MANUALE DI GESTIONE DEL

PROTOCOLLO INFORMATICO,

DEI FLUSSI DOCUMENTALI E DEGLI ARCHIVI

Ai sensi del Decreto del Presidente del Consiglio dei Ministri 03 dicembre 2013 "Regole tecniche per il protocollo informatico ai sensi degli artt. 40-bis, 41, 47, 57-bis e 71 del Codice dell'amministrazione digitale di cui D.Lgs. 82 del 2005".

INDICE

1 PRINCIPI GENERALI

1.1 Premessa 6

1.2 Ambito di applicazione del manuale 6

1.3 Definizioni 6

1.4 Norme di riferimento 6

2 DOCUMENTI E MODALITA' DI GESTIONE

2.1 Il documento informatico amministrativo 7

2.2 Il documento analogico – cartaceo amministrativo 7

2.3 Documento in ingresso 8

2.4 Documento in uscita 8

2.5 Documento interno formale 9

2.6 Documento interno informale 9

2.7 Formazione del documento informatico 9

2.8 La firma 9

2.9 Autenticazione firma 10

2.10 Immodificabilità ed integrità del documento informatico, copie, duplicati ed estratti 11

2.11 Requisiti degli strumenti informatici di scambio 12

2.12 Trasmissione documenti con il sistema pubblico di connettività 12

2.13 Uso della Posta Elettronica Certificata 13

2.14 Interoperabilità dei sistemi di protocollo informatico 14

3 ORGANIZZAZIONE DELL'ENTE E DEL PROTOCOLLO

3.1 Il protocollo informatico 14

3.2 Aree Organizzative Omogenee e modelli organizzativi 15

3.3 Accreditamento dell'amministrazione/AOO all'Indice delle Pubbliche Amministrazioni (IPA) 16

3.4 Individuazione del Responsabile della gestione documentale e del Servizio di Protocollo informatico 17

3.5 Requisiti minimi di sicurezza dei sistemi di gestione documentale e protocollo informatico 17

3.6 Tutela dei dati personali e attuazione del regolamento UE 679/216 e s.m.i. 18

3.7 Formazione del personale 18

4 DESCRIZIONE DEL FLUSSO DI LAVORAZIONE DEI DOCUMENTI

4.1 Generalità 19

4.2 Flusso dei documenti ricevuti dalla AOO 19

4.2.1 Ricezione di documenti informatici sulle caselle di posta elettronica certificata 19

4.2.2 Ricezione di documenti informatici sulla casella di posta elettronica tradizionale 20

4.2.3 Ricezione di documenti informatici su supporti rimovibili 20

4.2.4 Ricezione di documenti cartacei a mezzo servizio postale, (posta ordinaria e raccomandata) corriere o consegna a mano 21

4.2.5 Corrispondenza di particolare rilevanza e documenti esclusi 21

4.2.6 Errata ricezione di documenti 22

4.2.7 Rilascio di ricevute attestanti la ricezione di documenti informatici 22

4.2.8 Rilascio di ricevute attestanti la ricezione di documenti cartacei 22

4.2.9 Classificazione, assegnazione e presa in carico dei documenti 22

4.3 Flusso dei documenti creati e trasmessi dall'AOO 23

4.3.1 Sorgente interna dei documenti 23

4.3.2 Verifica formale dei documenti 23

4.3.3 Registrazione di protocollo e segnatura 23

4.3.4 Trasmissione di documenti informatici 23

4.3.5 Trasmissione di documenti cartacei a mezzo posta 24

4.3.6 Conteggi e spedizione corrispondenza cartacea 24

4.4 Documenti informali 24

5. GESTIONE DELLE REGISTRAZIONI DI PROTOCOLLO

5.1 Unicità del protocollo informatico 25

5.2 Registrazione di protocollo 25

5.3 Elementi facoltativi delle registrazioni di protocollo 26

5.4 Segnatura di protocollo dei documenti (Sigillo elettronico) 27

5.5 Modifiche e Annullamento delle registrazioni di protocollo 27

5.6 Protocollazione documenti interni formali (protocolli interni) 28

5.7 Registrazione differita di protocollo 28

5.8 Documenti riservati (Protocollo riservato) 28

6 IL SISTEMA DI GESTIONE DOCUMENTALE E DI PROTOCOLLAZIONE ADOTTATO DALL'ENTE

6.1 Descrizione funzionale ed operativa 29

7 SICUREZZA

7.1 Obiettivi 29

7.2 Credenziali di accesso al sistema documentale 31

7.3 Sicurezza nella formazione dei documenti 31

7.4 Trasmissione ed interscambio dei documenti informatici 32

7.5 Accesso ai documenti informatici 33

8 NORME TRANSITORIE E FINALI

8.1 Modalità di approvazione e aggiornamento del manuale 33

8.2 Pubblicità del manuale 34

8.3 Entrata in vigore 34

ALLEGATI

Allegato 1 – Glossario e definizioni
Allegato 2 – Norme di riferimento
Allegato 3 – I formati dei documenti
Allegato 4 – Il sistema documentale e di protocollazione adottato dall'Ente
Allegato 5 - Manuale di conservazione

1 PRINCIPI GENERALI

1.1 Premessa

Il manuale di gestione è uno strumento operativo che descrive e disciplina il sistema di produzione e di gestione documenti (analogici e digitali), come previsto dall'art. 5 del Decreto del Presidente del Consiglio dei Ministri 03 dicembre 2013.

Il manuale di gestione:

- individua le procedure e fornisce le istruzioni per la corretta redazione della documentazione analogica e digitale, descrivendo le modalità di gestione dei flussi documentali e degli archivi, in modo tale da organizzare i documenti ricevuti, inviati o comunque gestiti dall'Asm Costruire Insieme in armonia con quanto previsto dalla normativa vigente in tema di registrazione di protocollo, di assegnazione, classificazione, fascicolatura e reperimento dei documenti;

- affronta aspetti consolidati della registratura, ma anche nuove soluzioni e nuovi problemi posti dalla tecnologia e dalle richieste del legislatore orientato a un'amministrazione pubblica digitale;

- costituisce una guida ed è rivolto a tutto il personale, in quanto ciascun dipendente (a vario titolo e livello) è coinvolto nella gestione documentale.

1.2 Ambito di applicazione del manuale

Il presente Manuale di gestione del protocollo informatico, dei flussi documentali e degli archivi è adottato ai sensi del Decreto del Presidente del Consiglio dei Ministri 03 dicembre 2013: "Regole tecniche per il protocollo informatico ai sensi degli artt. 40-bis, 41, 47, 57-bis e 71 del Decreto Legislativo 7 marzo 2005, n. 82 "*Codice dell'amministrazione digitale"* (C.A.D.).

Esso descrive le attività di formazione, registrazione, classificazione, fascicolazione ed archiviazione dei documenti, oltre che la gestione dei flussi documentali dell'Ente.

Attraverso l'integrazione con le procedure di gestione dei procedimenti amministrativi, di accesso agli atti e di archiviazione dei documenti, il protocollo informatico realizza le condizioni operative per una più efficiente gestione del flusso informatico e documentale interno dell'amministrazione anche ai fini dello snellimento delle procedure e della trasparenza dell'azione amministrativa. Il protocollo fa fede, anche con effetto giuridico, dell'effettivo ricevimento e spedizione di un documento.

1.3 Definizioni

Le definizioni e gli acronimi utilizzati più di frequente sono elencate nell'Allegato 1 – Glossario e definizioni.

1.4 Norme di riferimento

Le principali norme di riferimento sono elencate nell'Allegato 2 - Norme di riferimento.

2 DOCUMENTI E MODALITA' DI GESTIONE

Nell'ambito del processo di gestione documentale, il documento amministrativo, in termini tecnologici, è classificabile in:

- informatico ("rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti");

- analogico ("rappresentazione non informatica di atti, fatti o dati giuridicamente rilevanti").

In termini operativi, il documento amministrativo è invece classificabile in:

- ricevuto da mittente esterno all'Ente (compresi i dipendenti dell'Ente qualora di si tratti di richieste, comunicazioni e note sindacali, ecc);

- inviato a destinatari esterni all'Ente;

- interno formale;

- interno informale.

2.1 Il documento informatico amministrativo

Il Codice dell'Amministrazione Digitale definisce il documento informatico come "rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti".

Gli atti formati dalle pubbliche amministrazioni con strumenti informatici, nonché i dati e i documenti informatici detenuti dalle stesse, costituiscono informazione primaria ed originale da cui è possibile effettuare, su diversi o identici tipi di supporto, duplicazioni e copie per gli usi consentiti dalla legge.

I documenti costituenti atti amministrativi con rilevanza interna al procedimento amministrativo sono sottoscritti con firma digitale ed hanno l'efficacia prevista dall'art. 2702 del codice civile.

Secondo quanto previsto dall'art. 40 del C.A.D. "1. Le pubbliche amministrazioni formano gli originali dei propri documenti con mezzi informatici secondo le disposizioni di cui al presente codice e le regole tecniche di cui all'articolo 71".

I formati dei documenti informatici sono elencati nell'Allegato 3.

2.2 Il documento analogico – cartaceo amministrativo

Per documento analogico si intende "la rappresentazione non informatica di atti, fatti o dati giuridicamente rilevanti" cioè un documento "formato utilizzando una grandezza fisica che assume valori continui, come: le tracce su carta (esempio: documenti cartacei), le immagini su

film (esempio: pellicole mediche, microfilm), le magnetizzazioni su nastro (esempio: cassette e nastri magnetici audio e video) su supporto non digitale".

2.3 Documento in ingresso

La corrispondenza in ingresso può essere acquisita dalla AOO (Area Organizzativa Omogenea) con diversi mezzi e modalità in base alla tecnologia utilizzata dal mittente.

Un documento informatico può essere recapitato, preferibilmente con lettera di trasmissione, a titolo esemplificativo:

- a mezzo posta elettronica o posta elettronica certificata;

- su supporto rimovibile consegnato direttamente o inviato per posta convenzionale o corriere;

- fax server;

- tramite portale/ spazio web dedicato;

Un documento analogico può essere tipicamente recapitato:

- a mezzo posta convenzionale o corriere;

- a mezzo posta raccomandata;

- per telefax o telegramma;

- con consegna diretta a una delle unità organizzative aperte al pubblico da parte dell'interessato o di persona delegata.

L'Ente dà piena attuazione a quanto disposto dall'art. 45, comma 1, del C.A.D., in base al quale "I documenti trasmessi da chiunque a una pubblica amministrazione con qualsiasi mezzo telematico o informatico, idoneo ad accertarne la fonte di provenienza, soddisfano il requisito della forma scritta e la loro trasmissione non deve essere seguita da quella del documento originale".

2.4 Documento in uscita

I documenti informatici e gli eventuali allegati sono inviati di norma per mezzo della posta elettronica certificata quando diretti ad altra pubblica amministrazione, a soggetti iscritti a ordini professionali, al registro imprese e nei casi in cui il cittadino abbia comunicato il proprio indirizzo di posta elettronica certificata.

Il documento informatico può inoltre essere riversato su supporto digitale rimovibile in formato non modificabile, per la trasmissione al destinatario con altri mezzi di trasporto.

Lo scambio di documenti con altre Pubbliche Amministrazioni avviene mediante l'utilizzo della posta elettronica certificata o in cooperazione applicativa.

Gli allegati inseriti sull'applicativo dovranno essere in uno dei formati riportati negli Allegati 3 e 4 (Manuale di conservazione), preferibilmente in Pdf/A.

Nel caso di spedizione o trasmissione in forma diversa da quella informatica (invio di documento analogico), nella fase di protocollazione in uscita sarà inserita la copia scansione del documento.

2.5 Documento interno formale

I documenti interni sono formati con tecnologie informatiche avvalendosi di software di produttività individuale e/o di applicazioni di gestione documentale.

2.6 Documento interno informale

La minuta corrispondenza, la conferma a riunioni e altre comunicazioni non aventi rilevanza giuridica vengono scambiate attraverso l'uso della posta elettronica.

2.7 Formazione del documento informatico

I documenti dell'amministrazione sono prodotti con sistemi informatici come previsto dalla vigente normativa.

Ogni documento formato per essere inoltrato all'esterno o all'interno in modo formale deve trattare un unico argomento indicato in maniera sintetica, ma esaustiva a cura dell'autore nello spazio riservato all'oggetto.

Le firme necessarie alla redazione e perfezione giuridica del documento in partenza devono essere apposte prima della sua protocollazione.

Il documento informatico assume la caratteristica di immodificabilità se formato in modo che forma e contenuto siano inalterabili nel tempo ovvero durante le fasi di tenuta e accesso e ne sia garantita la staticità nella fase di conservazione.

Nel caso di documento informatico, le caratteristiche di immodificabilità e di integrità sono delineate dalle Linee Guida sulla formazione, gestione e conservazione dei documenti informatici dell'Agid (Agenzia per l'Italia Digitale).

2.8 La firma

Nell'ambito del sistema di gestione documentale, questo Ente accetta l'utilizzo delle tipologie di firma citate dal C.A.D. e dal Regolamento UE n. 910/2014 sull'identità digitale - Regolamento eIDAS (electronic identification and trust services for electronic transactions in the internal market).

Firma elettronica: insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica in forma di PIN o insieme di Username e Password.

La firma elettronica viene utilizzata per l'autenticazione a fini di consultazione e accesso all'erogazione di servizi.

Firma avanzata: consente l'identificazione del firmatario e la connessione univoca ad esso. Le forme di firma avanzata utilizzabili da questo Ente sono: Certificati digitali, codici OTP (One Time Password), firma grafometrica, PEC con ricevuta completa, Carta Nazionale dei Servizi.

All'interno dell'Ente la firma avanzata può essere utilizzata come sistema di validazione in eventuali fasi procedimentali, di comunicazione interna, di abilitazione allo svolgimento di attività specifiche.

Firma qualificata: realizzata mediante dispositivo sicuro per la generazione di un certificato digitale e utilizzata mediate dispositivi quali Token, Smart card, Firma remota, Firma automatica.

Viene utilizzata per tutte le attività di natura pubblicistica che non richiedono che il documento informatico acquisisca le caratteristiche di immodificabilità ed integrità ed inoltre che non richieda l'apposizione di timbri o sigilli.

Firma digitale: costituita da un certificato qualificato e sistema di chiavi crittografiche, una pubblica e una privata, consente di rendere manifesta e di verificare la provenienza e l'integrità di uno o più documenti informatici. Si utilizza con dispositivi quali token, smart card, firma remota e firma automatica e massiva.

In relazione al valore legale di firma autografa e sottoscrizione, garantisce, oltre alla provenienza, anche l'integrità e l'autenticità del documento sottoscritto. L'apposizione della firma digitale sostituisce l'apposizione di timbri, sigilli e punzoni.

Viene utilizzata per la firma di provvedimenti con effetto costitutivo, modificativo o estintivo di rapporti giuridici, sia di natura pubblicistica (si portano ad esempio deliberazioni, provvedimenti dirigenziali, delibere presidenziali, documenti finanziari e contabili, pareri etc.) che privatistica e contrattuale che verranno versati nel sistema di conservazione.

La firma digitale viene rilasciata al Direttore al Presidente e al Responsabile Amministrativo, legittimati alla sottoscrizione di documenti aventi rilevanza esterna.

2.9 Autenticazione firma

L'autenticazione delle firme è prevista per la firma elettronica o qualsiasi altro tipo di firma avanzata (FEA, qualificata e digitale) e viene effettuata:

- da un pubblico ufficiale

- mediante l'acquisizione digitale della sottoscrizione autografa su apposito dispositivo atto a memorizzare i dati biometrici del sottoscrittore, o di qualsiasi altro tipo di firma elettronica avanzata.

