblici (gestione)	Permanente con sfoltimento	
	Vigilanza sui gestori dei servizi: un fasc. annuale per attività	Permanente con sfoltimento	
	Fascicoli relativi alle irregolarità	10 anni	
	Iniziative di sensibilizzazione degli utenti per consumi razionali: un fasc. per ciascuna iniziativa	Permanente con sfoltimento	
	Dichiarazioni di conformità degli impianti: repertorio annuale	1 anno	

9. Ambiente: autorizzazioni, monitoraggio e controllo			
	Valutazioni e pareri di impatto ambientale: un fasc. per ciascun parere	Permanente	
	Monitoraggi della qualità delle acque: fasc. annuale per attività	10 anni	
	Monitoraggi della qualità dell'aria: fasc. annuale per attività	10 anni	
	Monitoraggi della qualità dell'etere: un fasc. annuale per attività	10 anni	
	Altri eventuali monitoraggi: fasc. annuale per attività	10 anni	
	Fascicoli relativi alle irregolarità	10 anni	
	Controlli a campione sugli impianti termici dei privati: fasc. annuale per attività	2 anni	
	Fascicoli relativi alle irregolarità	10 anni	
10. Protezione civile ed emergenze			
	Segnalazioni preventive di condizioni metereologiche avverse: un fasc. annuale	2 anni	
	Addestramento ed esercitazioni per la protezione civile: un fasc. annuale	5 anni	
	Interventi per emergenze: un fasc. per ciascuna emergenza	Permanente con sfoltimento	

Titolo VII. Servizi alla persona	
Osservazioni generali	*L'autonomia dei Comuni si può esplicare in forme svariate soprattutto in questo titolo: perciò l'indicazione generica di evento o attività verrà riempita di contenuti concreti dalla singola amministrazione.*

Classi	Tipologie documentarie	Conservazione	Note
	Fascicoli per persona	Permanente, previo sfoltimento del carteggio temporaneo e strumentale dopo 5 anni	
1. Diritto allo studio e servizi			
	Concessione di borse di studio: - bando - domande - graduatorie - assegnazioni	 permanente 5 anni permanente 5 anni	
	Distribuzione buoni libro: un fasc. per scuola	2 anni	
	Gestione buoni pasto degli iscritti alle scuole: un fasc. per periodo	2 anni	
	Verbali del comitato genitori per la mensa	3 anni	
	Azioni di promozione e sostegno del diritto allo studio: un fasc. per intervento	5 anni	
	Gestione mense scolastiche: un fasc. per mensa scolastica e per periodo	10 anni	
	Integrazione di neo-immigrati e nomadi: un fasc. per intervento	10 anni	
	Gestione trasporto scolastico: un fasc. per periodo e per tratta	2 anni	
2. Asili nido e scuola materna	Domande di ammissione agli asili nido e alle scuole materne: un fasc. per asilo/scuola	2 anni	
	Graduatorie di ammissione	2 anni	
	Funzionamento. degli asili e delle scuole materne: un fasc. per struttura	10 anni	

3. Promozione e sostegno delle istituzioni di istruzione e della loro attività			
	Iniziative specifiche: un fasc. per iniziativa	10 anni	
	Registri scolastici (del professore e della classe) prodotti dalle Scuole civiche (ove presenti)	Permanenti	
4. Orientamento professionale; educazione degli adulti; media-zione culturale			
	Iniziative specifiche: un fasc. per iniziativa	10 anni	
5. Istituti culturali			
	Funzionamento delle diverse istituzioni culturali: un fasc. per istituto	Permanente	
	Verbali degli organi di gestione degli Istituti culturali	Permanente	
6. Attività ed eventi culturali			
	Attività ordinarie annuali: un fasc. per attività e per periodo)	10 anni	
	Eventi culturali: un fasc. per evento	Permanente, previo sfoltimento del carteggio temporaneo e strumentale dopo 10 anni	
	Feste civili e/o religiose: un fasc. per iniziativa	Permanente, previo sfoltimento del carteggio temporaneo e strumentale dopo 10 anni	
	Iniziative culturali. un fasc. per iniziativa	Permanente, previo sfoltimento del carteggio temporaneo e strumentale dopo 10 anni	
	Prestiti di beni culturali: un fasc. per affare	Permanente	
7. Attività ed eventi sportivi			
	Eventi e attività sportive: un fasc. per evento/attività	Permanente, previo sfoltimento del carteggio temporaneo e strumentale dopo 5 anni	

8. Pianificazione e accordi strate-gici con enti pubblici e privati e con il volontariato so-ciale			
	Piano sociale: un fasc. annuale eventualmente organizzato in sottofasc.	Permanente, previo sfoltimento del carteggio temporaneo e strumentale dopo 5 anni	
	Programmazione per settori: un fasc. per ciascun settore	Permanente, previo sfoltimento del carteggio temporaneo e strumentale dopo 5 anni	
	Accordi con i differenti soggetti: un fasc. per ciascun soggetto	Permanente, previo sfoltimento del carteggio temporaneo e strumentale dopo 5 anni	
9. Prevenzione, recupero e reintegrazione dei soggetti a rischio			
	Campagne di prevenzione: un fasc. per campagna	Permanente, previo sfoltimento del carteggio temporaneo e strumentale dopo 5 anni	
	Interventi di recupero e reintegrazione dei soggetti a rischio: un fasc. per intervento	Permanente, previo sfoltimento del carteggio temporaneo e strumentale dopo 5 anni	
	Ricognizione dei rischi: un fasc. per affare	Permanente, previo sfoltimento del carteggio temporaneo e strumentale dopo 5 anni	
10. Informazione, consulenza ed educazione civica			
	Funzionamento e attività delle strutture (consultori, informagiovani, etc.): un fasc. per struttura	Permanente, previo sfolti-mento del carteggio tempora-neo e strumentale dopo 10 anni	
	Iniziative di vario tipo: un fasc. per iniziativa	Permanente, previo sfoltimento del carteggio temporaneo e strumentale dopo 10 anni	

11. Tutela e curatela di incapaci			
	Interventi per le persone sottoposte a tutela e curatela: un fasc. per intervento.	Permanente, previo sfoltimento del carteggio temporaneo e strumentale dopo 10 anni	
12. Assistenza diretta e indiretta, benefici economici			
	Funzionamento e attività delle strutture: un fasc. annuale per ciascuna struttura	Permanente, previo sfoltimento del carteggio temporaneo e strumentale dopo 10 anni	
	Iniziative specifiche: un fasc. per ciascuna iniziativa	Permanente, previo sfoltimento del carteggio temporaneo e strumentale dopo 10 anni	
13. Attività ricreativa e di socia-lizzazione			
	Funzionamento e attività delle strutture (colonie, centri ricreativi, etc.): un fasc. annuale per ciascuna struttura	Permanente, previo sfoltimento del carteggio temporaneo e strumentale dopo 10 anni	
	Iniziative specifiche: un fasc. per ciascuna iniziativa	Permanente, previo sfoltimento del carteggio temporaneo e strumentale dopo 10 anni	
14. Politiche per la casa			
	Assegnazione degli alloggi: un fasc. per bando, organizzato in sottofascicoli: - bando - domande - graduatoria - assegnazione	permanente 5 anni permanente 5 anni	
	Fasc. degli assegnatari : un fasc. per assegnatario	5 anni dopo la scadenza del contratto	In assenza di contenzioso
15. Politiche per il sociale			
	Iniziative specifiche: un fasc. per iniziativa	Permanente, previo sfoltimento del carteggio temporaneo e strumentale dopo 10 anni	

Titolo VIII. Attività economiche

Classi	Tipologie documentarie	Conservazione	Note
	Fascicoli individuali degli esercenti attività economiche: un fasc. per persona	Permanente, previo sfoltimento del carteg-gio temporaneo e strumentale dopo 5 anni	
1. Agricoltura e pesca			
	Iniziative specifiche: un fasc. per affare	Permanente, previo sfoltimento del carteg-gio temporaneo e strumentale dopo 5 anni	
	Dichiarazioni raccolta e produzione: un fasc. per periodo	5 anni	
2. Artigianato			
	Iniziative specifiche: un fasc. per affare	Permanente, previo sfoltimento del carteg-gio temporaneo e strumentale dopo 5 anni	
	Autorizzazioni artigiane: repertorio	Permanente	
3. Industria			
	Iniziative specifiche: un fasc. per affare	Permanente, previo sfoltimento del carteg-gio temporaneo e strumentale dopo 5 anni	
4. Commercio			
	Iniziative specifiche: un fasc. per affare	Permanente, previo sfoltimento del carteg-gio temporaneo e strumentale dopo 5 anni	
	Comunicazioni dovute: un fasc. per periodo	1 anno	
	Autorizzazioni commerciali: repertorio	Permanente	

5. Fiere e mercati			
	Iniziative specifiche: un fasc. per affare	Permanente, previo sfoltimento del carteg-gio temporaneo e strumentale dopo 5 anni	
6. Esercizi turistici e strutture ricettive			
	Iniziative specifiche: un fasc. per affare	Permanente, previo sfoltimento del carteg-gio temporaneo e strumentale dopo 5 anni	
	Autorizzazioni turistiche: repertorio	Permanente	
7. Promozione e servizi			
	Iniziative specifiche: un fasc. per affare	Permanente, previo sfoltimento del carteg-gio temporaneo e strumentale dopo 5 anni	

Titolo IX. Polizia locale e sicurezza pubblica

Classi	Tipologie documentarie	Conservazione	Note
1. Prevenzione ed educazione stradale			
	Iniziative specifiche di prevenzione: un fasc. per iniziativa	5 anni	
	Corsi di educazione stradale nelle scuole: un fasc. per corso	5 anni	
2. Polizia stradale			
	Direttive e disposizioni: un fasc. annuale	Permanente	
	Organizzazione del servizio di pattugliamento: un fasc. annuale	3 anni	
	Verbali di accertamento di violazioni al Codice della strada: repertorio annuale	10 anni	
	Accertamento di violazioni al Codice della strada e conseguente erogazione di sanzioni: un fasc. per accertamento	5 anni	
	Verbali di rilevazione incidenti: repertorio annuale	20 anni	In assenza di contenzioso (ai sensi dell'art. 157 del Codice penale)
	Statistiche delle violazioni e degli incidenti: un fasc. annuale	Permanente	
	Gestione veicoli rimossi: un fasc. per ciascun veicolo	2 anni	
3. Informative			
	Informative su persone residenti nel Comune: un fasc. per ciascuna persona	5 anni	
4. Sicurezza e ordine pubblico			
	Direttive e disposizioni generali: un fasc. annuale	Permanente	
	Servizio ordinario di pubblica sicurezza: un fasc. annuale	5 anni	
	Servizio straordinario di pubblica sicurezza, in caso di eventi particolari (manifestazioni, concerti, etc.): un fasc. per evento	5 anni	
	Autorizzazioni di pubblica sicurezza: repertorio annuale, organizzata in sottoserie	Permanente	
	Fascicoli dei richiedenti l'autorizzazione di pubblica sicurezza: un fasc. per richiedente	5 anni	
	Verbali degli accertamenti nei diversi settori (edilizio, sanitario, commerciale, anagrafico, sociale, etc.): un repertorio annuale per ciascun settore di accertamento	Permanente	

Titolo X. Tutela della salute

Classi	Tipologie documentarie	conservazione	Note
1. Salute e igiene pubblica			
	Emergenze sanitarie: un fasc. per ciascun evento	Permanente	
	Misure di igiene pubblica: un fasc. per ciascun affare	Permanente	
	Interventi di derattizzazione, dezanzarizzazione etc.: un fasc. per ciascun intervento	1 anno	
	Trattamenti fitosanitari e di disinfestazione: un fasc. per ciascun intervento	1 anno	
	Autorizzazioni sanitarie: repertorio annuale	Permanente	
	Fascicoli dei richiedenti autorizzazioni sanitarie: un fasc. per ciascuna persona/ditta	5 anni dalla cessazione dell'attività	
	Concessioni di agibilità: repertorio annuale	Permanente	
	Fascicoli dei richiedenti l'agibilità: un fasc. per ciascun richiedente	Permanente	
2. Trattamenti Sanitari Obbligatori			
	TSO: un fasc. per ciascun procedimento	Permanente	
	ASO: un fasc. per ciascun procedimento	Permanente	
	Fascicoli personali dei soggetti a trattamenti: un fasc. per ciascuna persona	Permanente	
3. Farmacie			
	Istituzione di farmacie: un fasc. per ciascuna farmacia	Permanente	
	Funzionamento delle farmacie: un fasc. per ciascun periodo (anno o mese)	2 anni	
4. Zooprofilassi veterinaria			
	Fasc. relativi a epizoozie (epidemie animali): un fasc. per ciascun evento	Permanente	
5. Randagismo animale e ricoveri			
	Gestione dei ricoveri e degli eventi connessi: un fasc. per ciascun procedimento	3 anni	

Titolo XI. Servizi demografici

Classi	Tipologie documentarie	Conservazione	Note
1. Stato civile			
	Registro dei nati: repertorio annuale	Permanente	
	Registro dei morti: repertorio annuale	Permanente	
	Registro dei matrimoni: repertorio annuale	Permanente	
	Registro di cittadinanza: repertorio annuale	Permanente, se recanti registrazioni	
	Atti allegati per registrazioni	=	Trasmessi annualmente all'ufficio del governo competente per territorio
	Atti per annotazioni sui registri di stato civile: un fasc. per ciascun procedimento	10 anni	
	Comunicazione dei nati all'Agenzia per le entrate: un fasc. per ciascun periodo	1 anno	
2. Anagrafe e certificazioni			
	APR 4: iscrizioni anagrafiche: un fasc. per ciascuna persona	Permanente	
	AIRE: un fasc. per ciascuna persona	Permanente	
	Richieste certificati: un fasc. per ciascun periodo (mese o anno)	1 anno	
	Corrispondenza con altre amministrazioni per rilascio e trasmissione documenti: un fasc. per ciascun periodo (mese o anno)	1 anno	
	Cartellini per carte d'identità: uno per ciascuna persona	1 anno	Mediante incenerimento o triturazione
	Carte d'identità scadute e riconsegnate: un fasc. per ciascuna persona	5 anni	Mediante incenerimento o triturazione Circ. Min. interno – Direz. gen. PS 23 ott. 1950, n. 10-13070-12982-7-1
	Cambi di abitazione e residenza: un fasc. per ciascuna persona	10 anni	Salvo esigenze particolari
	Cancellazioni: un fasc. per ciascuna persona	10 anni	Salvo esigenze particolari
	Carteggio con la Corte d'appello per la formazione degli Albi dei giudici popolari: un fasc. per ciascun periodo	3 anni dall'ultima revisione	
	Registro della popolazione: su base di dati	Permanente	Salvataggi periodici per storicizzare la banca dati

3. Censimenti			
	Schedoni statistici del censimento	Si conservano quelli dell'ultimo censimento; quelli del precedente si scartano dopo 1 anno dall'ultimo	
	Atti preparatori e organizzativi	3 anni	
4. Polizia mortuaria e cimiteri			
	Registri di seppellimento	Permanente	
	Registri di tumulazione	Permanente	
	Registri di esumazione	Permanente	
	Registri di estumulazione	Permanente	
	Registri di cremazione	Permanente	
	Registri della distribuzione topografica delle tombe con annesse schede onomastiche	Permanente	
	Trasferimento delle salme: un fasc. per ciascun trasporto	50 anni	

Titolo XII. Elezioni e iniziative popolari	
Osservazioni	Ci si riferisca per i particolari a MINISTERO DELL'INTERNO-DIREZ. GEN. DELL'AMMINISTRAZIONE CIVILE –DIREZ CENTRALE PER I SERVIZI ELETTORALI, *Massimario per lo scarto degli atti elettorali,* Roma 1984

Classi	Tipologie documentarie	Conservazione	Note
1. Albi elettorali			
	Albo dei presidenti di seggio: un elenco per ciascuna elezione	5 anni	
	Albo degli scrutatori: un elenco per ciascuna elezione	5 anni	
2. Liste elettorali			
	Liste generali	1 anno dopo la redazione della successiva	
	Liste sezionali	1 anno dopo la redazione della successiva	
	Verbali della commissione elettorale comunale	Permanente	
	Copia dei verbali della Commissione elettorale mandamentale in ordine alle operazioni e deliberazioni adottate dalla Commissione elettorale comunale	5 anni	
	Schede dello schedario generale	5 anni dopo la redazione della successiva	
	Schede degli schedari sezionali	5 anni dopo la redazione della successiva	
	Fasc. personali degli elettori: un fasc. per ciascun elettore	5 anni dopo la cancellazione dalla lista	
	Elenchi recanti le proposte di variazione delle liste elettorali	5 anni dopo la redazione della lista successiva	
	Carteggio concernente la tenuta e la revisione delle liste elettorali	5 anni dopo la redazione della lista successiva	
3. Elezioni			
	Convocazione dei comizi elettorali: un fasc. per ciascuna elezione	Permanente	
	Presentazione delle liste: manifesto	Permanente	
	Presentazione delle liste: carteggio	5 anni	
	Atti relativi alla costituzione e arredamento dei seggi	5 anni	

