Approvato con delibera di Giunta n. 78 del 23/12/2024

MANUALE DI GESTIONE DOCUMENTALE DELL'UNIONE DEI COMUNI VALLI E DELIZIE

SOMMARIO

ALLEGATI

1. Organigramma con indicazione delle UU.OO.
2. Manuale del software di gestione documentale
3. Applicativi in uso presso l’ente Unione
4. Elementi essenziali del documento amministrativo informatico
5. Formato dei documenti degli uffici
6. Guida alla formazione del documento accessibile
7. Manuali d’uso del Sistema di protocollo informatico
8. Piano di classificazione (Titolario)
9. Modello registro di protocollo di emergenza
10. Linee Guida alla fascicolazione
11. Convenzione per lo svolgimento della funzione di conservazione
12. Piano di conservazione - Massimario di scarto
13. Manuale di conservazione (ParER)

PARTE PRIMA – DISPOSIZIONI PRELIMINARI

1. Riferimenti normativi

Il presente Manuale di gestione documentale (d'ora in avanti anche solo "Manuale") è adottato ai sensi delle *Linee guida sulla formazione, gestione e conservazione dei documenti informatici* (d'ora in avanti anche solo "Linee guida"), emanate dall'Agenzia per l'Italia Digitale con determinazione del Direttore generale del 9 settembre 2020, n. 407 e pubblicate il 10 settembre 2020, come modificate dalla recente determinazione del 17 maggio 2021 n. 371.

Gli allegati alle Linee guida sono parte integrante delle stesse e contengono disposizioni relative a:

1) Glossario dei termini e degli acronimi;
2) Formati di file e riversamento;
3) Certificazione di processo;
4) Standard e specifiche tecniche;
5) Metadati;
6) Comunicazione tra AOO di Documenti Amministrativi Protocollati, che sostituisce la circolare 60/2013 dell'AgID.

Ulteriori norme rilevanti ai fini della gestione documentale sono:

- le disposizioni in materia di formazione dei documenti informatici, anche di natura amministrativa, e di digitalizzazione dell'attività amministrativa di cui al d.lgs. 7 marzo 2005, n. 82 "*Codice dell'Amministrazione Digitale*" (di seguito anche solo "CAD")
- le disposizioni in materia di documentazione amministrativa di cui al d.P.R. 28 dicembre 2000, n. 445 *"Disposizioni legislative in materia di documentazione amministrativa"* (di seguito anche solo "TUDA");
- le norme sul procedimento amministrativo di cui alla l. 7 agosto 1990, n. 241 "*Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi*";
- le disposizioni sulla trasparenza di cui al d.lgs. 14 marzo 2013, n. 33 "*Riordino della disciplina riguardante gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni"*;
- le disposizioni in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno di cui al Regolamento (UE) 2014/910 del Parlamento europeo e del Consiglio del 24 luglio 2014 (Regolamento "eIDAS");
- le disposizioni sulla tutela della riservatezza dei dati personali di cui al regolamento (UE) 2016/679 del Parlamento europeo e del

Consiglio del 27 aprile 2016 *"Regolamento generale sulla protezione dei dati"* ("GDPR") e d.lgs. 30 giugno 2003 n. 196 "*Codice in materia di protezione dei dati personali*".

2. Finalità, contenuti e metodologia del documento

Il presente Manuale, ai sensi del paragrafo 3.5. delle Linee guida, descrive il sistema di gestione informatica dei documenti dell'Unione dei Comuni Valli e Delizie e fornisce le istruzioni per la formazione dei documenti informatici, per il corretto funzionamento del servizio per la tenuta del protocollo informatico, per la gestione dei flussi documentali e degli archivi, ivi compresa la conservazione dei documenti informatici. Esso è frutto del lavoro condiviso nell'ambito dei Comuni dell'Unione e dell'Unione stessa.

Il Manuale è un documento interno di contenuto sia organizzativo che operativo, utile quale strumento di supporto ai processi decisionali e operativi e, pertanto, è destinato alla più ampia diffusione presso tutto il personale dell'ente. Sono da considerarsi modifiche sostanziali quelle aventi a oggetto il Piano di classificazione (Titolario) e il Piano di conservazione dei documenti.

Con la pubblicazione nella sezione "Amministrazione Trasparente" del sito internet istituzionale (sottosezione "Atti Generali"), il Manuale è reso noto anche esternamente all'ente. In quest'ottica, il Manuale costituisce altresì un documento pubblico, funzionale al perseguimento del principio di trasparenza dell'azione amministrativa.

3. Approvazione e modalità di aggiornamento del Manuale

Il presente Manuale e i suoi allegati sono approvati con delibera di Giunta dell'Unione, su proposta del Responsabile della gestione documentale dell'ente.

I successivi aggiornamenti del Manuale devono essere sottoposti all'approvazione della Giunta dell'Unione. L'aggiornamento degli allegati, quando non comporta modifiche sostanziali ai contenuti del presente Manuale, è effettuato con determinazione del Responsabile della gestione documentale.

Il Manuale e gli allegati sono pubblicati sul sito istituzionale dell'Unione, nella sezione "Amministrazione Trasparente", sottosezione "Atti generali".

PARTE SECONDA – ORGANIZZAZIONE

4. Area organizzativa omogenea e Unità Organizzative

L'Unione dei Comuni Valli e Delizie si configura come un'unica Area Organizzativa Omogenea (AOO), denominata "aooprotuvd" (codice univoco AOO: A7D29D1), data dall'insieme di tutte le Unità Organizzative (UUOO) di cui si compone l'ente (Settori). L'AOO e gli indirizzi di posta elettronica a essa associati sono indicati nell'Indice PA.

Le UUOO che afferiscono alla AOO sono riportate nell'allegato 1, che potrà essere oggetto di modifiche e integrazioni per effetto di successivi interventi sulla struttura organizzativa dell'Unione da approvarsi nell'ambito del Piano Integrato di Attività e Organizzazione (PIAO). Le UUOO sono individuate in modo da rispecchiare l'organigramma dell'ente.

5. Responsabile della gestione documentale e altri soggetti responsabili

L'Unione dei Comuni Valli e Delizie, nell'ottica di gestire in modo integrato tutte le fasi del ciclo di vita dei documenti informatici, ha individuato un'unica figura dirigenziale, il "Responsabile della gestione documentale", dotata di competenze giuridiche, informatiche ed archivistiche, a cui affidare le funzioni e i compiti del Responsabile per la gestione documentale e del Responsabile della conservazione di cui rispettivamente ai parr. 3.4 e 4.5 delle Linee guida.

Il Responsabile della gestione documentale dell'Unione dei Comuni Valli e Delizie coincide con il Dirigente del Settore Risorse Umane ed Affari Generali, competente per materia. Il Dirigente, con proprio atto, può individuare apposito Responsabile della gestione documentale dell'Unione tra i funzionari dell'ente dotati di idonei requisiti professionali.

Il Responsabile della gestione documentale (d'ora in avanti anche solo "Responsabile"):

a) è preposto, ai sensi dell'art. 61 TUDA, al servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi della AOO unica dell'Unione;

b) provvede, d'intesa con il Responsabile per la Transizione Digitale (RTD), acquisito il parere del Responsabile per la Protezione dei Dati personali (RPD), alla predisposizione e al costante aggiornamento del presente Manuale e dei relativi allegati;

c) monitora i processi e le attività che governano le fasi di formazione, gestione e versamento in conservazione dei documenti informatici;

d) valuta e formula proposte di riprogettazione e reingegnerizzazione dei processi di cui alla lettera precedente;

e) vigila sul rispetto delle norme e delle procedure durante le operazioni di registrazione di protocollo, di segnatura di protocollo, di produzione e conservazione del registro giornaliero di protocollo;

f) assicura l'accesso al sistema di gestione documentale, provvedendo alla definizione delle abilitazioni di accesso, e vigila sul rispetto delle misure di sicurezza e di protezione dei dati avvalendosi del personale preposto;

g) effettua un periodico censimento degli strumenti software di gestione documentale in uso presso l'Unione e, di concerto con il RTD, ne verifica la conformità alla normativa vigente.

Ulteriori e specifici compiti del Responsabile sono indicati nelle sezioni pertinenti del presente Manuale. Il Responsabile può, sotto la propria responsabilità, delegare/assegnare in tutto o in parte i propri compiti al personale posto sotto la propria direzione, nonché al personale del SIA per quanto di competenza.

6. Sistema informatico di gestione documentale dell'Unione

Il Sistema informatico di gestione documentale dell'Unione si avvale dei seguenti principali strumenti software:

- *Folium*, che è il sistema di protocollo informatico dell'Unione;

- *Civiliaweb*, che è il sistema che consente la gestione dell'*iter* di formazione degli atti degli organi dell'Unione e del personale amministrativo; consente, inoltre, la gestione degli obblighi di pubblicazione nell'Albo pretorio online e nella sezione Amministrazione trasparente del sito istituzionale dell'Unione.

Tutti gli strumenti software sopra indicati sono resi accessibili al personale dell'Unione tramite il servizio di infrastruttura cloud (IaaS) fornito dalla Lepida ScpA, società in house della Regione Emilia-Romagna qualificata come CSP (Cloud Service Provider) dall'Agenzia per l'Italia Digitale.

La puntuale descrizione delle componenti e delle funzionalità del software relativo alla gestione di documenti ed atti è contenuta nel relativo manuale operativo, oggetto di costante aggiornamento, reperibile on-line all'interno dell'applicativo e riportato nella versione attuale all'allegato 2.

Il sistema informatico si avvale altresì di ulteriori strumenti software riportati nell'allegato 3, oggetto di revisione periodica da parte del SIA, nel quale vengono elencati gli applicativi in uso dall'Ente con la relativa descrizione, il nominativo dell'amministratore di sistema e la collocazione del servizio stesso.

7. Abilitazioni di accesso

Solo i soggetti che siano stati nominati amministratori di sistema, su indicazione del Responsabile e in funzione dei loro compiti, sono dotati di abilitazioni di accesso a livello sistemistico (sistemi operativi, gestione e manutenzione DB,

sistemi di controllo e apparati di rete). Le facoltà di concedere abilitazioni applicative ai sistemi di gestione documentale e al sistema di protocollo informatico dell'Unione sono assegnate ai dirigenti, che possono individuare e comunicare al responsabile del protocollo il personale addetto.

8. Utenti preposti alle attività di protocollazione

Tutto il personale che esercita funzioni amministrative è munito di un profilo utente che consente l'accesso al Sistema di protocollo informatico con funzioni di consultazione e di protocollazione dei documenti in uscita e interni afferenti all'ufficio di appartenenza.

Al personale del Servizio Protocollo e Archivio dell'Ente e al personale di altri servizi debitamente nominati, è assegnato il ruolo di "protocollatore", che consente:

- la protocollazione (anche riservata), la classificazione, l'assegnazione e riassegnazione (per competenza o per conoscenza) dei documenti in entrata;
- la creazione e la modifica dei fascicoli informatici, da effettuarsi secondo i criteri definiti nel presente Manuale;
- la modificazione delle informazioni memorizzate in rubrica/anagrafica;
- l'annullamento parziale della protocollazione nei casi ammessi di seguito.