2.10 Immodificabilità e integrità del documento informatico, copie, duplicati ed estratti.

L'immodificabilità e l'integrità di documenti informatici, copie, duplicati ed estratti viene assicurata mediante:

a) conversione in formato privo di contenuti dinamici (macro istruzioni e codici eseguibili) quali in PDF/A o altri formati esplicitati nell'apposito allegato;

b) sottoscrizione con firma digitale ovvero con firma elettronica qualificata;

c) apposizione di una validazione temporale (marca temporale);

d) trasferimento a soggetti terzi con posta elettronica certificata con ricevuta completa;

e) memorizzazione su sistemi di gestione documentale che adottino idonee politiche di sicurezza;

f) versamento ad un sistema di conservazione.

Con riferimento in particolare a documenti specifici quali:

1) le registrazioni di protocollo

2) la registrazione in ulteriori registri, repertori, albi, elenchi, archivi e raccolte di dati contenuti nel sistema di gestione documentale.

Al documento, una volta divenuto immodificabile, deve essere associato l'insieme minimo dei metadati (identificativo univoco e persistente, il riferimento temporale, l'oggetto, il soggetto che ha formato il documento, l'eventuale destinatario, l'impronta informatica).

Per metadati si intende:

- I metadati dei documenti informatici:

L'insieme minimo dei metadati del documento amministrativo informatico è quello indicato all'interno del DECRETO DEL PRESIDENTE DEL CONSIGLIO DEI MINISTRI 3 dicembre 2013 "Regole tecniche per il protocollo informatico ai sensi degli articoli 40-bis, 41, 47, 57 –bis e 71, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005 – Allegato 5".

- I metadati minimi del fascicolo informatico o della aggregazione documentale informatica:

Identificativo univoco e persistente è una sequenza di caratteri alfanumerici associata in modo univoco e permanente al fascicolo o aggregazione documentale informatica in modo da consentirne l'identificazione. Dublin Core raccomanda di identificare il documento per mezzo di una sequenza di caratteri alfabetici o numerici secondo un sistema di identificazione formalmente definito. Esempi di tali sistemi di identificazione includono l'Uniform Resource Identifier (URI), il Digital Object Identifier (DOI) e l'International Standard Book Number (ISBN).
Oggetto, metadato funzionale a riassumere brevemente il contenuto del documento o comunque a chiarirne la natura. Dublin Core prevede l'analoga proprietà "Description" che può includere ma non è limitata solo a: un riassunto analitico, un indice, un riferimento al contenuto di una rappresentazione grafica o un testo libero del contenuto.

2.11 Requisiti degli strumenti informatici di scambio

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

- l'integrità del messaggio;

- la riservatezza del messaggio;

- il non ripudio dei messaggi;

- l'automazione dei processi di protocollazione e smistamento dei messaggi all'interno della AOO;

- l'interconnessione tra le unità organizzative della AOO nel caso di documenti interni;

- la certificazione dell'avvenuto inoltro e ricezione.

2.12 Trasmissione documenti con il sistema pubblico di connettività

Lo scambio dei documenti informatici tra le varie amministrazioni, e con i privati, avviene attraverso meccanismi di "interoperabilità" e "cooperazione applicativa". L'articolo 72 del C.A.D., distinguendo due diversi livelli di interoperabilità, ne fornisce la seguente definizione:

- interoperabilità di base: i servizi per la realizzazione, gestione ed evoluzione di strumenti per lo scambio di documenti informatici fra le pubbliche amministrazioni e tra queste e i cittadini/privati;

- interoperabilità evoluta: i servizi idonei a favorire la circolazione, lo scambio di dati e informazioni, e l'erogazione fra le pubbliche amministrazioni e tra queste e i cittadini/privati;

- cooperazione applicativa: la parte del sistema pubblico di connettività finalizzata all'interazione tra i sistemi informatici delle pubbliche amministrazioni per garantire l'integrazione dei metadati, delle informazioni e dei procedimenti amministrativi.

2.13 Uso della Posta Elettronica Certificata

L'utilizzo della Posta Elettronica Certificata (PEC) o di altro sistema analogo consente di:

- conoscere in modo inequivocabile la data e l'ora di trasmissione;

- garantire l'avvenuta consegna all'indirizzo di posta elettronica certificata dichiarato dal destinatario;

- garantire l'integrità della trasmissione;

Il documento informatico trasmesso per via telematica si intende inviato e pervenuto al destinatario se trasmesso all'indirizzo elettronico dichiarato come domicilio digitale (IPA,INI-PEC, INAD). La dichiarazione da parte dell'utente del proprio indirizzo di posta elettronica certificata costituisce espressa accettazione dell'invio, tramite questo canale, degli atti e dei provvedimenti amministrativi relativi all'utente stesso. Quanto sopra vale anche per l'indirizzo di posta elettronica ordinaria, per le istanze, le comunicazioni e le dichiarazioni presentate all'Ente.

La trasmissione del documento informatico per via telematica, con una modalità che assicuri l'avvenuta consegna, equivale alla notificazione per mezzo della posta raccomandata, salvo che la legge disponga diversamente.

Le attuali tre banche dati nazionali sono:

- L'IPA (Indice dei domicili digitali delle Pubbliche Amministrazioni e dei Gestori di Pubblici Servizi): banca dati di libera consultazione contenente i riferimenti per comunicare con le Pubbliche Amministrazioni e i Gestori di Pubblici Servizi.
- INI-PEC: Indice Nazionale degli Indirizzi di Posta Elettronica Certificata) istituito dal Ministero dello Sviluppo Economico che raccoglie tutti gli indirizzi di PEC delle Imprese e dei Professionisti presenti sul territorio italiano;
- INAD (Indice nazionale dei domicili digitali delle persone fisiche, dei professionisti e degli altri enti di diritto privato non tenuti all'iscrizione in albi, elenchi o registri professionali o nel registro delle imprese): contiene l'indirizzo elettronico eletto presso un servizio di posta elettronica certificata (PEC) o un servizio elettronico di recapito certificato qualificato come definito dal Regolamento eIDAS, valido ai fini delle comunicazioni elettroniche aventi valore legale ai sensi dell'articolo 1, comma 1, lettera n-ter del CAD. Una volta eletto il proprio domicilio digitale su INAD, il cittadino deve ricevere le comunicazioni da parte della Pubblica Amministrazione (verbali di sanzioni amministrative e tutte le altre comunicazioni con valore legale ai sensi dell'art. 3-bis comma 4 del CAD)esclusivamente attraverso messaggio elettronico.

La AOO dispone della casella di Posta Elettronica Certificata istituzionali per la corrispondenza, sia in ingresso che in uscita, pubblicata sull'Indice delle Pubbliche Amministrazioni (IPA), reperibile all'indirizzo: www.indicepa.gov.it

Tale casella costituisce l'indirizzo virtuale della AOO e di tutti gli uffici che ad essa fanno riferimento.

2.14 Interoperabilità dei sistemi di protocollo informatico

Per interoperabilità dei sistemi di gestione documentale e protocollo informatico si intende la possibilità di trattamento automatico, da parte di un sistema, delle informazioni trasmesse da un diverso sistema mittente, allo scopo di automatizzare altresì le attività ed i processi amministrativi conseguenti (art. 55, comma 4, del Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445).

Per realizzare l'interoperabilità dei sistemi di protocollo informatico gestiti dalle pubbliche amministrazioni è necessario, in primo luogo, stabilire una modalità di comunicazione comune, che consenta la trasmissione telematica dei documenti sulla rete.

I sistemi di gestione informatica dei flussi documentali, orientati alla trasparenza amministrativa ed all'efficienza interna, si collocano in una dimensione più ampia nell'ottica della interconnessione e interoperabilità dei sistemi informativi pubblici.

3 ORGANIZZAZIONE DELL'ENTE E DEL PROTOCOLLO

3.1 Il protocollo informatico

L'Ente gestisce un unico protocollo informatico per tutti i documenti in arrivo e in partenza nell'ambito di un sistema di gestione documentale conforme alle previsioni di cui alle Regole Tecniche per il protocollo informatico ai sensi:

- degli articoli 40 bis, 41, 47, 57 bis e 71 del Codice dell'Amministrazione digitale di cui al Decreto legislativo 7 marzo 2005, n. 82 e s.m. e i. (C.A.D.) approvate con Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013 (di seguito indicato come Regole Tecniche);

- del Testo Unico sulla documentazione amministrativa approvato con Decreto del Presidente della Repubblica 28 dicembre *2000*, n. *445* (di seguito indicato come TU).

Il registro di protocollo è generato automaticamente dal sistema di protocollo che assegna a ciascun documento registrato il numero e la data di protocollazione.

All'unico sistema di protocollazione corrisponde un unico titolario di classificazione.

L'Ente produce un unico archivio, l'articolazione in archivio corrente, archivio di deposito ed archivio storico risponde esclusivamente a criteri di funzionalità.

Il modello operativo scelto dall'amministrazione è accentrato in un unico ufficio identificato in Amministrazione e Segreteria Generale.

L'ufficio provvede alla implementazione della eventuale fascicolazione della corrispondenza in arrivo ed alla protocollazione della corrispondenza in partenza, gestisce e custodisce i documenti dell'archivio corrente (ed eventualmente dell'archivio di deposito).

Si precisa che l'Azienda, nell'ambito della gestione documentale del sistema di protocollo, non ha previsto un piano di classificazione (titolario) e il piano di conservazione.

Nell'ambito della gestione documentale il sistema di protocollo si compone di:

- risorse normative riportate nell'apposito Allegato 2, il presente manuale e relativi allegati, ecc.

- risorse informatiche: software applicativo dedicato descritto nell'apposito Allegato 4, piattaforma documentale, PEC e posta elettronica ordinaria, cooperazione applicativa tra Pubbliche Amministrazioni, piattaforme di interscambio;

- risorse umane:

- Con Verbale del Consiglio di Amministrazione n. 5 del 01/04/2025 è stato conferito alla Dott. Antonello Paolo Zaccone l'incarico di responsabile del Servizio per la gestione informatica dei documenti, dei flussi documentali e degli archivi, nonché della conservazione del registro giornaliero di protocollo.

3.2 Aree Organizzative Omogenee e modelli organizzativi

L'amministrazione individua un'unica Area Organizzativa Omogenea (AOO) con sistema di protocollazione unico.

Nell'unica AOO è istituito un servizio per la tenuta del protocollo informatico, la gestione dei flussi documentali e degli archivi. All'interno della AOO il sistema di protocollazione è centralizzato, con la sola eccezione per la corrispondenza in entrata.

Gli operatori incaricati dell'attività di protocollazione sono abilitati dal Responsabile della gestione documentale e del Servizio di Protocollo informatico che ha anche il compito di vigilare sulla corretta esecuzione delle attività.

L'amministrazione, nell'ambito degli adempimenti previsti, si è accreditata presso l'Indice delle Pubbliche Amministrazioni (IPA) fornendo le informazioni che individuano l'amministrazione stessa e le unità organizzative in cui è articolata. Per maggiori dettagli si rimanda alla sezione 3.3 del presente manuale di gestione.

3.3 Accreditamento dell'amministrazione/ AOO all'Indice delle Pubbliche Amministrazioni (IPA)

Nell'ambito degli adempimenti previsti, l'Amministrazione si è accreditata presso l'Indice delle Pubbliche Amministrazioni (IPA) fornendo le seguenti informazioni che individuano l'amministrazione stessa e le AOO in cui è articolata:

- la denominazione della amministrazione;

- il codice identificativo proposto per la amministrazione;

- l'indirizzo della sede principale della amministrazione;

- l'elenco delle proprie Aree Organizzative Omogenee con l'indicazione:

- della denominazione;

- del codice identificativo;

- della casella di posta elettronica;

- del nominativo del RSP;

- della data di istituzione;

- dell'eventuale data di soppressione;

- l'elenco degli UOR e degli UU dell'AOO;

- i dati relativi alla fatturazione elettronica, la cui consultazione che prevede l'elenco dei codici di fatturazione per servizi è disponibile sul sito Indice delle Pubbliche Amministrazioni (IPA) all'indirizzo http://www.indicepa.gov.it

L'Indice delle Pubbliche Amministrazioni (IPA) è accessibile tramite il relativo sito internet da parte di tutti i soggetti pubblici o privati.

L'amministrazione comunica tempestivamente all'IPA ogni successiva modifica delle proprie credenziali di riferimento e la data in cui la modifica stessa sarà operativa in modo da garantire l'affidabilità di tutti i dati. L'Amministrazione ogni 6 mesi aggiorna i dati relativi all'IPA ai sensi dell'art. 6-ter comma 3 del C.A.D.

Il codice IPA attribuito all'amministrazione è" CIASM".

3.4 Individuazione del Responsabile della gestione documentale e del Servizio di Protocollo informatico

Nell'AOO è istituito un servizio per la tenuta del protocollo informatico, la gestione dei flussi documentali e degli archivi.

Alla guida del suddetto servizio è posto il Responsabile e il Vicario della gestione documentale e del Servizio di Protocollo informatico (RSP). La nomina è riportata nel punto 3.1 del presente manuale.

Il Responsabile è funzionalmente individuato nella figura del Direttore Generale.

È compito del Responsabile:

- provvedere all'aggiornamento e all'eventuale revisione del Manuale di gestione del Protocollo informatico, dei Flussi documentali e degli Archivi;

- provvedere alla pubblicazione e divulgazione del Manuale, anche attraverso il sito Internet dell'Amministrazione;

- abilitare gli addetti dell'amministrazione all'utilizzo del sistema software di gestione documentale e definire per ciascuno di essi il tipo di funzioni disponibili (ad esempio consultazione, modifica ecc.) e l'ambito di azione consentito;

- verificare il rispetto delle disposizioni normative durante le operazioni di registrazione e di segnatura di protocollo;

- supervisionare la corretta produzione del registro giornaliero di protocollo curata dall'ufficio protocollo;

- curare le funzionalità del sistema affinché, in caso di guasti o anomalie, siano ripristinate nel più breve tempo possibile;

- curare la conservazione delle copie di salvataggio delle informazioni del sistema di protocollo;

- supervisionare il buon funzionamento degli strumenti e curare il rispetto delle procedure concernenti le attività di registrazione di protocollo, di gestione dei documenti e dei flussi documentali, incluse le funzionalità di accesso dall'esterno;

- autorizzare le operazioni di annullamento della registrazione di protocollo;

3.5 Requisiti minimi di sicurezza dei sistemi di gestione documentale e protocollo informatico

1. Il sistema di gestione documentale e protocollo informatico assicura:

a) l'univoca identificazione ed autenticazione degli utenti;

b) la protezione delle informazioni relative a ciascun utente nei confronti degli altri;

c) la garanzia di accesso alle risorse esclusivamente agli utenti abilitati;

d) la registrazione delle attività rilevanti ai fini della sicurezza svolte da ciascun utente, in modo tale da garantirne l'identificazione;

e) l'univoca identificazione dei documenti;

2. Il sistema di gestione documentale e protocollo informatico deve consentire il controllo differenziato dell'accesso alle risorse del sistema per ciascun utente o gruppo di utenti.

3. Il sistema di gestione documentale e protocollo informatico deve consentire il tracciamento di qualsiasi evento di modifica delle informazioni trattate e l'individuazione del suo autore.

4. Le registrazioni di cui ai commi 1, lettera d), e 3 devono essere protette da modifiche non autorizzate.

5. Il registro giornaliero di protocollo è trasmesso automaticamente, attraverso l'applicativo che gestisce il flusso documentale, entro la giornata lavorativa successiva al conservatore digitale garantendone così l'immodificabilità del contenuto.

3.6 Tutela dei dati personali e attuazione del Regolamento UE 679/2016 e s.m.e i.

Relativamente agli adempimenti interni specifici, gli addetti autorizzati ad accedere al sistema di protocollo informatico e gestione documentale, sono formalmente incaricati.

Relativamente agli adempimenti esterni, l'Ente si è organizzato per garantire che i certificati e i documenti trasmessi ad altre pubbliche amministrazioni riportino le sole informazioni relative a stati, fatti e qualità personali previste da leggi e regolamenti e strettamente necessarie per il perseguimento delle finalità per le quali vengono acquisite.