	Verbali dei presidenti di seggio	=	Trasmessi al Min dell'interno
	Schede	=	Trasmesse al Min dell'interno
	Pacchi scorta elezioni	2 anni	
	Certificati elettorali non ritirati	2 anni	
	Istruzioni elettorali a stampa	2 anni	
4. Referendum			
	Atti preparatori	5 anni	
	Atti relativi alla costituzione e arredamento dei seggi	5 anni	
	Verbali dei presidenti di seggio	=	Trasmessi al Min dell'interno
	Schede	=	Trasmesse al Min dell'interno
5. Istanze, petizioni e iniziative popolari			
	Raccolta di firme per referendum previsti dallo statuto: un fasc. per ciascuna iniziativa	5 anni dopo il referendum	

Titolo XIII. Affari militari

Classi	Tipologie documentarie	Conservazione	Note
1. Leva e servizio civile sostitutivo			
	Liste di leva: una per anno	Permanente	
	Lista degli eliminati/esentati: una per anno	Permanente	
2. Ruoli matricolari			
	Uno per anno	Permanente	
3. Caserme, alloggi e servitù militari			
	Procedimenti specifici: un fasc. per ciascun procedimento	Permanente	
4. Requisizioni per utilità militari			
	Procedimenti specifici: un fasc. per ciascun procedimento	Permanente	

UNIMATICA RGI

MANUALE DEL SISTEMA DI CONSERVAZIONE

Sommario

Indice delle figure

Registro delle versioni

Revisione	Data	Motivo Revisione	Redatto da	Approvato da
1.0	03/10/2009	Emissione	Andrea Anghinolfi	Silvano Ghedini
2.0	12/02/2010	Aggiornamento funzionalità	Andrea Anghinolfi	Silvano Ghedini
3.0	20/06/2010	Aggiornamento funzionalità	Andrea Anghinolfi	Silvano Ghedini
4.0	28/09/2010	Aggiornamento funzionalità	Andrea Anghinolfi	Silvano Ghedini
5.0	15/10/2010	Aggiornamento funzionalità	Andrea Anghinolfi	Silvano Ghedini
6.0	10/02/2011	Modifica gestione anomalie – Ampliamento funzionalità Unistorage	Andrea Anghinolfi	Silvano Ghedini
7.0	20/05/2011	Aggiornamento composizione societaria Unimatica-RGI	Andrea Anghinolfi	Silvano Ghedini
8.0	30/11/2012	Aggiornamento Data Center	Andrea Anghinolfi	Silvano Ghedini
8.1	11/12/2012	Personalizzazioni	Andrea Anghinolfi	Silvano Ghedini
8.2	20/06/2013	Aggiornamento compiti e responsabilità della conservazione	Sabina Falcinelli	Andrea Anghinolfi
8.3	04/07/2013	Aggiornamento normative	Sabina Falcinelli	Andrea Anghinolfi
8.4	05/02/2014	Aggiornamento normative	Sabina Falcinelli	Andrea Anghinolfi
8.5	11/02/2014	Aggiornamento Data Center	Sabina Falcinelli	Andrea Anghinolfi
8.6	05/03/2014	Adeguamento normative	Sabina Falcinelli	Andrea Anghinolfi
8.7	17/02/2015	Adeguamento DPCM 03/12/2013	Roberta Rosatone	Silvano Ghedini
8.8	15/10/2015	Passaggio alla ISO 27001:2013	Roberta Rosatone	Silvano Ghedini
8.9	20/01/2016	Adeguamento Schema Manuale della conservazione AgID	Roberta Rosatone	Silvano Ghedini
9.0	11/04/2017	Modifica ruolo Responsabile della Funzione Archivistica	Roberta Rosatone	Silvano Ghedini
9.1	14/06/2017	Aggiornamento definizioni per termine “Produttore”	Roberta Rosatone	Silvano Ghedini
9.2	05/10/2017	· Aggiornamento Server farm · Visualizzazione di 200 risultati da portale	Roberta Rosatone	Silvano Ghedini
9.3	20/10/2017	· Capitolo Trasparenza · Aggiornamento elenco formati · Aggiunto testo alternativo mancante su alcune immagini · Sostituita immagine 7 precedentemente con parti nascoste	Roberta Rosatone	Silvano Ghedini
9.4	25/10/2018	· Aggiornamento par. 1.1 adeguamento GDPR · Modifica ruolo Privacy Manager cap. 4 · Aggiornamento tabella normativa par. 3.1 · Aggiunto ruolo DPO al par.4.1	Roberta Rosatone	Silvano Ghedini
9.5	29/01/2019	· Recepimento N.C. AgID Recepimento Oss. Audit interno · Aggiornamento Nomina ad Interim Responsabile della funzione archivistica · Aggiornamento proc. Gestione Incident par. 8.1.3	Roberta Rosatone	Silvano Ghedini

9.6	19/04/2019	· Revoca nomina ad Interim per la Responsabilità della funzione archivistica · Aggiornamento nomina ad interim DPO	Roberta Rosatone	Silvano Ghedini
9.7	27/09/2019	· Aggiornamento Ruoli (Delegato Responsabile del servizio di conservazione – Responsabile dello sviluppo e della manutenzione – Responsabile dei sistemi informative – DPO) · Aggiornamento proc. Gestione Incident par. 8.1.3 · Aggiornamento estensioni ISO 27017 – 27018 · Aggiornamento descrizione par. 7.5 Rifiuto PDV	Roberta Rosatone Paolo Vandelli	Silvano Ghedini
9.8	20/12/2019	· Aggiornamento capp. 4 e 5 a seguito della sostituzione del Delegato alla Responsabilità del servizio di conservazone, della Responsabile della funzione archivistica e della Responsabile dello sviluppo e manutenzione · A seguito delle NC ricevute in fase di audit è stato eliminato il par. 9.2 ed aggiornato il par. 8.1.3 sulla Gestione degli incident di sicurezza.	Roberta Rosatone Paolo Vandelli	Silvano Ghedini
9.9	13/01/2021	· Aggiornamento cap. 4 a seguito di Oss da Audit interno. Aggiunto nominativo Resp. dello sviluppo in carica. · Aggiornamento tabella formati par. 6.2	Roberta Rosatone	Silvano Ghedini
10	13/09/2021	· Aggiornamenti a seguito del cambio ragione sociale · Aggiornamento par. 1.1 sulla privacy · Aggiornamento par. 1.2 per certificazione ISO 14001 · Aggiornamento modifica sito d/r secondario Acilia (RM)	Roberta Rosatone	Silvano Ghedini
11	30/12/2021	· Aggiornamento a seguito dell'adeguamento alle Linee guida per la formazione, gestione e conservazione del documento informatico (revisionati cap. 1-2-3-4-6-7)	Eleonora Luzi	Paolo Vandelli
12	21/06/2022	· Capitolo 4.1.: riportato nuovo responsabile del servizio; rimossa evidenza della delega assegnata a Paolo Vandelli dal precedente responsabile del servizio; · Aggiunto capitolo '4.2. Precedenti responsabili' · Rivisto capitolo '5.1. Organigramma' in funzione della nuova nomina	Eleonora Luzi	Paolo Vandelli
13	01/09/2022	· Indicazione socio unico a piede pagina	Eleonora Luzi	Paolo Vandelli

1. Scopo e ambito del documento

Il presente documento costituisce il Manuale del servizio di conservazione erogato da Unimatica-RGI ed ha lo scopo di illustrare la struttura del sistema di conservazione descrivendone analiticamente gli oggetti sottoposti a conservazione, il processo di conservazione e le componenti logiche, tecnologiche e fisiche relative al suo funzionamento. Delinea, inoltre, i soggetti che sono coinvolti nelle attività e nei processi di conservazione i quali hanno la responsabilità del sistema.

Il Manuale del servizio unitamente alla Scheda cliente predisposta da Unimatica-RGI, al fine di personalizzare il rapporto contrattuale con il Cliente Soggetto produttore (da ora in poi Soggetto produttore), costituiscono parte integrante del contratto di fornitura del servizio e mira a garantire e illustrare formalmente ai propri clienti il sistema di conservazione e le sue caratteristiche di disponibilità nel tempo di documenti integri, autentici, legalmente validi e facilmente consultabili.

Questo documento è reso disponibile a tutte le parti interessate a seguito di apposita richiesta.

Torna al sommario

1.1. Trattamento dei dati personali

Ai sensi e per gli effetti dell'articolo 28 del Regolamento (UE) n. 2016/679 del Parlamento Europeo e del Consiglio relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (d'ora innanzi anche "GDPR" o "Regolamento") e del D.lgs. 30 giugno 2003 n. 196, relativamente e limitatamente ai trattamenti riguardanti la conservazione degli oggetti digitali affidati a Unimatica-RGI, a partire dalla data di sottoscrizione del contratto, il Soggetto produttore, nella sua qualità di Titolare del trattamento, affida a Unimatica-RGI, che diventa Responsabile del trattamento dei dati personali trattati in esecuzione del contratto, i seguenti compiti e impartisce le seguenti istruzioni per il trattamento dei dati cui Unimatica-RGI deve attenersi:

1. Unimatica-RGI per espletare le attività pattuite per conto del Soggetto produttore potrebbe trattare direttamente o anche solo indirettamente una o più delle seguenti categorie di dati:
- dati personali,
- dati rientranti nelle categorie "particolari" di dati personali,
- dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza,

di cui è Titolare il Soggetto produttore. Per i dettagli, occorre fare riferimento a quanto pattuito nel contratto/ordine/accordo.

2. I dati trattati da Unimatica-RGI si riferiscono potenzialmente, a titolo esemplificativo, ma non esaustivo, alle seguenti categorie di interessati: clienti, dipendenti, utenti, fornitori, richiedenti impiego, soci, etc.

3. Il trattamento dei dati in questione è effettuato da Unimatica-RGI esclusivamente per lo svolgimento del servizio di Conservazione a norma, in modo lecito e secondo correttezza, attenendosi alle prescrizioni della normativa sulla protezione dei dati personali nonché alle previsioni della specifica delega a Responsabile del Servizio di Conservazione o successivamente concordate tra le parti; è fatto esplicito divieto di diffondere o comunicare i dati in questione a soggetti che siano estranei all'esecuzione del trattamento.

4. Unimatica-RGI, nella sua qualità di Responsabile del trattamento, in particolare è tenuta a:

a) effettuare tutte le operazioni in termini di mansioni, definendo regole e modelli di comportamento che assicurino la riservatezza e il rispetto del divieto di comunicazione e diffusione dei dati ai quali si ha accesso;

b) trattare direttamente, o per il tramite dei propri dipendenti, collaboratori esterni, consulenti, etc. - designati autorizzati al trattamento - i dati personali del Soggetto produttore, Titolare del trattamento, per le sole finalità connesse allo svolgimento delle attività previste dal

contratto/ordine/accordo, in modo lecito e secondo correttezza, nonché nel pieno rispetto delle disposizioni impartite dal GDPR, nonché, infine, dalle presenti istruzioni;
c) non divulgare o rendere noti a terzi - per alcuna ragione ed in alcun momento, presente o futuro ed anche una volta cessati i trattamenti oggetto del contratto/ordine/accordo - i dati personali ricevuti dal Titolare o pervenuti a sua conoscenza in relazione all'esecuzione del servizio prestato, se non previamente autorizzato per iscritto dal Titolare, fatti salvi eventuali obblighi di legge o ordini dell'Autorità Giudiziaria e/o di competenti Autorità amministrative;
d) collaborare con il Titolare per garantire la puntuale osservanza e conformità alla normativa in materia di protezione dei dati personali;
e) incaricare per iscritto i soggetti che abbiano le caratteristiche di Responsabili di Sistema e di Amministratori di Sistema, tenerne l'elenco aggiornato a disposizione del Soggetto produttore e fornirne eventualmente copia a semplice richiesta dello stesso;
f) adottare, se del caso, adeguate misure di sicurezza, in modo da ridurre al minimo i rischi di distruzione e perdita, anche accidentale dei dati/documenti stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta;
g) informare immediatamente il Soggetto produttore di qualsiasi richiesta o comunicazione da parte dell'Autorità Garante e/o Giudiziaria, per concordare congiuntamente l'evasione delle stesse;
h) collaborare con il Soggetto produttore per l'attuazione delle prescrizioni eventualmente impartite dall'Autorità Garante;
i) comunicare al Soggetto produttore qualsiasi accadimento che possa compromettere il corretto trattamento dei dati personali;
j) segnalare eventuali criticità al Soggetto produttore che possono mettere a repentaglio la sicurezza dei dati, al fine di consentire idonei interventi da parte dello stesso;
k) prestare particolare attenzione all'eventuale trattamento di dati personali rientranti nelle categorie particolari e/o relative a condanne penali o reati degli interessati conosciuti, anche incidentalmente, in esecuzione dell'incarico affidato, procedendo alla loro raccolta e archiviazione solo ove ciò si renda necessario per lo svolgimento delle attività di competenza e istruendo in tal senso le persone autorizzate che operano all'interno della propria struttura.
5. Il trattamento dei dati deve intendersi effettuato sotto la vigilanza del Soggetto produttore il quale, in ogni momento e con congruo preavviso, potrà operare controlli e impartire eventuali ulteriori specifiche istruzioni per il suo svolgimento, nonché chiederne la cessazione se imposta dalla necessità di adempiere a divieti od obblighi di legge, ovvero a provvedimenti dell'Autorità Garante e/o Giudiziaria.
6. Unimatica-RGI, nella sua qualità di Responsabile esterno del trattamento, si impegna a notificare al Soggetto produttore, Titolare del trattamento, senza ingiustificato ritardo dall'avvenuta conoscenza, e comunque entro 24 ore dalla scoperta con comunicazione da inviarsi all'indirizzo PEC del Soggetto produttore, (salvo diversa email indicata) ogni violazione dei dati personali (*data breach*). Unimatica-RGI si impegna a prestare ogni più ampia assistenza al Soggetto produttore al fine di consentirgli di assolvere agli obblighi di cui agli artt. 32 - 34 del GDPR.
Una volta definite le ragioni della violazione, Unimatica-RGI di concerto con il Soggetto produttore e/o altro soggetto da quest'ultimo indicato, si attiverà per implementare nel minor tempo possibile tutte le misure di sicurezza fisiche e/o logiche e/o organizzative atte ad arginare il verificarsi di una nuova violazione della stessa specie di quella verificatasi.
7. In esecuzione degli accordi in essere con il Soggetto produttore, Unimatica-RGI potrà affidare l'esecuzione - parziale o totale - delle relative attività a soggetti terzi, dei quali garantisce il possesso dei requisiti di esperienza, capacità ed affidabilità, ivi compreso il profilo relativo alla sicurezza. Ove ricorra tale ipotesi, Unimatica-RGI , nella sua qualità di Responsabile esterno del trattamento, provvede personalmente a designare Responsabile del trattamento ai sensi dell'art. 28 del GDPR i suddetti soggetti terzi (nel seguito anche "Sub-Responsabile del trattamento") con idoneo atto giuridico e ne dà notizia al Soggetto produttore tramite il seguente link: https://www.unimaticaspa.it/it/gdpr-elenco-sub-responsabili.
8. Unimatica-RGI assicura che nessun dato personale potrà essere trasferito all'esterno dell'Area Economica Europea (EEA).

9. Premesso che l'accesso ai dati personali da parte degli interessati esercitato ai sensi degli artt. 15 e seguenti del GDPR sarà gestito direttamente dal Soggetto produttore, Unimatica-RGI si rende disponibile a collaborare con il Soggetto produttore stesso fornendogli tutte le informazioni necessarie a soddisfare le eventuali richieste ricevute in tal senso.
10. Unimatica-RGI – ove tale obbligo si applichi anche alla stessa, nella sua qualità di Responsabile del trattamento e in base alle disposizioni del comma 5 dell'art. 30 del GDPR - mantiene un registro di tutte le categorie di attività relative al trattamento svolte per conto del Soggetto produttore.
11. Unimatica-RGI si impegna a mettere a disposizione del Soggetto produttore tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di sicurezza descritti nel presente documento e, in generale, il rispetto delle obbligazioni assunte in forza del GDPR, consentendo e, su richiesta, contribuendo alle attività di audit, comprese le ispezioni, realizzate dal Soggetto produttore o da altro soggetto da esso incaricato.
12. L'autorizzazione al trattamento dei dati personali avrà la medesima validità ed efficacia della durata della conservazione legale dei documenti, stabilita dalla normativa.