Al Responsabile del Protocollo è assegnato il ruolo di "responsabile AOO", che consente inoltre:

- la modifica o la cancellazione delle registrazioni di protocollo;
- l'autorizzazione alla visualizzazione di registrazioni riservate;
- l'apertura e la chiusura dei registri;
- la modifica del titolario;
- la creazione di report tramite l'estrazione delle informazioni memorizzate dal Sistema;
- la gestione delle tipologie documentali di uso più frequente, con indicazioni predeterminate sulla classificazione e la conservazione;
- il versamento in conservazione dei documenti dei registi presenti sul gestionale;
- ogni altra funzione relativa all'amministrazione dell'AOO.

Ogni profilo utente è protetto da un sistema di credenziali (username e password), secondo le indicazioni previste nella Parte sesta del presente Manuale.

PARTE TERZA – FORMAZIONE DEI DOCUMENTI

Sezione prima – Modalità di formazione

9. Modalità di formazione dei documenti informatici

Tutti i documenti dell'Unione dei Comuni Valli e Delizie sono formati in originale digitale come documenti informatici accessibili, secondo le modalità individuate nella presente Parte del Manuale.

I documenti informatici dell'Unione dei Comuni Valli e Delizie sono formati mediante una delle seguenti modalità:

a) redazione:
   - mediante l'utilizzo delle funzioni dei sistemi di gestione documentale;
   - tramite l'utilizzo di servizi cloud qualificati come i programmi di redazione e condivisione inclusi in G-Suite di Google;
   - mediante strumenti software di produttività personale quali *Microsoft Office* e *Libreoffice;*
b) acquisizione:
   - solo nel caso in cui non sia disponibile un originale digitale, è consentita la copia per immagine di un documento analogico su supporto informatico (ad esempio, mediante scansione di documento cartaceo, integrando con dichiarazione di conformità della copia digitale);
   - della copia informatica di un documento analogico (ad esempio, acquisizione del documento tramite lettore OCR);
   - del duplicato di un documento informatico per via telematica o da supporto informatico (ad esempio, mediante download da posta elettronica o da chiave usb);
c) memorizzazione su supporto informatico delle informazioni risultanti da transazioni o processi informatici, oppure delle informazioni risultanti dall'acquisizione telematica di dati attraverso moduli o formulari (ad esempio, memorizzazione dei dati immessi in un *form* reso disponibile online agli utenti);
d) generazione o raggruppamento anche in via automatica di un insieme di dati o registrazioni secondo una struttura logica predeterminata (ad esempio, generazione del registro di protocollo giornaliero e flussi OpenData).

Di seguito sono fornite indicazioni specifiche per ciascuna delle modalità sopra descritte.

9.1. Creazione e redazione tramite software di documenti informatici

Gli uffici dell'Unione dispongono di almeno uno dei seguenti strumenti software per la creazione dei documenti informatici mediante redazione:

- programmi della suite *Libreoffice*: *Writer, Calc, ecc.*;
- programmi della suite *Microsoft Office: Word, Excel, ecc.;*
- programmi della suite *Google Workspace* accessibili in cloud e utili per il lavoro in team: *Docs, Fogli, ecc.;*

Il testo del documento informatico creato dagli uffici dell'Unione deve essere redatto utilizzando esclusivamente font a sorgente aperto ed accessibile Verdana.

Gli operatori, al fine di verificare il rispetto delle indicazioni sulla redazione dei documenti, sono tenuti a consultare le bozze e i fac-simile predisposti e diffusi a cura del Responsabile.

9.2. Elementi essenziali del documento amministrativo informatico

Ogni documento amministrativo informatico creato e redatto dall'Ente deve essere conforme allo schema di cui all'allegato 4 e contenere i seguenti elementi essenziali:

1. denominazione dell'Amministrazione;
2. autore e ufficio responsabile;
3. oggetto del documento;
4. sottoscrizione;
5. data e luogo;
6. indicazione degli allegati (se presenti);
7. identificazione e dati dei destinatari (se si tratta di documento in uscita);
8. dati dell'Amministrazione (compresi indirizzo e recapiti, se si tratta di documento in uscita);
9. mezzo di spedizione (se documento in uscita).

9.3. Scelta del formato e modalità di sottoscrizione

Il formato del documento informatico creato dall'Unione deve essere scelto tra quelli indicati nell'allegato 5 al presente Manuale e secondo i criteri ivi stabiliti. Eventuali formati differenti possono essere utilizzati in relazione a specifiche e comprovate esigenze. Il formato del documento informatico in ogni caso deve essere individuato tra quelli previsti nell'Allegato 2 alle Linee guida AgID.

I documenti interni o precedenti alla versione definitiva (bozze, minute, ecc.), devono essere salvate in un formato che ne consenta, anche in futuro, la corretta e libera visualizzazione e modificabilità. Per la compressione sono consigliati .7Z e .ZIP (.RAR è deprecato). Si fa notare che in un archivio

compresso, firmato digitalmente, i documenti contenuti non godono della stessa validità legale pertanto sono considerati riversamenti (si veda paragrafo 9.6). Per testi e tabelle, il formato OASIS/OpenDocument (.ODT .ODS) è dichiarato conforme da Agid.

Il formato Microsoft OOXML (.DOCX .XLSX) è dichiarato adatto all'utilizzo a lungo termine solo se:

• il documento è salvato con profilo strict;

• sono utilizzati esclusivamente caratteri tipografici standard e aperti;

• è privo di contenuti dinamici ad eccezione di campi compilabili o campi-firma;

• è privo di contenuti audiovisivi (suoni, video);

• eventuali immagini o altri contenuti multimediali sono contenute direttamente nel documento e non mediante collegamenti a file esterni al documento.

I formati Microsoft .DOC e .XLS (tecnicamente CFB) sono soggetti a problemi di degradazione strutturale poiché di concezione obsoleta pertanto sono deprecati.

Nonostante l'obbligo per le PP.AA. di accettare e aprire documenti nei deprecati .doc .xls .rtf, si raccomanda di non formarne altri esemplari e di valutare il riversamento nei formati sopra descritti.

I formati .ACCDB .MDB .ODB sono deprecati perché proprietari, obsoleti o estensioni.

Alcuni tipi di file come .exe .com .bat .reg .pif hanno contenuto attivo o eseguibile e non sono ammessi alla protocollazione: tali tipi di file non vanno aperti ma cestinati e contestualmente segnalati al SIA. Quest'ultimo, attraverso propria comunicazione, potrà ampliare l'elenco dei file non protocollabili.

Per ulteriori valutazioni sui formati è opportuno consultare l'Allegato 2 alle *Linee Guida sulla formazione, gestione e conservazione dei documenti informatici* dell'AgID (cfr. in particolare pagg. 25 e 51).

La versione definitiva del documento, salvo rare eccezioni, deve essere in formato PDF/A.

I documenti di rilevanza giuridico-amministrativa (ad esempio, gli atti del Presidente e degli organi collegiali, i contratti, le determine a contenuto provvedimentale, ecc.), prima della firma digitale, devono essere convertiti in formato PDF/A (PDF autonomo, adatto alla conservazione). I documenti in formato PDF e PDF/A sono sottoscritti con firma PADES solo eccezionalmente CADES.

Nella situazione in cui il documento definitivo assuma un formato diverso dal PDF, ad esempio nel caso di elaborati grafici vettoriali, la sottoscrizione avviene con firma CADES (P7M) o con la firma di documento principale contenente il nome del file e il relativo hash, questo soprattutto nel caso ci siano molti file da firmare o siano di grandi dimensioni.

9.4. Acquisizione di documenti informatici

La formazione di documenti informatici per acquisizione può avvenire secondo una delle seguenti modalità:

a) acquisizione di un documento informatico per via telematica o da supporto informatico (ciò avviene, ad esempio, quando si effettua il download di un documento dalla casella di posta elettronica, oppure, quando si trasferisce un documento da un dispositivo di archiviazione esterno);

b) acquisizione della copia per immagine su supporto informatico di un documento analogico di tutte le pagine e dei suoi allegati esclusi i casi in cui il formato non lo consente (ciò avviene, ad esempio, quando si effettua la scansione di un documento cartaceo, memorizzandolo in un formato digitale);

c) acquisizione della copia informatica di un documento analogico, ciò avviene, ad esempio, quando un documento di testo analogico viene riversato in formato digitale tramite OCR (riconoscimento ottico dei caratteri).

In caso di acquisizione di copia di documento analogico o informatico, al fine di assicurare l'efficacia giuridico-probatoria, occorre attestare la conformità all'originale con le modalità indicate nelle disposizioni successive. In assenza di attestazione di conformità, la copia acquisita è utilizzata esclusivamente come "copia per uso lavoro" e andrà sempre conservato l'originale del documento.

In caso di acquisizione di un duplicato informatico, ai sensi dell'art. 23-*bis* del CAD, esso ha la stessa efficacia giuridico-probatoria del documento informatico originale, pertanto non è richiesta l'attestazione di conformità.

9.5. Copie per immagine di documenti analogici

La copia per immagine su supporto informatico di documento analogico è prodotta mediante strumenti che assicurano che il documento informatico abbia aspetto esteriore confrontabile con quello del documento analogico da cui è tratto.

Nel caso in cui si debba garantire la medesima efficacia giuridico-probatoria riconosciuta al documento analogico originale, il funzionario all'uopo delegato e che agisce in veste di pubblico ufficiale, attesta la conformità all'originale, archivia il documento analogico e appone sulla copia informatica la propria firma digitale o altra tipologia di firma forte, previa iscrizione sul documento o in foglio elettronico a esso congiunto mediante impronta hash di dicitura del seguente tenore:

"*Io sottoscritto/a* [nome e cognome – nome ente e ufficio], *ai sensi dell'art. 22, comma 2, d.lgs. n. 82/2005, attesto che la presente copia per immagine è*

conforme in ogni sua parte al documento originale analogico dal quale è stata estratta. [indicazione di data e luogo]*.*"

Nel caso sia necessario attestare la conformità all'originale di più documenti, acquisiti per copia di immagine, il funzionario delegato, effettuato il raffronto, potrà sottoscrivere digitalmente un'unica attestazione di conformità, su foglio separato e collegato alle copie, contenente la raccolta delle impronte hash associate a ciascun documento scansionato.

L'attestazione di conformità della copia per immagine al documento originale analogico è richiesta nei casi in cui è necessario o, comunque, si vuole assicurare l'efficacia giuridico probatoria del documento. Così deve avvenire, ad esempio:

- quando si deve provvedere a notificazione via PEC di documento (o allegato a documento) acquisito in originale analogico;
- quando si deve formare un contratto tra l'ente e un privato che sottoscrive con firma autografa. In questi casi andrà attestata la conformità all'originale della scansione del documento firmato in originale cartaceo dal privato, andrà poi apposta l'attestazione di conformità sottoscritta digitalmente da chi effettua l'attestazione e, infine, andrà effettuata la sottoscrizione (sempre con firma digitale), da parte del soggetto competente alla stipula. Nel caso questi ultimi due soggetti coincidano, sarà sufficiente apporre un'unica firma digitale.