Viene garantito il diritto dei cittadini e delle imprese ad ottenere che il trattamento dei dati effettuato mediante l'uso di tecnologie telematiche sia conformato al rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato.

3.7 Formazione del personale

Nell'ambito delle attività di attivazione ed applicazione del sistema di gestione documentale e di workflow, l'Ente organizza periodicamente percorsi formativi specifici e generali che coinvolgono il personale.

In particolare, considerato che il personale assegnato al servizio di protocollo deve conoscere sia l'organizzazione e i compiti svolti da ciascun servizio, sia gli strumenti informatici e le norme

di base per la tutela dei dati personali, la raccolta, la registrazione e l'archiviazione delle informazioni, periodicamente vengono effettuati percorsi formativi e di aggiornamento volti ad assicurare l'operatività del personale stesso.

4 DESCRIZIONE DEL FLUSSO DI ELABORAZIONE DEI DOCUMENTI

Il presente capitolo descrive il flusso di lavorazione dei documenti ricevuti, spediti o interni, incluse le regole di registrazione per i documenti pervenuti secondo particolari modalità di trasmissione.

4.1 Generalità

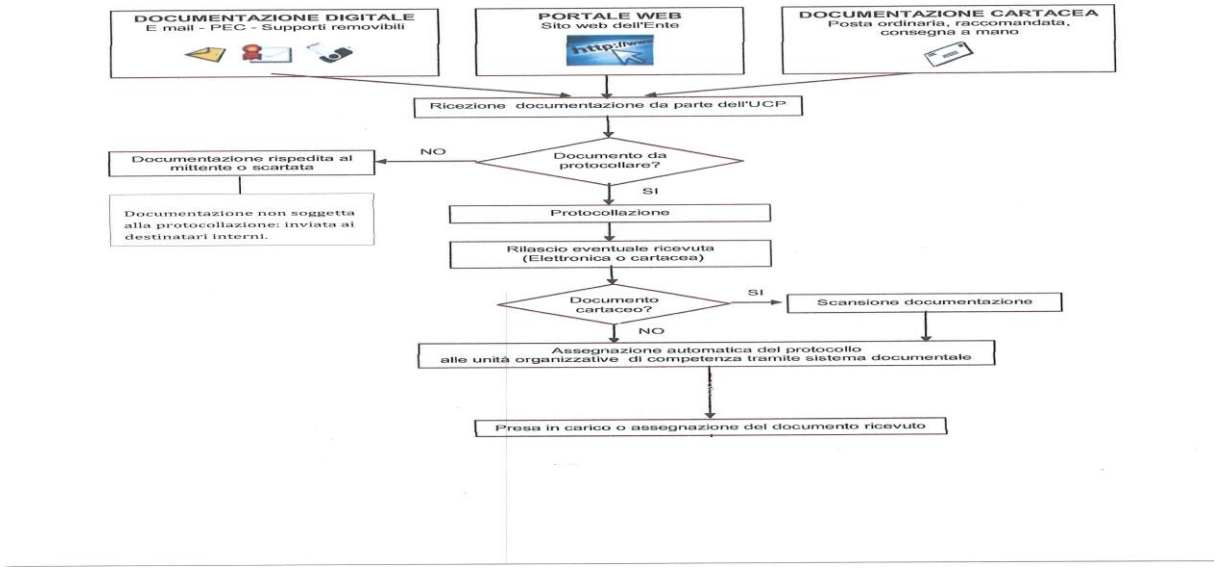
Per descrivere i flussi di lavorazione dei documenti all'interno della AOO si fa riferimento ai diagrammi di flussi riportati nelle pagine seguenti.

Essi si riferiscono, in particolare, ai documenti:

- ricevuti dalla AOO, dall'esterno

- inviati dalla AOO, all'esterno

4.2 Flusso dei documenti ricevuti dalla AOO



4.2.1 Ricezione di documenti informatici sulle caselle di posta elettronica certificata

Di norma la ricezione dei documenti informatici è assicurata tramite le caselle di posta elettronica certificata.

Ogni messaggio deve riferirsi a un solo documento. Anche nel caso in cui vengano inviati contestualmente più documenti si attribuisce all'invio un unico numero di protocollo e una unica classificazione.

Quando i documenti informatici pervengono all'ufficio protocollo si procede alla registrazione di protocollo.

L'operazione di ricezione dei documenti informatici avviene con le modalità previste dalle regole tecniche vigenti recanti standard del formato dei documenti, modalità di trasmissione, definizioni dei tipi di informazioni minime ed accessorie e associate ai documenti protocollati.

Per motivi di gestione documentale a norma, di sicurezza informatica e compliance privacy, l'Ente non accetta, per l'acquisizione al protocollo generale, la trasmissione formale di documenti attraverso link di file sharing (quali ad esempio Dropbox, WeTransfer ecc.). Eventuale documentazione trasmessa tramite i suddetti link sarà considerata come non pervenuta.

I documenti ricevuti per via telematica sono resi disponibili ai destinatari interni attraverso il sistema di gestione documentale adottato dall'Ente subito dopo le operazioni di protocollazione e di classificazione.

4.2.2 Ricezione di documenti informatici sulla casella di posta elettronica non istituzionale

Nel caso in cui un messaggio venga ricevuto su una casella di posta elettronica non istituzionale e il titolare della casella ritenga che il documento debba essere protocollato, tale messaggio viene autonomamente protocollato dal servizio con l'indicazione degli uffici destinatari. L'Ufficio Protocollo sarà sempre tra i destinatari.

I documenti pervenuti tramite fax server a indirizzi diversi da quello assegnato al Protocollo sono trattati con gli stessi criteri indicati per la posta elettronica tradizionale. È intendimento dell'Amministrazione sostituire i fax tradizionali con i fax management.

A ogni messaggio di posta elettronica corrisponde una unica operazione di registrazione di protocollo. Quest'ultima si può riferire sia al corpo del messaggio, sia a uno o più file allegati.

4.2.3 Ricezione di documenti informatici su supporti rimovibili

I documenti digitali possono essere recapitati su supporti rimovibili. L' AOO si riserva la facoltà di acquisire e trattare tutti i documenti informatici ricevuti su supporto rimovibile nei casi in cui sia possibile verificare la provenienza e decodificare e/o interpretare la documentazione con le tecnologie a sua disposizione.

4.2.4 Ricezione di documenti cartacei a mezzo servizio postale (posta ordinaria e raccomandata), corriere o consegna a mano

I documenti pervenuti a mezzo posta convenzionale o tramite corriere sono consegnati all'ufficio protocollo nei giorni lavorativi. I documenti consegnati a mano ai vari uffici sono verificati e protocollati direttamente dall'ufficio ricevente nel caso in cui sia abilitato alle attività di protocollazione in entrata; nel caso contrario saranno consegnati all'ufficio protocollo per la protocollazione e per l'inserimento nel sistema di gestione documentale.

La corrispondenza cartacea relativa a bandi di gara è registrata con scansione della busta e annotazione dell'orario preciso di ricezione ove richiesto e successivamente consegnata in busta chiusa all'ufficio responsabile della gara.

La corrispondenza nominativa che dovesse pervenire al protocollo con la dicitura "personale" o "riservata", non viene aperta né protocollata bensì consegnata al destinatario per la valutazione del contenuto. Nel caso in cui dovesse riguardare l'Ente, il documento torna all'ufficio protocollo per l'eventuale protocollazione.

Quando la corrispondenza non rientri nelle categorie da ultimo indicate, si procede all'apertura delle buste e si eseguono gli ulteriori controlli preliminari alla registrazione. La corrispondenza in arrivo è aperta il giorno lavorativo in cui è pervenuta, e protocollata nel più breve tempo possibile.

4.2.5 Corrispondenza di particolare rilevanza, anonimi e documenti esclusi

Sono esclusi dalla registrazione di protocollo i seguenti documenti:

- bollettini ufficiali, notiziari della pubblica amministrazione;

- note di ricezione delle circolari e altre disposizioni;

- materiale statistico e promozionale;

- atti preparatori interni;

- giornali, riviste, materiale pubblicitario, inviti a manifestazioni, stampe varie, plichi di libri e tutti i documenti che per loro natura non rivestono alcuna rilevanza giuridico - amministrativa presente o futura;

Altre categorie documentali potranno essere escluse dalla protocollazione, su disposizione del Responsabile della gestione documentale e del Servizio di Protocollo informatico debitamente comunicata a tutti gli interessati.

Al di fuori di queste categorie, non sono ammesse eccezioni all'obbligo di protocollazione, segnatura e corretta gestione dei documenti.

4.2.6 Errata ricezione di documenti

Nel caso in cui pervengano erroneamente all'Ente documenti indirizzati ad altre Amministrazioni o soggetti, si contattano i destinatari in indirizzo e si riconsegna il documento se cartaceo, se il documento è digitale si comunica al mittente dell'avvenuta protocollazione ma dell'impossibilità di proseguire l'iter per non competenza dell'Ente.

4.2.7 Rilascio di ricevute attestanti l'avvenuta protocollazione di documenti informatici

La ricezione di documenti attraverso le caselle di posta elettronica certificata comporta automaticamente la notifica al mittente dell'avvenuto recapito al destinatario, assicurata dallo stesso servizio di posta certificata.

4.2.8 Rilascio di ricevute attestanti la ricezione di documenti cartacei

Quando il documento cartaceo è consegnato direttamente dal mittente o da altra persona incaricata al protocollo, è previsto il rilascio di una ricevuta attestante l'avvenuta consegna consistente nella fotocopia della sola prima pagina dell'istanza sulla quale viene posto un timbro con la data di arrivo. Qualora l'utente richieda il rilascio della ricevuta dell'avvenuta protocollazione, una volta effettuata la protocollazione l'ufficio rilascia una ricevuta generata dal sistema di protocollo recante data, numero di protocollo e assegnatari dello stesso.

4.2.9 Classificazione, assegnazione e presa in carico dei documenti

L'assegnazione viene fatta valutando il contenuto del documento nella sua totalità (compresi eventuali messaggio .eml, lettera di trasmissione, allegati, ecc.).

Qualora il mittente abbia indicato espressamente i nominativi dei destinatari, l'assegnazione tende a seguire la volontà manifesta del mittente, tranne nei casi in cui appaia opportuna una diversa e/o più ampia assegnazione (es: evidenti errori nell'identificazione dei destinatari, casi particolari per cui l'assegnazione di certe tipologie di pratiche sia stata richiesta, per iscritto, da uffici o assessorati, ecc.).

Una volta protocollata, attraverso il flusso documentale gestito dall'applicativo, il documento viene recapitato ai destinatari identificati dal protocollatore.

In caso di errore, nel minor tempo possibile si ritrasmette il documento al protocollatore.

Il flusso documentale dell'Ente è unico e va gestito esclusivamente attraverso l'applicativo in dotazione. Al fine di preservare la continuità del flusso, non è consentito lo scambio di documentazione protocollata attraverso le e-mail.

Tutti i documenti ricevuti dall'AOO per via telematica, o comunque disponibili in formato digitale, sono assegnati al servizio competente attraverso il sistema di gestione documentale.

I documenti ricevuti dall'amministrazione in formato cartaceo, di regola acquisiti in formato immagine o altro formato standard non modificabile con l'ausilio di scanner, una volta concluse le operazioni di registrazione, segnatura e assegnazione sono fatti pervenire al Servizio di competenza per via informatica attraverso il sistema di gestione documentale. Tali scansioni del documento possono essere parziali (limitandosi alla sola lettera di trasmissione, istanza…) oppure integrali. L'originale cartaceo viene anch'esso trasmesso al servizio, nell'ambito della gestione giornaliera della posta cartacea interna.

4.3 Flusso dei documenti creati e trasmessi dall'AOO

4.3.1 Sorgente interna dei documenti

Per documenti in partenza s'intendono quelli prodotti dal personale degli uffici dell'AOO nell'esercizio delle proprie funzioni, aventi rilevanza giuridico - probatoria e destinati ad essere trasmessi a soggetti esterni all'Ente.

Il documento viene predisposto in formato digitale, secondo gli standard illustrati nei precedenti capitoli, e inviato tramite posta elettronica certificata (la posta elettronica certificata è la modalità di inoltro dell'applicativo in uso). I documenti vengono prodotti con il sistema documentale in dotazione all'Ente.

Per i documenti che devono necessariamente essere inviati in formato analogico, il mezzo di recapito della corrispondenza è tipicamente costituito dal servizio postale, nelle sue diverse forme.

4.3.2 Verifica formale dei documenti

Il personale interno all'Ente registrato sull'applicativo di gestione del flusso documentale è autorizzato dal Direttore/Responsabile della gestione documentale e del Servizio di Protocollo informatico a svolgere attività di registrazione di protocollo e provvedere a tutte le verifiche necessarie per la trasmissione della documentazione predisposta che verrà effettuata dall'Ufficio Protocollo.

4.3.3 Registrazione di protocollo e segnatura

La protocollazione e la segnatura della corrispondenza in partenza, sia essa in formato digitale che in formato analogico, è effettuata direttamente dai singoli servizi abilitati, in quanto collegati al sistema di protocollo informatico della AOO.

4.3.4 Trasmissione di documenti informatici

I documenti informatici sono trasmessi all'indirizzo elettronico dichiarato dai destinatari, ovvero abilitato alla ricezione della posta per via telematica.

Per la spedizione dei documenti informatici, l'AOO si avvale di un servizio di "Posta Elettronica Certificata", conforme al decreto del Presidente della Repubblica 11 febbraio 2005, n. 68,

offerto da un soggetto esterno in grado di garantire la sicurezza del canale di comunicazione, e di dare certezza sulla data di spedizione e di consegna dei documenti attraverso una procedura di rilascio di ricevute di ritorno elettroniche. In particolare, la PEC è strumento ordinario di trasmissione verso le pubbliche amministrazioni ed i gestori di pubblici servizi, i cittadini che hanno dichiarato il loro domicilio digitale, nonché verso i soggetti inseriti nell'Indice nazionale degli indirizzi PEC delle imprese e dei professionisti, o in altri indici analoghi che si rendessero disponibili in futuro.

In caso di più destinatari riferiti a un unico numero di protocollo, si generano tante PEC quanti sono i destinatari.

Nel caso di trasmissione di allegati al documento che eccedano la capienza della casella di posta elettronica, è possibile utilizzare supporti rimovibili o avvalersi di adeguati canali telematici alternativi.

La trasmissione telematica di comunicazioni che necessitano di una ricevuta di invio e di una ricevuta di consegna avviene sempre, ove tecnicamente possibile, mediante posta elettronica certificata, con effetto equivalente alla notificazione per mezzo della posta raccomandata.

Gli allegati inseriti sull'applicativo dovranno essere in uno dei formati riportati negli Allegati 3 e Allegato 5 (Manuale di conservazione), preferibilmente in Pdf/A.

4.3.5 Trasmissione di documenti cartacei a mezzo posta

L'ufficio protocollo gestisce le operazioni di spedizione della corrispondenza predisposta dagli uffici/servizi.

Gli uffici/servizi consegnano al protocollo i plichi da spedire in tempo utile per consentire di organizzare al meglio la gestione. L'ufficio protocollo verifica i destinatari delle lettere da affrancare e rimanda agli uffici quelle che sono in modo evidente indirizzate ad altre pubbliche amministrazioni, a imprese e professioni di cui è possibile reperire l'indirizzo pec da questi dichiarato, al fine di contenere le spese di spedizione e di implementare nel modo più completo possibile il fascicolo digitale del procedimento amministrativo.

4.3.6 Conteggi e spedizione corrispondenza cartacea

L'ufficio protocollo effettua i conteggi relativi alle spese sostenute per le operazioni di invio della corrispondenza cartacea e cura il costante monitoraggio della spesa interagendo strettamente con l'Economo aziendale, presente nel medesimo ufficio.

4.4 Documenti informali

Si considerano documenti informali quelli che non assumono rilievo all'interno di procedimenti (informazioni etc).

Gli scambi di documenti informali all'interno dell'AOO o verso l'esterno, non danno luogo a protocollazione.