Torna al sommario

1.2. Trasparenza

La conservazione a norma di Unimatica-RGI è rivolta a Pubbliche amministrazioni, banche, assicurazioni, strutture sanitarie ed ai privati in genere.
Al fine di rendere tali servizi agevoli ed accessibili ad un pubblico variegato e disomogeneo, Unimatica-RGI rende disponibili una serie di strumenti ed informazioni utili a garantire una totale trasparenza delle proprie attività mediante canali diretti ed indiretti.
In generale, nel sito internet aziendale www.unimaticaspa.it sono disponibili:

- i contatti principali quali telefono, fax, email ed indirizzo.
- La certificazione per la Qualità ISO 9001:2015 (Unimatica-RGI è certificata dal 2006)
- La certificazione per il Sistema di Gestione Ambientale ISO 14001:2015
- La certificazione per la Sicurezza delle Informazioni ISO 27001:2013 (Unimatica-RGI è certificata dal 2014) con estensioni alle Linee guida ISO 27017:2015, ISO 27018:2019 ed ISO 27701:2019
- Il Codice Etico aziendale
- Il Modello di Organizzazione, Gestione e Controllo (MOG), ai sensi della L. 231/01 (consultabile a richiesta)
- La Politica Aziendale (consultabile a richiesta)
- L'elenco delle Associazioni di cui l'azienda fa parte e delle Partnership tecnico/commerciali
- La descrizione dei servizi e prodotti offerti dall'azienda e le modalità attraverso cui ottenere informazioni dettagliate su di essi e su come richiederli
- Le informazioni sulle principali attività svolte o in corso

Oltre alle certificazioni sopra elencate, Unimatica-RGI sta implementando un sistema di gestione anticorruzione ISO 37001:2016.
Tale certificazione, obbligatoria ai fini dell'adeguamento alle Linee guida per la formazione, gestione e conservazione dei documenti informatici in vigore dal 1° gennaio 2022, verrà aggiunta alle altre presenti nella sezione Trasparenza.

Negli anni, il settore Conservazione di Unimatica-RGI ha ottemperato a tutti gli obblighi normativi applicabili. Nello specifico, infatti, da marzo del 2015 ha mantenuto l'accreditamento presso l'Agenzia per l'Italia Digitale (AgID) con la pubblicazione del Manuale della conservazione nell'apposita area a ciò dedicata sul sito web di AgID.
Dall'ottobre del 2017 fino ad abrogazione, in continuità con le disposizioni normative, ha ottenuto e mantenuto la certificazione in conformità all'art. 24 del Regolamento Eidas e alla check list "*Lista di riscontro per la visita ispettiva AgID e la certificazione di conformità*".
Tali strumenti, oltre ad essere sinonimo di eccellenza, sono risultati negli anni passi indispensabili per la crescita dell'azienda, del team e per migliorare continuamente il prodotto Unistorage e il servizio offerto ai clienti.

Unimatica-RGI considera altrettanto importante il concetto di trasparenza rivolto ai propri dipendenti. Sull'intranet aziendale, infatti, ogni dipendente ha a disposizione strumenti e materiali informativi relativi al sistema di gestione integrato della Qualità, della Sicurezza, dell'Ambiente, e della Privacy (ISO 27001, ISO 9001, ISO 14001) e a tutte le Procedure di conservazione. L'impegno, l'attenzione, la formazione e le competenze di tutta l'azienda sulla tematica specifica ed i risultati raggiunti nel corso degli anni di attività hanno permesso ad Unimatica-RGI di ottenere l'iscrizione quale socio sostenitore presso l'associazione ANORC (Associazione Nazionale per Operatori e Responsabili della Conservazione Digitale).

Per dimostrare trasparenza ed affidabilità, inoltre, Unimatica-RGI garantisce da sempre la propria disponibilità ad ospitare audit finanziari e/o di seconda parte, rispettando così le disposizioni delle autorità di controllo e, previo accordo, anche gli accordi stabiliti con clienti per i quali presta servizi.

Torna al sommario

2. Terminologia

La terminologia e gli acronimi utilizzati in questo manuale richiamano quelli elencati *nell'Allegato 1 Glossario dei termini e degli acronimi* alle Linee guida per la formazione, gestione e conservazione dei documenti informatici al quale si rimanda.

Torna al sommario

3. Normativa e standard di riferimento

Il sistema di conservazione sviluppato da Unimatica-RGI è conforme alla normativa e agli standard elencati nei successivi paragrafi.

Periodicamente vengono effettuate verifiche per l'aggiornamento dei requisiti normativi al fine di assicurare una puntuale conformità alle disposizioni legislative. Eventuali ulteriori riferimenti normativi non direttamente riconducibili alla conservazione, ma comunque applicabili per via di servizi correlati ad essa, sono elencati in uno specifico documento facente parte del sistema di gestione integrato, denominato SIC040 – Monitoraggio.

Torna al sommario

3.1. Normativa di Riferimento

Notazione abbreviata	Riferimento
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], art. 2215 bis – Documentazione informatica.
RD 1163/1911	Regolamento per gli archivi di Stato
DPR 1409/1963	Norme relative all'ordinamento ed al personale degli archivi di Stato
Legge 241/1990	Nuove norme sul procedimento amministrativo
DPR 445/2000	Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa
DPR 37/2001	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
D.lgs 196/2003	Recante il Codice in materia di protezione dei dati personali
D.lgs 42/2004	Codice dei beni culturali e del paesaggio, ai sensi dell'articolo 10 della legge 6 luglio 2002,n.137
Legge 9 gennaio 2004, n. 4 aggiornata dal decreto legislativo 10 agosto 2018, n. 106	Disposizioni per favorire e semplificare l'accesso degli utenti e, in particolare, delle persone con disabilità agli strumenti informatici
D.lgs 82/2005 e ss.mm.ii.	Codice dell'amministrazione digitale
D.lgs 33/2013	Riordino della disciplina riguardante il diritto di accesso civico e gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni
DPCM 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
DPCM 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;

Reg. UE 910/2014	In materia di identificazione elettronica e servizi fiduciari per le transazionielettroniche nel mercato interno e che abroga la direttiva 1999/93/CE - Regolamento eIDAS;
Circolare 40 e 41 del 14 dicembre 2015 della Direzione generale degli archivi	Autorizzazionealla distruzione di originali analogici riprodotti secondo le regole tecniche di cui al DPCM 13.11.2014 econservati secondo le regole tecniche di cui al DPCM 13.12.2013;
Reg. UE 679/2016 (GDPR)	Relativo alla protezione delle persone fisiche con riguardo al trattamento deidati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE;
Circolare 18 aprile 2017 n. 2/2017 dell'Agenzia per l'Italia Digitale	Recante le misure minime disicurezza ICT per le pubbliche amministrazioni;
Circolare n. 2 del 9 aprile 2018	Recante i criteri per la qualificazione dei Cloud Service Provider per laPA;
Circolare n. 3 del 9 aprile 2018	Recante i criteri per la qualificazione di servizi SaaS per il Cloud dellaPA;
Reg. UE 2018/1807	Relativo a un quadro applicabile alla libera circolazione dei dati non personalinell'Unione europea;
DPCM 19 giugno 2019 n. 76	Regolamento di organizzazione del Ministero per i beni e le attivitàculturali, degli uffici di diretta collaborazione del Ministro e dell'Organismo indipendente di valutazione dellaperformance.
Linee guida AgID ed Allegati	Linee guida sulla Formazione, Gestione, Conservazione dei documenti informatici Allegato 1 Glossario dei termini e degli acronimi Allegato 2 Formati di File e Riversamento Allegato 3 Certificazione di processo Allegato 4 Standard e specifiche tecniche Allegato 5 Metadati
Regolamento AgID ed Allegati	Regolamento sui criteri di conservazione Allegato A Requisiti per l'erogazione del servizio di conservazione per conto delle pubbliche amministrazioni Allegato B Piano di cessazione del servizio di conservazione dei documenti informatici

Torna al sommario

3.2. Standard di Riferimento

Sigla	Titolo standard
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	

Torna al sommario

4. Ruoli e responsabilità

Conformemente al par. 4.4 delle Linee guida sulla Formazione, gestione e conservazione dei documenti informatici, si individuano i seguenti ruoli coinvolti nel processo di conservazione:

- **Titolare dell'oggetto della conservazione** (citato nel manuale come soggetto produttore), identificato come il soggetto produttore degli oggetti di conservazione.
- **Produttore dei PdV**, ovvero la 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, identificato con il responsabile della gestione documentale nelle pubbliche amministrazioni
- **Utente abilitato**, ossia la persona, l'ente o il sistema che interagisce con i servizi di un sistema per la conservazione dei documenti informatici, al fine di fruire delle informazioni di interesse
- **Responsabile della conservazione**, ovvero il soggetto che definisce e attua le politiche complessive del sistema di conservazione e ne governa la gestione con piena responsabilità ed autonomia.
- **Conservatore**, identificato come l'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.

Il processo di conservazione vede direttamente coinvolti tutti i soggetti sopra elencati.

Unimatica-RGI ha individuato le seguenti figure di responsabilità per l'erogazione del servizio di conservazione, a garanzia di elevati standard di qualità e sicurezza:

Il **Responsabile del servizio di conservazione** espleta, a seguito di delega formale e in ogni caso rimanendo inteso che la responsabilità giuridica generale sui processi di conservazione, non essendo delegabile, rimane in capo al responsabile della conservazione, le seguenti attività:

1. definisce le politiche di conservazione e i requisiti funzionali del sistema di conservazione, in conformità alla normativa vigente e tenuto conto degli standard internazionali, in ragione delle specificità degli oggetti digitali da conservare (documenti informatici, aggregazioni informatiche, archivio informatico), della natura delle attività che il Titolare dell'oggetto di conservazione svolge e delle caratteristiche del sistema di gestione informatica dei documenti adottato
2. gestisce il processo di conservazione e ne garantisce nel tempo la conformità alla normativa vigente;
3. genera e sottoscrive il Rapporto di Versamento, secondo le modalità previste dal manuale di conservazione;
4. genera il pacchetto di archiviazione conforme allo Standard SInCRO UNI 11386 - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali e lo sottoscrive con firma digitale;
5. genera e sottoscrive il pacchetto di distribuzione con firma digitale o firma elettronica qualificata, nei casi previsti dal manuale di conservazione, ai fini dell'esibizione richiesta dall'utente;
6. effettua il monitoraggio della corretta funzionalità del sistema di conservazione;
7. effettua la verifica periodica, con cadenza non superiore ai cinque anni, dell'integrità e della leggibilità dei documenti informatici e delle aggregazioni documentarie degli archivi;

8. al fine di garantire la conservazione e l'accesso ai documenti informatici, adotta misure per rilevare tempestivamente l'eventuale degrado dei sistemi di memorizzazione e delle registrazioni e, ove necessario, per ripristinare la corretta funzionalità. Adotta analoghe misure con riguardo all'obsolescenza dei formati;
9. provvede alla duplicazione o copia dei documenti informatici in relazione all'evolversi del contesto tecnologico, secondo quanto previsto dal manuale di conservazione;
10. adotta le misure necessarie per la sicurezza fisica e logica del sistema di conservazione;
11. 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;
12. assicura agli organismi competenti previsti dalle norme vigenti l'assistenza e le risorse necessarie per l'espletamento delle attività di verifica e di vigilanza;
13. 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

garantendo un particolare riguardo alla:

- 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 all'ente produttore;
- giostione 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.

Il **Responsabile del servizio di conservazione** nominato da Unimatica-RGI è **Paolo Vandelli**.

In assenza del Responsabile del servizio di conservazione, le sue funzioni operative vengono delegate a **Cecilia Canova.**

Il **Responsabile della funzione archivistica di conservazione**, in accordo con il Responsabile del servizio di conservazione, si occupa di

- definire e gestire il processo di conservazione, incluse le modalità di trasferimento da parte del produttore dei PDV, 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
- monitorare set di metadati di conservazione dei documenti, dei fascicoli informatici e delle aggregazioni documentali informatiche
- monitorare il processo di conservazione e analisi archivistica per lo sviluppo di nuove funzionalità del sistema
- collaborare con il Produttore dei PDV 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.

La **Responsabile della funzione archivistica di conservazione** nominata da Unimatica-RGI è **Eleonora Luzi.**

Responsabile sicurezza dei sistemi per la conservazione il quale si occupa di:

- monitorare e rispettare i requisiti di sicurezza del sistema di conservazione stabiliti dagli standard, dalle normative e dalle politiche e procedure interne di sicurezza. In caso di eventuali difformità si occupa di segnalarle al Responsabile del servizio di conservazione e, quindi, individua e pianifica le necessarie azioni correttive.

Il **Responsabile sicurezza dei sistemi per la conservazione** nominato da Unimatica-RGI è **Massimo Ortensi**.

Responsabile dei sistemi informativi per la conservazione il quale si occupa di:

- gestire l'esercizio delle componenti hardware e software del sistema di conservazione e monitorare il mantenimento dei livelli di servizio (SLA) concordati con il Titolare e il Produttore
- segnalare le eventuali difformità degli SLA al Responsabile del servizio di conservazione e individuare e pianificare le necessarie azioni correttive
- pianificare lo sviluppo delle infrastrutture tecnologiche del sistema di conservazione e verifica i livelli di servizio erogati da terzi con segnalazione delle eventuali difformità al Responsabile del servizio di conservazione.

Il **Responsabile dei sistemi informativi per la conservazione** nominato da Unimatica-RGI è **Massimo Ortensi.**

Responsabile sviluppo e manutenzione del sistema di conservazione il quale si occupa di:

- coordinare lo sviluppo e la manutenzione delle componenti hardware e software del sistema di conservazione
- pianificare e monitorare i progetti di sviluppo del sistema di conservazione
- monitora gli SLA relativi alla manutenzione del sistema di conservazione
- interfacciarsi con il Produttore dei PDV relativamente alle modalità di trasferimento dei documenti, fascicoli informatici e aggregazioni documentali informatiche in merito ai formati elettronici da utilizzare, all'evoluzione tecnologica hardware e software, alle eventuali migrazioni verso nuove piattaforme tecnologiche
- gestire lo sviluppo di siti web e portali connessi al servizio di conservazione.

La **Responsabile dello sviluppo e manutenzione del sistema di conservazione** nominata da Unimatica-RGI è **Annachiara Coviello**.

Nell'attribuire ruoli e responsabilità Unimatica-RGI presta importante attenzione alle competenze delle risorse valutate, vanta infatti personale altamente specializzato e formato sulle tematiche legate alla conservazione e all'archiviazione digitale.

Tale personale è costantemente aggiornato sull'evoluzione della normativa e sugli aspetti tecnologici, grazie alla documentazione interna messa a disposizione dall'azienda e garantisce, inoltre, l'opportunità ai dipendenti di partecipare ad appositi corsi qualificanti di approfondimento, interni ed esterni.