9.6. Duplicati, copie mediante riversamento, concatenazione di documenti informatici

Il duplicato informatico ha lo stesso valore giuridico del documento informatico da cui è tratto se è ottenuto mediante la memorizzazione della medesima evidenza informatica, come avviene, ad esempio, quando si duplica un documento trasferendolo dall'hard disk del proprio personal computer a un dispositivo di archiviazione esterno quale una chiave usb. Tale modalità di formazione della copia del documento informatico non richiede alcuna attestazione di conformità all'originale, perché vi è perfetta coincidenza tra le due evidenze informatiche, tale identità è rilevabile tramite raffronto delle hash.

Il riversamento di un documento informatico è un documento con diversa evidenza informatica ma il cui contenuto è il medesimo dell'originale, ad esempio, quando si trasforma un .docx in .pdf, i due documenti avranno hash differenti. Spesso l'hash cambia anche solo se il documento viene aperto con un programma di videoscrittura e salvato nel medesimo formato.

L'estrazione di parti o la concatenazione di diversi documenti informatici è considerata un riversamento.

Affinché un riversamento conservi la medesima efficacia giuridico-probatoria del documento informatico originale, è necessario attestarne la conformità all'originale.

Come per le copie per immagine, dunque, il funzionario, che agisce in veste di pubblico ufficiale, dovrà apporre la propria firma digitale (o altra tipologia di firma forte), previa iscrizione sul documento (a margine o in calce) o in foglio elettronico a esso congiunto di dichiarazione del seguente tenore:

"*Io sottoscritto/a* [nome e cognome – nome ente e ufficio]*, ai sensi dell'art. 23-bis, comma 2, d.lgs. n. 82/2005, attesto che la presente copia informatica è conforme in ogni sua parte al documento originale informatico dal quale è stata estratta.* [indicazione di data e luogo]."

9.7. Acquisizione di istanze tramite moduli online

Le istanze provenienti dagli utenti possono essere formate anche tramite la compilazione di moduli e *form* messi a disposizione sul sito web dell'Unione e resi accessibili previa identificazione dell'utente con gli strumenti di identificazione forte SPID e CIE. I dati immessi dall'istante sono acquisiti e memorizzati su supporto informatico. Le istanze così formate sono acquisite dal Sistema di protocollo informatico dell'Unione, costituiscono a tutti gli effetti documenti amministrativi informatici validamente sottoscritti dall'utente e sono trattati come documenti in entrata soggetti a registrazione di protocollo. Il file di log relativi agli accessi e alle attività svolte dagli utenti sono conservati secondo le stesse modalità di conservazione delle istanze ricevute tramite PEC. Sono previsti inoltre le cooperazioni applicative.

9.8. Formazione di registri, repertori e open data

I registri e repertori e open data tenuti dall'Ente, ivi compreso il registro giornaliero di protocollo, sono formati mediante la generazione/raggruppamento e memorizzazione e conservati in via automatica, in forma statica o pubblicati se richiesto dalle disposizioni di legge.

Sezione seconda – Disposizioni comuni a tutte le modalità di formazione

10. Firma elettronica

L'Unione garantisce che tutti i dipendenti e i titolari di cariche che firmano documenti siano dotati di dispositivi di firma elettronica. A tal fine, l'Unione è dotata di sistemi di gestione documentale che consentono ai dipendenti in possesso di profilo utente l'apposizione della firma digitale.

L'utilizzo del dispositivo di firma è strettamente personale e riconducibile al suo titolare. Pertanto, il dispositivo non deve essere ceduto, né devono essere diffuse le chiavi dei certificati e i PIN.

Ogni titolare di dispositivo di firma verifica periodicamente la validità e la data di scadenza del certificato di firma, al fine di provvedere tempestivamente al rinnovo.

Quando la firma è apposta utilizzando un certificato prossimo alla scadenza, il titolare ne dà avviso al Responsabile, affinché provveda a costituire un riferimento temporale giuridicamente valido tale da attestare che la firma sia stata apposta in un momento in cui il certificato era valido. In particolare, costituiscono riferimento temporale giuridicamente valido le seguenti attività sul documento firmato:

- apposizione di marca temporale;
- apposizione della segnatura di protocollo;
- versamento in conservazione.

Documenti, dati e altre informazioni trasmesse in cooperazione applicativa non richiedono la sottoscrizione digitale o l'apposizione della marca temporale.

11. Identificazione univoca del documento informatico

Ogni documento informatico di rilevanza per l'Ente deve essere identificato in modo univoco e persistente.

L'identificazione univoca dei documenti è effettuata con l'associazione al documento dell'impronta crittografica *hash*. Per i documenti soggetti a registrazione di protocollo, l'associazione è effettuata tramite le apposite funzioni del Sistema di protocollo informatico. L'impronta crittografica deve essere basata su una funzione di hash conforme alle tipologie di algoritmi previste nell'Allegato 6 alle Linee guida (cfr. p. 2.2, tab. 1).

Il calcolo e la verifica dell'impronta *hash* deve essere effettuato attraverso l'utilizzo di appositi strumenti informatici messi a disposizione dal SIA.

12. Associazione degli allegati al documento principale

Gli allegati sono congiunti in modo univoco al documento informatico principale tramite l'associazione delle impronte hash effettuata dai sistemi di gestione documentale.

Le operazioni di associazione degli allegati, quando possibile, sono effettuate in modo automatizzato dallo strumento software utilizzato per la formazione del documento principale.

In alternativa, è possibile associare gli allegati al documento principale manualmente, riportando in calce al documento stesso l'elenco degli allegati, indicando per ciascuno il nome del file e la relativa impronta *hash*. L'associazione sarà assicurata una volta che il documento informatico principale sia divenuto immodificabile (ad esempio, dopo l'apposizione della firma digitale – cfr. par. 15 del presente Manuale).

Al documento principale, in ogni caso, devono essere associati i seguenti metadati:

- numero allegati;
- indice allegati:
- identificativo del documento allegato (IdDoc):
- titolo dell'allegato (Descrizione).

13. Accessibilità del documento informatico

Tutti i documenti informatici sono creati in formato accessibile al fine di garantirne l'accessibilità a soggetti portatori di disabilità ed anche ai fini della pubblicazione e della ricerca documentale. I soggetti responsabili della formazione del documento seguono le indicazioni contenute nelle linee guida sull'accessibilità degli strumenti informatici di AGID e, nello specifico, le indicazioni operative riportate nell'**allegato 6** al presente Manuale.

14. Metadati del documento informatico

Al documento informatico e al documento amministrativo informatico devono essere associati i metadati obbligatori previsti dall'Allegato 5 alle Linee guida dell'AgID. Ulteriori metadati facoltativi sono associati secondo le indicazioni riportate nell'**allegato 5 cit.** al presente Manuale.

L'associazione dei metadati al documento è effettuata tramite le apposite funzioni dei software di gestione documentale utilizzati per la formazione degli atti. A tal fine, il Responsabile verifica la conformità degli strumenti software utilizzati e, eventualmente, richiede al fornitore i necessari interventi evolutivi.

15. Immodificabilità e integrità del documento informatico e dei metadati

Affinché sia garantito il valore giuridico-probatorio del documento informatico, ne deve essere assicurata l'immodificabilità e l'integrità.

Il documento informatico è immodificabile se la sua memorizzazione su supporto informatico in formato digitale non può essere alterata nelle fasi di accesso, gestione e conservazione.

L'immodificabilità e l'integrità dei documenti informatici dell'ente sono garantite:

- per i documenti sottoscritti mediante apposizione di una firma elettronica qualificata, di una firma digitale o di un sigillo elettronico qualificato o firma elettronica avanzata;
- per i documenti di cui non è richiesta la sottoscrizione, a partire dal momento in cui sono memorizzati nel sistema di gestione documentale, purché sia garantito il rispetto delle misure di sicurezza previste (cfr. Parte sesta del presente Manuale);

- per tutte le tipologie documentali, a partire dal momento in cui sono versati nel sistema di conservazione.

In ogni caso, il versamento nel sistema di conservazione è il metodo che offre le maggiori garanzie di immodificabilità e integrità, nel tempo, dei documenti informatici. Pertanto, è essenziale che tutti i documenti di rilevanza amministrativa siano versati in conservazione, secondo i tempi e le modalità descritte nella Parte Quinta del presente Manuale.

Il Responsabile assicura, attraverso il versamento giornaliero in conservazione dei dati, che i documenti informatici a cui è apposta una firma elettronica siano versati in conservazione prima che scada il certificato di firma.

Sezione terza - Disposizioni sulla formazione di documenti analogici

16. Copie analogiche di documenti informatici

Fermo restando l'obbligo di formare i documenti in originale informatico, in alcuni casi può essere necessario effettuare delle copie analogiche affinché siano spedite a mezzo posta ai soggetti che non sono muniti di domicilio digitale e agli altri soggetti indicati all'art. 3-*bis*, comma 4-*bis*, CAD.

Quando è necessario che al destinatario giunga un documento avente la medesima efficacia giuridico probatoria del documento originale (ad esempio, quando bisogna assicurare l'efficacia legale della notificazione dell'avviso di accertamento relativo a tributi o a violazioni da cui discendono sanzioni amministrative), ai sensi dell'art. 3, d.lgs. n. 39/1993, la copia analogica dovrà essere accompagnata dall'indicazione della fonte del documento originale e del soggetto responsabile dell'immissione, riproduzione, trasmissione o emanazione del documento stesso. Quando il documento originale informatico è sottoscritto con firma digitale o altra firma elettronica qualificata, la firma è sostituita dall'indicazione a stampa del nominativo del soggetto responsabile e dell'UO di appartenenza (c.d. stampigliatura).

La copia analogica inviata/consegnata al cittadino, inoltre, deve contenere apposita dicitura che specifichi che il documento informatico, da cui la copia è tratta, è stato predisposto come documento nativo digitale ed è rintracciabile presso l'amministrazione. Esemplificando, in aggiunta alla stampigliatura, vi dovrà essere apposta una dicitura del seguente tenore: "Copia conforme ai sensi dell'art.18, comma 2, del D.P.R. N.445/2000, e dell'art.23, comma 1, del D.Lgs. n.82/2005, dell'originale sottoscritto con firma digitale e conservato presso questo Ente, composta da n. … pagine.
Resa in carta libera per uso amministrativo.
Firma del funzionario".

17. Casi in cui è ammessa la formazione di documenti originali analogici

Fermo restando l'obbligo di produrre i propri documenti in originale informatico, è legittimo formare documenti in originale analogico:

- ai sensi dell'art. 2, comma 6, CAD, esclusivamente nell'ambito dell'esercizio di attività e funzioni di ordine e sicurezza pubblica, difesa e sicurezza nazionale, polizia giudiziaria e polizia economico-finanziaria e consultazioni elettorali, nonché alle comunicazioni di emergenza e di allerta in ambito di protezione civile;

- in tutti i casi in cui il documento è consegnato a sportello e il richiedente è un soggetto privato che non agisce in qualità di professionista (ad esempio, la tessera elettorale, la carta d'identità, ecc.).