5 GESTIONE DELLE REGISTRAZIONI DI PROTOCOLLO

Il presente capitolo illustra le modalità di produzione delle registrazioni di protocollo informatico, nonché le modalità di registrazione delle informazioni annullate o modificate nell'ambito di ogni sessione di attività di registrazione.

5.1 Unicità del protocollo informatico

Nell'ambito della AOO il registro di protocollo è unico e la numerazione progressiva delle registrazioni di protocollo è unica indipendentemente dal modello organizzativo.

La numerazione si chiude al 31 dicembre di ogni anno e ricomincia dal primo gennaio dell'anno successivo.

Il numero di protocollo individua un unico documento e, di conseguenza, ogni documento reca un solo numero di protocollo. Il numero di protocollo è costituito da almeno sette cifre numeriche.

Non è consentita l'identificazione dei documenti mediante l'assegnazione manuale di numeri di protocollo che il sistema informatico ha già attribuito ad altri documenti, anche se questi documenti sono strettamente correlati tra loro. Non è pertanto consentita in nessun caso la cosiddetta registrazione "a fronte", cioè l'utilizzo di un unico numero di protocollo per il documento in arrivo e per il documento in partenza.

La documentazione che non è stata registrata sul protocollo viene considerata giuridicamente inesistente presso l'amministrazione, fatta eccezione per quella soggetta a registrazione particolare.

Non è consentita la protocollazione di un documento già protocollato (doppio protocollo ad uno stesso documento). Qualora ciò avvenisse per errore, la seconda protocollazione va annullata.

Il registro di protocollo è il registro informatico di atti e documenti in ingresso e in uscita che permette la registrazione e l'identificazione univoca del documento informatico all'atto della sua immissione cronologica nel sistema di gestione informatica dei documenti. Di fatto è un atto pubblico munito di fede privilegiata ed è idoneo a produrre effetti giuridici.

Il registro giornaliero di protocollo è trasmesso entro la giornata lavorativa successiva al sistema di conservazione, garantendone l'immodificabilità del contenuto.

5.2 Registrazione di protocollo

Di seguito vengono illustrate le regole di registrazione del protocollo valide per tutti i tipi di documenti trattati dall'AOO (ricevuti, trasmessi ed interni formali, digitali o informatici e analogici).

Su ogni documento ricevuto o spedito dall'AOO è effettuata una registrazione di protocollo con il sistema di gestione del protocollo informatico, consistente nella memorizzazione dei dati obbligatori.

Tale registrazione è eseguita in un'unica operazione, senza possibilità per l'operatore di inserire le informazioni in più fasi successive.

Ciascuna registrazione di protocollo contiene, almeno, i seguenti dati obbligatori:

- il numero di protocollo, generato automaticamente dal sistema e registrato in forma non modificabile;

- la data di registrazione di protocollo, assegnata automaticamente dal sistema e registrata in forma non modificabile;

- l'indicazione del mittente o del destinatario, registrata in forma non modificabile;

- l'oggetto del documento, registrato in forma non modificabile;

- la data e protocollo del documento ricevuto, se disponibili;

L'oggetto di un protocollo deve descrivere il contenuto della documentazione trattata in maniera chiara e sintetica, riportando "parole chiave" che consentano in futuro di effettuare una ricerca. L'oggetto è la sintesi dei contenuti di carattere giuridico, amministrativo e narrativo di un documento. Oltre a costituire un elemento indispensabile per la ricerca del documento, l'oggetto contribuisce a identificarlo e a definirne la relazione con il fascicolo a cui appartiene.
L'oggetto di un documento in lingua straniera si riporta per esteso nella lingua originale seguito dalla descrizione in lingua italiana.
L'oggetto non deve contenere riferimenti normativi muti o richiami non espliciti: I riferimenti normativi non possono da soli costituire l'oggetto del documento, semmai ne formano il presupposto. Non è corretto, quindi, redigere l'oggetto di un documento limitandosi a richiamare un riferimento normativo senza ulteriori specificazioni Il semplice rinvio a norme – talvolta anche in modo incompleto, citando cioè solo il numero o la data – di solito non fornisce alcuna informazione sul reale contenuto del documento, al pari delle sigle e degli acronimi che non vengano opportunamente sciolti.

5.3 Elementi facoltativi delle registrazioni di protocollo

Il Direttore/Responsabile del Servizio Protocollo, con proprio provvedimento e al fine di migliorare la gestione, la ricerca e la conservazione della documentazione, può modificare e integrare gli elementi facoltativi del protocollo, anche per singole categorie o tipologie di documenti.

5.4 Segnatura di protocollo dei documenti (Sigillo Elettronico)

L'operazione di segnatura di protocollo è effettuata contemporaneamente all'operazione di registrazione di protocollo.

La segnatura di protocollo è l'apposizione o l'associazione all'originale del documento, in forma permanente non modificabile, delle informazioni riguardanti il documento stesso. Essa consente di individuare ciascun documento in modo inequivocabile.

Le informazioni previste sono:

- l'identificazione in forma sintetica o estesa dell'amministrazione e dell'area organizzativa omogenea (AOO) individuata ai fini della registrazione e della gestione documentale;

- il codice identificativo dell'amministrazione;

- il codice identificativo del registro di protocollo;

- titolo e classe di riferimento;

- il numero progressivo di protocollo, costituito da almeno sette cifre numeriche

- la data di protocollo

Per i documenti analogici le informazioni sopra riportate vengono riportate sul documento attraverso il timbro di registratura di protocollo.

Per i documenti informatici tutte le informazioni sopra riportate sono generate automaticamente dal sistema e sono incluse nella segnatura informatica di ciascun messaggio protocollato

5.5 Modifiche e annullamento delle registrazioni di protocollo

Il Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013, all'art. 8, comma 2, dispone che:
2. L'annullamento anche di un solo campo delle altre informazioni registrate in forma immodificabile, necessario per correggere errori intercorsi in sede di immissione di dati delle altre informazioni, deve comportare la rinnovazione del campo stesso con i dati corretti e la contestuale memorizzazione, in modo permanente, del valore precedentemente attribuito unitamente alla data, l'ora e all'autore della modifica. La disposizione di cui al primo periodo si applica per lo stesso campo, od ogni altro, risultato successivamente errato.

Le informazioni relative alla registrazione di protocollo modificata o annullata rimangono memorizzate nel registro informatico del protocollo per essere sottoposte alle elaborazioni previste dalla procedura, ivi comprese le visualizzazioni e le stampe, insieme a data, ora e autore dell'annullamento e agli estremi dell'autorizzazione all'annullamento del protocollo.

Solo il Direttore/Responsabile della gestione documentale e del Servizio di Protocollo informatico e l'Ufficio Protocollo debitamente incaricato, è autorizzato ad annullare, direttamente, una registrazione di protocollo.

5.6 Protocollazione documenti interni formali – protocolli interni

I documenti formali prodotti e scambiati internamente sono soggetti a protocollazione e indicati come protocolli interni, se necessario per proseguire un iter procedurale.

5.7 Registrazione differita di protocollo

Per *"protocollo differito"* si intende la registrazione di documento in arrivo che indica nello specifico la data alla quale si riferisce il ricevimento del documento stesso e la causa che ne ha determinato il differimento. (es: concorsi, gare e più in generale tutto ciò che ha una scadenza).

Il documento in argomento viene comunque protocollato inserendo la data di ricezione (che sarà diversa da quella della protocollazione) e la motivazione per cui è stato protocollato successivamente al suo ingresso nell'Ente.

5.8 Documenti riservati (Protocollo riservato)

Sono previste particolari forme di riservatezza per i documenti relativi a procedimenti disciplinari nei confronti dei dipendenti, vicende o a fatti privati, politici o giudiziari (giudizi pendenti) o documenti che richiedono, comunque, una trattazione riservata. Per tali atti sul registro di protocollo generale compare solo il numero attribuito a ciascun documento e l'annotazione "Riservato", "Secretato" o "Sensibile".

I documenti registrati con tali forme appartengono al cosiddetto "protocollo riservato" costituito dalle registrazioni il cui accesso è autorizzato solo alle persone espressamente abilitate. Queste ultime hanno comunque la visibilità dei soli documenti riservati trattati dall'unità di appartenenza. Le procedure adottate per la gestione dei documenti ad accesso riservato, comprese le registrazioni, la segnatura, la classificazione e la fascicolazione, sono le stesse adottate per gli altri documenti.

Qualora nella formulazione dell'oggetto del documento fosse necessario introdurre elementi riconducibili a dati "*sensibili*", è opportuna l'indicazione della persona fisica direttamente interessata con le iniziali puntate di cognome e nome (senza spazio fra le iniziali) sia nell'oggetto sia nel campo mittente.

6 IL SISTEMA DI GESTIONE DOCUMENTALE E DI PROTOCOLLAZIONE ADOTTATO DALL'ENTE

Il sistema di gestione documentale e di protocollazione adottato dall'Ente è basato su applicativo software.

La soluzione per la protocollazione prevede un modulo specifico che gestisce tutte le fasi di protocollazione in arrivo/ partenza nonché di registro interno pratiche in modo totalmente integrato con il sistema documentale.

La soluzione gestisce la ricezione e trasmissione dei messaggi informatici con la protocollazione e l'archiviazione nel sistema documentale in modo sicuro e non modificabile.

I documenti pervenuti vengono assegnati agli uffici ed operatori destinatari e vengono tracciati nell'iter burocratico/ flusso documentale.

I documenti prodotti dall'Ente vengono gestiti nell'ambito del sistema documentale sia nella fase di redazione che in quella di archiviazione, di protocollazione e di trasmissione.

6.1 Descrizione funzionale ed operativa

La descrizione funzionale ed operativa del sistema di protocollo informatico viene specificata in dettaglio all'interno dell'Allegato 4.

7 SICUREZZA

La sicurezza e l'integrità dei dati di protocollo e dei documenti elettronici archiviati sono garantiti dall'applicazione informatica adottata dall'Ente.

Il piano di sicurezza informatica del sistema informativo dell'amministrazione è definito dall'organizzazione dell'Ente che gestisce il sistema informatico generale.

Il presente capitolo riporta le misure di sicurezza adottate specifiche per l'infrastruttura di protocollo informatico anche in relazione alle norme sulla protezione dei dati personali.

7.1 Obiettivi

La politica in merito alla sicurezza di questo Ente è finalizzata a assicurare che:

- i documenti e le informazioni trattati dall'amministrazione/AOO siano resi disponibili, integri e riservati;

- i dati personali, compresi i dati sensibili, vengano custoditi in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta, in relazione alle conoscenze acquisite in base al progresso tecnico, alla loro natura e alle specifiche caratteristiche del trattamento.

A tale fine l'Ente definisce:

- le politiche generali e particolari di sicurezza da adottare all'interno della AOO;

- le modalità di accesso al servizio di protocollo, di gestione documentale ed archivistico;

- gli interventi operativi adottati sotto il profilo organizzativo, procedurale e tecnico, con particolare *riferimento alle misure minime di sicurezza,* di cui al disciplinare tecnico richiamato nell'Allegato B) del regolamento UE 679/2016 e smi – Regolamento europeo in materia di protezione dei dati personali, in caso di trattamento di dati personali;

- i piani specifici di formazione degli addetti;

- le modalità con le quali deve essere effettuato il monitoraggio periodico dell'efficacia e dell'efficienza delle misure di sicurezza.

Il Responsabile dei Servizi ICT del Comune di Alessandria incaricato dall'Ente Costruire Insieme, identifica le misure tecniche e organizzative di seguito specificate, al fine di assicurare la sicurezza dell'impianto tecnologico dell'AOO, la riservatezza delle informazioni registrate nelle banche dati, l'univoca identificazione degli utenti interni ed esterni:

- protezione periferica della Intranet dell'amministrazione/AOO;

- protezione dei sistemi di accesso e conservazione delle informazioni;

- assegnazione ad ogni utente del sistema di gestione del protocollo e dei documenti, di una credenziale di identificazione pubblica (user ID), di una credenziale riservata di autenticazione (password) e di un profilo di autorizzazione;

- cambio delle password con frequenza prestabilita durante la fase di esercizio;

- piano di continuità del servizio con particolare riferimento, sia alla esecuzione e alla gestione delle copie di riserva dei dati e dei documenti da effettuarsi con frequenza giornaliera, sia alla capacità di ripristino del sistema informativo in caso di disastro;

- conservazione delle copie di riserva dei dati e dei documenti, in locali diversi e se possibile lontani da quelli in cui è installato il sistema di elaborazione di esercizio che ospita l'applicativo di gestione del Protocollo;

- impiego e manutenzione di un adeguato sistema antivirus e di gestione dei "moduli" (patch e service pack) correttivi dei sistemi operativi;

- cifratura o uso di codici identificativi (o altre soluzioni ad *es. separazione della parte anagrafica da quella "sensibile*") dei dati sensibili e giudiziari contenuti in elenchi, registri o banche di dati, tenuti con l'ausilio di strumenti elettronici, allo scopo di renderli temporaneamente inintelligibili anche a chi è autorizzato ad accedervi e permettendo di identificare gli interessati solo in caso di necessità;

- impiego delle misure precedenti anche nel caso di supporti cartacei di banche dati idonee a rilevare lo stato di salute e la vita sessuale;

- archiviazione giornaliera, in modo non modificabile, delle copie del registro di protocollo;

- conservazione dei file di log di sistema, di rete e applicativo contenenti le informazioni sulle operazioni effettuate da ciascun utente durante l'arco della giornata, comprese le operazioni di backup e manutenzione del sistema. I dati personali registrati nel log del sistema operativo, del sistema di controllo degli accessi e delle operazioni svolte con il sistema di protocollazione e gestione dei documenti utilizzato saranno consultati solo in caso di necessità dal Responsabile del Servizio Protocollo e dal titolare dei dati con la supervisione e il supporto tecnico del Responsabile della sicurezza informatica e, ove previsto, dalle Forze dell'Ordine.

7.2 Credenziali di accesso al sistema documentale

Il controllo degli accessi è il processo che garantisce l'impiego degli oggetti/servizi del sistema informatico di gestione documentale e protocollo informatico nel rispetto di modalità prestabilite.

Il processo è caratterizzato da utenti che accedono ad oggetti informatici (applicazioni, dati, programmi) mediante operazioni specifiche (lettura, aggiornamento, esecuzione).

Gli utenti del programma di gestione documentale e protocollo, in base alle rispettive competenze, dispongono di autorizzazioni di accesso differenziate.

Ad ogni utente è assegnata:

- una credenziale di accesso, costituita da una componente pubblica che permette l'identificazione dell'utente da parte del sistema (userID), e da una componente privata o riservata di autenticazione (password);

- una autorizzazione di accesso (profilo) che limita le operazioni di protocollo, gestione documentale e work flow effettuabili alle sole funzioni necessarie.

La visibilità normalmente attribuita ad un utente si limita alla documentazione relativa ai servizi di competenza. La visibilità su altri documenti può essere attribuita dal Direttore.

L'accesso diretto alla banca dati, l'inserimento di nuovi utenti, la modifica dei diritti e le impostazioni sui documenti sono consentiti esclusivamente agli amministratori del sistema identificato nella figura del Dirigente dei Servizi ICT del Comune di Alessandria.

I diversi livelli di autorizzazione sono assegnati agli utenti dal Direttore/Responsabile della gestione documentale, in base alle indicazioni fornite dai Responsabili dei servizi di appartenenza.

7.3 Sicurezza nella formazione dei documenti

Le risorse strumentali e le procedure utilizzate per la formazione dei documenti informatici garantiscono:

- l'identificabilità del soggetto che ha formato il documento e il servizio di riferimento;

- la sottoscrizione dei documenti informatici, quando prescritta, con firma digitale ai sensi delle vigenti norme tecniche;

- l'idoneità dei documenti ad essere gestiti mediante strumenti informatici e ad essere registrati mediante il protocollo informatico;

- l'accesso ai documenti informatici tramite sistemi informativi automatizzati;

- la leggibilità dei documenti nel tempo;

- l'interscambiabilità dei documenti all'interno dello stesso Ente/AOO.