Torna al sommario

4.1. Ruoli di ausilio al processo di conservazione

In ottemperanza a quanto previsto dal Regolamento (UE) 2016/679 Unimatica-RGI, al fine di garantire una maggior tutela dei dati propri e di quelli dei clienti, ha nominato un **Data Protection Officer** il quale si occupa di

- offrire idonea consulenza per progettare, verificare e mantenere un sistema organizzato di gestione dei dati personali, interagendo coi sistemi di gestione aziendali, compreso il sistema di conservazione, per curare l'adozione di misure di sicurezza finalizzate alla tutela dei dati trattati dall'azienda, che soddisfino i requisiti di legge e per evitare i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

La **DPO** nominato da Unimatica-RGI è **Anna Veltri.**

Torna al sommario

4.2. Precedenti responsabili

Nominativo	Ruolo	Periodo
Silvano Ghedini	Responsabile servizio di conservazione	01-2004 – 06-2022

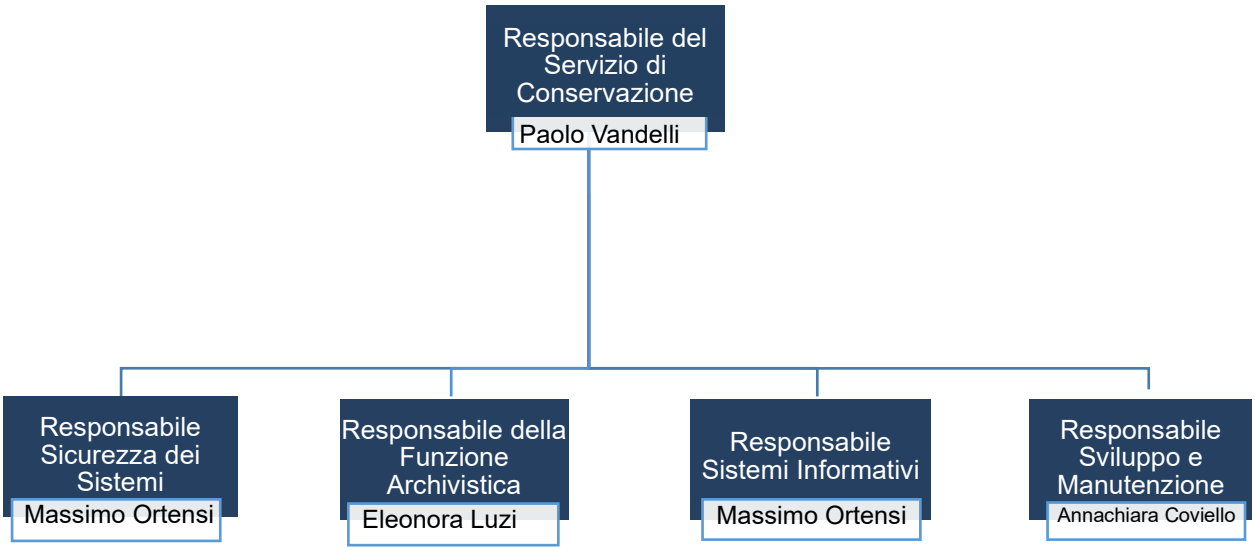
Torna al sommario

5. Struttura organizzativa per il servizio di conservazione

Il presente capitolo ha lo scopo di illustrare la struttura organizzativa del settore conservazione di Unimatica-RGI. L' espletamento di un processo di conservazione prevede una serie di complesse attività, pertanto la società si avvale di personale altamente qualificato e con esperienza decennale. Si riporta di seguito l'organigramma della struttura organizzativa e una sintetica descrizione[1] delle funzioni e delle responsabilità che intervengono nel processo di conservazione.

Torna al sommario

5.1. Organigramma



Torna al sommario

[1] La descrizione dettagliata del processo di conservazione è riportata nel capitolo 7 "Il processo di erogazione del servizio di conservazione".

5.2. Strutture organizzative

Nel presente paragrafo vengono descritte sinteticamente le fasi principali del processo di conservazione e le attività di gestione dei sistemi informativi, individuando per ciascuna di queste le figure che ne assumono le responsabilità.

Attività proprie di ciascun contratto di servizio			
Fase	Attività	Descrizione	Responsabilità
1	Attivazione del servizio di conservazione (a seguito della sottoscrizione del contratto).	Il Soggetto produttore invia una richiesta di attivazione del servizio che avviene in seguito alla compilazione del modulo "Scheda cliente" dove vengono dichiarati dettagli degli oggetti da conservare, come: dimensioni, frequenza invio, ecc.	RSC PM RFA RSM
2	Acquisizione, verifica e gestione dei Pacchetti di versamento e generazione del Rapporto di versamento.	Sui PdV vengono effettuate verifiche circa l'identificazione certa del Soggetto produttore, la firma digitale, formati e metadati sulla base di quanto concordato nella Fase 1. In caso di verifiche andate a buon fine viene generato il RdV, altrimenti viene generata la Comunicazione delle anomalie.	RSC RFA
3	Preparazione e gestione dei Pacchetti di archiviazione[2].	Gli oggetti versati vengono trasformati in PdA contenenti, oltre agli oggetti da conservare, l'IdPA[3] formato secondo le regole dello standard SInCRO. L'IdPA viene sottoscritto con firma digitale dal RSC e viene marcato temporalmente.	RSC RFA
4	Preparazione e gestione del pacchetto di distribuzione ai fini dell'esibizione e della produzione di duplicati e copie informatiche su richiesta.	I PdD, vengono creati in base alle richieste dell'Utente. Possono essere visualizzati mediante interfaccia web, WS o, se richiesto, tramite memorizzazione su supporto.	RSC RFA PM
5	Scarto dei pacchetti di archiviazione	Prima della scadenza del periodo di conservazione, Unimatica-RGI contatta il Soggetto produttore il quale in caso di rescissione del contratto comunicherà in forma scritta la decisione. Unimatica-RGI eliminerà fisicamente i PdA. Per i PdA provenienti da enti pubblici o da archivi privati per i quali è stato dichiarato l'interesse culturale si terrà	RSC RFA PM

[2] Traduzione di Archival Information Package dal Modello OAIS Open Archival Information Standard che individua nel sistema di archiviazione tre diversi tipi di Pacchetti: Submission Information Package (SIP), Archival Information Package (AIP) e Dissemination Information Package (DIP).
[3] Indice del pacchetto di archiviazione.

		conto dei massimari di scarto di questi e della decisione ultima della Soprintendenza archivistica.	
6	Chiusura del servizio di conservazione (al termine di un contratto)	Il Soggetto produttore comunicherà ad Unimatica-RGI la rescissione del contratto.	RSC PM

Attività proprie di gestione dei sistemi informativi			
Fase	Attività	Descrizione	Responsabilità
1	Conduzione e manutenzione del sistema di conservazione	Le attività di manutenzione vengono svolte sia sui processi che sulle strutture hardware e software e viene condotta una quotidiana verifica delle attività sulle infrastrutture parallelamente ad una pianificazione delle eventuali procedure straordinarie da condurre in caso di anomalie.	RSM RSSI
2	Monitoraggio del sistema di conservazione	Viene effettuato il monitoraggio del sistema di Log che consente la registrazione degli accessi e degli eventi (operazioni). Tra le attività di monitoraggio rientrano anche la verifica dell'integrità degli archivi e la gestione delle anomalie.	RSC RFA RSSI
3	Change management	Vengono definite politiche, priorità e tempistiche dell'adeguamento all'evoluzione tecnologica affinché il sistema di conservazione possa garantire nel tempo integrità, disponibilità e sicurezza.	RFA RSI
4	Verifica periodica di conformità a normativa e standard di riferimento	La conformità a normativa e standard è costantemente monitorata ed eventualmente aggiornata.	RSC RSSI

Legenda	
RSC	Responsabile del Servizio di Conservazione
RSSI	Responsabile Sicurezza dei Sistemi Informativi per la Conservazione
PM	Privacy Manager
RFA	Responsabile Funzione Archivistica per la Conservazione
RSI	Responsabile Sistemi Informativi per la Conservazione
RSM	Responsabile Sviluppo e Manutenzione del Sistema di Conservazione

Torna al sommario

6. Oggetti sottoposti a conservazione

Unimatica-RGI mediante il proprio sistema di conservazione Unistorage, sviluppato integralmente dalla società, è in grado di accettare e gestire, come richiesto ai sensi dell'art. 44, comma 1-bis, del CAD[4],

a) I fascicoli informatici chiusi e le serie informatiche chiuse,
b) i fascicoli informatici e le serie non ancora chiusi accettando i documenti in essi contenuti sulla base di specifiche esigenze del soggetto produttore. In particolare, in questo caso, il Titolare e il Conservatore garantiscono specifico monitoraggio al fine di evitare rischi di obsolescenza tecnologica che possono sopravvenire prima della chiusura.

Unistorage è predisposto per accettare aggregazioni documentali e tutte le tipologie di documenti informatici relativi a diversi ambiti applicativi.

In accordo con il soggetto produttore, Unimatica-RGI si riserva infatti la facoltà di accettare qualsiasi tipologia documentale. L'indicazione delle tipologie documentali, compresa la gestione di queste, verrà indicata nella scheda cliente allegata al contratto stipulato con il soggetto produttore.

Unimatica-RGI accetta e conserva solo documenti informatici. Il sistema di conservazione permette l'acquisizione sia di documenti firmati digitalmente, sia di documenti non firmati. Entrambe le tipologie entrano nel medesimo processo di Ingestion. Con l'ausilio del Responsabile del servizio di conservazione, è il Soggetto produttore a definire nella scheda cliente le modalità di trattamento dei documenti firmati o non firmati.

Torna al sommario

6.1. Metadati

Come previsto dal par. 4.1 delle Linee guida, il sistema di conservazione assicura dalla presa in carico fino all'eventuale scarto, la conservazione di oggetti digitali tramite l'adozione di regole, procedure e tecnologie, necessarie al mantenimento delle caratteristiche di autenticità, integrità, affidabilità, leggibilità e reperibilità.

Al fine di rendere agevole ed efficiente la ricerca di un documento, di un fascicolo, o di un'aggregazione documentale informatica conservati, è necessario corredare tali oggetti da un set di metadati che ne descrivono il contenuto e lo identificano all'interno del sistema. Unimatica-RGI, in piena conformità alle Linee guida e all'Allegato 5, garantisce l'acquisizione, la gestione e la conservazione di:

- Metadati del documento informatico
- Metadati del documento amministrativo informatico
- Metadati delle aggregazioni documentali informatiche
- Metadati del documento informatico di natura fiscale e contabile

Nei paragrafi successivi si elencano per ogni tipologia, a titolo esemplificativo e non esaustivo, i metadati obbligatori individuati dalle Linee guida. Per tutti i dettagli specifici sul lessico, campi e schemi si rimanda alle schede di dettaglio presenti all'interno dell'*Allegato 5* alle Linee guida e

[4] L'art. 44, comma 1-bis, del CAD prevede che: "[…] Almeno una volta all'anno il responsabile della gestione dei documenti informatici provvede a trasmettere al sistema di conservazione i fascicoli e le serie documentarie anche relative a procedimenti non conclusi"

all'Elenco AgID "*L'utilizzo dei metadati del documento informatico - I metadati del documento informatico di natura fiscale e contabile*"

Torna al sommario

6.1.1 Metadati del documento informatico

Di seguito vengono elencati i metadati, ed i principali campi e sottocampi *obbligatori* del documento informatico:

IdDoc: Identificativo univoco e persistente associato in modo univoco e permanente al documento informatico in modo da consentirne l'identificazione

Il metadato è costituito dai seguenti:

- 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

Modalità di formazione: modalità di generazione del documento informatico

Sono previste le seguenti modalità:

- creazione tramite l'utilizzo di strumenti software che assicurino la produzione di documenti nei formati previsti nell'Allegato 2 delle Linee Guida;
- 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;
- 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;
- 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

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)

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 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.

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 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.
- 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

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

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

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 (*facoltativo*, per le specifiche si rimanda all'Allegato 5)
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.

Identificativo del formato: indica il formato del documento e la versione del software utilizzato per la creazione del documento stesso.

É costituito da:

- 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:
  - nome prodotto
  - versione prodotto
  - produttore

Verifica: heck di controllo presenza Firma elettronica, Sigillo, Marcatura temporale e Conformità copie immagine nelle modalità di formazione del documento informatico previste nelle Linee Guida.

Identificativo dell'Aggregazione documentale: identificativo univoco dell'Aggregazione come definito nel paragrafo dei Metadati delle aggregazioni documentali informatiche. Metadato ricorsivo (*facoltativo*, per le specifiche si rimanda all'Allegato 5).

Identificativo del Documento Primario: identificativo univoco e persistente del Documento primario (*obbligatorio nel caso in cui sia presente un documento primario*).

Nome del documento\file: nome del documento\file così come riconosciuto all'esterno.

Versione del documento: versione del documento.

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" (*obbligatorio nel caso di versione > 1 o in caso di annullamento*).

Tempo di conservazione: tempo di conservazione del documento desunto dal Piano di conservazione integrato con il Piano di classificazione (ove presenti) o prescritto dalla normativa salvo contenzioso. In generale il tempo di conservazione a livello di singolo documento deve essere indicato solo qualora esso presenti un tempo di conservazione distinto da quello assegnato all'aggregazione documentale informatica a cui il documento stesso appartiene. Espresso in numero di anni, il valore 9999 indica un tempo di conservazione "Permanente" (*facoltativo*).

Note: eventuali indicazioni aggiuntive utili ad indicare situazioni particolari (*facoltativo*).

Nella scheda cliente è possibile personalizzare ed indicare i set di metadati in base alle esigenze del soggetto produttore e alle diverse tipologie documentali conservate. In un'apposita tabella il cliente specificherà i metadati di proprio interesse.

Torna al sommario

6.1.2 Metadati del documento amministrativo informatico

Di seguito vengono elencati i metadati, ed i principali campi e sottocampi obbligatori del documento informatico:

IdDoc: Identificativo univoco e persistente associato in modo univoco e permanente al documento informatico in modo da consentirne l'identificazione

Il metadato è costituito dai seguenti:

- Impronta crittografica del documento: a sua volta suddiviso in:
  - 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
- Segnatura: segnatura di protocollo, da indicare obbligatoriamente nel caso di documento amministrativo protocollato, a sua volta strutturato come da Allegato 6 delle Linee Guida.

Modalità di formazione: modalità di generazione del documento informatico

Sono previste le seguenti modalità:

- creazione tramite l'utilizzo di strumenti software che assicurino la produzione di documenti nei formati previsti nell'Allegato 2 delle Linee Guida;
- 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;
- 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;
- 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

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 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.
- 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

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

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

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.

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.

Identificativo del formato: indica il formato del documento e la versione del software utilizzato per la creazione del documento stesso.

É costituito da:

- 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:
  - nome prodotto
  - versione prodotto
  - produttore

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.

Identificativo dell'Aggregazione documentale: identificativo univoco dell'Aggregazione come definito nel paragrafo dei Metadati delle aggregazioni documentali informatiche. Metadato ricorsivo.

Identificativo del Documento Primario: identificativo univoco e persistente del Documento primario (*obbligatorio nel caso in cui sia presente un documento primario*).

Nome del documento\file: nome del documento\file così come riconosciuto all'esterno.

Versione del documento: versione del documento.

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" (*obbligatorio nel caso di versione > 1 o in caso di annullamento*).

Tempo di conservazione: tempo di conservazione del documento desunto dal Piano di conservazione integrato con il Piano di classificazione (ove presenti) o prescritto dalla normativa salvo contenzioso. In generale il tempo di conservazione a livello di singolo documento deve essere indicato solo qualora esso presenti un tempo di conservazione distinto da quello assegnato all'aggregazione documentale informatica a cui il documento stesso appartiene. Espresso in numero di anni, il valore 9999 indica un tempo di conservazione "Permanente" (*facoltativo*).

Note: eventuali indicazioni aggiuntive utili ad indicare situazioni particolari (*facoltativo*).

Nella Scheda Cliente predisposta da Unimatica-RGI, è possibile personalizzare ed indicare i set di metadati in base alle esigenze del soggetto produttore e alle diverse tipologie documentali conservate. In un'apposita tabella il cliente specificherà i metadati di proprio interesse.

6.1.3 Metadati delle aggregazioni documentali informatiche

Di seguito vengono elencati i metadati, ed i principali campi e sottocampi obbligatori delle aggregazioni documentali informatiche:

Identificativo dell'Aggregazione documentale: si tratta di 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.

Sono definiti i seguenti attributi:

- TipoAggregazione
  - Fascicolo
  - Serie Documentale
  - Serie Di Fascicoli
- IdAggregazione: come da sistema di identificazione formalmente definito

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.

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:
  - Amministrazione titolare
  - Amministrazioni partecipanti
  - Assegnatario
  - Soggetto intestatario persona fisica
  - Soggetto intestatario persona giuridica
  - 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 corrispondente.

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 (obbligatorio in caso di fascicolo)
- Soggetto assegnatario (obbligatorio in caso di fascicolo)
- Data inizio assegnazione (obbligatorio in caso di fascicolo)
- Data fine assegnazione (facoltativo)

Il metadato ha una struttura ricorsiva.

Data Apertura: data di apertura dell'aggregazione documentale.

Classificazione: classificazione dell'aggregazione:

- Indice di classificazione: Codifica del documento secondo il Piano di classificazione utilizzato
- Descrizione: Descrizione per esteso dell'Indice di classificazione indicato.
- Piano di classificazione: se presente, riportare eventualmente l'URI di pubblicazione del Piano di classificazione (facoltativo)

Progressivo: progressivo numerico calcolato nell'ambito della chiave della classificazione o in ordine cronologico nell'ambito dell'anno.

Chiave descrittiva: metadato funzionale volto a chiarire la natura del fascicolo o della serie.

È costituito da seguenti campi:

- Oggetto: testo libero

Data Chiusura: data di chiusura dell'aggregazione documentale.

Procedimento Amministrativo: metadato funzionale volto ad indicare il procedimento a cui il fascicolo afferisce, nonché lo stato di avanzamento e le relative fasi.

È costituito da seguenti campi:

- Materia\ Argomento\ Struttura: indicare la materia o l'argomento o la struttura per la quale sono stati catalogati i procedimenti amministrativi
- Procedimento: denominazione del Procedimento
- Catalogo procedimenti: URI di pubblicazione del catalogo
- Fasi: a sua volta suddiviso, in una struttura ricorsiva:
  - Tipo Fase
    - Preparatoria
    - Istruttoria
    - Consultiva
    - decisoria o deliberativa
    - integrazione dell'efficacia
  - Data inizio fase
  - Data fine fase (facoltativo)

  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.