PARTE QUARTA - GESTIONE DOCUMENTALE

Sezione prima - Flussi documentali esterni

18. Ricezione telematica di documenti informatici in entrata

I documenti informatici in entrata, pervenuti tramite i canali di ricezione previsti, sono oggetto di registrazione di protocollo secondo quanto previsto nella Sezione seconda della presente Parte del Manuale. Una volta che ne sia accertata la provenienza, i documenti sono validi ai fini del procedimento amministrativo.

Le istanze, le dichiarazioni e le comunicazioni trasmesse per via telematica, in ogni caso, devono ritenersi valide a tutti gli effetti di legge quando:

a) sono contenute in documenti sottoscritti con firma digitale o firma elettronica qualificata;

b) sono trasmesse a mezzo posta elettronica certificata da un indirizzo PEC iscritto in uno degli elenchi di domicili digitali previsti dalla normativa vigente;

c) sono trasmesse attraverso un sistema informatico che consente la previa identificazione dell'utente con i sistemi SPID, CIE o CNS;

d) sono trasmesse da un domicilio digitale;

e) sono ricevute come copie digitali di documenti originali cartacei sottoscritti e presentati unitamente a copia del documento d'identità dell'autore;

f) è comunque possibile accertarne la provenienza secondo la normativa vigente o, comunque, in base a criteri di attendibilità e riconducibilità al mittente dichiarato.

Per indicazioni sulla gestione dei documenti relativi a istanze, dichiarazioni e comunicazioni degli utenti, pervenuti ai Comuni ma di competenza dell'Unione, si vedano le indicazioni di cui al par. 23.1 del presente Manuale (*Ricezione di documenti e istanze dei cittadini indirizzate ai Comuni ma di competenza dell'Unione*).

19. Canali di ricezione

La ricezione di comunicazioni e documenti informatici è assicurata tramite i seguenti canali:

- casella PEC: protocollo@pec.unionevalliedelizie.fe.it;
- *form* resi disponibili tramite sito web;
- in via residuale, altro canale di ricezione quale la posta elettronica ordinaria istituzionale; in tal caso, se necessario, i documenti ricevuti verranno poi riversati nel protocollo.

L’indirizzo di posta elettronica certificata è abilitato alla ricezione dei documenti provenienti da indirizzi di posta elettronica ordinaria.

L’indirizzo di posta elettronica certificata è riportato nell'Indice delle Pubbliche Amministrazioni e pubblicizzato sul sito web istituzionale.

Nel caso in cui un soggetto tenuto a effettuare comunicazioni esclusivamente in via telematica (imprese, professionisti, altre PP.AA., salvi i casi di cui all’art. 2, comma 6, CAD) faccia pervenire agli uffici dell’Unione comunicazioni e documenti in modalità analogica, questi non saranno ritenuti validamente trasmessi. In tali casi, la circostanza è segnalata in nota alla registrazione di protocollo. Il responsabile dell’UO assegnataria della comunicazione, o comunque il soggetto individuato quale responsabile del procedimento, ai sensi dell’art. 6 L. n. 241/1990, provvede a comunicare al mittente il motivo della mancata accettazione dei documenti e a indicare modalità di trasmissione valide. La comunicazione, quando possibile, è trasmessa al domicilio digitale del mittente estratto dagli indici di cui agli articoli 6-*bis* e 6-*ter* del CAD.

20. Formati accettati

Sono accettati, e conseguentemente registrati al protocollo, documenti informatici esclusivamente nei formati comuni: .pdf, .pdf/a, .xml, .txt, .jpg .tiff, .rtf, .docx, .odt, .xlsx, .ods, .eml.

Sono accettati, altresì, ulteriori formati eventualmente previsti nell’allegato 5 cit. al presente Manuale. Possono essere accettati, inoltre, i formati contemplati dall’Allegato 2 delle Linee guida dell’AgID. Resta salva la possibilità, da parte del Responsabile del procedimento, di prevedere espresse limitazioni in relazione allo specifico procedimento, purché le limitazioni siano ragionevoli e giustificate da obiettive esigenze.

Il controllo preliminare sulla conformità del formato dei documenti in entrata è effettuato dal personale addetto alla protocollazione prima della registrazione di protocollo. Qualora pervengano documenti in formati non conosciuti o non gestiti la mancata accettazione e protocollazione deve essere comunicata al mittente.

Nel caso in cui si tratti di file considerati pericolosi come indicato al paragrafo 9.3 del presente Manuale, gli stessi vanno cestinati e segnalati al servizio SIA per le opportune verifiche di sicurezza.

Nel caso di formati altamente specializzati, è consigliabile protocollare il documento accompagnato ad una copia informatica in un formato ammesso, ad esempio un disegno tecnico vettoriale .DWG potrebbe essere accompagnato dal PDF con la stessa rappresentazione semplificata.

20.1. Verifica sul formato dei documenti allegati

L’eventuale presenza di allegati al documento principale in formati non ammessi deve essere verificata dal Responsabile del procedimento, il quale provvede a

comunicare al mittente la non conformità del documento e/o l'assenza dei requisiti previsti per l'utilizzo ai fini del procedimento amministrativo.

L'accettazione di formati non previsti dal presente Manuale, dalle Linee Guida o dalla disciplina del singolo procedimento deve essere consentita nel caso in cui, per obiettive esigenze rappresentate dal mittente, il documento non può essere riversato in formato tra quelli ammessi.

21. Controllo dei certificati di firma

Il personale abilitato alla protocollazione effettua una prima verifica sui certificati di firma contestualmente alla registrazione di protocollo del documento in entrata. In caso di certificati scaduti, revocati o sospesi, procede alla registrazione, segnalando in nota il risultato della verifica di firma.

Il Responsabile del procedimento verifica la validità dei certificati di firma e, in caso di certificato scaduto o revocato, valuta le azioni da intraprendere a seconda della tipologia di procedimento.

22. Trasmissione telematica di documenti informatici in uscita

La trasmissione di comunicazioni e documenti avviene sempre per via telematica, salvo il caso trasmissione a soggetti privati, privi di domicilio digitale ai sensi degli artt. 6 e ss. del CAD.

I documenti informatici in uscita vengono classificati, fascicolati e protocollati secondo le disposizioni della presente parte del manuale e contestualmente trasmessi a mezzo posta elettronica certificata.

Nel caso di trasmissione in uscita, se si necessita di dare comunicazione anche ad un ufficio interno, occorre fare sempre un protocollo in uscita alla pec del destinatario e SOLO un'assegnazione all'ufficio interno evitando invii all'indirizzo di posta elettronica del dipendente.

Per la trasmissione di documenti tramite PEC, se il documento principale non ha un contenuto sufficientemente esplicativo (ad esempio, un provvedimento, un certificato, ecc.) deve essere predisposta una nota di accompagnamento alla trasmissione.

La trasmissione di dati e altre informazioni in cooperazione applicativa è soggetta a protocollazione secondo le medesime regole per la registrazione dei documenti.

23. Comunicazioni e trasmissione di documenti con altre Pubbliche Amministrazioni

Ai sensi dell'art. 47 C.A.D., la trasmissione di comunicazioni e documenti verso altre pubbliche amministrazioni avviene per via telematica (preferibilmente

tramite Posta Elettronica Certificata o tramite posta elettronica ordinaria istituzionale dei singoli uffici) oppure tramite cooperazione applicativa.

I documenti che devono essere prodotti entro un determinato termine sono sempre trasmessi a mezzo PEC.

Gli indirizzi di spedizione sono rilevati tramite la consultazione dell'Indice delle Pubbliche Amministrazioni (indicepa.gov.it) di cui all'art. 6-ter del CAD.

23.1. Ricezione di documenti e istanze dei cittadini indirizzate ai Comuni ma di competenza dell'Unione

Al fine di facilitare l'accesso degli utenti ai servizi gestiti dall'Unione, sono accettate le istanze e le comunicazioni relative a servizi di competenza dell'Unione ma che sono formalmente indirizzate ai Comuni. In tal caso il Comune ricevente, previa protocollazione in ingresso del documento (assegnazione titolario 01.06), procede alla trasmissione all'Unione tramite protocollo in uscita specificando nell'oggetto: "*RICEVUTO DAL COMUNE DI … PER SERVIZIO DI COMPETENZA UNIONE*".

Nel caso in cui la competenza sia tanto del Comune quanto dell'Unione, la dicitura da indicare nel protocollo in uscita (previa sempre la protocollazione in ingresso) è la seguente: "*RICEVUTO ED ASSEGNATO NEL COMUNE DI …, SI INOLTRA PER QUANTO DI COMPETENZA UNIONE*" .

Il documento ricevuto in Unione viene protocollato in ingresso sostituendo il mittente con quello originario.

23.2. Ricezione di documenti e istanze di competenza di Enti diversi dall'Unione

In caso di ricezione di comunicazioni evidentemente di competenza di altro Ente, diverso dai Comuni facenti parte l'Unione e dall'Unione stessa, l'operatore di protocollo provvede alla restituzione al mittente, con procedura di inoltro, riportando nel Messaggio E-mail la seguente dicitura: *"Si restituisce l'email pari oggetto, RICEVUTA PER ERRORE e NON PROTOCOLLATA, poiché non di competenza dell'Unione dei Comuni Valli e Delizie. Questo Ente non darà alcun ulteriore corso alla comunicazione ricevuta"* - Firma completa dell'operatore.

23.3. Ricezione di documenti e istanze dei cittadini indirizzate all'Unione ma di competenza di uno dei comuni

In caso di ricezione di comunicazioni evidentemente di competenza di uno dei Comuni facenti parte dell'Unione, l'operatore di protocollo dell'Unione, previa protocollazione in ingresso del documento (assegnazione titolario 01.06), procede alla trasmissione tramite protocollo in uscita al Comune di competenza, specificando nell'oggetto: "*RICEVUTO IN UNIONE PER SERVIZIO DI COMPETENZA DEL COMUNE DI …*".

Nel caso in cui la competenza sia tanto del Comune quanto dell'Unione, la dicitura da indicare nel protocollo in uscita è la seguente: "*RICEVUTO E ASSEGNATO IN UNIONE, SI INOLTRA PER QUANTO DI COMPETENZA DEL COMUNE DI …*" .

Il documento ricevuto in Comune viene protocollato in ingresso sostituendo il mittente con quello originario.

24. Disposizioni sui documenti analogici

I documenti su supporto analogico possono pervenire all'Unione attraverso:

- il servizio postale;

- la consegna diretta agli uffici o ai funzionari addetti alle attività di sportello;

La ricezione di documenti a mezzo fax provenienti da altre pubbliche amministrazioni è esclusa (come previsto dall'art. 47, comma 2, lett. c del CAD). Pertanto, tali comunicazioni non devono essere ritenute valide. Fanno eccezione i soli casi di esclusione dell'applicazione della normativa del CAD previsti dall'art. 2, comma 6, D.lgs. n. 82/2005 (ad es., comunicazioni di protezione civile).

Gli orari definiti per la presentazione della documentazione analogica sono indicati sul sito web istituzionale dell'Unione.

Le buste delle comunicazioni cartacee sono conservate insieme ai documenti in esse contenuti.