I documenti sono prodotti con l'ausilio dell'applicativo specificato nell'Allegato 4 che possiede i requisiti di leggibilità, interscambiabilità, non alterabilità, immutabilità nel tempo del contenuto e della struttura.

Si adottano preferibilmente i formati PDF/A, XML, TIFF. I documenti informatici prodotti dall'AOO con altri prodotti di *text editor* sono convertiti, prima della loro sottoscrizione con firma digitale, nei formati standard (PDF/A, XML e TIFF) come previsto dalle regole tecniche per la conservazione dei documenti, al fine di garantire la leggibilità per altri sistemi, la non alterabilità durante le fasi di accesso e conservazione e l'immutabilità nel tempo del contenuto e della struttura del documento.

Per attribuire in modo certo la titolarità del documento, la sua integrità e, se del caso, la riservatezza, il documento è sottoscritto con firma digitale.

Per attribuire una data certa a un documento informatico prodotto all'interno della AOO, si applicano le regole per la validazione temporale e per la protezione dei documenti informatici.

L'esecuzione del processo di marcatura temporale avviene utilizzando le procedure previste dal certificatore accreditato, con le prescritte garanzie di sicurezza; i documenti così formati, prima di essere inviati a qualunque altra stazione di lavoro interna all'AOO, sono sottoposti ad un controllo antivirus centralizzato onde eliminare qualunque forma di contagio che possa arrecare danno diretto o indiretto all'amministrazione/AOO.

7.4 Trasmissione ed interscambio dei documenti informatici

Gli addetti alle operazioni di trasmissione per via telematica di atti, dati e documenti formati con strumenti informatici non possono prendere cognizione della corrispondenza telematica, duplicare con qualsiasi mezzo o cedere a terzi, a qualsiasi titolo, informazioni anche in forma sintetica o per estratto sull'esistenza o sul contenuto di corrispondenza, comunicazioni o messaggi trasmessi per via telematica, salvo che si tratti di informazioni che, per loro natura o per espressa indicazione del mittente, sono destinate ad essere rese pubbliche.

Al fine di tutelare la riservatezza dei dati personali, i dati, i certificati ed i documenti trasmessi all'interno della AOO o ad altre pubbliche amministrazioni, contengono soltanto le informazioni

relative a stati, fatti e qualità personali di cui è consentita la diffusione e che sono strettamente necessarie per il perseguimento delle finalità per le quali vengono trasmesse.

Il server di posta certificata del fornitore esterno (*provider*) di cui si avvale l'Ente, oltre alle funzioni di un server SMTP tradizionale, svolge anche le seguenti operazioni:

- accesso all'indice dei gestori di posta elettronica certificata allo scopo di verificare l'integrità del messaggio e del suo contenuto;

- tracciamento delle attività nel file di log della posta;

- gestione automatica delle ricevute di ritorno.

Lo scambio per via telematica di messaggi protocollati tra AOO di amministrazioni diverse presenta, in generale, esigenze specifiche in termini di sicurezza, quali quelle connesse con la protezione dei dati personali, sensibili e/o giudiziari come previsto dal regolamento UE 679/2016 GDPR.

7.5 Accesso ai documenti informatici

Il controllo degli accessi è assicurato utilizzando le credenziali di accesso ed un sistema di autorizzazione basato sulla profilazione degli utenti in via preventiva.

La profilazione preventiva consente di definire le abilitazioni/ autorizzazioni che possono essere effettuate/rilasciate ad un utente del servizio di protocollo e gestione documentale.

Ciascun utente dell'applicativo di gestione del Protocollo può accedere solamente ai documenti che sono stati assegnati al suo Servizio/Unità Organizzativa (UO).

Il sistema consente altresì di associare un livello differente di riservatezza per ogni tipo di documento trattato dall'amministrazione. I documenti non vengono mai visualizzati dagli utenti privi di diritti di accesso, neanche a fronte di una ricerca generale nell'archivio.

8 NORME TRANSITORIE E FINALI

8.1 Modalità di approvazione e aggiornamento del manuale

L'Ente adotta il "Manuale di gestione" che sarà aggiornato a seguito di:

- normativa sopravvenuta;

- introduzione di nuove pratiche tendenti a migliorare l'azione amministrativa in termini di efficacia, efficienza e trasparenza;

- inadeguatezza delle procedure rilevata nello svolgimento delle attività correnti;

- introduzione di nuove procedure

Il Manuale viene approvato e modificato con deliberazione del Consiglio di Amministrazione.

8.2 Pubblicità del manuale

Il Manuale, a norma dell'art. art.15 della legge n. 15 del 2005, è reso disponibile alla consultazione del pubblico che ne può prendere visione in qualsiasi momento.

Inoltre copia del presente Manuale è:

- pubblicata sul sito internet nella sezione di Amministrazione Trasparente

- resa disponibile a tutto il personale dell'Ente;

- inviata al Revisore dei Conti;

8.3 Entrata in vigore

Il presente documento diventa efficace a seguito di approvazione da parte del Consiglio Di Amministrazione.

Allegato 1

al manuale di gestione del protocollo informatico,
dei flussi documentali e degli archivi

Glossario e definizioni

Definizioni

Ai fini del presente Manuale si intende:

- per “C.A.D.”, il decreto legislativo 7 marzo 2005 n. 82 – Codice dell’amministrazione digitale, nel testo vigente.

- per “Regole tecniche”, il decreto del Presidente del Consiglio dei Ministri 03 dicembre 2013 – Regole tecniche per il protocollo informatico ai sensi dell’artt. 40-bis, 41, 47, 57-bis e 71, del C.A.D. di cui D.L. 82/2005.

Si riportano, di seguito, gli acronimi utilizzati più frequentemente:

AOO - Area Organizzativa Omogenea;

UO – Unità Organizzativa – unità organizzativa interna (settore, servizio, ufficio)

UOR - Uffici Organizzativi di Riferimento - un insieme di uffici che, per tipologia di mandato istituzionale e di competenza, di funzione amministrativa perseguita, di obiettivi e di attività svolta, presentano esigenze di gestione della documentazione in modo unitario e coordinato;

RSP - Responsabile della gestione documentale e del Servizio di Protocollo informatico;

Allegato 2

al manuale di gestione del protocollo informatico,
dei flussi documentali e degli archivi



Norme di riferimento

1. Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 “Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa”

2. Deliberazione AIPA n. 42 del 2001 “Regole tecniche per la riproduzione e conservazione di documenti su supporto ottico idoneo a garantire la conformità dei documenti agli originali - articolo 6, commi 1 e 2, del Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa, di cui al decreto del Presidente della Repubblica 28 dicembre 2000, n. 445”

3. Decreto del Presidente della Repubblica 07 aprile 2003, n. 137 “Regolamento recante disposizioni di coordinamento in materia di firme elettroniche a norma dell'articolo 13 del d.lgs. 23 gennaio 2002, n. 10”

4. Decreto del Presidente del Consiglio dei Ministri 13 gennaio 2004 “Regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici.”

5. Deliberazione CNIPA n. 11/2004 del 19 febbraio 2004 “Regole tecniche per la riproduzione e conservazione di documenti su supporto ottico idoneo a garantire la conformità dei documenti agli originali- Art. 6, commi 1 e 2, del testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa, di cui al decreto del Presidente della Repubblica 28 dicembre 2000, n. 445“

6. Decreto del Presidente della Repubblica 11 febbraio 2005, n.68 “Regolamento recante disposizioni per l'utilizzo della posta elettronica certificata, a norma dell'art. 27 della legge 16 gennaio 2003, n. 3”

7. Decreto legislativo 07 marzo 2005 n. 82 “Codice dell’amministrazione digitale (C.A.D.)”

8. Decreto del Presidente del Consiglio dei Ministri 30 marzo 2009 “Regole tecniche in materia di generazione, apposizione e verifica delle firme digitali e validazione temporale dei documenti informatici”

9. Deliberazione CNIPA 21 maggio 2009, n. 45 “Regole per il riconoscimento e la verifica del documento informatico”

10. Decreto Legge n. 5 del 09 febbraio 2012 “Disposizioni urgenti in materia di semplificazione e di sviluppo”

11. Decreto del Presidente del Consiglio dei Ministri 22 febbraio 2013 “Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali, ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma 3, lettera b), 35, comma 2, 36, comma 2, e 71“

12. Decreto del Presidente del Consiglio dei Ministri 21 marzo 2013 “Individuazione di particolari tipologie di documenti analogici originali unici per le quali, in ragione di esigenze di natura pubblicistica, permane l'obbligo della conservazione dell'originale analogico oppure, in caso di conservazione sostitutiva, la loro conformità all'originale deve essere autenticata da un notaio o da altro pubblico ufficiale a ciò autorizzato con dichiarazione da questi firmata digitalmente ed allegata al documento informatico, ai sensi dell'art. 22, comma 5, del Codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82 e successive modificazioni”

13. Decreto del Presidente del Consiglio dei Ministri 03 dicembre 2013 “Regole tecniche per il protocollo informatico ai sensi dell’artt. 40-bis, 41, 47, 57-bis e 71, del C.A.D. di cui D.L. 82/2005”

14. Circolare AgID n. 65 del 10 aprile 2014 “Modalità per l’accreditamento e la vigilanza sui soggetti pubblici e privati che svolgono attività di conservazione dei documenti informatici di cui all'articolo 44- bis, comma 1, del D.Lgs. 7 marzo 2005, n. 82“

15. Decreto del Presidente del Consiglio dei Ministri 14 novembre 2014 “Istituzione del tavolo tecnico dei soggetti aggregatori, ai sensi dell'articolo 9, comma 2, terzo periodo, del decreto-legge 24 aprile 2014, n. 66, convertito, con modificazioni, dalla legge 23 giugno 2014, n. 89, unitamente ai relativi elenchi recanti gli oneri informativi”

16. Regolamento UE n. 910/2014 sull’identità digitale -Regolamento eIDAS (electronic identification and trust services for electronic transactions in the internal market)

17. Decreto Legislativo 26 agosto 2016, n. 179 “Modifiche ed integrazioni al Codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82, ai sensi dell'articolo 1 della legge 7 agosto 2015, n. 124, in materia di riorganizzazione delle amministrazioni pubbliche”

18. Regolamento UE 679/2016 (Regolamento generale sulla protezione dei dati –GDPR)

Allegato 3

al manuale di gestione del protocollo informatico,
dei flussi documentali e degli archivi

I formati dei documenti

(Estratto dell'allegato 2 al D.P.C.M 3 dicembre 2013)

Indice

1 INTRODUZIONE

2 I FORMATI

2.1 Identificazione

2.2 Le tipologie di formato

2.3 Formati Immagini

2.3.1 Raster

2.3.2 Vettoriale

2.4 Altri Formati

2.5 Le caratteristiche generali dei formati

3 CRITERI DI SCELTA DEI FORMATI

3.1 Caratteristiche

3.1.1 Apertura

3.1.2 Sicurezza

3.1.3 Portabilità

3.1.4 Funzionalità

3.1.5 Supporto allo sviluppo

3.1.6 Diffusione

4 SCELTA

4.1 Formati e prodotti per la formazione e gestione

4.2 Formati per la conservazione

1 INTRODUZIONE

Il presente allegato fornisce indicazioni iniziali sui formati dei documenti informatici che per le loro caratteristiche sono, al momento attuale, da ritenersi coerenti con le regole tecniche del documento informatico, del sistema di conservazione e del protocollo informatico.

I formati descritti sono stati scelti tra quelli che possono maggiormente garantire i principi dell'interoperabilità tra i sistemi di conservazione e in base alla normativa vigente riguardante specifiche tipologie documentali.

Il presente allegato, per la natura stessa dell'argomento trattato, viene periodicamente aggiornato sulla base dell'evoluzione tecnologica e dell'obsolescenza dei formati, in base anche a quanto pubblicato online sul sito dell'Agenzia per l'Italia Digitale.

2 I FORMATI

La leggibilità di un documento informatico dipende dalla possibilità e dalla capacità di interpretare ed elaborare correttamente i dati binari che costituiscono il documento, secondo le regole stabilite dal formato con cui esso è stato rappresentato.

Il formato di un file è la convenzione usata per interpretare, leggere e modificare il file.

2.1 Identificazione

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

1. l'estensione: una serie di lettere, unita al nome del file attraverso un punto, ad esempio [nome del file].docx identifica un formato testo di proprietà della Microsoft;

2. I metadati espliciti: l'indicazione "application/ msword" inserita nei tipi MIME che indica un file testo realizzato con l'applicazione Word della Microsoft;

3. il *magic number*: i primi byte presenti nella sequenza binaria del file, ad esempio 0xffd8 identifica i file immagine di tipo .jpeg.

2.2 Le tipologie di formato

L'evolversi delle tecnologie e la crescente disponibilità e complessità dell'informazione digitale ha indotto la necessità di gestire sempre maggiori forme di informazione digitale (testo, immagini, filmati, ecc.) e di disporre di funzionalità più specializzate per renderne più facile la creazione, la modifica e la manipolazione.

Questo fenomeno porta all'aumento del numero dei formati disponibili e dei corrispondenti programmi necessari a gestirli nonché delle piattaforme su cui questi operano.

In particolare, volendo fare una prima sommaria, e non esaustiva, catalogazione dei più diffusi formati, secondo il loro specifico utilizzo possiamo elencare:

Testi/documenti (PDF, PDF/A, DOC, HTML,...)

Calcolo (XLS, ...)

Immagini (GIF, JPG, BMP, TIF, EPS, SVG, ...)

Suoni (MP3, WAV, ...)

Video (MPG, MPEG, AVI, WMV,...)

Eseguibili (EXE, ...)

Archiviazione e Compressione (ZIP, RAR, ...)

Formati email (SMTP/MIME, …)

2.3 Formati Immagini

Per la rappresentazione delle immagini sono disponibili diversi formati, che possono essere distinti secondo la grafica utilizzata: Raster o vettoriale.

2.3.1 Raster

Nel caso della grafica raster, l'immagine digitale è formata da un insieme di piccole aree uguali (pixel), ordinate secondo linee e colonne.

I formati più diffusi sono il .tiff (usato dai fax), il .jpg, il .bmp.

2.3.2 Vettoriale

La grafica vettoriale è una tecnica utilizzata per descrivere un'immagine mediante un insieme di primitive geometriche che definiscono punti, linee, curve e poligoni ai quali possono essere attribuiti colori e anche sfumature.

I documenti realizzati attraverso la grafica vettoriale sono quelli utilizzati nella stesura degli elaborati tecnici, ad esempio progetti di edifici.

Attualmente i formati maggiormente in uso sono:

- DWG, un formato proprietario per i file di tipo CAD, di cui non sono state rilasciate le specifiche;
- DXF, un formato simile al DWG, di cui sono state rilasciate le specifiche tecniche x Shapefile un formato vettoriale proprietario per sistemi informativi geografici (GIS) con la caratteristica di essere interoperabile con con i prodotti che usano i precedenti formati;
- SVG, un formato aperto, basato su XML, in grado di visualizzare oggetti di grafica vettoriale, non legato ad uno specifico prodotto.

2.4 Altri Formati

Per determinate tipologie di documenti informatici sono utilizzati specifici formati. In particolare in campo sanitario i formati più usati sono:

- DICOM (immagini che arrivano da strumenti diagnostici) anche se il DICOM non è solo un formato, ma definisce anche protocolli e altro;
- HL7 ed in particolare il CDA2 (Clinical Document Architecture) che contiene la sua stessa descrizione o rappresentazione.

  [..]

2.5 Le caratteristiche generali dei formati

L’informazione digitale è facilmente memorizzata, altrettanto facilmente è possibile accedere e riutilizzarla, modificarla e manipolarla, in altre parole, elaborarla ed ottenere nuova informazione.

