REGIONE PIEMONTE

ENTE DI GESTIONE DELLE AREE PROTETTE DEL PO PIEMONTESE

DELIBERAZIONE DEL CONSIGLIO N. 131

OGGETTO:

Approvazione del " Manuale di Gestione Documentale del Protocollo Informatico, dei Flussi Documentali e degli Archivi".

*L'anno **duemilaventitré** il giorno **18** del mese di **dicembre** alle ore **17.10**, presso la sede operativa in Viale Lungo Po Gramsci n. 10 - Casale Monferrato si è riunito il Consiglio dell'Ente di gestione delle Aree protette del Po piemontese, nelle persone di:*

PRESENTI	ASSENTI
ROBERTO SAINI (Presidente)	
UGO BALDI	X
MATILDE CASA	
ALICE CERUTTI (Vice Presidente)	
LIBERO FARINELLI	
LUCA FERRARI	X
ANDREA MANDARINO	
LAURA POMPEO	
DANIELE RONCO	X

Il Presidente, riconosciuta legale l'adunanza, dichiara aperta la seduta.

Partecipa all'adunanza con voto consultivo la Direttrice, Monica Perroni, in qualità di segretario.

IL CONSIGLIO

Udita la relazione del Presidente;

richiamato il D. Lgs. 82/2005, recante "Codice dell'amministrazione digitale" e ss.mm. e ii.;

visto il D.P.R.445/2000, recante "Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa" e, in particolare, l'art.50 c.3, che prevede l'obbligo per le pubbliche amministrazioni di provvedere a realizzare e a revisionare i sistemi informatici e automatizzati dedicati alla gestione del protocollo informatico e dei procedimenti amministrativi;

preso atto del DPCM 3 dicembre 2013 contenente le regole tecniche per il protocollo informatico ed in particolare l'art. 3 c.1 lett. d), e l'art.5 che prevedono per le Pubbliche Amministrazioni l'adozione di un manuale per la gestione, anche ai fini della conservazione dei documenti informatici, in grado di fornire precise istruzioni per il corretto funzionamento del servizio del protocollo informatico, della gestione dei flussi documentali e degli archivi; considerati gli aggiornamenti delle Linee guida AGID sulla formazione, gestione e conservazione dei documenti informatici, la cui applicazione era prevista a partire dal 1° gennaio 2022;

visto il D.Lgs.196/2003 e ss.mm.eii.;

visto il Regolamento generale sulla protezione dei dati (GDPR, General Data Protection Regulation – Regolamento UE2016/679);

considerato che il "Manuale di Gestione Documentale del Protocollo Informatico, dei flussi documentali, del sistema di conservazione digitale dei documenti informatici e degli archivi ", presente in allegato, è uno strumento operativo che riflette le modalità organizzative di gestione dei flussi documentali e risponde alla sperimentazione di soluzioni innovative che potrebbero richiedere un periodico aggiornamento;

valutato inoltre che il manuale in allegato è redatto secondo i criteri di efficacia ed efficienza quali corollari del principio di buon andamento della Pubblica Amministrazione;

ritenuto opportuno procedere all'approvazione del manuale di gestione comprensivo dei 12 allegati che si considerano parte integrante e sostanziale del presente atto;

dato atto che è stato espresso il parere favorevole da parte dell'Avvocato Ramello Responsabile della protezione dati e della Direttrice, dott.ssa Monica Perroni, in ordine alla regolarità tecnico-amministrativa;

ritenuto di adottare il presente provvedimento, vista l'urgenza, con immediata esecutività,

con unanimi favorevoli espressi nei modi e nelle forme di legge;

d e l i b e r a

1. di approvare il "Manuale di gestione Documentale del Protocollo Informatico, dei flussi documentali, del sistema di conservazione digitale dei documenti informatici e degli archivi" corredato da n. 12 allegati facenti parte integrante e sostanziale del presente atto e più precisamente:

- Allegato 1: Norme di riferimento

- Allegato 2: Nomina del Responsabile
- Allegato 3: Certificazione di processo
- Allegato 4: Standard e specifiche tecniche
- Allegato 5: Formato minimo dei metadati
- Allegato 6: Comunicazioni
- Allegato 7: Sistema documentale adottato dall'Ente
- Allegato 8: Sistema di conservazione adottato dall'Ente
- Allegato 9: Misure di sicurezza ITC
- Allegato 10: Rilevazione delle Misure di sicurezza e dell'Ambiente SAAS
- Allegato 11: Manuale della conservazione documenti del protocollo
- Allegato 12: Interoperabilità AIP sistemi di conservazione

2. di dare atto che il "Manuale di gestione del protocollo informatico, dei flussi documentali e degli archivi" è strumento di lavoro necessario alla corretta tenuta del protocollo e alla gestione del flusso documentale e dell'archivio e pertanto dovrà essere aggiornato quando innovazioni tecnologiche, nuove situazioni organizzative o normative lo richiederanno o, comunque, ogniqualvolta si renderà necessario alla corretta gestione documentale;

3. di provvedere alla pubblicazione del manuale sul sito internet dell'Ente di gestione;

4. di comunicare il presente provvedimento a tutti gli uffici per tutti gli adempimenti conseguenti a tale manuale;

5. di adottare il presente provvedimento, vista l'urgenza, con immediata esecutività.