Sezione seconda - Protocollo informatico

25. Sistema di protocollo informatico

L'Unione, per la protocollazione dei documenti, utilizza il Sistema di protocollo informatico *Folium* della ditta Dedagroup SpA. La puntuale descrizione funzionale e operativa del Sistema di protocollo informatico è illustrata nei manuali di utilizzo reperibili on-line all'interno dell'applicativo e riportati nella versione attuale all'**allegato 7** al presente Manuale.

26. Responsabile del Servizio Protocollo e Archivio Informatico

La corretta tenuta del protocollo informatico è garantita dal Responsabile della gestione documentale. In particolare, il Responsabile, nella veste di responsabile del Servizio Protocollo e Archivio Informatico:

a. coordina la gestione del sistema di protocollo informatico;
b. assegna al personale addetto alla protocollazione l'abilitazione all'utilizzo delle funzioni di protocollo del Sistema;
c. esercita il controllo generale sui flussi documentali esterni e interni;
d. assicura la corretta esecuzione delle attività di protocollazione;

e. autorizza l’attivazione del protocollo di emergenza;
f. autorizza le operazioni di annullamento o modifica delle registrazioni di protocollo;
g. vigila sull’osservanza della normativa e delle disposizioni del presente Manuale da parte del personale addetto.

Le attività di protocollazione sono eseguite dagli utenti nominati. La modalità di individuazione dei soggetti preposti alle attività di protocollazione è definita al par. 8 del presente Manuale.

27. Registro generale di protocollo

Nell'ambito della AOO il Registro generale di protocollo è unico, al pari della numerazione progressiva delle registrazioni di protocollo.

Il numero di protocollo è costituito da almeno sette cifre numeriche.

La numerazione è progressiva, si chiude al 31 dicembre di ogni anno e ricomincia dall’1 gennaio dell'anno successivo.

Il numero di protocollo è associato in modo univoco e immodificabile al documento, pertanto esso individua un unico documento e, di conseguenza, ogni documento reca un solo numero di protocollo. Non è consentita la protocollazione di un documento già protocollato.

28. Registro giornaliero di protocollo

Il Registro giornaliero di protocollo è costituito dall'elenco delle informazioni inserite con l'operazione di registrazione di protocollo nell'arco di uno stesso giorno. Esso è prodotto automaticamente dal sistema di protocollo informatico, che provvede altresì al versamento automatico al Sistema di conservazione.

29. Documenti soggetti a registrazione di protocollo e documenti esclusi

Tutti i documenti prodotti e ricevuti dall’Ente, indipendentemente dal supporto sul quale sono formati, sono registrati al protocollo, ad eccezione di quelli indicati successivamente.

Ai sensi dell’articolo 53 del TUDA sono esclusi dalla registrazione di protocollo:

- Gazzette Ufficiali, Bollettini Ufficiali, notiziari della Pubblica Amministrazione;
- note di ricezione delle circolari e altre disposizioni;
- materiale statistico;
- atti preparatori interni;
- giornali, riviste, materiale pubblicitario, stampe varie, plichi di libri;
- biglietti augurali, inviti a manifestazioni e documenti di occasione vari che non attivino procedimenti amministrativi;

- bolle accompagnatorie;
- richiesta/invio comunicazioni informali.

Non sono soggetti a protocollazione, inoltre, gli atti e i documenti registrati in repertori e registri differenti dal registro di protocollo ai sensi del par. 39 del presente Manuale.

30. Disposizioni per particolari tipologie di documenti

La protocollazione della documentazione di gara e delle offerte, scaricabili dalle piattaforme e-procurement dei mercati elettronici della Pubblica Amministrazione o della Regione, istituite ai sensi di legge, non è necessaria quando i gestori di tali sistemi assicurano la conservazione a tempo indeterminato della documentazione relativa alle singole gare. In tali casi si ritiene comunque opportuno, anche se non necessario, la protocollazione della richiesta d'offerta o dell'ordine diretto di acquisto e dell'offerta dell'impresa aggiudicataria acquisendo, per questa, tutti i documenti relativi e specificando, negli appositi campi, data e ora di arrivo.

31. Registrazione di protocollo

La registrazione di protocollo è l'insieme dei metadati che il registro di protocollo deve memorizzare in forma non modificabile al fine di garantirne l'identificazione univoca e certa. Ai sensi dell'art. 53, comma 1, TUDA, metadati di registrazione di protocollo sono:

a) numero di protocollo del documento generato automaticamente dal sistema;
b) data di registrazione di protocollo assegnata automaticamente dal sistema;
c) mittente per i documenti ricevuti o, in alternativa, il destinatario o i destinatari per i documenti spediti;
d) oggetto del documento;
e) data e protocollo del documento ricevuto, se disponibili;
f) l'impronta del documento informatico, se trasmesso per via telematica.

A suddetti metadati registrati in forma non modificabile, inoltre, si aggiungono:

g) tipologia di documento;
h) classificazione (titolo e classe) sulla base del Titolario (v. allegato 8);
i) fascicolo di appartenenza;
j) assegnazione in competenza e in copia conoscenza;
k) data e ora di arrivo;
l) allegati;
m) livello di riservatezza;
n) mezzo di ricezione o invio;
o) annotazioni;

p) (eventualmente) estremi del provvedimento di differimento della registrazione;
q) (se necessario) elementi identificativi del procedimento amministrativo.

32. Modalità di registrazione

La registrazione di protocollo di un documento è eseguita dopo averne verificato l'autenticità, la provenienza e l'integrità.

La registrazione dei documenti ricevuti, spediti e interni è effettuata in un'unica operazione, utilizzando le apposite funzioni previste dal Sistema di protocollo informatico. Al documento indirizzato a più destinatari deve essere assegnato un solo e unico numero di protocollo.

Il Sistema genera automaticamente il numero progressivo e la data di protocollazione associata. Alla registrazione di protocollo, inoltre, sono associate le ricevute generate dal sistema di protocollo informatico e, nel caso di registrazione di messaggi PEC in uscita, anche i dati relativi alla consegna rilasciati dal sistema di posta certificata correlati al messaggio oggetto di registrazione. L'eventuale indicazione dell'ufficio utente, ovvero del soggetto destinatario del documento, va riportata nella segnatura di protocollo.

Tutte le comunicazioni tra imprese ed Ente devono avvenire esclusivamente tramite PEC ed essere inoltrate all'indirizzo di posta elettronica certificata istituzionale dell'Unione Valli e Delizie: protocollo@pec.unionevalliedelizie.fe.it.

Solo per casi residuali e straordinari, per la protocollazione della posta elettronica ordinaria, gli utenti non abilitati alla protocollazione in entrata provvedono a scaricare il file .EML contenente il messaggio in entrata ed a inoltrarlo in allegato all'indirizzo di posta ordinaria del Servizio Protocollo e Archivio, inserendo in oggetto la seguente dicitura "SI PREGA DI PROTOCOLLARE".

In tali casi, dunque, l'operatore addetto alla protocollazione in Ingresso provvede alla registrazione del messaggio inoltrato in allegato (e non del messaggio di inoltro), indicando il mittente originario e mezzo di spedizione E-mail.

Al fine di evitare doppie registrazioni dello stesso documento, prima dell'inoltro per la registrazione l'operatore deve verificare che nella comunicazione sia stato indicato anche il recapito PEC. In tali casi, infatti, non serve provvedere all'inoltro per la protocollazione.

33. Annullamento e modifiche della registrazione di protocollo

La registrazione degli elementi obbligatori del protocollo non può essere modificata né integrata, né cancellata, ma soltanto annullata attraverso l'apposita procedura conforme all'art. 54 del TUDA.

Se le informazioni della registrazione di protocollo sono errate (anche in caso di mera svista), dunque, sarà necessario procedere alla richiesta di annullamento.

Come previsto dal par. 3.1.5 delle Linee guida AgID, le uniche informazioni che possono essere modificate – e che, dunque, non richiedono l'annullamento – sono quelle relative a:

- classificazione;

- assegnazione interna.

Pertanto, è opportuno che ogni operatore al momento della protocollazione presti la massima attenzione. Il registro di protocollo, infatti, è un atto pubblico a cui la legge riconosce un particolare valore giuridico-probatorio. Come per ogni atto pubblico, la formazione richiede solennità e, dunque, la massima accortezza e precisione.

Ogni annullamento della registrazione deve:

- essere autorizzato con provvedimento del Responsabile all'interno dell'applicativo o con strumenti simili (e-mail);
- comportare la memorizzazione di data, ora e estremi del provvedimento di annullamento;
- consentire sempre la memorizzazione e la visibilità delle informazioni oggetto di annullamento.

Le richieste di annullamento rivolte al Responsabile devono essere motivate. Le richieste sono accolte, di norma, in casi di mero errore materiale (quali ad es., registrazione di informazioni errate, doppia registrazione, registrazione di documenti non destinati all'Unione).

L'annullamento e le modifiche avvengono secondo la procedura guidata dal Sistema, che consente di mantenere traccia di ogni operazione, così come richiesto alla normativa. In particolare, per annullare o modificare i dati di un documento già protocollato è necessario richiamarlo dal Registro tramite la modalità di ricerca e salvare i nuovi dati o le eventuali modifiche tramite il pulsante "Salva".

34. Gestione degli allegati

Il numero e la descrizione degli allegati sono elementi essenziali per l'efficacia di una registrazione. Tutti gli allegati devono pervenire con il documento principale al fine di essere inseriti nel Sistema di protocollo informatico ed essere sottoposti a registrazione. Gli allegati dei documenti ricevuti tramite il canale PEC sono gestiti in forma automatizzata dal sistema di protocollo informatico.

Non è ammessa l'associazione al documento informatico già registrato di allegati non indicati nella registrazione di protocollo. L'associazione di allegati successivamente alla registrazione non può essere effettuata, dunque in tali casi è necessario procedere ad annullamento ed a nuova registrazione, attraverso la procedura di cui al precedente paragrafo.

Per la trasmissione di allegati di dimensioni superiori a 100 mb, sono previsti appositi canali di trasmissione diversi dalla PEC. Pertanto, la trasmissione e successiva registrazione delle comunicazioni dovrà avvenire tramite tali canali. A tal fine, ogni Responsabile del procedimento deve curare la corretta informazione degli utenti, fornendo tutte le informazioni necessarie sulle modalità di trasmissione ed i relativi canali predisposti dall'ente.

35. Tempi di registrazione e casi di differimento

La registrazione della documentazione in entrata deve avvenire in giornata o comunque non oltre il giorno lavorativo successivo a quello di arrivo. Ai fini della gestione del protocollo non sono in ogni caso considerati lavorativi il sabato e la domenica.

In casi eccezionali ed imprevisti che non permettono di evadere la corrispondenza ricevuta e qualora dalla mancata registrazione di protocollo del documento nella medesima giornata lavorativa di ricezione possa venire meno un diritto di terzi (ad esempio per la registrazione di un consistente numero di domande di partecipazione ad un concorso in scadenza), con motivato provvedimento del Responsabile è autorizzato il differimento dei termini di registrazione (protocollo differito).

Il protocollo differito si applica solo ai documenti in entrata e per tipologie omogenee che il Responsabile deve descrivere nel provvedimento. Il provvedimento individua i documenti da ammettere alla registrazione differita, le cause e il termine entro il quale la registrazione di protocollo deve essere comunque effettuata.