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.

È costituito da seguenti campi:

- Tipo documento
  - documento amministrativo informatico
  - documento informatico
- IdDoc
  - se documento amministrativo informatico
    IdDoc come definito nel precedente paragrafo dei Metadati del documento amministrativo informatico
  - se documento informatico
    IdDoc come definito nel precedente paragrafo dei Metadati del documento informatico

Posizione fisica Aggregazione Documentale: posizione fisica dell'aggregazione. Nel caso di fascicoli ibridi indica la posizione della componente cartacea del fascicolo.

6.1.4 Metadati del documento informatico di natura fiscale e contabile

In relazione alla valorizzazione dei metadati specifici del documento informatico di natura fiscale e contabile si rimanda alle specifiche descritte nelle istruzioni dal titolo *I metadati del documento informatico di natura fiscale e contabile* pubblicato nella sezione Linee guida del sito di AgID.

Torna al sommario

6.2 Formati

Unistorage, in conformità all'*Allegato 2 "Formati di file e riversamento"* alle Linee guida AgID, accetta e gestisce formati aperti, non proprietari, standard de iure, estendibili, parlanti, completamente robusti, indipendenti dal dispositivo e che garantiscano i principi dell'interoperabilità.
Tuttavia, in accordo con il soggetto produttore, Unimatica-RGI permette anche l'accettazione di formati non esplicitati nell'Allegato 2. Infatti qualora l'ordinamento giuridico preveda degli obblighi relativamente all'uso di formati specifici per alcuni Titolari, questi assolvendo tali obblighi, sono chiamati ad effettuare una valutazione di interoperabilità utile anche per garantire la conservazione e la fruibilità degli stessi nel tempo. L'indicazione di tali formati, compresa la gestione di questi, verrà indicata nella scheda cliente.

Torna al sommario

6.2.1 Riversamento

Unistorage, in relazione all'obsolescenza dei formati, tiene un censimento dei formati di file ricevuti in conservazione a seguito di un'attività di ingestion (compreso il recupero da precedente conservatore). Il responsabile del servizio di conservazione, assieme al responsabile della funzione archivistica, al responsabile sviluppo e manutenzione del sistema di conservazione e al responsabile sicurezza dei sistemi per la conservazione, con cadenza non superiore ai 5 anni, fatta una fotografia dei formati di file censiti al momento sul sistema, ne valuta il grado di obsolescenza.
In fase di analisi dei formati, come da procedura stabilita, per ogni formato si attribuisce un grado di obsolescenza, basandosi sulle caratteristiche di apertura, sicurezza, portabilità, funzionalità,

supporto allo sviluppo e diffusione. Al termine della verbalizzazione di questo processo di verifica, a fronte di evidenze di formati di file per cui è impossibile individuare soluzioni in grado di rappresentare fedelmente il contenuto di questi file, il responsabile del servizio di conservazione attiva il processo di riversamento dei file appartenenti ai formati risultati a rischio di obsolescenza, previa certificazione di processo.
Per tutti i dettagli inerenti l'intero processo di gestione del riversamento si rimanda al documento di sistema "PRO_CONS01 - Procedure di Conservazione".

Torna al sommario

6.3 Struttura dati del Pacchetto di versamento

Unimatica-RGI mediante il prodotto applicativo UniStorage, con la supervisione del Responsabile del servizio di conservazione permette un duplice iter per la ricezione dei Pacchetti di Versamento: ricezione dei file tramite canale SSH File Transfert Protocol e ricezione tramite sistema Web service.

- La ricezione mediante SSH File Transfert Protocol prevede l'upload del Pacchetto di versamento composto da un file indice e da un insieme di file, in formato .zip. Per maggiori dettagli circa la struttura dei Pacchetti di versamento, fare riferimento al documento Flusso per la conservazione dei Documenti in Unistorage.

- La ricezione tramite Sistema Web Service è possibile da qualsiasi piattaforma che permetta di eseguire e ricevere chiamate Web Service conformi allo standard WS-I Basic Profile 1.0. Con questo servizio il sistema di conservazione riceve singoli documenti ed eventuali allegati, ne verifica la firma digitale se presente e ne gestisce la conservazione autentica. Per maggiori dettagli circa la ricezione degli oggetti digitali tramite Sistema Web Service si rimanda al documento "Specifiche del servizio web per la consegna anticipata di documenti nel Sistema di conservazione".

Torna al sommario

6.4 Struttura dati del Pacchetto di archiviazione

Terminato il processo di acquisizione dei Pacchetti di versamento, il prodotto applicativo UniStorage sotto la supervisione del Responsabile del servizio di conservazione e del Responsabile della funzione archivistica provvede alla creazione dei Pacchetti di archiviazione e dell'Indice del pacchetto di archiviazione previsto dallo standard UNI 11386 SInCRO – Supporto all'interoperabilità nella conservazione e nel recupero degli oggetti digitali.
I Pacchetti di archiviazione contengono[5]:

- l'oggetto o gli oggetti da conservare;
- l'Indice del Pacchetto di archiviazione, formato secondo le regole dettate dallo Standard UNI 11386 SInCRO – Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali.

[5] Sono elencate le caratteristiche indicate nell'allegato 4 al DPCM 3 dicembre 2013 Regole tecniche in materia di sistema di conservazione.

Tutti i pacchetti di archiviazione prodotti fino al 31 dicembre 2021 implementano lo standard UNI 11386:2010 SInCRO. A partire dal 1° gennaio 2022 viene applicata la versione 2020 dello standard.

Torna al sommario

6.5 Struttura dati del Pacchetto di distribuzione

La produzione di Pacchetti di distribuzione avviene in seguito alla richiesta da parte dell'Utente.

L'esibizione del materiale di interesse avviene via interfaccia web o mediante memorizzazione su supporto ottico. La descrizione dettagliata delle procedure è indicata nel capitolo 7 "Il processo di erogazione del servizio di conservazione", Fase 6.
Per quanto riguarda i Pacchetti di distribuzione memorizzati su supporto ottico, questi coincidono con i Pacchetti di archiviazione, come previsto delle Regole tecniche in materia di sistemi di conservazione, ma saranno corredati di informazioni aggiuntive necessarie per la creazione dei DVD, CD, ecc. nel caso di richiesta di esibizione da parte dell'Utente.

UniStorage consente la produzione di supporti rimovibili che possono essere forniti all'Utente.
In ogni supporto vengono trasferiti Pacchetti di distribuzione chiamati "Registrazioni", contenenti sia gli oggetti che l'insieme delle evidenze di conservazione.
La registrazione generata è auto-esplicativa, intendendo con questo che i dati sono affiancati da indici e informazioni di riferimento tali da poter permettere la comprensione del contenuto anche da programmi esterni al sistema di conservazione.
La registrazione è contenuta in una directory, il cui nome contiene un'indicazione del blocco dei documenti e data/ora dell'inizio della creazione della registrazione stessa.

Contenuto della directory della registrazione:

- file README.txt
- file autorun
- icona
- directory chrome
- directory chrome_profile
- directory viewer

I vari Pacchetti di distribuzione a seconda delle dimensioni possono venire raggruppati in volumi auto consultanti, la struttura dei volumi è la seguente:

Figura 1 - Struttura volumi

All'interno della directory viewer avremo una directory contenente i documenti suddivisi per Pacchetti. Questi volumi sono auto consultanti e permettono la ricerca e visualizzazione dei documenti conservati, i metadati associati e le marche di conservazione.

Torna al sommario

7. Il processo di erogazione del servizio di conservazione

Il processo di conservazione eseguito da Unimatica-RGI adotta il modello standard OAIS - Open Archival Information System[6] che definisce concetti e funzionalità degli archivi digitali. Lo schema seguente illustra brevemente gli aspetti principali di un generico processo di conservazione: il Soggetto produttore invia il Pacchetto di versamento, di cui ha piena responsabilità, al Soggetto conservatore il quale provvede a trasformarlo in Pacchetto di archiviazione. Ai fini dell'esibizione e della distribuzione richiesti dalla comunità di riferimento[7], il Soggetto conservatore provvederà a creare i Pacchetti di distribuzione in una forma tale che venga garantita la corretta visualizzazione di questi.

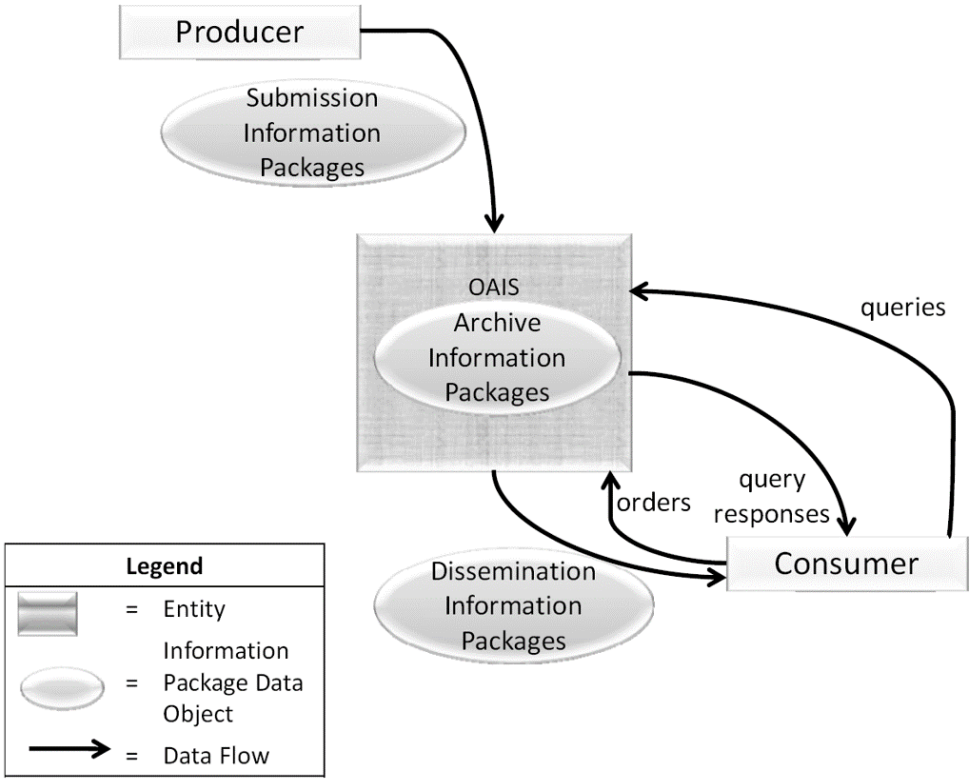


Figura 2 - Modello OAIS

Torna al sommario

[6] L'Open Archival Information System è lo standard ISO per la conservazione a lungo termine di archivi digitali.
[7] Comunità di riferimento: il sottoinsieme degli utenti in grado di comprendere autonomamente l'informazione archiviata nella forma in cui è conservata e resa disponibile dall'OAIS

7.1 Il processo di conservazione

Il servizio offerto da Unimatica-RGI ad ogni Soggetto produttore viene avviato al termine di un processo di attivazione che segue queste fasi fondamentali:

- condivisione di informazioni tecniche di richiesta configurazione e invio dei Pacchetti di versamento;
- verifiche sui Pacchetti di versamento e sugli oggetti in esso contenuti;
- accettazione dei Pacchetti di versamento e generazione del Rapporto di versamento di presa in carico;
- rifiuto dei Pacchetti di versamento e modalità di comunicazione delle anomalie;
- preparazione e gestione del Pacchetto di archiviazione;
- preparazione e gestione del Pacchetto di distribuzione ai fini dell'esibizione;

Ognuno degli step sopra indicati viene eseguito per ogni tipologia di configurazione richiesta.

Di seguito vengono dettagliate le fasi del processo.

Torna al sommario

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

In questa fase il Soggetto produttore veicola al Responsabile del servizio di conservazione, al Privacy Manager e al Responsabile della funzione archivistica la richiesta di attivazione del servizio per l'invio di Pacchetti di versamento. Le tre figure responsabili sopracitate, con l'ausilio del Responsabile dello sviluppo e della manutenzione, incaricato di curare l'interfaccia con il Soggetto produttore relativamente alle modalità di trasferimento dei documenti, valuteranno la domanda di acquisizione del servizio affinché venga accertato che i requisiti del Soggetto produttore siano compatibili con le policy di Unimatica-RGI

L'attivazione del servizio avviene attraverso la compilazione del Modulo 'Scheda cliente'. In particolare, tale modulo deve essere compilato con le seguenti informazioni:

- ragione sociale;
- indirizzo;
- partita iva;
- e-mail
- oggetti documentali gestiti
- tipo di protocollo da utilizzare per lo scambio dei Pacchetti.
- metadati specifici di tipologia
- utenze da abilitare per l'accesso al portale di distribuzione.

Per ogni Pacchetto di versamento dichiarato dal Soggetto produttore, è possibile definire:

- i volumi in termini di numero documenti annui previsti da gestire e spazio di occupazione previsto per i dati da Conservare (GB);
- la dimensione massima del Pacchetto di versamento;
- la frequenza di invio dei Pacchetti;

Il Responsabile del servizio di conservazione, valuterà in accordo con il Privacy manager, con il Responsabile della funzione archivistica e con il Responsabile dello sviluppo e della manutenzione la domanda di acquisizione del servizio collaborando con il Soggetto produttore guidandolo nella compilazione della domanda per l'attivazione del servizio.

Il Responsabile del servizio di conservazione e il Responsabile della funzione archivistica una volta ricevuta la richiesta, si impegnano a valutarne l'impatto stimando la data di evasione e fornendo al Soggetto produttore una pianificazione delle fasi successive. Se la richiesta di configurazione implica un aggravio di costi, verrà fornita parallelamente al Soggetto produttore la quotazione economica dell'attività redatta dal Referente Commerciale di Unimatica-RGI

L'acquisizione dei Pacchetti di versamento avviene mediante due canali: tramite SSH File Transfert Protocol e tramite canale Web service descritti dettagliatamente nel capitolo "Oggetti sottoposti in conservazione", paragrafo 6.3.

Ad ogni attivazione verranno consegnate le credenziali per accedere all'applicativo web reso disponibile da Unimatica-RGI, in base ai dati presenti nella Scheda cliente. Tale accesso garantirà la piena esibizione dei Pacchetti di distribuzione.

Torna al sommario

7.3 Verifiche effettuate sui Pacchetti di versamento e sugli oggetti in esso contenuti

I parametri gestionali del Pacchetto di versamento vengono verificati e messi a punto dal Responsabile del servizio di conservazione e dal Responsabile della funzione archivistica in accordo con il Soggetto produttore. Le verifiche effettuate sui Pacchetti di versamento sono le seguenti:

- **identificazione certa del Soggetto produttore**;

- verifica delle **firme digitali** se presenti mediante un controllo crittografico dell'integrità del documento e della validità formale delle firme stesse. In un secondo momento viene verificata l'identità del sottoscrittore. Se una chiave privata sia stata usata in una firma è verificabile, mediante processo crittografico, con la corrispondente chiave "pubblica". Le chiavi pubbliche sono riportate nei "certificati di firma digitale", documenti informatici anch'essi, che definiscono anche i dati d'identità del sottoscrittore. I certificati sono a loro volta firmati da una autorità di certificazione emittente (C.A. - Certification Authority). In generale si risalirà la catena di certificazione fino a raggiungere un "certificato fidato", ovvero pubblicamente noto. Tra le evidenze informatiche che Unimatica-RGI conserva ci sono, per ogni Pacchetto, tutti i certificati a vario modo coinvolti nelle catene di certificazione necessarie alle verifiche di firma digitale. Questo consente di costituire un insieme "auto-contenuto" di evidenze che possono essere verificate anche a posteriori. Si può anche verificare il caso che l'autorità emittente non sia direttamente un'autorità pubblicamente nota, ma che esista

una “catena di certificazione” (trust chain) per cui l'autorità di un certificato vada a sua volta identificata risalendo ad un'autorità terza.

- verifica che i **formati** degli oggetti da conservare siano conformi con quanto dichiarato nella scheda cliente e nell’Allegato 2 alle Linee guida per la Formazione, gestione e conservazione dei documenti informatici. Alla ricezione del documento il sistema, attraverso l’uso di una libreria WAZFORMAT, la cui procedura utilizzerà un metodo di indagine diretta con tecniche euristiche, riconosce il formato controllando il valore descritto nel magic number. Questo passaggio permette di associare il formato al documento per garantirne la corretta visualizzazione e quindi leggibilità utilizzando gli opportuni i visualizzatori.
- relativamente alle verifiche dei **metadati** sono previste tre livelli di controllo:
    - *strict:* l’assenza di anche solo un metadato obbligatorio (Allegato 5 alle Linee guida) comporta la restituzione di un errore alla richiesta di versamento ed il documento non viene conservato
    - *permissive*: l’assenza di metadati obbligatori (Allegato 5 alle Linee guida) viene segnalata con un warning, ma il processo di conservazione prosegue generando i metadati assenti con un valore nullo.
    - *skip*: applicato a tutti i soggetti produttori non vincolati alla normativa italiana (Allegato 5 alle Linee guida). In questo caso i metadati obbligatori sono concordati con il soggetto produttore in base alle buone prassi o ai vincoli normativi del paese di origine.