Questi formati e i programmi che li gestiscono, che sono poi quelli che consentono e facilitano l’operatività giorno per giorno sul digitale, vanno valutati in funzione di alcune caratteristiche quali:

- La diffusione, ossia il numero di persone ed organizzazioni che li adotta
- La portabilità, ancor meglio se essa è indotta dall’impiego fedele di standard documentati e accessibili

- Le funzionalità che l'utente ha a disposizione per elaborare l'informazione e collegarla ad altre (ad esempio gestione di link)

- La capacità di gestire contemporaneamente un numero congruo (in funzione delle esigenze dell'utente) di formati

- La diffusione di visualizzatori che consentono una fruibilità delle informazioni in essi contenute indipendentemente dalla possibilità di rielaborarle.

Altre caratteristiche importanti sono la capacità di occupare il minor spazio possibile in fase di memorizzazione (a questo proposito vanno valutati, in funzione delle esigenze dell'utente, gli eventuali livelli di compressione utilizzabili) e la possibilità di gestire il maggior numero possibile di metadati, compresi i riferimenti a chi ha eseguito modifiche o aggiunte.

3 CRITERI DI SCELTA DEI FORMATI

Ai fini della formazione, gestione e conservazione, è necessario scegliere formati che possano garantire la leggibilità e la reperibilità del documento informatico nel suo ciclo di vita.

La scelta tra i formati dipende dalle caratteristiche proprie del formato e dei programmi che lo gestiscono.

3.1 Caratteristiche

Le caratteristiche di cui bisogna tener conto nella scelta sono:

1. apertura

2. sicurezza

3. portabilità

4. funzionalità

5. supporto allo sviluppo

6. diffusione

3.1.1 Apertura

Un formato si dice "aperto" quando è conforme a specifiche pubbliche, cioè disponibili a chiunque abbia interesse ad utilizzare quel formato. La disponibilità delle specifiche del formato rende sempre possibile la decodifica dei documenti rappresentati in conformità con dette specifiche, anche in assenza di prodotti che effettuino tale operazione automaticamente.

Questa condizione si verifica sia quando il formato è documentato e pubblicato da un produttore o da un consorzio al fine di promuoverne l'adozione, sia quando il documento è conforme a formati definiti da organismi di standardizzazione riconosciuti. In quest'ultimo caso tuttavia si confida che quest'ultimi garantiscono l'adeguatezza e la completezza delle specifiche stesse.

Nelle indicazioni di questo documento si è inteso privilegiare i formati già approvati dagli Organismi di standardizzazione internazionali quali ISO e ETSI.

3.1.2 Sicurezza

La sicurezza di un formato dipende da due elementi: il grado di modificabilità del contenuto del file e la capacità di essere immune dall'inserimento di codice maligno.

3.1.3 Portabilità

Per portabilità si intende la facilità con cui i formati possano essere usati su piattaforme diverse, sia dal punto di vista dell'hardware che del software, inteso come sistema operativo. Di fatto è indotta dall'impiego fedele di standard documentati e accessibili.

3.1.4 Funzionalità

Per funzionalità si intende la possibilità da parte di un formato di essere gestito da prodotti informatici, che prevedono una varietà di funzioni messe a disposizione dell'utente per la formazione e gestione del documento informatico.

3.1.5 Supporto allo sviluppo

E' la modalità con cui si mettono a disposizione le risorse necessarie alla manutenzione e sviluppo del formato e i prodotti informatici che lo gestiscono (organismi preposti alla definizione di specifiche tecniche e standard, società, comunità di sviluppatori, ecc.).

3.1.6 Diffusione

La diffusione è l'estensione dell'impiego di uno specifico formato per la formazione e la gestione dei documenti informatici,

Questo elemento influisce sulla probabilità che esso venga supportato nel tempo, attraverso la disponibilità di più prodotti informatici idonei alla sua gestione e visualizzazione.

Inoltre nella scelta dei prodotti altre caratteristiche importanti sono la capacità di occupare il minor spazio possibile in fase di memorizzazione (a questo proposito vanno valutati, in funzione delle esigenze dell'utente, gli eventuali livelli di compressione utilizzabili) e la possibilità di gestire il maggior numero possibile di metadati, compresi i riferimenti a chi ha eseguito modifiche o aggiunte.

4 SCELTA

4.1 Formati e prodotti per la formazione e gestione

Per la scelta dei formati idonei alla formazione e gestione dei documenti informatici, sono da tenere in considerazione le caratteristiche indicate nei paragrafi precedenti. Ulteriori elementi da valutare sono l'efficienza in termini di occupazione di spazio fisico e la possibilità di gestire il maggior numero possibile di metadati, compresi i riferimenti a modifiche o aggiunte intervenute sul documento.

4.2 Formati per la conservazione

La scelta dei formati idonei alla conservazione oltre al soddisfacimento delle caratteristiche suddette deve essere strumentale a che il documento assuma le caratteristiche di immodificabilità e di staticità previste dalle regole tecniche del Codice dell'Amministrazione Digitale. Per quanto fin qui considerato, è opportuno privilegiare i formati che siano standard internazionali (de jure e de facto) o, quando necessario, formati proprietari le cui specifiche tecniche siano pubbliche, dandone opportuna evidenza nel manuale di conservazione dei documenti informatici. Ulteriore elemento di valutazione nella scelta del formato è il tempo di conservazione previsto dalla normativa per le singole tipologie di documenti informatici. I formati per la conservazione adottati per le diverse tipologie di documenti informatici, devono essere indicati nel manuale di conservazione.

Allegato 4

al manuale di gestione del protocollo informatico,
dei flussi documentali e degli archivi

Il sistema documentale e di protocollazione adottato dall'Ente

INDICE

1. Premessa: il sistema documentale e di protocollazione adottato dall'Ente: applicativo hyperSIC di APK s.r.l.
2. Gestione accessi
3. Fascicolazione di un documento
4. Ricerca dei documenti in archivio
5. Condivisione dei documenti
6. Assegnazione dei documenti
7. Sottoscrizione documenti informatici
8. Invio di un documento a destinatari esterni
9. Iter documento
10. Operatività del flusso dei documenti ricevuti dall'AOO
11. Operatività del flusso dei documenti da trasmettere

1. Premessa: Il sistema documentale e di protocollazione adottato dall'Ente

L'Ente ha adottato e sta operando con la piattaforma di gestione documentale denominata "hyperSIC".

La soluzione riunisce tutte le funzionalità necessarie per gestire la documentazione ed i procedimenti amministrativi informatici relazionandosi con gli altri applicativi gestionali e integrando i servizi di protocollo Informatico, gestione Elettronica Documentale, scrivania digitale, archiviazione digitale, fascicolazione, gestione dei Procedimenti Amministrativi (Workflow), interscambio con il sito web per il Cittadino e conservazione.

Il sistema permette la gestione di documenti indipendentemente dal loro formato nativo (informatico all'origine o cartaceo digitalizzato).

Tutti i documenti informatici, sia creati dall'AOO che ricevuti dall'esterno sono archiviati automaticamente dal sistema di gestione documentale, contestualmente alle operazioni di registrazione e segnatura di protocollo, in un repository che ne garantisce la sicurezza e l'immodificabilità.

L'archivio è accessibile ai solo operatori accreditati e la ricerca è garantita da un sistema di reperimento parametrico dei documenti.

La piattaforma permette la protocollazione e l'archiviazione digitale di tutta la corrispondenza in arrivo dell'Ente e gestisce, in modo totalmente digitale, la distribuzione della posta agli uffici.

L'operazione di smistamento digitale è supportata da un'apposita area di monitoraggio all'interno della quale ogni operatore, abilitato, è in grado di visionare la corrispondenza in arrivo, prenderla in carico, fascicolarla, assegnarla ed evaderla.

La corrispondenza in partenza viene gestita direttamente dalle unità organizzative che producono i documenti.

I documenti informatici possono essere creati direttamente dalla scrivania digitale o essere prodotti dagli applicativi gestionali integrati alla piattaforma di gestione documentale

Le operazioni di firma digitale, condivisione interna, protocollatura e segnatura, archiviazione, trasmissione e conservazione sono tutte integrate all'interno della piattaforma e sono riportate in evidenza all'operatore competente nell'area di monitoraggio sopra citata.

L'area di monitoraggio supporta così passo a passo l'operatore nell'espletamento di tutte le sue incombenze.

2. Gestione accessi

Il sistema hyperSIC gestisce un sistema di profilazione degli utenti e dei relativi diritti di accesso.

Tutte le operazioni che si possono svolgere all'interno della procedura sono predeterminate: ogni singolo utente può avere il "diritto" o meno di svolgerle. In tal modo tutto ciò che accade nel

sistema è controllato dal sistema stesso. Le azioni di ciascun utente vengono continuamente monitorate e registrate in automatico in appositi file di LOG, immodificabili.

A ciascun addetto vengono attribuiti un nome utente e una password, dei quali sarà unico responsabile sin dal momento della formale attribuzione. Con il primo accesso al sistema, l'utente è tenuto a modificare la password personale, individuandone un'altra nel rispetto dei parametri formali prestabiliti. Il sistema è configurato in modo tale che la password, da questo momento in avanti, non possa essere conosciuta da nessuno, nemmeno dall'amministratore di sistema.

Sono ammesse soltanto password conformi alla vigente normativa in materia di protezione, sicurezza e tutela dei dati personali. E' prevista la sostituzione periodica della password di accesso, in conformità alle disposizioni vigenti.

3. Fascicolazione di un documento

L'operazione di fascicolazione è particolarmente importante per la ricerca sistematica dei documenti ed è prevista dalle regole tecniche del CAD. La classificazione dell'Ente viene riportata in dettaglio all'interno dell'apposito capitolo del manuale di gestione del protocollo informatico, dei flussi documentali e degli archivi.

HyperSIC prevede una funzionalità specifica per la gestione dei fascicoli digitali. La struttura dei fascicoli digitali di hyperSIC è correlata ai procedimenti gestiti dalle procedure gestionali e dalle procedure del sistema di workflow. Pertanto i fascicoli vengono alimentati da:

1. Documenti prodotti dall'Ente:

- da sistema documentale

- da procedure gestionali

- da procedure workflow

2. Documenti pervenuti all'Ente

4. Ricerca dei documenti in archivio

HyperSIC possiede un efficiente sistema di ricerca e reperimento dei documenti basato sui dati inseriti nelle maschere di indicizzazione, al momento della memorizzazione del documento o anche in momenti successivi per i soli dati facoltativi.

La ricerca di documenti può essere effettuata per documento singolo, per procedimento o per fascicolo, o in base ad altri criteri di individuazione (es. tipologia, classificazione, ecc.).

La ricerca delle informazioni sul sistema è effettuata secondo criteri basati su tutti i tipi di informazione registrati. I criteri di selezione possono essere costituiti da espressioni semplici o da combinazioni di espressioni legate per mezzo di operatori logici.

La ricerca può essere effettuata su singoli campi, o su parti del contenuto dei campi stessi.

5. Condivisione dei documenti

Tramite il sistema documentale è possibile condividere/ inviare internamente un documento ad altri operatori con l'abilitazione alle specifiche operazioni da compiere sul documento (consultazione, correzione, apposizione di firma digitale, protocollazione, invio all'esterno ecc..);

Grazie a questo sistema di condivisione/assegnazione interno si evita la replicazione del documento ed è possibile la consultazione del flusso documentale aggiornato in tempo reale.

6. Assegnazione dei documenti

Tramite il sistema documentale è possibile assegnare un documento ad uno o più Settori, Servizi o Nuclei organizzativi.

Il documento assegnato viene ricevuto in apposito nodo del loro quaderno di lavoro di hyperSIC.

L'assegnazione può inoltre essere accompagnata da una nota.

L'assegnatario può monitorare in qualsiasi momento lo stato di avanzamento delle operazioni sul documento.

7. Sottoscrizione documenti informatici

La firma digitale è strettamente connessa alla gestione documentale in quanto permette il passaggio definitivo dal formato cartaceo dei documenti, al formato digitale e alla conseguente eliminazione degli archivi cartacei. Questo strumento rappresenta un prerequisito ineludibile per l'evoluzione della documentazione, sempre più destinata a trasformarsi da foglio di carta a file memorizzato nel sistema.

Nei casi consentiti dalla legge, la firma digitale è sostituita da altre forme di firma elettronica o firma elettronica avanzata contemplate dal CAD e dalle regole tecniche vigenti.

8. Invio di un documento a destinatari esterni

E' possibile protocollare in uscita sia un documento già presente nell'archivio interno, sia un documento in corso di inserimento nel sistema. Dopo avere compilato gli indici, il documento sarà opportunamente fascicolato e archiviato.

9. Iter documento

Tutte le azioni effettuate su un documento all'interno del sistema documentale (visualizzazione, lettura, presa in carico, assegnazione, ecc.) vengono memorizzate automaticamente sul documento stesso in una specifica sezione di riepilogo delle operazioni effettuate; in questo modo è possibile monitorare, in qualunque momento, lo stato di avanzamento lavori del documento in esame.

10. Operatività del flusso dei documenti ricevuti dall'AOO

Una delle prime operazioni effettuate su documenti ricevuti è quella di procedere alla protocollazione della documentazione tramite l'applicativo hyperSIC.

HyperSIC permette infatti di protocollare:

- E-mail Certificate/E-mail: il sistema importa automaticamente le informazioni contenute nel *messaggio di posta selezionato (*oggetto, mittente, allegati, riferimenti del protocollo ricevuto, ecc*);*

- Istanze pervenute tramite apposito servizio on line dal sito dell'Ente: il sistema protocolla automaticamente tutte le informazioni ricevute;

- File informatici da supporti digitali esterni (*CD-ROM, DVD, hard disk, pen drive ecc.*);

- Documentazione cartacea (*posta ordinaria, raccomandata o consegnata a mano*) allegando la scansione della documentazione.

Ultimata la protocollazione di un documento pervenuto, esso è reso immediatamente disponibile ai componenti delle varie unità organizzative competenti tramite il sistema di Gestione documentale hyperSIC all'interno dell'area di monitoraggio.

Le operazioni che possono essere effettuate sul documento ricevuto sono le seguenti:

- Presa visione e mantenimento del documento sul quaderno di lavoro

Il documento pervenuto può essere visionato e mantenuto attivo sul quaderno di lavoro fino a quando non si procede con la sua gestione o assegnazione ad incaricato competente.

Anche nel caso in cui il documento venga archiviato, rimane sempre consultabile.

- Presa in carico del documento se di propria competenza

Ciascun documento pervenuto deve essere preso in carico dall'operatore competente tramite l'apposita funzione.

La presa in carico viene automaticamente comunicata sul quaderno di lavoro a tutti gli operatori abilitati alla visione/ gestione di quel documento.

- Fascicolazione digitale del documento

L'operazione di fascicolazione digitale avviene con le modalità descritte nell'apposito capitolo del presente allegato.

- Assegnazione di un documento ad incaricato del procedimento

Il Responsabile di un'unità organizzativa può assegnare un documento ricevuto ad uno o più incaricati del procedimento, i quali lo ricevono in apposito nodo del quaderno di lavoro.

Le modalità di gestione sono descritte nel capitolo "*7. Assegnazione dei documenti"* del presente allegato.

- Inoltro a soggetti esterni all'AOO;

All'interno del sistema documentale è possibile inviare all'esterno dell'AOO qualsiasi documento ricevuto. L'invio potrà avvenire per via telematica (E-mail certificata nel caso di invio a indirizzo elettronico).

- Risposta al documento ricevuto

Il documento ricevuto può essere evaso rispondendo con un nuovo documento e indicando la modalità con cui si è evasa la documentazione. Le modalità di gestione sono descritte nel capitolo *3* "Inserimento/ Formazione di un nuovo documento" *del presente allegato.*

11. Operatività del flusso dei documenti da trasmettere

Il sistema documentale permette di creare un documento in risposta ad uno ricevuto.