Al momento della registrazione differita devono essere indicati in nota alla registrazione gli estremi del provvedimento di differimento.

In ogni caso, della ricezione del documento informatico da parte dell'Unione, fa fede la ricevuta di consegna generata dal gestore della casella PEC.

36. Segnatura di protocollo

La segnatura di protocollo è l'associazione ai documenti amministrativi informatici in forma permanente e non modificabile di informazioni riguardanti i documenti stessi, in ingresso e in uscita al sistema di protocollo, utile alla sua identificazione univoca e certa, come indicate all'art. 53, comma 1, TUDA.

Le operazioni di segnatura sono effettuate contemporaneamente alla registrazione di protocollo o ad altra registrazione cui il documento è soggetto.

I requisiti necessari di ciascuna segnatura di protocollo sono:

a. indicazione della Amministrazione mittente;
b. codice identificativo dell'AOO mittente;

c. codice identificativo del registro;
d. numero progressivo di protocollo;
e. data di registrazione;
f. oggetto del messaggio di protocollo;
g. classificazione del messaggio di protocollo;
h. indicazione del fascicolo in cui è inserito il messaggio di protocollo.

Per i documenti informatici trasmessi ad altre Pubbliche Amministrazioni, i dati relativi alla segnatura di protocollo sono contenuti, un'unica volta nell'ambito dello stesso messaggio, in un file XML conforme alle indicazioni previste al p. 2 e ss. dell'Allegato 6 alle Linee guida dell'AgID e, in particolare, deve rispettare lo schema di cui all'Appendice A (v. p. 4.1. "Segnatura di protocollo XML Schema").

37. Protocollo riservato

Sono previste particolari forme di riservatezza e di accesso controllato al Sistema di protocollo per:

- documenti contenenti categorie particolari di dati personali ai sensi dell'art. 9 del Regolamento UE 2016/679 che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche o l'appartenenza sindacale, dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona (ad es. documenti che contengono certificati medici con diagnosi o patologie, certificati di invalidità, documenti attestanti l'adesione a partiti politici, documenti contenenti sfratti esecutivi e pignoramenti, ecc.), dati personali relativi a condanne penali e reati o a connesse misure di sicurezza (ad es. documenti provenienti da Case di Reclusione);
- documenti di carattere politico e di indirizzo che, se resi di pubblico dominio, potrebbero ostacolare il raggiungimento degli obiettivi prefissati o procurare pregiudizio a terzi o al buon andamento dell'attività amministrativa (tipologie documentarie definite all'art. 24 della legge n. 241/1990).
- segnalazioni indirizzate al RPCT ai sensi della normativa in materia di whistleblowing.

I documenti registrati con tali forme appartengono al protocollo riservato dell'Unione, costituito dalle registrazioni sul Sistema di protocollo il cui accesso è consentito solamente agli utenti autorizzati.

Le tipologie di documenti da registrare nel protocollo riservato sono codificate all'interno del Sistema di protocollo informatico a cura del Responsabile.

38. Registro di emergenza

L'utilizzo del registro di protocollo emergenza, ai sensi dell'art. 63 del TUDA, è autorizzato dal Responsabile, in situazioni nelle quali per cause tecniche non sia possibile utilizzare il registro generale di protocollo informatico e la sospensione del servizio si protragga per un tempo tale da poter pregiudicare la registrazione a protocollo in giornata. In tali casi, il Responsabile dà immediata comunicazione a tutti gli uffici della temporanea sospensione dell'utilizzo della procedura informatizzata ordinaria di protocollazione e della necessità, per la protocollazione sia in entrata che in uscita, di consegnare la documentazione al Servizio di Protocollo e Archivio.

Il registro di protocollo di emergenza ha una numerazione progressiva propria, perciò ai documenti protocollati su tale registro, una volta riversati, saranno associati due numeri di protocollo, quello del registro di emergenza e quello del registro di protocollo generale. Le registrazioni sul registro di emergenza avvengono, quando possibile, secondo le medesime regole e con le stesse modalità adoperate per le registrazioni sul registro generale di protocollo.

Sul registro di emergenza, inoltre, sono riportati:

- gli estremi del provvedimento di autorizzazione all'utilizzo del registro;
- la causa, la data e l'ora di inizio dell'interruzione;
- il numero totale di registrazioni effettuate nel corso di ogni giornata di utilizzo;
- la data e l'ora del ripristino della funzionalità del sistema
- ogni altra annotazione ritenuta rilevante.

Al ripristino della piena funzionalità del Sistema di protocollo informatico, il Responsabile provvede alla chiusura del registro di emergenza, annotando il numero delle registrazioni effettuate, la data e l'ora di chiusura, e dà disposizioni per il riversamento delle registrazioni sul registro di protocollo generale.

Per le ipotesi di sospensione del servizio dovute a guasti del Sistema di protocollo informatico, l'Unione si è dotata di un supporto informatico alternativo su cui effettuare le registrazioni di emergenza in modalità informatica, che consiste in una postazione munita di un applicativo sui client locale, che permette di riversare le registrazioni nel protocollo generale una volta terminata l'emergenza. Nei casi in cui non sia possibile l'utilizzo del registro di emergenza su supporto informatico, il Responsabile provvede alla formazione del registro di emergenza su supporto analogico, redatto secondo lo schema di cui all'**allegato 9**.

39. Documenti soggetti a registrazione particolare

La registrazione particolare dei documenti richiede lo svolgimento delle medesime operazioni di gestione documentale effettuate per la registrazione di protocollo, ivi incluse la classificazione e la fascicolazione.

Sono soggette a registrazione particolare nei repertori e registri all'uopo istituiti le tipologie di documenti di seguito riportate:

- delibere di Giunta;
- delibere del Consiglio;
- decreti e ordinanze del Presidente;
- determinazioni dirigenziali;
- repertorio atti pubblici;
- permessi invalidi;
- registro scritture private;
- segnalazioni/reclami pervenuti da parte dei cittadini attraverso applicativi dedicati;
- CDU;
- verbali SCIA, SCEA, CILA;
- verbali di accertamento della polizia locale.

I registri e repertori diversi dal protocollo contengono almeno le seguenti informazioni:

- tipologia del registro o repertorio;
- numero di registro o repertorio (cronologico e progressivo);
- data;
- elementi identificativi dell'atto (soggetto o soggetti; oggetto);
- eventuali dati di classificazione e di fascicolazione;
- annotazioni.

Al fine di garantire i medesimi effetti della registrazione di protocollo, i registri e repertori di cui al presente paragrafo sono conservati con modalità analoghe a quelle del registro giornaliero di protocollo informatico.

Il Responsabile, al fine di dare attuazione ai principi di unicità e onnicomprensività del registro di protocollo, valuta periodicamente l'opportunità di sopprimere le forme di registrazione particolare non necessarie per legge, prevedendo in sostituzione esclusivamente la registrazione di protocollo.

39.1 Lettere anonime e documenti non firmati

Le lettere anonime aventi rilevanza dal punto di vista amministrativo per l'attività dell'Ente sono protocollate in modo riservato ed assegnate agli uffici competenti che valuteranno la modalità di trattazione del documento.

Le lettere anonime non rilevanti dal punto di vista amministrativo non sono registrate al protocollo ma consegnate direttamente al Sindaco, il quale valuterà l'opportunità di dare seguito a tali comunicazioni, stabilendo eventualmente procedure da seguire e/o azioni da intraprendere.

Le lettere contenenti ingiurie o diffamazione ai danni di una specifica persona non sono registrate al protocollo ma consegnate al Dirigente responsabile dell'ufficio preposto alla tenuta del Protocollo, che disporrà apposita comunicazione al fine di rendere noti i contenuti delle lettere alla persona interessata.

La valutazione della rilevanza dal punto di vista amministrativo spetta allo stesso Dirigente, eventualmente sentito il Segretario Generale.

Le lettere con mittente, prive di firma, sono regolarmente protocollate. E' compito dell'unità organizzativa di competenza e, in particolare, del responsabile del procedimento, valutare, caso per caso, se il documento privo di firma debba ritenersi valido e come tale trattato dall'ufficio assegnatario.

40. Disposizioni sulla protocollazione di documenti analogici

Il personale addetto a effettuare la registrazione di protocollo informatico in entrata è competente anche per la protocollazione dei documenti analogici in entrata (consegnati a mano o pervenuti tramite servizio postale), prima della registrazione effettuata una copia per immagine su supporto informatico (scansione).

La copia per immagine, se sprovvista di attestazione di conformità, apposta ai sensi della normativa vigente (v. le procedure definite al par. 9.5 del presente Manuale), può essere adoperata solo per uso lavoro.

40.1. Registrazione, segnatura, annullamento

Alla registrazione di protocollo dei documenti cartacei si applicano, in quanto compatibili, le medesime regole previste per la registrazione dei documenti informatici.

Le lettere anonime sono soggette a registrazione di protocollo, eventualmente riservato, indicando nel campo del mittente la dicitura "Anonimo".

Per i documenti analogici la segnatura è apposta con timbro ed etichetta riportante i dati indicati al par. 37, lett. da a) a e).

Sul documento analogico soggetto ad annullamento della registrazione si deve riportare a margine il numero di protocollo e la data dell'autorizzazione di annullamento. La segnatura (timbro ed etichetta) deve essere barrata con la dicitura "*annullato*".

40.2. Corrispondenza contenente dati particolari

I documenti contenenti categorie particolari di dati o soggetti a riservatezza, pervenuti in modalità cartacea, dopo essere stati scansionati e allegati alla registrazione effettuata con protocollo riservato, devono essere inseriti in busta chiusa recante la dicitura "contiene dati particolari" e successivamente nelle apposite cassettine dedicate allo smistamento.

40.3. Corrispondenza personale o riservata

La corrispondenza nominativamente intestata è regolarmente aperta dagli uffici incaricati della registrazione di protocollo dei documenti in arrivo, ad eccezione di quella diretta ai titolari di cariche istituzionali. Se la corrispondenza riveste carattere "riservato" o "personale", e ciò è desumibile prima dell'apertura della busta, questa viene inviata chiusa direttamente al destinatario priva di registrazione. Se il carattere "riservato" o "personale" della corrispondenza viene desunto dopo averne preso visione, il plico viene richiuso e inviato al destinatario privo di registrazione. L'eventuale registrazione di protocollo potrà essere effettuata in un momento successivo, qualora il destinatario la ritenga opportuna.

40.4. Corrispondenza cartacea non di competenza dell'Amministrazione

La corrispondenza cartacea che non è evidentemente di competenza dell'Unione (es. altro destinatario) non va aperta e va riconsegnata al Servizio postale; in caso di errata apertura, la busta va richiusa indicando la dicitura "aperta per errore", apponendo timbro datario e riconsegnata al Servizio postale. La corrispondenza cartacea che invece riporta l'indirizzo corretto sulla busta, ma non è di competenza dell'Unione, a seguito dell'apertura e valutazione, va richiusa indicando la dicitura "aperta e non di competenza", apponendo timbro datario e riconsegnata al Servizio postale.

Sezione terza – Classificazione e fascicolazione

41. Classificazione dei documenti

I documenti formati e acquisiti dall'Unione sono classificati mediante indicazione del titolo e della classe secondo i criteri previsti nel Titolario di cui all'allegato 8 cit.