Torna al sommario

7.4 Accettazione dei Pacchetti di versamento e generazione del Rapporto di versamento di presa in carico

L’esito positivo delle verifiche effettuate sui Pacchetti di versamento viene registrato in un Rapporto di versamento di presa in carico. Il Rapporto conterrà un’impronta del file originale comprensivo di algoritmo con la quale tale impronta viene calcolata (hash) e un riferimento temporale certificato che costituisce evidenza dell'esistenza e dell'esatta composizione del Rapporto collegato all'istante indicato (Tcons).
Apponendo un timestamp al Rapporto di versamento, lo si “sigilla” e contemporaneamente si fissa il riferimento temporale. Tale procedimento costituisce un riferimento temporale certificato per il Rapporto di versamento.
Il Rapporto di versamento attesta la corretta esecuzione del processo di immissione dei Pacchetti, ha la funzione di raccogliere evidenze indirette di tutti i documenti del Pacchetto e garantisce due principali funzioni:

- la possibilità di provare l’integrità dei dati di ogni file contenuto nel pacchetto,
- di permettere il controllo dell’integrità per ogni file in modo separato, senza creare un’interdipendenza tra i file ai fini dell’esibizione e del controllo.

Il Rapporto di versamento è un file in formato XML che riporta, per ognuno dei file inclusi nel Pacchetto, alcune informazioni tra cui un “URN” (unified resource name) e un “hash”. L'URN è una stringa univoca che identifica l'oggetto digitale, mentre l’hash è un'impronta del documento, ovvero una sequenza di bit che può essere ricavata dal file in modo ripetibile e standardizzato e che

garantisce una corrispondenza esatta col contenuto originale (in modo pratico possiamo dire di avere la garanzia che a due file differenti corrispondono sempre due impronte distinte).

La modalità di conservazione mediante Rapporto di versamento permette di verificare l'integrità di ogni singolo file, a prescindere da tutti gli altri file conservati nello stesso pacchetto. Infatti sarà sufficiente essere in possesso di un file "candidato" e conoscere il suo URN identificativo per poter eseguire la funzione di hash e confrontare l'impronta ricalcolata con la stringa riportata nel Rapporto. In questa fase vengono associate all'indice tutte le evidenze di autenticità delle firme digitali che verranno verificate all'istante del riferimento temporale:

- i certificati di firma di tutte le firme presenti nel Pacchetto di versamento,
- tutti i certificati appartenenti alle catene di certificazione (trusting chain),
- le liste di revoca dei singoli certificati (CRL).

Il Rapporto di versamento viene conservato all'interno del sistema garantendone l'ininterrotta custodia e la non modificabilità.

Torna al sommario

7.5 Rifiuto dei Pacchetti di versamento e modalità di comunicazione delle anomalie

Le verifiche effettuate sui Pacchetti di versamento possono risultare negative. Nei casi in cui anche solo su uno dei controlli indicati nella fase 2 si dovesse riscontrare una mancanza o non corrispondenza di informazioni viene generato un file di Comunicazione delle anomalie che verrà comunicato mediante un file di esito al Soggetto produttore. Tale Comunicazione comprenderà i dettagli delle verifiche eseguite sui Pacchetti di versamento comprensive delle precisazioni sulle anomalie.
Le anomalie, in relazione a quanto descritto nella fase 2, possono essere identificate nell'assenza dei metadati obbligatori ovvero nella mancata corrispondenza di ciò che viene versato a quanto dichiarato dal soggetto produttore nella scheda cliente in termini di firma digitale, formati e metadati. Qualora l'anomalia venisse riscontrata soltanto su una parte di documenti inclusi nel Pacchetto di versamento, è facoltà del soggetto produttore decidere se bloccare l'intero pacchetto o soltanto i documenti segnalati. In questo ultimo caso i file conformi vengono inviati in conservazione e gli altri spediti successivamente mediante nuovo Pacchetto di versamento.

Torna al sommario

7.6 Preparazione e gestione dei Pacchetti di archiviazione

I Pacchetti versati in UniStorage, con la supervisione del Responsabile del servizio di conservazione e del Responsabile della funzione archivistica vengono raggruppati in Pacchetti di archiviazione. Questi pacchetti vengono assemblati dal sistema nei tempi e con i criteri di raggruppamento scelti e concordati con il Soggetto produttore, indicati nella Scheda Cliente (ad es. Pacchetti di archiviazione per tipologie documentali o in base alla cadenza temporale di consegna).
Il processo di costruzione dei Pacchetti di archiviazione, così come previsto dallo standard SInCRO UNI 11386– Supporto all'interoperabilità nella conservazione e nel recupero degli oggetti digitali, avviene con le seguenti modalità:

- individuazione dei documenti destinati a far parte del pacchetto di archiviazione sulla base dei criteri scelti. Tali criteri vengono concordati con il cliente e sono definiti nella scheda cliente e si possono basare sia su caratteristiche legate allo stato del documento, sia sui metadati.
- i Pacchetti di archiviazione vengono chiusi in seguito a due tipi di regole:
  - automatiche: collocano nel pacchetto i documenti per i quali ci sia almeno un certificato di firma prossimo alla scadenza. Questa tipologia di regole ha la precedenza su quelle descritte nel punto successivo, le quali riguardano la dimensione massima del Pacchetto di archiviazione e il tempo limite oltre il quale un Pacchetto di archiviazione deve essere forzatamente chiuso,
  - attuate dal Responsabile del servizio di conservazione in accordo con il soggetto produttore: definite nella scheda cliente.

Nei casi in cui i Pacchetti di archiviazione contengano referti sanitari, questi vengono crittografati mediante funzione crittografica della suite standard del linguaggio Java. In particolare è definita nel package crypto di JCE e impiega l'algoritmo AES a 128 bit ECB.

I Pacchetti di archiviazione vengono sottoscritti con firma digitale dal Responsabile del servizio di conservazione e marcati temporalmente.
La sottoscrizione dei Pacchetti di archiviazione effettuata da Unimatica-RGI attesta esclusivamente la corretta esecuzione del processo di conservazione secondo la normativa vigente in materia di conservazione. Unimatica-RGI non è responsabile dell'errato contenuto informativo degli oggetti versati.

Torna al sommario

7.7 Preparazione e gestione dei Pacchetti di distribuzione ai fini dell'esibizione

La gestione dei Pacchetti di distribuzione fa capo al Responsabile del Servizio di Conservazione, al Responsabile della Funzione archivistica e al Privacy manager.

La produzione di Pacchetti di distribuzione avviene in seguito alla richiesta da parte dell'utente.

UniStorage, prevedendo la conservazione dei Pacchetti di archiviazione firmati, implementa un formato di composizione delle marche tale da permettere l'esibizione probatoria di un singolo documento. Quindi, ogni singolo file può essere esibito insieme ai suoi metadati, registrati nel data base, e alle sue prove di conservazione in maniera assolutamente INDIPENDENTE dagli altri documenti.
Unimatica-RGI permette l'accesso ai Pacchetti di distribuzione esclusivamente agli utenti autorizzati. I livelli di accesso vengono definiti in base alle esigenze delle richieste effettuate, rendendo disponibile soltanto il materiale richiesto grazie all'utilizzo di filtri predefiniti che selezionano i canali previsti per la visualizzazione di un determinato pacchetto.

È possibile visualizzare i documenti tramite duplice canale:

- via web: i Soggetti produttori titolari dei documenti potranno ricercare e visualizzare tutti i documenti conservati direttamente sul portale di Unimatica-RGI attraverso l'apposita funzionalità. L'accesso avviene tramite il portale al quale è demandata la sicurezza e la gestione della sessione. I documenti saranno disponibili per l'esibizione on-line per tutto il

periodo di conservazione. Per maggiore chiarezza si precisa che al fine di garantire una veloce e corretta visualizzazione dei documenti conservati, tramite ricerca libera il portale permette la visualizzazione di 200 risultati. Per la ricerca di tutti gli altri documenti sarà necessario valorizzare gli appositi campi delle maschere di ricerca con i metadati dichiarati in fase di versamento. La descrizione di dettaglio dell'interfaccia web per le richieste di esibizione dei documenti è contenuta nell'allegato 'Funzionalita_portale'. Vengono inoltre resi disponibili servizi web (Web Services) per le eventuali integrazioni con i portali dei Soggetti produttori.

- copia del documento su supporto ottico. La descrizione dettagliata circa la visualizzazione dei Pacchetti di distribuzione mediante supporto ottico è presente nel capitolo 6 Oggetti sottoposti a conservazione, paragrafo 6.5.

La struttura architetturale di UniStorage consente di definire diversi livelli operativi e garantisce che ciascuna Azienda/Ente, Area Organizzativa, Agenzia, Ufficio, Dipartimento, ecc. possa accedere solo ed esclusivamente ai propri documenti, in base alle credenziali e alle politiche di accesso attivate.

Torna al sommario

7.8 Produzione di duplicati e copie informatiche e descrizione dell'eventuale intervento di un pubblico ufficiale

Con la richiesta da parte dell'utente di esibizione dei Pacchetti di distribuzione mediante supporto ottico, viene generata una copia autentica del documento, conforme all'originale. Per i dettagli sulla modalità di richiesta di esibizione dei Pacchetti di distribuzione, fare riferimento al capitolo 6 "Oggetti sottoposti a conservazione" paragrafo 6.5 e al capitolo 7 "Il processo di erogazione del servizio di conservazione", fase 6.

Nei casi in cui, come previsto dall'art. 23-bis, c. 2 del Codice dell'Amministrazione Digitale[8] il Soggetto produttore richieda la presenza di un pubblico ufficiale, Unimatica-RGI garantirà tale presenza mettendo a disposizione tutte le necessarie risorse che serviranno all'espletamento delle attività, rimandando in ogni caso la scelta al Soggetto produttore al quale saranno addebitate le spese.

Inoltre, in caso di adeguamento del formato dovuto all'evoluzione tecnologica verranno rispettate tutte le procedure elencate nell'Allegato 'Infrastrutture' al presente Manuale. Anche in questo caso, l'eventuale presenza del pubblico ufficiale per l'attestazione di conformità, sarà garantita in seguito alla richiesta del Soggetto produttore a cui vengono attribuiti i costi di gestione.

Torna al sommario

[8] "Le copie e gli estratti informatici del documento informatico, se prodotti in conformità alle vigenti regole tecniche di cui all'articolo 71, hanno la stessa efficacia probatoria dell'originale da cui sono tratte se la loro conformità all'originale, in tutti le sue componenti, è attestata da un pubblico ufficiale a ciò autorizzato o se la conformità non è espressamente disconosciuta. Resta fermo, ove previsto, l'obbligo di conservazione dell'originale informatico."

7.9 Scarto dei Pacchetti di archiviazione

Sette mesi prima della scadenza del periodo di conservazione dei documenti stabilito dal contratto, Unimatica-RGI comunica al Soggetto produttore, in modalità certa, che in assenza di ulteriori comunicazioni, trascorsi i termini previsti, provvederà alla cancellazione dei documenti.
In caso di proroga della conservazione, Unimatica-RGI rinnova la marca temporale sui documenti per il periodo richiesto (uno o più anni).

Le attività di scarto dei Pacchetti di archiviazione vengono svolte sulla base di accordi tra il Responsabile del servizio di conservazione di Unimatica-RGI e il soggetto produttore. Il responsabile del servizio è tenuto a generare l'elenco dei pacchetti di archiviazione contenenti i documenti destinati allo scarto e ad inviarlo al soggetto produttore che a sua volta, verificato il rispetto dei termini temporali stabiliti dal piano di conservazione, lo comunica al responsabile della gestione documentale o al coordinatore della gestione documentale.

In caso degli archivi pubblici o privati dichiarati di interesse storico particolarmente importante l'autorizzazione finale è rilasciata ai sensi della normativa vigente in materia di beni culturali[9].

Il Titolare dell'oggetto di conservazione, una volta effettuate le verifiche e/o ricevuta l'autorizzazione da eventuali parti coinvolte, che può essere concessa anche solo su una parte dell'elenco proposto, provvede a trasmetterlo al conservatore affinché provveda alla distruzione dei pacchetti di archiviazione.

Unimatica-RGI provvede a tracciare tutte le operazioni mediante la produzione di informazioni essenziali sullo scarto, inclusi gli estremi della richiesta di nulla osta allo scarto e il conseguente provvedimento autorizzatorio.

I documenti e le aggregazioni documentali informatiche scartate da Unistorage vengono distrutti anche su tutti i sistemi di backup.

Al termine delle operazioni di distruzione dal sistema di conservazione dei pacchetti di archiviazione scartati, Unimatica-RGI provvede a comunicare in via ufficiale il termine delle operazioni al Titolare dell'oggetto che provvederà a sua volta a notificarlo a chi di competenza

Torna al sommario

7.10 Predisposizione di misure per l'interoperabilità e la trasferibilità ad altri conservatori

Unimatica-RGI, come descritto al par. 6.4 Struttura dati del Pacchetto di archiviazione, genera i PDA applicando le specifiche tecniche dalla norma UNI 11386 - Standard SInCRO - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali. Accoglie, inoltre, formati conformi all'Allegato 2 delle Linee guida o concordati a seguito di opportuna valutazione di interoperabilità, pertanto Unistorage supporta sia l'acquisizione di PDD provenienti da altri conservatori, sia il riversamento verso altro sistema di conservazione.

[9] L'intervento della Soprintendenza archivistica è previsto anche nel caso di archivi privati per i quali è stato dichiarato l'interesse culturale, secondo quanto disposto dall'art. 21, comma 1, lettera d del Codice dei beni culturali (D. Lgs. 22 gennaio 2004, n. 42).

Torna al sommario

7.11 Chiusura del contratto

Il Soggetto produttore, in qualsivoglia momento, ha il diritto di rescindere dal contratto. La procedura prevede la compilazione di un apposito modulo, debitamente firmato e timbrato, da inviare ad Unimatica-RGI utilizzando una delle modalità di seguito indicate:

1. Invio dell'originale cartaceo con firma autografa tramite posta all'indirizzo:
   Unimatica-RGI S.p.A.
   Via Cristoforo Colombo, 21
   40131 Bologna

2. Invio dell'originale firmato digitalmente dal rappresentante legale, all'indirizzo di posta elettronica certificata (PEC): fatturaelettronica@pec.unimaticaspa.it

Il soggetto produttore che intende disdire il servizio di conservazione a norma dei documenti informatici affidato alla società Unimatica-RGI può scegliere di:

- mantenere la conservazione a norma dei documenti informatici già versati in conservazione fino al termine precedentemente concordato mantenendo la possibilità di utilizzare le credenziali di accesso al sistema per i soli scopi di consultazione

- non mantenere la conservazione a norma dei documenti informatici già versati in conservazione e di procedere allo scarto degli stessi e quindi disattivare le credenziali di accesso al sistema per i soli scopi di consultazione. L'Utente pertanto, dalla data della disdetta esonera la società Unimatica-RGI da ogni adempimento e responsabilità in merito alla custodia e conservazione dei documenti informatici versati in conservazione ed interessati dal servizio.

  I documenti informatici che sono stati oggetto di conservazione a norma possono essere restituiti, a richiesta, all'utente su supporto ottico nel formato standard previsto dalla normativa in vigore (SInCRO – standard UNI 11386 – Supporto all'Interoperabilità nella Conservazione e nel recupero degli Oggetti digitali).

Torna al sommario

8. Procedure di gestione e di evoluzione

A coordinare la gestione del sistema, l'aggiornamento di questo e le procedure di adeguamento all'evoluzione tecnologica è la figura del Responsabile sviluppo e manutenzione che esegue una costante attività di controllo dell'attività di conservazione in conformità agli standard di qualità e sicurezza ISO 9001 e ISO 27001.
Affinché venga garantito un controllo totale sul sistema e un buon funzionamento di questo, le attività di manutenzione vengono svolte sia sui processi che sulle strutture hardware e software e viene condotta una quotidiana verifica delle attività sulle infrastrutture parallelamente ad una pianificazione delle eventuali procedure straordinarie da condurre in caso di anomalie.