Esistono diverse modalità per inserire un nuovo documento in hyperSIC:

Le modalità di gestione sono *descritte nel capitolo* 3 "Inserimento/ Formazione di un nuovo documento" *del presente allegato.*

Dopo aver individuato la tipologia di documento che si desidera creare/ utilizzare è necessario compilare e verificare i dati della maschera di dettaglio del documento, contenente i metadati con tutte le informazioni.

Nel caso di risposta a documento in entrata, questi dati sono già proposti in automatico dal sistema sulla maschera di dettaglio del nuovo documento e riportati automaticamente sul testo (qualora si sia scelto di partire da un modello predisposto).

Il testo così creato può essere redatto dall'operatore competente.

La risposta ad un documento propone automaticamente l'eventuale evasione dell'istanza ricevuta.

Le operazioni che possono essere effettuate su un documento in redazione sono le seguenti:

- Condivisione/assegnazione di un documento all'interno dell'AOO

Le modalità di gestione sono descritte nei capitoli *"5. Condivisione dei documenti"* e "*6. Assegnazione dei documenti"* del presente allegato.

- Fascicolazione digitale del documento

L'operazione di fascicolazione digitale avviene con le modalità descritte nel capitolo *"Fascicolazione di un documento"* del presente allegato.

- Firmare digitalmente i file di un documento

Previo inserimento di un dispositivo di firma digitale nel PC è possibile firmare digitalmente i file di un documento in hyperSIC sfruttando la funzione di firma automatica così come specificato nel capitolo "7. Sottoscrizione documenti informatici" *del presente allegato.*

- Protocollare automaticamente il documento in uscita

All'interno del sistema documentale è possibile, da parte degli utenti preventivamente abilitati dal Responsabile del protocollo, protocollare in uscita i documenti.

I riferimenti del protocollo vengono poi riportati automaticamente all'interno del file sul quale si stava *lavorando (*se si trattava di modello di testo modificabile*).*

- Archiviare un documento

Terminate le operazioni di redazione del documento si può procedere all'archiviazione del medesimo.

- Invio del documento ai destinatari

È possibile inviare all'esterno dell'AOO qualsiasi documento creato all'interno del sistema documentale. Se la trasmissione avviene per via telematica (e-mail certificata), il messaggio di posta elettronica viene automaticamente salvato all'interno del documento inviato, così come le ricevute di accettazione e consegna qualora l'invio avvenga ad un indirizzo di Posta Elettronica Certificata.

Per qualsiasi informazione operativa e tecnica, è possibile consultare i manuali, le pillole Formative e le Release Notes messi a disposizione dalla Ditta fornitrice sull’applicativo stesso.

Allegato 5

al manuale di gestione del protocollo informatico,
dei flussi documentali e degli archivi



COSTRUIRE INSIEME

MANUALE DI CONSERVAZIONE

(in conformità alle Linee Guida AgID del 10/09/2020 e s.m.i.
sulla formazione, gestione e conservazione dei documenti informatici)

EMISSIONE DEL DOCUMENTO

AZIONE	DATA	NOMINATIVO	FUNZIONE

REGISTRO DELLE VERSIONI

VERSIONE	DATA EMISSIONE	MODIFICHE	NOTE

Sommario

1. Premessa 3
2. Scopo del Documento 5
3. Definizioni 6
4. Modello organizzativo 7
5. Soggetti coinvolti, ruoli e responsabilità 8
6. Modello di funzionamento 10
7. Formato dei documenti informatici e dei metadati 10
8. Tipologie di Pacchetti e Metadati 11
9. Pacchetto informativo 12
10. Processo di conservazione 14
11. Procedura 14
12. Controlli periodici 14
13. Gestione delle Anomalie 15
14. Produzione di copie e duplicati 15
15. Architetture e infrastrutture utilizzate 15
16. Misure di sicurezza adottate 15
17. Trattamento dei dati personali 16
18. Misure per la protezione ed il trattamento dei dati personali 16
19. Struttura organizzativa 17

1. Premessa

Il quadro normativo italiano ha progressivamente valorizzato la digitalizzazione documentale nei procedimenti amministrativi, seguendo il principio *digital first*. In tale contesto, la conservazione digitale dei documenti, sia nativi digitali che digitalizzati, è imprescindibile per garantirne il valore giuridico, l'integrità e l'accessibilità nel tempo. (analogamente a quelli cartacei)

Per maggiore chiarezza occorre distinguere tra: *digitalizzazione* (o storicamente, "conservazione sostitutiva"), che produce una copia digitale di un documento cartaceo e *conservazione digitale a norma*, che assicura una conservazione informatica accessibile nel lungo periodo mediante l'utilizzo di specifiche tecniche e procedure normate. La confusione tra questi due concetti è ancora diffusa ed è pertanto utile ribadirne che la conservazione è l'attività svolta a proteggere e custodire nel tempo gli archivi di documenti informatici. Il sistema di conservazione deve assicurare, dalla presa in carico fino all'eventuale scarto, la conservazione dei seguenti oggetti digitali in esso conservati, tramite l'adozione di regole, procedure e tecnologie, garantendone le caratteristiche di autenticità, integrità, affidabilità, leggibilità, reperibilità come previsto dall'art. 44 del Codice dell'Amministrazione Digitale (CAD):

- i documenti informatici e i documenti amministrativi informatici con i metadati ad essi associati;
- le aggregazioni documentali informatiche (fascicoli e serie) con i metadati ad esse associati contenenti i riferimenti che univocamente identificano i singoli oggetti documentali che costituiscono le aggregazioni medesime.

A livello normativo si fa riferimento alle "Linee Guida sulla formazione, gestione e conservazione dei documenti informatici" emanate dall'Agenzia per l'Italia Digitale (Agid) il cui scopo è duplice:

- aggiornare le attuali regole tecniche in base all'art. 71 del CAD, concernenti la formazione, protocollazione, gestione e conservazione dei documenti informatici;
- incorporare in un'unica linea guida le regole tecniche e le circolari in materia, addivenendo ad un "unicum" normativo che disciplini gli ambiti sopracitati, nel rispetto della disciplina in materia di Beni culturali.

Le Linee Guida pertanto costituiscono la nuova versione aggiornata delle regole tecniche in materia di formazione, protocollazione, gestione e conservazione del documento, già precedentemente regolate nel DPCM 3 dicembre 2013 (Regole tecniche in materia di sistema di conservazione) e nel DPCM 13 novembre 2014 (Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici).

Considerata la velocità dell'innovazione, le linee guida devono garantire un adattamento costante ai cambiamenti imposti dall'incessante rivoluzione digitale e sono costituite da un testo "statico" che contiene la base normativa della materia e una serie di "allegati" i cui contenuti più "flessibili" possono adeguarsi agevolmente all'evoluzione tecnologica.
Nello specifico le linee guida stabiliscono:

- l'adozione obbligatoria di standard avanzati (ISO/IEC 27001, ISO 14721 OAIS, ETSI TS 101 533-1);
- la garanzia permanente delle qualità dei documenti informatici (autenticità, integrità, affidabilità, leggibilità, reperibilità);
- l'obbligo, per le PA, di adottare e pubblicare il Manuale di Conservazione e il Manuale di Gestione, designare i ruoli dei responsabili e inserire tali atti nell'ambito dell'"Amministrazione trasparente".

Parallelamente, a livello europeo, le novità in corso (eIDAS 2.0, NIS2) stanno spingendo verso un'armonizzazione delle normative in materia di firma elettronica, identità digitale e sicurezza dei documenti informatici
In conclusione, il Manuale di Conservazione Digitale deve:

- dettagliare l'organizzazione interna e i ruoli coinvolti;
- descrivere il modello operativo, le tecnologie e le infrastrutture utilizzate;
- esplicitare le misure di sicurezza e le procedure di verifica nel tempo;
- allinearsi integralmente alle Linee Guida Agid (2021/2022) e alle disposizioni del CAD, integrando la compliance con standard tecnici riconosciuti e gli obblighi di pubblicazione e aggiornamento richiesti alla PA.

2. Scopo del Documento

Il presente Manuale descrive il sistema di conservazione dei documenti informatici dell'Azienda, in qualità di soggetto Titolare e Produttore degli oggetti di conservazione (i documenti), dal punto di vista organizzativo, tecnico ed operativo, in conformità alle "Linee Guida Agid sulla formazione, gestione e conservazione dei documenti informatici del 10/09/2020 e smi" (in seguito LLGG).

> *LLGG Agid sulla formazione, gestione e conservazione dei documenti informatici*
> *"Il manuale di conservazione è un documento informatico che deve illustrare dettagliatamente l'organizzazione, i soggetti coinvolti e i ruoli svolti dagli stessi, il modello di funzionamento, la descrizione del processo, la descrizione delle architetture e delle infrastrutture utilizzate, le misure di sicurezza adottate e ogni altra informazione utile alla gestione e alla verifica del funzionamento, nel tempo, del sistema di conservazione."*

Non è scopo del presente Manuale descrivere il processo di conservazione del Conservatore esterno delegato, a cui l'Azienda ha affidato l'intera attività di conservazione.

Per tale motivo, nel presente documento sono riportati i riferimenti al "Manuale del sistema di Conservazione" del conservatore esterno, da cui poter desumere le caratteristiche di merito.

Il presente Manuale di Conservazione è predisposto ai sensi delle Linee Guida Agid, in vigore dal 10 settembre 2020 ed integra, per quanto riguarda i rapporti tra il Soggetto Produttore ed il Conservatore, il manuale di Conservazione del Conservatore.

3. Definizioni

Per una migliore comprensione del presente manuale si riportano le seguenti definizioni:

a) **Aggregazione documentale informatica**: insieme di documenti informatici o insieme di fascicoli informatici riuniti per caratteristiche omogenee, in relazione alla natura e alla forma dei documenti o in relazione all'oggetto e alla materia o in relazione alle funzioni dell'Azienda;

b) **Archivio**: complesso organico di documenti, di fascicoli e di aggregazioni documentali di qualunque natura e formato, prodotti o comunque acquisiti da un soggetto produttore durante lo svolgimento dell'attività;

c) **Area Organizzativa Omogenea (AOO)**: un insieme di funzioni e di strutture, individuate dalla amministrazione, che opera su tematiche omogenee e che presenta esigenze di gestione della documentazione in modo unitario e coordinato ai sensi dell'articolo 50, comma 4, del D.P.R. 28 dicembre 2000, n. 445;

d) **CAD o Codice**: Codice Amministrazione Digitale, decreto legislativo 7 marzo 2005, n. 82 e successive modificazioni e integrazioni;

e) **Conservazione**: insieme delle attività finalizzate a definire ed attuare le politiche complessive del sistema di conservazione e a governarne la gestione, in relazione al modello organizzativo adottato;

f) **Esibizione**: operazione che consente di acquisire e visualizzare gli oggetti digitali conservati;

g) **Fascicolo informatico**: aggregazione strutturata e univocamente identificata di atti, documenti o dati informatici, prodotti e funzionali all'esercizio di una specifica attività o di uno specifico procedimento. Nella Pubblica Amministrazione il fascicolo informatico collegato al procedimento amministrativo è creato e gestito secondo le disposizioni stabilite dall'articolo 41 del Codice;

h) Gestore del Servizio di Conservazione (RSC): gestore della piattaforma e sistema di conservazione;

i) **LLGG**: Linee Guida Agid per la formazione, gestione e conservazione dei documenti informatici del 10/09/2020;

j) **Manuale di conservazione**: strumento che descrive il sistema di conservazione dei documenti informatici;

k) **Manuale di gestione**: “Manuale di Gestione del protocollo informatico dei flussi documentali e degli archivi”, documento di regolamentazione che descrive il sistema di gestione informatica dei documenti;
l) **Piano di archiviazione**: strumento, integrato con il sistema di classificazione per la definizione dei criteri di organizzazione dell'archivio, di selezione periodica e di conservazione ai sensi dell'articolo 68 del D.P.R. 28 dicembre 2000, n. 445;
m) **Processo o sistema di conservazione**: insieme delle attività finalizzate alla conservazione dei documenti informatici di cui all'art. 4.1 delle LLGG delle regole tecniche del sistema di conservazione;
n) **Produttore**: persona fisica o giuridica, di norma diversa dal soggetto che ha formato il documento, che produce il pacchetto di versamento ed è responsabile del trasferimento del suo contenuto nel sistema di conservazione.
o) **Regole tecniche del sistema di conservazione**: le regole tecniche contenute nelle LLGG in materia di conservazione, ai sensi degli art.i 20 c.3 e 5-bis, 23-ter c.4, 43 c.1 e 3, 44 e 71 c.1 del CAD;
p) **Responsabile del sistema di conservazione**: responsabile del RSC;
q) **Responsabile del trattamento dei dati**: la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro Azienda, associazione od organismo preposti dal titolare al trattamento di dati personali;
r) **Responsabile della conservazione**: soggetto responsabile dell'insieme delle attività elencate nell’art. 4.5 delle LLGG;
s) **Responsabile della sicurezza**: soggetto al quale compete la definizione delle soluzioni tecniche e organizzative in attuazione delle disposizioni in materia di sicurezza;
t) **Serie**: Raggruppamento di documenti con caratteristiche omogenee (vedi anche aggregazione documentale informatica);
u) **Titolare** degli oggetti di conservazione: soggetto produttore degli oggetti di conservazione.

4. Modello organizzativo

Il modello organizzativo adottato dall’Azienda è quello in outsourcing: l’Azienda affida il servizio di conservazione ad un Conservatore esterno, che dispone e garantisce di possedere “requisiti di elevato livello in termini di qualità e sicurezza” (vedi par. 4.3 LLGG), ai sensi dall’art. 34, c. 1-bis del C.A.D., fatte salve le competenze del Ministero della cultura,

ai sensi del Codice dei Beni Culturali e del paesaggio D.Lgs 42/2004.

L'Azienda affida il servizio di Conservazione a :

MAGGIOLI S.p.A
Sede legale: Via del Carpino 8, Santarcangelo di Romagna (RN)
Sito web: https://www.maggioli.com/it - it
Pec: segreteria@maggioli.legalmail.it
Partita IVA: 02066400405
per i documenti implementati attraverso la WebApp Hypersic della Software House APKappa S.R.L

Si rimanda, per quanto non esplicitamente indicato dal presente documento al Manuale del Conservatore, reperibile sul sito Istituzionale dell'Azienda.
Il soggetto esterno a cui è affidato il processo di conservazione assume inoltre il ruolo di Responsabile del trattamento dei dati, come previsto dal Codice in materia di protezione dei dati personali.
Il presente manuale di conservazione mira a fornire una chiara presentazione del sistema di conservazione e dei processi erogati, descrivere l'insieme delle fasi del processo nonché ad includere le informazioni rilevanti con un livello di dettaglio sufficiente ad agevolare le ispezioni, evitando informazioni tecniche articolate e non necessarie.