I documenti devono essere classificati prima della registrazione di protocollo. Non è ammessa la registrazione di protocollo di documenti non classificati.

La classificazione dei documenti in entrata è effettuata dal personale addetto alla protocollazione, mentre la classificazione dei documenti prodotti dall'Unione è effettuata dalla UO Responsabile.

42. Fascicolazione informatica dei documenti

Al fine di garantire la consultazione dei documenti informatici, da parte sia di altre amministrazioni che degli utenti, questi sono raccolti in fascicoli informatici, secondo le indicazioni fornite nelle linee guida alla fascicolazione di cui all'allegato 10. I fascicoli eventualmente possono essere organizzati in sottofascicoli.

I documenti soggetti a protocollazione sono inseriti nel pertinente fascicolo tramite l'apposita funzione del Sistema di protocollo informatico *Folium*. Quando è necessario aprire un nuovo fascicolo informatico, l'utente abilitato alla creazione dei fascicoli della UO che ha prodotto il documento provvede all'apertura del fascicolo in cui inserire il documento.

Per i documenti in entrata, quando occorre provvedere all'apertura di un nuovo fascicolo informatico e vi sia incertezza sul criterio di fascicolazione da adottare, il personale addetto alla protocollazione provvede di concerto con il Responsabile della UO a cui è previsto sia assegnato per competenza il documento.

I fascicoli informatici possono essere organizzati:

a. per affare, quando i documenti raccolti nel fascicolo, accomunati secondo un criterio di classificazione basato sulla competenza amministrativa, non sono tutti riferibili a un singolo procedimento amministrativo. Il fascicolo per affare deve avere una data di apertura e una durata circoscritta;
b. per attività, quando i documenti raccolti nel fascicolo attengono allo 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;
c. per persona (fisica o giuridica), quando i documenti raccolti nel fascicolo, anche con classificazioni diverse, sono riferibili a un medesimo soggetto. Sono fascicoli di tipo "aperto", con durata pluriennale e indeterminata;

d. per procedimento amministrativo, quando i documenti raccolti nel fascicolo rappresentano azioni amministrative omogenee e destinate a concludersi con un provvedimento amministrativo.

I fascicoli informatici devono recare i metadati obbligatori delle aggregazioni documentali previsti nell'Allegato 5 alle Linee guida AgID.

Nelle more dell'implementazione di modalità automatizzate creazione e gestione dei fascicoli, organizzate secondo il piano di fascicolazione dell'Unione, gli utenti tenuti alla formazione dei fascicoli informatici assicurano che siano associati almeno i seguenti metadati, distinti per tipologia di fascicolo.

Il fascicolo informatico organizzato per affare deve recare:

1. tipologia di fascicolo;
2. codice identificativo del fascicolo (IdAggregazione);
3. codice IPA Amministrazione titolare;
4. codice IPA Amministrazioni partecipanti.

Il fascicolo informatico organizzato per persona deve recare:

(a) tipologia di fascicolo;
(b) codice identificativo del fascicolo (IdAggregazione);
(c) dati anagrafici della persona a cui fa riferimento il fascicolo (almeno nome e cognome per le persone fisiche, denominazione per le persone giuridiche, denominazione e codice IPA per le PA).

Il fascicolo informatico organizzato per attività deve recare:

1. tipologia di fascicolo;
2. codice identificativo del fascicolo (IdAggregazione);
3. dati anagrafici dell'assegnatario dell'attività (nome, cognome, codice IPA dell'Amministrazione di appartenenza).

Il fascicolo informatico organizzato per procedimento amministrativo deve recare:

1. tipologia di fascicolo;
2. codice identificativo del fascicolo (IdAggregazione);
3. dati anagrafici del RUP (nome, cognome, codice IPA dell'Amministrazione di appartenenza).

Sezione quarta – Flussi documentali interni

43. Assegnazione dei documenti in entrata agli uffici

L'assegnazione dei documenti in entrata, quando possibile, è effettuata con modalità automatizzate. In particolare, sono automaticamente assegnati alle UO Responsabili preventivamente individuate i documenti provenienti dai portali dei servizi online e le fatture provenienti dal Sistema Di Interscambio (SDI). Ulteriori criteri di assegnazione automatica sono definiti dal Responsabile, sentite le UUOO interessate.

I documenti non assegnati automaticamente sono assegnati alle UO Responsabili dal personale addetto alla protocollazione in base all'oggetto del documento e alla classificazione (cfr. allegato 10 cit.). Quando un documento è di interesse anche per più UUOO, si provvede a più assegnazioni, sia "per competenza" che "per conoscenza".

Lo scambio di documenti tra il Servizio Protocollo e Archivio e le diverse UUOO dell'Unione è effettuato per mezzo del Sistema di protocollo. Scambi tra gli uffici possono essere effettuati attraverso posta elettronica o cartelle condivise. In ogni caso, nelle attività di trasmissione e scambio dei documenti tutto il personale deve utilizzare esclusivamente gli strumenti di comunicazione messi a disposizione dall'Unione.

44. Comunicazioni interne

Tutte le comunicazioni interne sono effettuate esclusivamente in modalità telematica, ivi compresa la pubblicazione di avvisi e comunicazioni a carattere informativo.

Le comunicazioni personali sono trasmesse a mezzo posta elettronica ordinaria. Quando la comunicazione è indirizzata a più destinatari, per evitare la divulgazione di dati personali, il mittente provvede a invii individuali o in copia conoscenza nascosta (ccn).

45. Pubblicazioni nell'Albo pretorio

Tutti gli atti prodotti dall'Unione che, ai sensi della normativa vigente, sono soggetti a pubblicazione nell'Albo pretorio online, sono trasmessi per la pubblicazione in modo automatizzato solo dopo che il documento sia divenuto immodificabile (cfr. par. 15 del presente Manuale). Gli altri atti oggetto di pubblicazione, una volta ricevuti e protocollati, sono inseriti manualmente dal personale abilitato.

PARTE QUINTA – CONSERVAZIONE DEI DOCUMENTI

46. Sistema di conservazione dei documenti informatici

Per la conservazione a lungo termine dei documenti informatici, l'Unione dei Comuni Valli e Delizie si avvale di un sistema esterno ai sensi dell'art. 44, comma 1-quater, CAD.

Il servizio di conservazione dei documenti informatici dell'ente è stato affidato al Conservatore PARER (Servizio Polo Archivistico Regionale dell'Emilia-Romagna, d'ora in avanti anche solo "Conservatore").

Le attività affidate al Conservatore sono puntualmente indicate nella convenzione per l'affidamento del servizio, di cui all'allegato 11.

47. Responsabile della conservazione

Come precisato al par. 5 del presente Manuale, l'Unione ha designato un unico soggetto che riveste i ruoli di Responsabile della gestione documentale e Responsabile della conservazione.

È compito del Responsabile assicurare il rispetto della normativa vigente da parte del Conservatore e degli obblighi contrattuali dallo stesso assunti, ivi compreso il rispetto delle misure di sicurezza dei dati trattati. A tal fine, il Responsabile agisce d'intesa con il RTD e con il RPD dell'ente.

Il Responsabile, sotto la propria responsabilità, può delegare in tutto o in parte una o più attività di propria competenza relative alla conservazione, affidandola a soggetti interni all'ente dotati di adeguate competenze. Gli atti di delega devono individuare le specifiche attività e funzioni delegate.

48. Oggetti della conservazione

Gli oggetti della conservazione sono:

- i documenti informatici formati dall'Ente e i rispettivi metadati (conformi all'Allegato 5 alle Linee guida dell'AgID);
- i fascicoli informatici e rispettivi metadati (conformi all'Allegato 5 alle Linee guida dell'AgID);
- il registro del protocollo informatico generale e giornaliero;
- gli altri registri e repertori tenuti dall'ente.

Gli oggetti della conservazione sono trattati dal sistema di conservazione del Conservatore in pacchetti informativi che si distinguono in:

a) pacchetti di versamento;
b) pacchetti di archiviazione;

c) pacchetti di distribuzione.

Il Responsabile provvede ad associare a ogni pacchetto di versamento almeno i seguenti metadati:

1. identificativo univoco e persistente del pacchetto di versamento;
2. riferimento temporale valido, attestante la data e l'ora di creazione del pacchetto;
3. denominazione del soggetto responsabile della produzione del pacchetto;
4. impronta del pacchetto di versamento;
5. numero dei documenti compresi nel pacchetto.

Le specifiche operative e le modalità di descrizione e di versamento delle singole tipologie di documenti oggetto del servizio di conservazione sono dettagliatamente individuate nel Disciplinare tecnico per lo svolgimento della funzione di conservazione dei documenti informatici sottoscritto dall'Unione unitamente alla convenzione di affidamento del servizio al Conservatore PARER (**allegato 11 cit.**).

49. Formati ammessi per la conservazione

I formati ammessi per la conservazione sono individuati nell'allegato 2 alle Linee guida dell'AgID sulla formazione, gestione e conservazione dei documenti informatici e nel Disciplinare tecnico del Conservatore vengono definiti i formati accettati.

Gli standard raccomandati da Agid sono quelli che possono essere facilmente estesi, rivisti o aggiornati nel tempo per adattarsi all'immanente obsolescenza tecnologica. Tra questi, eccellono gli standard che sono "ab initio" disegnati con il preciso scopo di evolvere a lungo termine; per questo motivo essi sono detti formati "compatibili in avanti" o anche "future-proof".

Questi standard "virtuosi" devono essere scelti come formati di riferimento, sono l'XML e il JSON; il PDF e l'OpenDocument (ODT e ODS) per i documenti impaginati; il TIFF (e il DNG), il PNG e il DPX per le immagini raster; l'SVG e il DXF per i modelli vettoriali; il TTML per i dialoghi; l'MXF e l'MP4 come contenitori multimediale; l'IMF come pacchetto di file multimediali.

Il Responsabile, prima del versamento in conservazione, valuta i casi in cui è opportuno procedere al riversamento del documento in diverso formato, purché conforme ai formati indicati nell'allegato 2 alle Linee guida. In tal caso, la corrispondenza fra il formato originale e quello di riversamento è garantita dal Responsabile attraverso attestazione di conformità rilasciata secondo le modalità indicate nella Parte Seconda del presente Manuale.

50. Modalità e tempi di trasmissione dei pacchetti di versamento

All'inizio di ogni anno ciascuna UO individua i fascicoli da versare all'archivio di deposito, dandone comunicazione al Responsabile, che provvede alla formazione e alla trasmissione dei pacchetti di versamento, secondo le modalità operative definite nel manuale del Conservatore e nel Disciplinare tecnico.

Il Responsabile genera il rapporto di versamento relativo a uno o più pacchetti di versamento e una o più impronte relative all'intero contenuto del pacchetto, secondo le modalità descritte nel manuale del Conservatore.

Prima del versamento in conservazione, il Responsabile verifica che agli oggetti della conservazione siano stati correttamente associati i rispettivi metadati e, se mancanti, richiede al produttore dell'oggetto di provvedere correttamente all'associazione dei metadati.