Torna al sommario

8.1. Misure di sicurezza logica

Il presente paragrafo ha l'obiettivo di descrivere le misure di sicurezza adottate per l'erogazione del Servizio e per la protezione dei dati che fanno riferimento al Piano per la sicurezza del sistema di conservazione di Unimatica-RGI In particolare, verranno descritte, a titolo esemplificativo ma non esaustivo, le misure di sicurezza tecniche e organizzative adeguate adottate da Unimatica-RGI per garantire un livello di sicurezza adeguato al rischio ai sensi dell'art. 32 del GDPR:

- la gestione utenze,
- la gestione sistemi di protezione,
- la gestione degli incidenti di sicurezza,
- la gestione dei backup,
- la gestione dei supporti di memorizzazione.

Torna al sommario

8.1.1 Gestione utenze

La policy di riferimento per la gestione delle utenze applicative e di sistema adottata da Unimatica-RGI prevede che le utenze siano rilasciate da un ente (o persona) differente dall'ente o persona che le utilizzerà.
Nell'ambito del servizio di conservazione, le utenze applicative e di sistema sono gestite secondo criteri idonei a garantire il rispetto dell'applicazione di misure di sicurezza tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio ai sensi dell'art. 32 del GDPR. Si riportano di seguito alcune delle misure di sicurezza adottate:

- Utilizzo di password complesse definite secondo i seguenti criteri:
  - la password non deve essere visibile in fase di inserimento nelle sessioni di login e sia criptata all'interno del Data Base;
  - la password:
    - deve avere una lunghezza compresa fra 8 e 25 caratteri,
    - deve contenere almeno un carattere speciale, un carattere maiuscolo, un carattere minuscolo ed un numero
    - non può contenere il nome dell'utente,
    - non può contenere il cognome dell'utente,

  - non può contenere l'username dell'utente,
  - non può essere una delle ultime 4 utilizzate;

- la scadenza della password è configurabile attraverso un parametro;
- il sistema deve forzare l'utente a cambiare la password al primo utilizzo;
- il sistema deve avvertire l'utente della necessità di rinnovare la password;

- Applicazione del principio 'segregation of duty' nel rilascio delle credenziali (utente, password e profilo), vale a dire separazione tra chi rilascia e chi utilizza le credenziali di accesso ai dati;
- Applicazione del principio 'need to know' nel rilascio dei profili, vale a dire rilascio dei soli diritti per eseguire le attività di competenza;
- Assegnazione ad ogni utente di credenziali (user e password) personali, uniche e non assegnabili ad altri utenti;
- Revisione periodica degli utenti e dei relativi profili.

Torna al sommario

8.1.2 Gestione sistemi di protezione

Net Security
La realizzazione logica della rete è fatta secondo i seguenti criteri:

- controllo degli accessi e dei flussi realizzato tramite firewall in cross-mode (doppio Cisco Pix-535) ed utilizzo di software IP Tables per il port e IP filtering;
- filtro sui flussi di traffico da/per Internet costituito da sistemi McAfee Sidewinder ridondati, che effettuano deep packet inspection e forniscono funzionalità di firewall applicativo (livello 7 OSI);
- segregazione della rete e suddivisione della medesima in differenti porzioni dedicate alla rete di Back End dati per i server contenenti i data base, alla rete di Front End per la parte di presentazione, alla rete di gestione per l'amministrazione (funzione di supporto tecnico) della piattaforma;

Gli accessi alla rete sono segregati a livello di porte ed indirizzi IP. Gli accessi agli apparati di rete sono sottoposti a misure rigide di controllo e sono consentiti solamente agli amministratori della medesima.

IDS e IPS
Allo scopo di evitare che eventuali malintenzionati possano forzare le protezioni presenti per accedere in maniera illecita a dati riservati, la barriera di firewall applicativi fornisce anche un costante monitoraggio contro accessi non autorizzati tramite funzionalità IPS (Intrusion Prevention System).

Torna al sommario

8.1.3 Gestione degli incidenti di sicurezza

Si definisce incident uno stato, in un sistema, un servizio od una rete, che implichi il mancato funzionamento, il possibile mancato rispetto di uno SLA o il mancato funzionamento di contromisure.

Se l'incident coinvolge le proprietà di sicurezza dell'informazione (RID), si configura come incident di sicurezza.

La segnalazione di anomalie può scaturire

- dalle attività di monitoraggio
- da specifica segnalazione da parte di un utente o di personale interno

In entrambi i casi, qualora la segnalazione implichi un problema di sicurezza inficiando quindi l'integrità, riservatezza o disponibilità del dato, la prassi per la gestione degli incident può prevedere l'apertura di un ticket sulla specifica coda OTRS (strumento elettronico di ticketing Open-source Ticket Request System) del servizio di conservazione oppure dell'area sistemi.

Una volta preso in carico il ticket dal Responsabile del settore Conservazione o da un operatore designato egli diventa Incident Owner, cui sono delegate le azioni di: Contenimento[10], Eliminazione delle cause[11], Ripristino[12].

La gestione degli incidenti di sicurezza è regolamentata da specifiche procedure dettagliatamente descritte secondo requisiti conformi allo standard ISO 27001:2013. Maggiori dettagli sono descritti nel capitolo 3 del Piano della Sicurezza.

Torna al sommario

8.1.4 Gestione dei backup e Disaster Recovery

8.1.4.1 Siti Settimo e Firenze

L'architettura del sistema backup è composta da un master server per ogni sito e da differenti media server che hanno il compito di archiviare i dati ed inserirli in una rete dedicata, parallela a quella di erogazione dei singoli servizi, per non impattare sulle prestazioni e sulla disponibilità di questi ultimi, durante la normale esecuzione delle attività di backup.
I singoli agent installati sull'infrastruttura di virtualizzazione e sui server non virtualizzati comunicano con il backup server che esegue il salvataggio dei dati su un appliance Data Domain. Il salvataggio dei dati su un appliance Data Domain viene replicato sul sito secondario. Questo sistema consente:

- Semplicità di integrazione anche con future evoluzioni del software di backup
- De-duplicazione del dato ad alta velocità

[10] **Contenimento**: processo che rappresenta la fase di esecuzione delle attività di contrasto, atte a mitigare le compromissioni della sicurezza derivanti da un incidente. Una delle attività principali del processo di contenimento è quella di determinare il patrimonio informativo che viene messo a rischio a seguito di un incidente.
[11] **Eliminazione delle cause**: processo che elenca le azioni indirizzate alla rimozione delle cause che scatenano un incidente informatico. E' opportuno sottolineare l'importanza che rappresenta la comprensione del problema che è all'origine dell'incidente; a tale scopo appare determinante descrivere con il maggior dettaglio possibile il modo con cui l'evento di sicurezza si è verificato.
[12] **Ripristino**: processo tramite il quale viene attuato il ritorno alle normali condizioni di operatività aziendale e di chiusura formale dell'incidente. Un obiettivo determinante che emerge dalla corretta applicazione delle misure qui contemplate, è garantire che per i dati e per i sistemi/applicazioni siano ristabilite le funzionalità e performance in essere prima dell'incidente.

- Replica efficiente in rete
- Scalabilità dell'infrastruttura

L'architettura di backup utilizza le seguenti tecnologie:

- Data Domain DD4200
- Data Domain DD4100
- Data Domain DD2500
- Software di backup NetBackup di Symantec
- Software di backup vRanger di DELL
- Software di backup con modulo di cifratura dei dati
- Rete di backup con throughput a 10 Gbit/s
- Replica dei dati di backup tramite link a 400 Mbit/s fra sito primario e secondario

La funzionalità di backup sulla base dati è implementata utilizzando Oracle RMAN o BARMAN, con cadenza giornaliera e settimanale a seconda delle necessità.

Torna al sommario

8.1.4.2 Siti di Bologna e Acilia (Roma)

L'architettura di backup si basa sul software open-source bacula, costituito da un modulo director che sovrintende le operazioni di backup, su due unità dischi SATA (una con dischi fissi e una con dischi rimuovibili) collegate a server di backup su cui gira il modulo storage di bacula, e su una serie di moduli client (agenti) di bacula disposti sulle macchine contenenti i dati di cui effettuare il backup.

Le categorie di dati oggetto del backup sono:

- Directory di sistema dei sistemi Unimatica-RGI
- DB Postgres[nella modalità export DB]

Nell'ambito del backup dei dati appartenti alla categoria Directory di sistema, è eseguito anche il backup delle cartelle di rete utilizzate dal personale Unimatica-RGI.
Il backup avviene in due modalità:

- diretto: i dati vengono backuppati direttamente sul server che li contiene tramite un agente bacula
- indiretto: i dati vengono backuppati su NAS da uno script di backup che gira sul server da backuppare, e dal NAS vengono poi prelevati da un agente bacula che li inserisce nel flusso dei backup diretti

Le modalità di backup sono riassumibili in estrema sintesi nei seguenti punti:

- i dati di backup sono conservati per 7 giorni su Dischi, i backup full eseguiti ogni fine settimana sono conservati per 1 mese su dischi;
- vengono eseguiti backup mensili su dischi rimuovibili, in singola copia, conservati in cassaforte ignifuga, con retention di un anno;
- l'ultimo backup mensile su disco di ogni anno viene conservato con ritenzione infinita;
- backup su disco di dati con esigenze di retention specifiche (superiori all'anno), sono eseguiti in doppia copia, in base a specifiche degli "owner" dei dati;
- il salvataggio dei documenti su CD-ROM con consegna al Soggetto produttore, può essere eseguito su richiesta;

- il salvataggio dell'applicazione sia server che client è realizzato su supporto fisico esterno (Data tape o CD-ROM) per eseguire una rapida reinstallazione in caso di necessità;
- i supporti di backup hanno rotazione con frequenza settimanale.

Per le attività di salvataggio si eseguono i seguenti controlli:

- monitoraggio e controllo dei log-files dei risultati dei salvataggi (con frequenza quotidiana);
- ripristino periodico a campione dei dati;
- controllo della validità e della funzionalità (leggibilità) dei supporti.

Torna al sommario

8.1.4.3 Disaster Recovery

I servizi di conservazione di Unimatica-RGI sono erogati tramite due Data Center Primari due Data Center Secondari che svolgono il compito di Backup Remoto e di Disaster Recovery (D/R), al fine di garantire gli opportuni livelli di continuità del servizio.
I Data Center hanno una distanza fra loro superiore 200 e 300 Km e la disponibilità di servizio è H24 per tutti e 4.
I Data Center secondari permettono di usufruire dei servizi in Produzione anche in caso di indisponibilità dei Data Center Primari.
Per questo servizio Unimatica-RGI definisce con il Cliente il livello dei parametri che caratterizzano il servizio di D/R e di continuità operativa.

- Recovery Point Objective (RPO)
  Rappresenta il massimo tempo che intercorre tra la produzione di un dato sui siti primari e la sua messa in sicurezza (ad esempio attraverso backup) e, conseguentemente, fornisce la misura della massima quantità di dati che il sistema può perdere a causa di disastro e che devono essere successivamente ripresi.
- Recovery Time Objective (RTO)
  È il tempo necessario per il pieno recupero dell'operatività di un sistema e del relativo processo organizzativo.

Torna al sommario

8.1.5 Gestione dei supporti di memorizzazione

La gestione dei supporti di memorizzazione, ove richiesti, segue i seguenti criteri:

- i media di memorizzazione elettronica sono correttamente etichettati in modo da fornire le seguenti informazioni: tipologia del media, tecnica della scrittura, data delle scrittura, contenuto. Per tecnica della scrittura si intende il formato in cui il media è stato preparato, nel nostro caso formato ISO, dipendentemente dal tipo supporto (CD o DVD);
- in caso di media che vengano riutilizzati per altri dati, essi vengono preventivamente riformattati tramite le tecniche di formattazione a basso livello, allo scopo di evitare che le informazioni ed i dati in essi contenuti possano essere presi e divulgati a soggetti non autorizzati;
- nel caso in cui i dati registrati sui media non più utilizzati non possano essere definitivamente cancellati si procede alla distruzione del media stesso, impedendone quindi il riutilizzo;

- i media sui quali sono eseguiti i salvataggi aziendali sono conservati in una sede differente rispetto a quella dove sono le strumentazioni cui i salvataggi si riferiscono ed in un luogo non accessibile se non al personale autorizzato,
- periodicamente è eseguita una verifica dei media e della disponibilità degli strumenti di accesso ai medesimi. In caso che per qualche media sia verificata la non disponibilità (anche prevista nel breve futuro) degli strumenti di accesso, si procede allo svecchiamento dei media tramite riversamento del loro contenuto in altro media.

Torna al sommario

8.2. Procedure di evoluzione e Change management

I cambiamenti che vengono apportati al sistema di conservazione di Unimatica-RGI risultano essere il prodotto di un'adeguata corrispondenza alle procedure di evoluzione tecnologica sia sulle strutture hardware sia su quelle software. Il Responsabile della funzione archivistica e il Responsabile dei sistemi informativi definiscono politiche, priorità e tempistiche affinché vengano garantite nel tempo integrità, disponibilità e sicurezza.

In caso di disservizi causati da problematiche riscontrate durante il processo di aggiornamento, è possibile effettuare il ripristino delle versioni precedenti così da assicurare il corretto e continuo svolgimento delle attività.

Il Responsabile del servizio di conservazione e il Responsabile della sicurezza dei sistemi informativi periodicamente si occuperanno di aggiornare la normativa e gli standard di riferimento in base all'evoluzione di questi.
La descrizione delle procedure di evoluzione e gestione dei cambiamenti è riportata nel paragrafo 3.2.2 del documento "Piano della sicurezza del sistema di conservazione".

Torna al sommario

8.3. Cessazione del Servizio di conservazione

Il servizio di Conservazione digitale a norma è, dal 2005, uno dei principali asset di Unimatica-RGI e gli obiettivi della Direzione per gli anni futuri sono di continuare ad evolvere il sistema ed il servizio di conservazione per mantenerlo adeguato alla tecnologia ed alla normativa e di espandere sempre più nel mercato target, non solo italiano, la penetrazione dell'azienda.
A fronte dei suddetti obiettivi, è stata comunque stabilita una procedura per definire le modalità secondo le quali dovrà essere gestito l'evento, ad oggi non prevedibile, di cessazione del servizio di Conservazione da parte di Unimatica-RGI
La gestione della cessazione del Servizio di Conservazione, in fase iniziale, è in carico alla Direzione la quale stabilisce un tempo di almeno 10 mesi prima della data di attuazione prevista.

Dal momento della comunicazione, la Direzione, supportata in questo dal Responsabile del servizio di conservazione, provvede a far sì che non vengano stipulati nuovi contratti, in vista della cessazione del servizio.

Alla ricezione della comunicazione suddetta il Responsabile del servizio di conservazione coinvolge i Responsabili delle diverse aree inerenti la Conservazione (Sicurezza, Servizio, Archivistica,

Sviluppo) con i quali deve collaborare strettamente per la gestione della cessazione e la relativa pianificazione delle attività.
La procedura e le attività che verranno eventualmente eseguite sono descritte nel dettaglio all'interno del documento PRO_CONS - Piano di Cessazione, qualora venga richiesto, tale procedura viene resa disponibile fornendola al soggetto produttore interessato.

Torna al sommario

9. Monitoraggio e controlli

L'attività di monitoraggio e controllo viene portata avanti dal Responsabile della sicurezza dei sistemi e dal Responsabile della funzione archivistica, in accordo con il Responsabile del sistema di conservazione. Tale attività è finalizzata alla rilevazione di eventi di sicurezza, identificabili come stati che indicano il mancato rispetto delle politiche di sicurezza, che possano costituire una possibile fonte di rischio per il sistema di conservazione. Nello specifico gli obiettivi delle attività di monitoraggio sono la valutazione del livello del rischio associato agli eventi di sicurezza e la gestione di tali eventi, mediante strumenti come i Report dei controlli, agendo per il contenimento e/o eliminazione delle cause.

Gli eventi di sicurezza sono monitorati tramite il sistema di Log che consente la registrazione degli accessi e degli eventi (operazioni). Il sistema di Log è organizzato per registrare eventi ai vari livelli di astrazione della piattaforma:

- log del sistema operativo (incluso file system) atto ad identificare ingressi, anomalie ed errori;
- log del Data Base atti ad identificare ingressi, anomalie ed errori;
- log dei sistemi di rete (firewall e router) atti ad identificare ingressi, anomalie ed errori;
- log delle applicazioni software utilizzate (realizzati con vista a livello di singolo utente) atti ad identificare ingressi, principali attività svolte dagli utenti, sequenze del processo, accessi ai dati.

I log file degli applicativi contengono almeno le seguenti informazioni:

- utente che ha eseguito l'operazione;
- data e ora dell'operazione;
- operazione eseguita.