5. Soggetti coinvolti, ruoli e responsabilità

Nel sistema di conservazione dell'Azienda sono individuati i seguenti ruoli:

- **Titolare:** l'Azienda è il soggetto Titolare dei documenti e dei fascicoli informatici posti in conservazione e, in relazione al modello organizzativo adottato, affida ai Conservatori la gestione del Servizio di Conservazione secondo quanto previsto dalla normativa in materia e specificato nei contratti di servizio;
- **Produttore**: l'Azienda alimenta con le proprie procedure la gestione dei flussi documentali e degli archivi, ai fini della formazione degli atti e dei documenti da inviare in conservazione;
- **Utente**: persona, ente o sistema che interagisce con i servizi di un sistema di

gestione informatica dei documenti e/o di un sistema per la conservazione dei documenti informatici, al fine di fruire delle informazioni di interesse;

- **Responsabile della conservazione**: soggetto responsabile - previsto dall'organigramma del Titolare dell'oggetto di conservazione (l'Ente) - che "*definisce e attua le politiche complessive del sistema di conservazione e ne governa la gestione con piena responsabilità ed autonomia*" (CAD art. 44 c.1-quater, LLGG art. 4.5). Il Responsabile della Conservazione è persona fisica inserita stabilmente nell'organico dell'Amministrazione titolare dell'oggetto della conservazione; la normativa gli attribuisce compiti riguardanti le funzioni, gli adempimenti, le attività e le responsabilità del processo di conservazione. L'obiettivo principale del Responsabile della Conservazione è definire e impostare le modalità di trattamento della documentazione soggetta a conservazione. Le Linee Guida di Agid enfatizzano il ruolo del Responsabile della Conservazione che diviene fondamentale all'interno del processo di conservazione, insieme ai suoi delegati o ai terzi affidatari.
- Anche nel caso in cui il servizio di conservazione venga affidato ad un conservatore terzo, al Responsabile della conservazione dell'Azienda rimane in capo la responsabilità giuridica generale sui processi di conservazione.
- **Responsabile del servizio di gestione documentale e gestione protocollo informatico, della gestione dei flussi documentali e degli archivi:** Figura interna all'azienda che cura il protocollo informatico, organizzando e controllando i flussi documentali e gli archivi dell'ente, coordina e verifica periodicamente il corretto funzionamento del sistema, in raccordo con i responsabili di conservazione, sistemi informativi e privacy.
- **Delegato dei servizi di conservazione (Conservatore):** con affidamento in outsourcing, è il soggetto esterno delegato dal Responsabile della conservazione allo svolgimento di attività correlate ai processi di conservazione a norma dei documenti informatici, le cui mansioni e responsabilità sono chiaramente formalizzate tramite atto. Gli obiettivi dei conservatori tramite il Servizio di Conservazione sono quelli di garantire conservazione, archiviazione e gestione dei documenti informatici e dei fascicoli informatici, erogare servizio di accesso basato sui contenuti digitali conservati, fornire supporto, formazione e consulenza al Titolare dell'oggetto di conservazione per i processi di dematerializzazione. I conservatori assumono l'incarico di svolgere le attività affidate dal Responsabile della Conservazione dell'Azienda in accordo con quanto previsto dal contratto, dagli

allegati tecnici contrattuali e dalle disposizioni delle Linee Guida di Agid.

L'utente richiede al sistema di conservazione l'accesso ai documenti per acquisire le informazioni di interesse nei limiti previsti dalla legge. Tali informazioni vengono fornite dal sistema di conservazione secondo le modalità previste nel presente Manuale.
Il Responsabile della conservazione, sotto la propria responsabilità, può delegare ad un suo vicario lo svolgimento del processo di conservazione o di parte di esso ad uno o più soggetti dispecifica competenza ed esperienza in relazione alle attività ad essi delegate. Tale delega è formalizzata, esplicitando chiaramente il contenuto della stessa, e - in particolare - le specifiche funzioni e competenze affidate al delegato.

L'Azienda è il Titolare dei documenti informatici posti in conservazione e, attraverso il proprio Responsabile della Conservazione, definisce e attua le politiche complessive del sistema di conservazione, governandone quindi la gestione con piena responsabilità ed autonomia, in relazione al modello organizzativo esplicitato nel presente Manuale.
Pertanto, i ruoli di Produttore, Titolare del trattamento e di Responsabile della conservazione sono ricoperti dall'Azienda, mentre il ruolo di Responsabile del servizio di conservazione e Responsabile esterno del trattamento dei dati è ricoperto da soggetti esterni.
Il Responsabile del servizio di conservazione è delegato allo svolgimento delle attività specificatamente indicate nel contratto o convenzione di affidamento del processo di conservazione e nel rispetto delle modalità previste nel Manuale operativo del Conservatore, pubblicato sul sito Internet dell'Agenzia dell'Italia Digitale.

6. Modello di funzionamento

Mediante procedure automatizzate il sistema gestionale si integra con la piattaforma di conservazione del soggetto delegato, inviando (versando) a quest'ultima i pacchetti di documenti da conservare. Il sistema di gestione del processo di conservazione prende in carico i pacchetti dei documenti da conservare e finalizza il processo di conservazione dando riscontro al sistema gestionale dell'avvenuta conservazione.
Al termine del processo di conservazione, il software di conservazione fornisce all'applicazione gestionale informazioni di dettaglio sulle operazioni effettuate, in particolare l'identificativo univoco assegnato al documento (lotto) nel sistema di conservazione.

7. Formato dei documenti informatici e dei metadati

La corretta conservazione dei documenti nel tempo è determinata anche dalla scelta dei formati idonei a tale scopo; il formato è l'insieme di informazioni che determinano la modalità con cui un oggetto digitale viene creato, memorizzato e riprodotto.
Un oggetto digitale è una sequenza di bit fissati con una certa organizzazione fisica su di una memoria; tale contenuto digitale viene memorizzato e definito come file. La possibilità di fruire e utilizzare un file è determinata dalla capacità di rappresentare la sequenza di bit per mezzo di un apposito software che riproduca, sulla base dei codici e delle regole che costituiscono il file stesso, il contenuto e la forma che gli era stata conferita dall'autore.
Attualmente la soluzione più sicura è adottare, fin dal momento della formazione dei contenuti digitali, formati che abbiano le caratteristiche per fornire le maggiori garanzie in termini di conservazione a lungo termine come indicato nel DPCM 3/12/2013 Regole tecniche per il protocollo informatico, Allegato 2 Formati sino al 1° gennaio 2022 e successivamente Linee Guida Agid, Allegato 2 Formati di file e riversamento.
Vengono inviati in conservazione i formati file ritenuti idonei ed accettati dal conservatore come specificato alla voce 'formati file' del seguente link:
https://assistenza.maggioli.it/conservazione-digitale-documentazione/

Risulta opportuno, per una corretta attività di conservazione, che il file siano prodotti in un formato idoneo ad essere conservato a norma.

8. Tipologie di Pacchetti e Metadati

Insieme alla scelta dei formati, la definizione dei metadati è un'operazione fondamentale per l'attività conservativa delle memorie digitali a medio e lungo termine.
I metadati vengono esplicitamente citati come oggetti da sottoporre a conservazione associati ai documenti informatici, ai documenti amministrativi informatici e ai fascicoli informatici o aggregazioni documentali al paragrafo 4.1 delle Linee Guida Agid.
I metadati sono informazioni associate ai dati primari creati e trattati: sono a loro volta dati che descrivono e localizzano una risorsa informativa rendendo più semplice il suo recupero, utilizzo e gestione; sono infatti un insieme di dati associati a un documento informatico, o a un fascicolo informatico, o ad un'aggregazione documentale informatica per identificarlo e descriverne il contesto, il contenuto e la struttura, nonché per permetterne la gestione nel tempo nel Sistema di Conservazione.
Sono metadati, ad esempio, il riferimento all'autore o alla tipologia di dato, il riferimento temporale alla creazione o registrazione del dato, la classificazione, etc.
Come si può intuire, i metadati associati a una risorsa sono potenzialmente infiniti e,

tipicamente, vengono distinti in tre principali categorie:

- metadati descrittivi, descrivono una risorsa con lo scopo di scoprirla ed identificarla;
- metadati strutturali, indicano la struttura di oggetti composti (ad esempio, i capitoli che assemblano le pagine);
- metadati amministrativi / gestionali, descrivono le informazioni volte a favorire la gestione del file (tipo di file, nome del produttore, riferimento temporale, etc.).

Ad esempio, i dati e i metadati relativi all'oggetto informativo e alle informazioni sulla rappresentazione costituiscono un'unità denominata contenuto informativo e in tale forma viene conservata al fine di assicurare la fruibilità e la comprensibilità nel lungo periodo; i metadati descrittivi, invece, che descrivono e identificano le informazioni archiviate, potrebbero essere conservati separatamente in appositi database.
Si rimanda al Manuale del Conservatore che integra il presente documento in cui sono definite le specifiche operative e le modalità di descrizione e di versamento nei Sistemi di Conservazione digitale delle diverse tipologie documentali oggetto di conservazione, incluse l'individuazione e la gestione dei metadati relativi ai documenti versati nei Sistemi di Conservazione.

9. Pacchetto informativo

Gli oggetti sottoposti a conservazione, siano essi aggregazioni documentali informatiche, documenti informatici, o metadati, sono trasmessi dal Soggetto produttore, memorizzati e conservati nei Sistemi di Conservazione e distribuiti ai soggetti abilitati sotto forma di pacchetti informativi.
Il pacchetto informativo, a seconda sia utilizzato per versare, conservare o distribuire gli oggetti sottoposti a conservazione, assume la forma, rispettivamente, di Pacchetto di Versamento (PdV), Pacchetto di Archiviazione (PdA) e Pacchetto di Distribuzione (PdD).

- Il Pacchetto di versamento (SIP-Submission Information Package o PdV) è un pacchetto informativo inviato ad un Sistema di Conservazione dal produttore secondo un formato predefinito e concordato ed identifica, in maniera univoca, l'insieme dei dati che vengono inviati al sistema di conservazione. Il PdV eventualmente integrato da ulteriori informazioni concordate con il cliente, viene trasferito dal produttore al soggetto conservatore tramite una apposita procedura informatica automatizzata che consente l'identificazione certa del soggetto che ha formato e trasmesso il documento.

- Il Pacchetto di archiviazione (AIP-Archival Information Package o PdA) è il pacchetto conservato in un Sistema di Conservazione, ovvero pacchetto informativo composto dalla trasformazione di uno o più pacchetti di versamento secondo le specifiche contenute nell'allegato "Specifiche tecniche del pacchetto di conservazione" del C.A.D. Il pacchetto di archiviazione è un "derivato" del pacchetto di versamento e ha la funzione di archiviare i dati in esso contenuti. Il PdA viene generato dai Sistemi di Conservazione in seguito alla conclusione del processo di acquisizione e presa in carico dei PdV. Per dettagli in merito alla formazione del PdA si rimanda al Manuale del Conservatore che integra il presente documento.
- Il Pacchetto di distribuzione (DIP-Dissemination Information Package o PdD) è il pacchetto inviato ad un utente da un Sistema di Conservazione, ovvero pacchetto informativo inviato dal Sistema di conservazione all'utente in risposta ad una sua richiesta. E' un pacchetto informativo che viene ricevuto da un utente come risposta a una richiesta di esibizione del contenuto conservato inoltrata a un sistema di conservazione; viene generato dai Sistemi a partire dai PdA conservati ed è finalizzato a mettere a disposizione dei richiedenti abilitati, in una forma idonea alle specifiche esigenze di utilizzo, gli oggetti sottoposti a conservazione. Per dettagli si rimanda al Manuale del Conservatore che integra il presente documento.

10. Processo di conservazione

Il Processo di Conservazione si basa su di una logica caratterizzata dal versamento da parte del Produttore degli oggetti da conservare secondo le modalità e le procedure sotto riportate.

L'Azienda periodicamente procede alla gestione dei Lotti (PdV) da inviare in conservazione trattandoli in modo automatico (A), con i lotti preparati e inviati direttamente dal sistema.

Area applicativa	Tipologia	Frequenza estrazione
Protocollo	PROTOCOLLO GENERALE	7 gg
	PROTOCOLLO REG. GIORNALIERO	1 g
Finanziaria	PROTOCOLLO - FATTUREPA	7 gg

11. Procedura

L'applicativo, secondo la periodicità suindicata, estrae i documenti da conservare, genera i relativi lotti, inserisce i documenti al loro interno, prepara e trasmette al Conservatore i lotti così generati.

12. Controlli periodici

Compito dell'operatore è quello di eseguire periodicamente una serie di controlli sia in merito alla procedura sia in merito all'avvenuto versamento dei lotti. Di seguito una breve descrizione riepilogativa:

- verifica che per ogni categoria sia presente un solo lotto in stato "aperto" e non siano presenti lotti in stato "pronto, da correggere, rifiutato o errore di trasmissione".
- Verifica mediante il menù delle procedure automatiche che il numero dei documenti estratti coincida con quelli realmente importati nel lotto da versare.
- Verifica del corretto funzionamento degli automatismi con particolare riguardo al registro di protocollo giornaliero
- Controlli approfonditi per identificare le anomalie nel caso in cui il Conservatore rifiuti un versamento (notificando l'anomalia mezzo mail)

- Accesso periodico alla piattaforma del Conservatore Maggioli S.p.A

13. Gestione delle Anomalie

- In caso di anomalie relative alla presenza di lotti in stato non conforme, le operazioni di bonifica vengono gestite e risolte in collaborazione con la Software House ApKappa
- Nel caso in cui il numero dei documenti estratti non coincida con quelli importati dalle procedure automatiche, vengono svolti controlli atti a verificare che la mancata importazione non costituisca un'anomalia ma bensì sia imputabile ad uno o più documenti non idonei ad essere conservati (ad esempio un protocollo generale privo di allegati).
- In caso di blocco degli automatismi, l'anomalia viene prontamente segnalata alla Software House ApKappa per l'immediata riattivazione della procedura.
- Nel caso di lotti rifiutati dal Conservatore, normalmente a causa di allegati non conformi o corrotti, si procede con la gestione o, ove non possibile, l'eliminazione del file danneggiato.

14. Produzione di copie e duplicati

I Sistemi di Conservazione consentono il rilascio, al personale opportunamente autorizzato dal Soggetto produttore, di duplicati e copie informatiche dei documenti digitali presenti nei propri archivi, secondo modalità condivise con il Responsabile della protezione dei dati e il Titolare del trattamento dei dati personali.

Per ulteriori dettagli, si rimanda ai Manuale del Conservatore che integra il presente documento.

15. Architetture e infrastrutture utilizzate

Avendo delegato il processo di conservazione ad un soggetto esterno in outsourcing, per la spiegazione dell'architettura e delle infrastrutture utilizzate, si rimanda al Manuale del processo di conservazione del soggetto delegato.

16. Misure di sicurezza adottate

Ai sensi delle Linee Guida sulla formazione, gestione e conservazione dei documenti informatici paragrafo 4.10 Misure di sicurezza "le Pubbliche Amministrazioni sono tenute ad ottemperare alle misure minime di sicurezza ICT emanate dall'Agid con circolare del 18

aprile 2017, n. 2/2017". Essendo il servizio di conservazione affidato esternamente, le misure minime di sicurezza sono state concordare con il Conservatore Maggioli reperibili nel manuale.

17. Trattamento dei dati personali

L'Amministrazione, con la sottoscrizione dell'affidamento, esprime il proprio consenso al trattamento dei dati personali per le finalità previste ed è consapevole che in mancanza di tale consenso il Conservatore potrebbe non essere in condizione di erogare correttamente il servizio.

18. Misure per la protezione ed il trattamento dei dati personali

Nelle fasi di creazione, digitalizzazione, trattamento e invio in conservazione dei documenti informatici, l'Amministrazione pone massima cura nel rispetto delle disposizioni previste dal Codice in materia di protezione dei dati personali (D.Lgs 196/2003 aggiornato con il D.Lgs 10 agosto 2018, n. 101 recante le disposizioni per l'adeguamento dell'ordinamento nazionale al nuovo Regolamento UE 2016/679 (GDPR).

Maggioli s.p.a. opera all'interno dell'affidamento secondo quanto riportato nel Manuale di conservazione limitatamente ai flussi documentali puntualmente indicati nel Modulo di affidamento del Servizio di conservazione digitale degli Archivi informatici della Pubblica Amministrazione e per le quantità e per i tempi in esso indicati, in base all'offerta ricevuta e al relativo ordine/contratto nel rispetto delle vigenti normative e della informativa privacy resa disponibile, ai sensi del regolamento 679/2016 art. 13-14 (GDPR), da Maggioli s.p.a. all'indirizzo https://assistenza.maggioli.it/privacy/

19. Struttura organizzativa

Dati dei soggetti che nel tempo hanno assunto la responsabilità del sistema di conservazione, descrivendo in modo puntuale, in caso di delega, i soggetti, le funzioni e gli ambiti oggetto della delega stessa:

Soggetto	Funzione	Ambito delega
Antonello Paolo Zaccone	Responsabile della conservazione	
Nadia Nicolini	Operatore	Incaricato

POSTI AGLI ATTI:

Manuale Conservatore Maggioli