La presente deliberazione sarà pubblicata all'Albo Pretorio dell'Ente-Parco, sul sito istituzionale www.parcopopiemontese.it.

Letto, confermato e sottoscritto *(con firma digitale, ai sensi degli artt. 20 e 21 del D.Lgs. 82/2005)*

IL SEGRETARIO	IL PRESIDENTE
Firmato Digitalmente	**Firmato Digitalmente**
Dott.ssa Monica Perroni	**Roberto Saini**

PUBBLICAZIONE ON LINE

La presente deliberazione, anche ai fini della pubblicità degli atti e della trasparenza amministrativa, sarà pubblicata sul sito dell'Ente www.parcopopiemontese.it per 15 giorni consecutivi, alla Sezione Albo Pretorio ALBO PRETORIO DIGITALE - Ente G. A. P. Po Piemontese (servizipubblicaamministrazione.it).

Aree protette
Po piemontese

United Nations Educational, Scientific and Cultural Organization
MaB Man and Biosphere Reserve
CollinaPo

ENTE DI GESTIONE DELLE AREE PROTETTE DEL PO PIEMONTESE

MANUALE DI GESTIONE DOCUMENTALE DEL PROTOCOLLO INFORMATICO, DEI FLUSSI DOCUMENTALI E DEGLI ARCHIVI

Ai sensi delle linee guida Agid 2021–
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

INDICE

11 NORME TRANSITORIE E FINALI

11.1 Modalità di approvazione e aggiornamento del manuale
11.2 Pubblicità del manuale Gestione documentale
11.3 Entrata in vigore

ALLEGATI

Allegato 1 - Norme di riferimento
Allegato 2 - Nomina del Responsabile della gestione documentale e del Servizio di Protocollo informatico
Allegato 3 - Certificazione di processo
Allegato 4 – Standard e Specifiche tecniche
Allegato 5 - Formati minimi dei metadati dei documenti informatici
Allegato 6 - Sistema di comunicazioni tra enti
Allegato 7 - Il sistema documentale e di protocollazione adottato dall'Ente
Allegato 8 - Il sistema di conservazione adottato dall'Ente

1 PRINCIPI GENERALI

1.1 Premessa

Obiettivo del Manuale di gestione documentale è descrivere sia il sistema di gestione documentale a partire dalla fase di protocollazione della corrispondenza in ingresso e in uscita e di quella interna, sia le funzionalità disponibili agli addetti interni e ai soggetti esterni che a diverso titolo interagiscono con l'amministrazione.
Il protocollo informatico costituisce l'infrastruttura di base tecnico-funzionale su cui avviare il processo di ammodernamento e di trasparenza dell'amministrazione. Il Manuale è destinato alla più ampia diffusione interna ed esterna, in quanto fornisce indicazioni complete circa la corretta esecuzione delle operazioni di formazione, registrazione, classificazione, fascicolazione e archiviazione dei documenti informatici. Il presente documento pertanto si rivolge non solo agli operatori di protocollo ma, in generale, a tutti i dipendenti e ai soggetti esterni che si relazionano con l'amministrazione.
Esso disciplina:

- la gestione dei documenti in un contesto di dematerializzazione e di digitalizzazione dei procedimenti;
- i livelli di esecuzione, le responsabilità e i metodi di controllo dei processi e delle azioni amministrative;
- le modalità operative di gestione del protocollo, dei flussi documentali e procedimentali, degli archivi;
- l'uso del titolario di classificazione e del piano di fascicolazione;
- le modalità di accesso alle informazioni da parte di coloro che ne hanno titolo ed interesse, in attuazione del principio di trasparenza dell'azione amministrativa;

1.2 Ambito di applicazione del manuale

Il presente Manuale di gestione documentale del protocollo informatico, dei flussi documentali e degli archivi è adottato ai sensi degli artt. 40-bis, 41, 47 e 71 del C.A.D. di cui D.L. 82/2005 ed aggiornato alle Linee guida AgID sulla formazione, gestione e conservazione dei documenti informatici in vigore dal 01/01/2022. Esso descrive le attività di formazione, registrazione, classificazione, fascicolazione ed archiviazione dei documenti, oltre che la gestione dei flussi documentali dell'Ente, ed ai sensi del DPCM 3 dicembre 2013, contenente "Regole tecniche per il protocollo informatico", per i seguenti articoli:
• art. 2 comma 1, *Oggetto e ambito di applicazione*;
• art. 6, *Funzionalità*;
• art. 9, *Formato della segnatura di protocollo*;
• art. 18 commi 1 e 5, *Modalità di registrazione dei documenti informatici*;
• art. 20, *Segnatura di protocollo dei documenti trasmessi*;
• art. 21, *Informazioni da includere nella segnatura*.
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 informativo 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