I file di log non sono modificabili o eliminabili da parte degli Utenti che usano il sistema (che non dispongono dei diritti di accesso).
I log di sistema sono analizzati da parte dei sistemisti qualora si rendesse necessaria un'indagine a seguito di un malfunzionamento del sistema.
La dettagliata descrizione dei processi relativi alle attività di monitoraggio e controlli è riportata nel documento "Piano della sicurezza del sistema di conservazione", capitolo 3 e nella PRO_CONS - Procedure di conservazione.
I log vengono successivamente inviati in conservazione per mantenere traccia delle comunicazioni tra Soggetto produttore e sistema di conservazione.

Torna al sommario

9.1 Audit interni e Verifica dell'integrità degli archivi

Le verifiche ispettive interne vengono pianificate dal Responsabile del sistema di gestione per la sicurezza delle informazioni e dal Responsabile della qualità in accordo con il Responsabile sviluppo e manutenzione del sistema di conservazione, dal Responsabile sicurezza dei sistemi per la conservazione e dal Responsabile del servizio di conservazione tenendo conto dello stato e dell'importanza dei processi e delle aree oggetto di verifica, nonché dei risultati delle precedenti verifiche. La frequenza con la quale vengono disposte le verifiche ispettive interne è almeno annuale. Unimatica-RGI si rende disponibile qualora un soggetto produttore volesse richiedere audit di terza parte.

La scelta del personale verificatore viene fatta in modo da garantire obiettività ed imparzialità nel processo di verifica.
Unimatica-RGI prevede in allegato al Manuale "Elenco delle modifiche apportate al Manuale della conservazione e dei documenti obsoleti" tenente traccia delle seguenti informazioni:

- registro delle modifiche al Manuale del sistema di conservazione
- registro dei documenti distrutti

Torna al sommario

9.2 Reportistica di servizio

Il sistema di conservazione UniStorage gestisce un sistema di tracciatura nel quale vengono registrati tutti i singoli eventi che riguardano sia la gestione dei Pacchetti, dalla fase di versamento a quella di distribuzione, sia i singoli documenti. Questa tracciatura, costruita per implementare un "forensic log", è in un formato rigido e non disabilitabile. La tracciatura è prerequisito indispensabile per l'esecuzione delle operazioni.
Nel dettaglio, il sistema di log prevede la registrazione di informazioni relative alle diverse funzioni del processo di conservazione per tutte le fasi descritte nel capitolo 7 "Il processo di erogazione del servizio di conservazione".

La reportistica di servizio che Unimatica-RGI gestisce è di due Tipologie:

1. Reportistica relativa al processo di Conservazione,
2. Reportistica del servizio di Supporto Utente (Service Desk e AM Settore conservazione e Settore sistemi).

Tipologia 1:
vengono prodotti periodicamente i seguenti report:

- Report Consuntivo Pacchetti di archiviazione,
- Report Excel che fornisce la lista dei Pacchetti di archiviazione e che comprende questo set Minimo di informazioni:
    1. Ragione Sociale Cliente;
    2. Numero documenti conservati e spazio occupato nel periodo totali e per tipologia di documento;
    3. Numero documenti conservati e spazio occupato totali e per tipologia di documento.

Tipologia 2:
viene prodotto un report di Servizio che fornirà le seguenti evidenze:

- Numero Incident Segnalati
- Media Tempo di presa in carico Incident
- Media Tempo di chiusura Incident
- Numero Service Request
- Media Tempo di presa in Carico Service Request

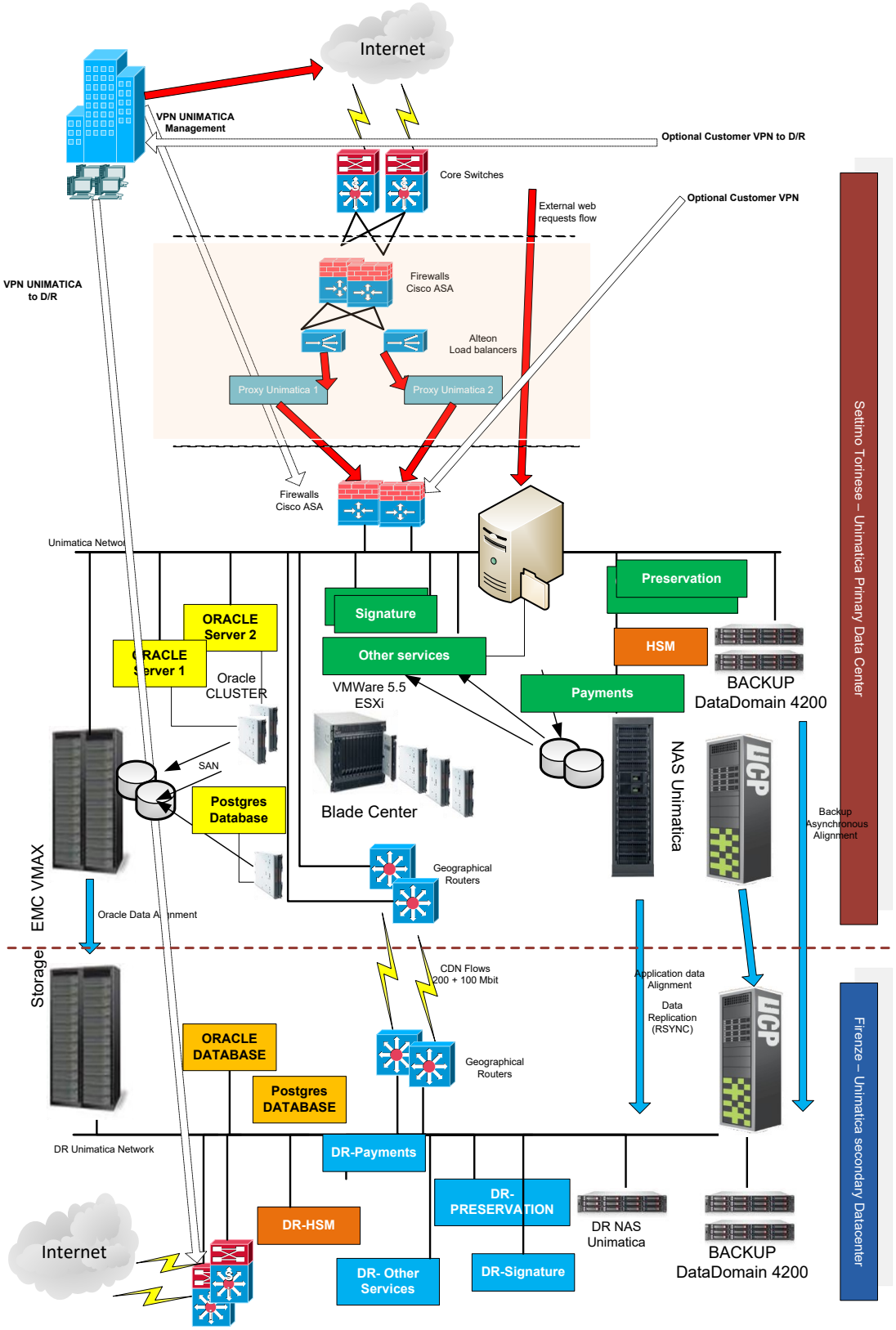
- Media Tempo di Chiusura Service Request

Torna al sommario

10. La server farm di Unimatica-RGI

Dal punto di vista infrastrutturale, i data center dai quali Unimatica-RGI eroga i propri servizi consentono di offrire un servizio di alta qualità in termini di continuità e affidabilità. Tale qualità deriva dalle caratteristiche progettuali che hanno contraddistinto la realizzazione dei Data Center, con criteri focalizzati sempre sull'obiettivo di fornire le massime garanzie di sicurezza, disponibilità e continuità, sia per quanto riguarda l'erogazione di energia elettrica, sia attraverso un opportuno condizionamento climatico, sia attraverso un adeguato meccanismo di sicurezza fisica (impianto antincendio e sorveglianza con allarmi 24x7), sia attraverso la ridondanza architetturale dei sistemi, delle infrastrutture di rete e delle connessioni verso l'esterno.

Lo schema seguente rappresenta l'implementazione hardware/software dell'architettura di conservazione presso i siti di Settimo Torinese e Bologna (siti primari), Firenze, e Acilia (Roma) (siti secondari) nei quali sono allocati i data center:


Internet
VPN UNIMATICA Management
Optional Customer VPN to D/R
Core Switches
External web requests flow
Optional Customer VPN
VPN UNIMATICA to D/R
Firewalls Cisco ASA
Alteon Load balancers
Proxy Unimatica 1
Proxy Unimatica 2
Firewalls Cisco ASA
Unimatica Networ
Settimo Torinese – Unimatica Primary Data Center
Preservation
Signature
HSM
ORACLE Server 2
ORACLE Server 1
Other services
Oracle CLUSTER
VMWare 5.5 ESXi
Payments
BACKUP DataDomain 4200
SAN
Postgres Database
Blade Center
NAS Unimatica
UCP
Backup Asynchronous Alignment
EMC VMAX
Geographical Routers
Oracle Data Alignment
Storage
CDN Flows 200 + 100 Mbit
Application data Alignment
Data Replication (RSYNC)
ORACLE DATABASE
Postgres DATABASE
Geographical Routers
DR Unimatica Network
DR-Payments
DR-PRESERVATION
DR-HSM
DR NAS Unimatica
BACKUP DataDomain 4200
Internet
DR- Other Services
DR-Signature
Firenze – Unimatica secondary Datacenter

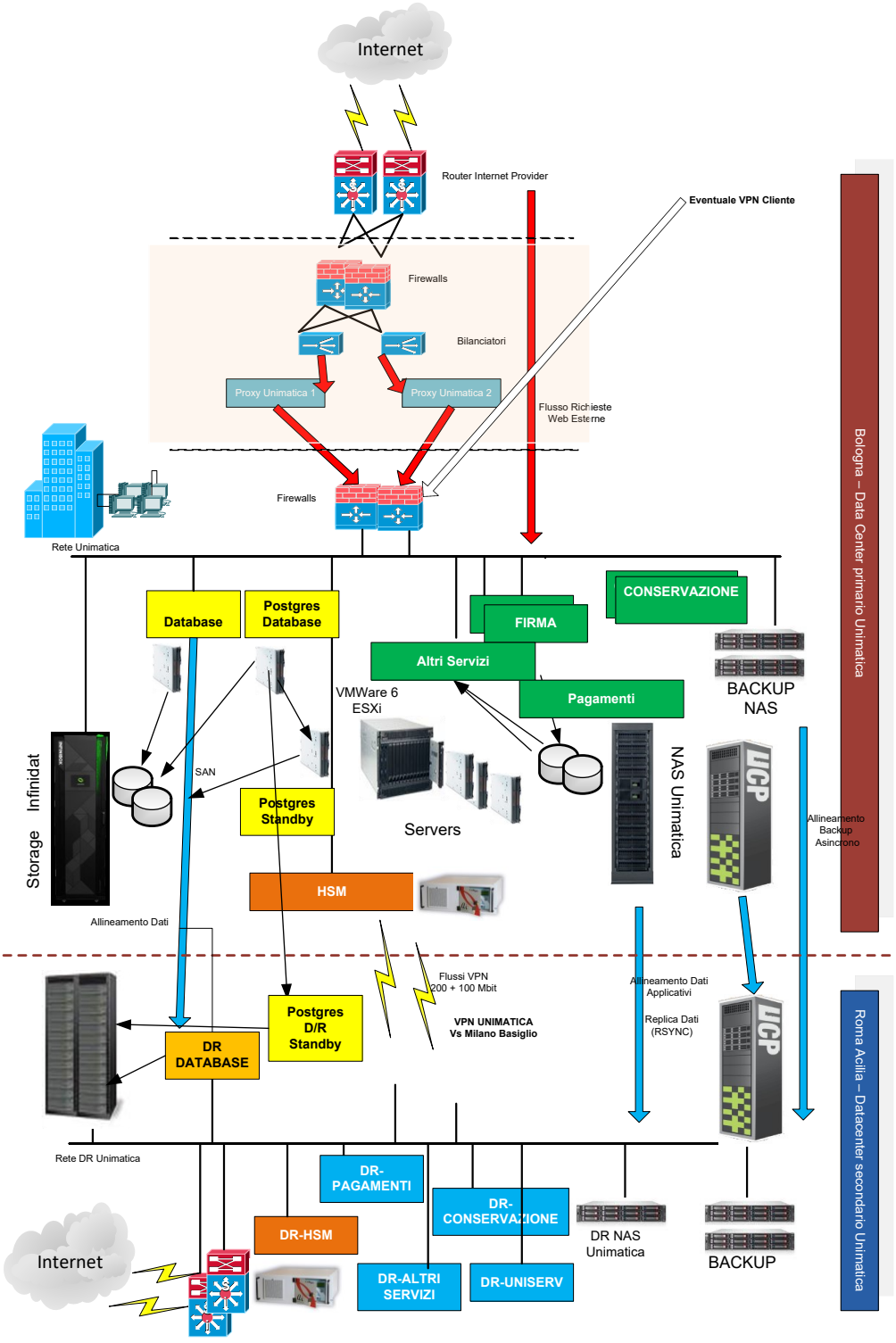


Figura 3 - Architettura di conservazione

Torna al sommario

10.1 UniStorage - Il sistema per la conservazione

Il sistema software utilizzato per la gestione del processo di conservazione dei documenti informatici è costituito dal prodotto applicativo UniStorage.
UniStorage, sviluppato internamente e totalmente da Unimatica-RGI, è un sistema integrato e completo per la conservazione dei documenti informatici che viene fornito in modalità Outsourcing/ASP/SaaS congiuntamente a tutti i servizi di gestione e supporto correlati, oppure in modalità pacchetto applicativo, installando le applicazioni presso il Data Center del Soggetto produttore.
I servizi offerti, oltre che di tipo applicativo e tecnologico, comprendono tutto il necessario supporto normativo, organizzativo e contrattuale (deleghe, privacy, ecc.).

UniStorage esegue la conservazione nel tempo dei documenti sottoscritti con firma digitale e le seguente caratteristiche generali:

- completezza - presenza di qualsiasi documento emesso
- robustezza - garanzia di consistenza dei dati inseriti
- sicurezza - protezione dalla manipolazione non autorizzata dei dati
- affidabilità - indipendenza dai guasti dell'hardware
- chiarezza - facilità di consultazione secondo diversi criteri di ricerca

garantendo:

- la completezza e l'inalterabilità delle registrazioni dei Pacchetti documenti inviati in conservazione
- la possibilità di verifica dell'integrità delle registrazioni
- i riferimenti temporali certi.

Il sistema è progettato per partizionare in maniera opportuna i dati gestiti al fine di garantire la separazione per contesto organizzativo e la consistenza dei dati. Il partizionamento opera tra i dati di Aziende diverse o di diversi dipartimenti o uffici afferenti ad una stessa Azienda (Aree Organizzative Omogenee). I Pacchetti versati provenienti anche da flussi diversi di conservazione, vengono mantenuti separati tramite una chiave primaria che li identifica, fin dal loro ingresso in conservazione, come appartenenti ad una data AOO e non ad un'altra. Il sistema di partizionamento è direttamente collegato al sistema di controllo degli accessi e tracciatura, viene quindi garantita la riservatezza dei dati presenti in archivio.
UniStorage è una applicazione Web a tre livelli (desktop, application e database) e utilizzabile da posti di lavoro dotati di sistema operativo Windows o Linux, per mezzo dei principali browser di riferimento sul mercato. Per le postazioni che dovranno operare sulle funzionalità di firma è necessario che localmente siano attivi i driver del dispositivo di firma (lettore, smart card o token USB di firma, tablet per la firma grafometrica, ecc.), oppure che sia utilizzato un dispositivo HSM (Hardware Security Module) raggiungibile via rete.

Il servizio in outsourcing ASP del servizio di conservazione dei documenti informatici prodotti ed inviati dal Soggetto produttore prevede lo svolgimento da parte di Unimatica-RGI, dietro apposita nomina e delega da parte del Soggetto produttore, delle funzioni e responsabilità di conservazione dei documenti.

La descrizione dettagliata delle componenti logiche, tecnologiche e fisiche è riportata nel documento “Infrastruttura” allegato al Manuale del sistema di conservazione.

Torna al sommario

Appendice A

Allegati al Manuale del sistema di conservazione:

- Allegato ‘Infrastrutture’.
- PRO_CONS - Piano di Cessazione

Specificità del contratto e documenti di riferimento:

- Scheda Cliente.
- Flusso per la conservazione dei Documenti in Unistorage
- Specifiche del servizio web per la consegna anticipata di documenti nel Sistema di conservazione.
- ‘Funzionalita_portale'.
- Elenco delle modifiche apportate al Manuale della conservazione e dei documenti obsoleti.

Torna al sommario