Il versamento dei documenti avviene tramite sistema automatizzato entro le 24 ore successive al momento della produzione. Il Responsabile può individuare altre tipologie di versamento automatizzato a determinate scadenze per particolari tipologie di documenti.

51. Memorizzazione dei dati e dei documenti informatici e salvataggio della memoria informatica

I dati e i documenti informatici sono memorizzati nel sistema di gestione documentale al termine delle operazioni di registrazione. Le procedure di memorizzazione sono le seguenti:

a) salvataggio immediato su server di rete collocato presso Datacenter Lepida presente in marketplace AgId che si prefigura come private Cloud;
b) alla fine di ogni giorno sono create, a cura del Servizio sistemi informativi, copie di backup della memoria informatica dell'Amministrazione, che verranno poi riversate su supporti di memorizzazione tecnologicamente avanzati e conservati secondo quanto previsto dai Piano di Continuità Operativa e *Disaster Recovery* e dalle procedure di salvataggio dati descritte del Piano per la sicurezza informatica dell'Amministrazione.

52. Accesso al Sistema di conservazione

Gli utenti espressamente autorizzati dall'Unione possono accedere al Sistema tramite credenziali personali rilasciate da PARER e comunicate al singolo utente. L'accesso al Sistema consente di consultare i documenti digitali versati nel Sistema e le configurazioni specifiche adottate.

53. Selezione e scarto dei documenti

Periodicamente, secondo quanto previsto nel Piano di conservazione - Massimario di scarto (allegato 12), viene effettuata la procedura di selezione della documentazione da proporre allo scarto ed attivato il procedimento amministrativo di scarto documentale, con eventuale invio di proposta alla competente Soprintendenza Archivistica. Le modalità per effettuare le operazioni di selezione e scarto dei documenti informatici sono descritte nel Manuale di conservazione (allegato 13).

54. Conservazione, selezione e scarto dei documenti analogici

La documentazione analogica corrente è conservata a cura del responsabile del procedimento fino al trasferimento in archivio di deposito.

I documenti analogici dell'Amministrazione sono conservati nei locali dell'Amministrazione. Il Responsabile cura il versamento nell'archivio di deposito delle unità archivistiche non più utili per la trattazione degli affari in corso, individuate dagli uffici produttori. I fascicoli non soggetti a operazioni di scarto sono conservati nell'archivio di deposito secondo i termini di legge, per poi essere trasferiti nell'archivio storico per la conservazione permanente. Delle operazioni di trasferimento deve essere lasciata traccia documentale.

Periodicamente il Responsabile valuta l'opportunità, anche sotto il profilo economico, di provvedere al riversamento in formato digitale di tutti o parte dei documenti analogici giacenti negli archivi.

55. Misure di sicurezza e monitoraggio

Il Manuale di conservazione e il Piano della Sicurezza di PARER descrivono le modalità con cui il Conservatore assicura gli obiettivi di sicurezza richiesti per la conservazione a lungo termine degli archivi, dettagliando i controlli di sicurezza delle diverse componenti del sistema (organizzazione, accessi, infrastruttura, gestione dell'esercizio, gestione dello sviluppo) e le procedure adottate per garantire i *backup* degli archivi e il *Disaster recovery*.

Il Conservatore provvede altresì al periodico monitoraggio al fine di verificare lo stato delle componenti infrastrutturali del sistema e l'integrità degli archivi.

Il Responsabile vigila affinché il Conservatore provveda alla conservazione integrata dei documenti, dei fascicoli e dei metadati associati nelle fasi di gestione e di conservazione. A tal fine, con cadenza almeno annuale, richiede al Conservatore l'esibizione di un campione di documenti o fascicoli.

Nel caso siano riscontrate irregolarità, provvede a sollecitare il Conservatore affinché vi ponga rimedio, anche attraverso gli strumenti previsti nell'atto di affidamento del servizio.

PARTE SESTA – SICUREZZA E PROTEZIONE DEI DATI PERSONALI

56. Sicurezza dei sistemi informatici dell'Unione

Tutti gli strumenti software indicati al par. 6 del presente manuale, utilizzati per la formazione e gestione dei documenti informatici, sono analizzati e sottoposti a costante rivalutazione/aggiornamento attraverso le linee guida per le misure minime di sicurezza ICT emanate dall'AGID con la circolare del 18 aprile 2017, n. 2/2017.

Suddetti strumenti sono resi accessibili al personale dell'Ente tramite il servizio di infrastruttura fornito come cloud privato da società in house della Regione Emilia-Romagna qualificata come CSP (Cloud Service Provider) dall'Agenzia per l'Italia Digitale. Il servizio consente altresì l'archiviazione dei documenti, prodotti mediante l'utilizzo dei software, nel rispetto degli standard di sicurezza previsti dalla normativa, garantendone così l'integrità e l'immodificabilità ai sensi delle Linee guida (cfr. parr. 2.1.1. e 3.9).

La memorizzazione dei documenti correnti, diversi da quelli formati con l'ausilio dei suddetti strumenti software, è effettuata sui server dell'Unione, in attesa dell'archiviazione tramite versamento al sistema di conservazione del Conservatore PARER, o della selezione per lo scarto.

57. Amministratori di sistema

Gli amministratori di sistema vengono nominati con apposito atto e muniti di credenziali di accesso personali e robuste.

All'interno dell'organizzazione sono individuate le seguenti definizioni di Amministratori:

- Amministratori di Sistema, per i Sistemi Operativi dei Server e dei sistemi di virtualizzazione;

- Amministratori di DBMS, per la gestione (accesso e manutenzione) dei database;

- Amministratori di PdL, per la gestione delle postazioni di lavoro;

- Amministratori di Rete, per la gestione (accesso e manutenzione) degli apparati di rete: switch, router, firewall, ecc…;

Queste posizioni all'interno dell'organizzazione possono talvolta essere concentrate nelle stesse persone con generali competenze informatiche / telematiche.

Altre posizioni da amministratore, presenti in Organizzazione e spesso distinguibili dalle precedenti, sono:

- Amministratore Applicativo, che si occupa di creare gli utenti ed abilitare i relativi permessi su di uno specifico applicativo;

- Controllore, attività solitamente esternalizzata con funzioni di controllo e notifica di anomalie su elementi specifici dell'infrastruttura; per questa posizione in genere non sono richieste conoscenze informatiche generali ma serve un'alta specializzazione sui singoli applicativi.

Alcune di queste funzioni possono essere gestite anche da esterni da parte ad esempio della ditta che ha fornito il software.

In termini di sicurezza l'Organizzazione sta valutando l'acquisizione di sistemi di raccolta dei log e di gestione centralizzata degli asset per il monitoraggio e l'individuazione di eventi critici.

Suddetti sistemi si devono occupare:

- della raccolta di dati generati dagli ambienti operativi (dispositivi, applicazioni, database, in generale considerati come "sorgenti") a fronte del manifestarsi di eventi di sistema alcuni dei quali di estrema rilevanza per la sicurezza;
- di prelevare i tracciati di accesso di tutte le sorgenti e in particolare degli amministratori;
- di organizzare e rappresentare graficamente suddetti eventi, evidenziando e segnalando le anomalie ed i tentativi multipli di accesso non andati a buon fine.

Questo permette agli amministratori di:

- in caso di tentativi multipli di accesso, individuare eventuali attacchi;
- effettuare continue verifiche sulle vulnerabilità dei sistemi sorgenti;
- gestire gli eventuali incidenti di sicurezza;
- effettuare il controllo puntuale degli accessi ai dati e alle applicazioni;
- avere un feedback automatico sullo stato dei sistemi Sorgenti;
- mantenere traccia immutabile nel tempo degli eventi rilevanti.

Suddetti sistemi devono permettere la raccolta delle informazioni secondo i principi di minimizzazione e proporzionalità e di mantenere i dati inalterabili durante l'intero ciclo di vita garantendo l'integrità degli stessi e la conservazione in termini di data retention policy.

I dati dovranno essere memorizzati per 180 giorni su DBMS relazionale accessibile in manutenzione e per controllo continuo solo dall'Amministratore DBMS della ditta appaltatrice e non dagli amministratori dell'Organizzazione.

I dati devono essere criptati all'origine e mai trasmessi o memorizzati in chiaro.

Il DBMS dovrà essere su Server di proprietà dell'Organizzazione e non accessibile esternamente.

L'unità di memorizzazione deve essere opportunamente dimensionata per accogliere i dati con una Data Retention garantita di 10 anni.

Il data base e l'unità di memorizzazione saranno sottoposti a piani di backUp differenziali, incrementali e completi come da policy dell'Ente.

L'accesso al dato originale, in qualsiasi forma, può avvenire solo attraverso l'abilitazione congiunta alla connessione al Server da parte dell'amministratore di Sistema dell'Organizzazione ed al Data Base da parte dell'amministratore DBMS della ditta appaltante, garantendo un meccanismo di accesso sempre supervisionato.

Ogni accesso deve essere tracciato automaticamente.

58. Uso del profilo utente per l'accesso ai sistemi informatici

Per l'accesso ai sistemi informatici dell'Unione è necessaria l'assegnazione di un profilo utente di tipo Active Directory, rilasciabile solo su indicazione del Responsabile di AOO all'Amministratore di Sistema. Ogni profilo è protetto da un sistema di credenziali (username e password) robuste e definite dalle policy descritte di seguito sulla gestione degli accessi. Al momento della creazione del profilo utente, sono attribuiti all'utente lo username e una password temporanea. Al primo accesso dell'utente, viene automaticamente richiesto l'aggiornamento delle credenziali.

Le credenziali hanno una validità di 90 giorni per qualsiasi categoria di utente (anche gli amministratori).

Policy di generazione password:

- non possono essere utilizzate password già inserite negli ultimi 5 rinnovi;
- la password deve essere lunga almeno 9 caratteri e non deve contenere il nome dell'account dell'utente o parte del nome;
- devono essere garantite almeno tre delle caratteristiche seguenti:
  - almeno una lettera maiuscola;
  - almeno una lettera minuscola;
  - almeno un numero;
  - almeno un carattere speciale (ad esempio !, $, #, %).

L'uso di ogni profilo utente è strettamente personale e ogni dipendente, sotto la propria responsabilità, è tenuto a custodire e non diffondere le proprie credenziali. Ciascun dipendente è tenuto a rispettare la policy di generazione

delle password definita in questo manuale. Il Sistema garantisce che per ogni profilo utente, alla scadenza della password, sia automaticamente richiesto il rinnovo da parte dell'utente.

59. Accesso alle postazioni di lavoro, ai locali e agli archivi dell'Unione

L'accesso alle postazioni e l'uso di ogni profilo utente è strettamente personale e ogni dipendente, sotto la propria responsabilità, è tenuto a custodire e non diffondere le proprie credenziali. Ciascun dipendente è tenuto a rispettare la policy di generazione delle password definita in questo manuale ed il Regolamento sull'uso degli strumenti informatici dell'Organizzazione allegato al manuale. Il sistema provvede affinché, almeno a cadenza trimestrale, per ogni profilo utente sia richiesto il rinnovo della password.
Gli archivi del materiale cartaceo sono presenti in diverse sedi comunali in locali predisposti e non di libero accesso. Le chiavi per accedere sono date in custodia al responsabile dell'archivio presso la sede specifica.