Ai fini del presente Manuale s'intende:
• per "CAD", il decreto legislativo 7 marzo 2005 n. 82 – Codice dell'amministrazione digitale, nel testo vigente.
• 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.
Per "Linee Guida" le linee Guida AgID sulla formazione, gestione e conservazione dei documenti informatici in vigore dal 01/01/2022

Si riportano di seguito, gli acronimi utilizzati più frequentemente:

- AOO - Area Organizzativa Omogenea;
- PdP - Prodotto di Protocollo informatico – l'applicativo sviluppato o acquisito dall'amministrazione/AOO per implementare il servizio di protocollo informatico;
- UO – Unità Organizzativa – unità organizzativa interna (settore, servizio, ufficio)
- UCP - Unità Organizzativa Centrale di registrazione di Protocollo – rappresenta l'ufficio centrale di protocollo

- UOP – Unità Organizzativa di registrazione di Protocollo – unità organizzativa abilitata alla protocollazione, diversa dall'ufficio centrale di protocollo.
- 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;
- RPA Responsabile del Procedimento Amministrativo - il dipendente che ha la responsabilità dell'esecuzione degli adempimenti amministrativi relativi ad un affare;
- RSP - Responsabile della gestione documentale e del Servizio di Protocollo informatico;
- MdG - Manuale di Gestione del protocollo informatico, dei flussi documentali e degli archivi;

1.4 Norme di riferimento

Le principali norme di riferimento sono elencate nell'allegato 1 - Norme di riferimento"

2 DOCUMENTI E MODALITA' DI GESTIONE

La gestione documentale è un processo che può essere suddiviso in tre fasi principali: formazione, gestione e conservazione. Nell'ambito di ognuna delle suddette fasi si svolgono una serie di attività che si distinguono per complessità, impatto, natura, finalità e/o effetto, anche giuridico, alle quali corrispondono approcci metodologici e prassi operative distinte.

Il sistema di gestione informatica dei documenti è presidiato da specifiche procedure e strumenti informatici, in grado di governare con efficacia ogni singolo accadimento che coinvolge la vita del documento ed effettuata secondo i principi generali applicabili in materia di trattamento dei dati personali anche mediante un'adeguata analisi del rischio

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;
- inviato;
- interno formale
- interno informale

2.1 Il documento informatico

Il Codice dell'Amministrazione Digitale definisce il documento informatico come "la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti"
Il documento informatico è formato mediante una delle seguenti modalità:

a) creazione tramite l'utilizzo di strumenti software o servizi cloud qualificati che assicurino la produzione di documenti nei formati e nel rispetto delle regole di interoperabilità
b) acquisizione di un documento informatico per via telematica o su supporto informatico, acquisizione della copia per immagine su supporto informatico di un documento analogico, acquisizione della copia informatica di un documento analogico;
c) memorizzazione su supporto informatico in formato digitale delle informazioni risultanti da transazioni o processi informatici o dalla presentazione telematica di dati attraverso moduli o formulari resi disponibili all'utente;
d) generazione o raggruppamento anche in via automatica di un insieme di dati o registrazioni, provenienti da una o più banche dati, anche appartenenti a più soggetti interoperanti, secondo una struttura logica predeterminata e memorizzata in forma statica.

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.
Il documento informatico deve essere identificato in modo univoco e persistente L'identificazione dei documenti oggetto di registrazione di protocollo è rappresentata dalla segnatura di protocollo univocamente associata al documento. L'identificazione deidocumenti non protocollati è affidata alle funzioni del sistema di gestione informatica deidocumenti. In alternativa l'identificazione univoca può essere realizzata mediante associazione al documento di una sua impronta crittografica basata su funzioni di hashche siano ritenute c rittograficamente sicure, e conformi alle tipologie di algoritmi previsti nell'allegato 6 delle Linee Guida sulla formazione, gestione e conservazione dei documenti informatici.

2.1.1 Immodificabilità e integrità del documento informatico

Il documento amministrativo informatico assume le caratteristiche di immodificabilità e di integrità, oltre che con le modalità di cui al paragrafo 2.11, anche con la sua registrazione nel registro di protocollo, negli ulteriori registri, nei repertori, negli albi, negli elenchi, negli archivi o nelle raccolte di dati contenute nel sistema di gestione informatica dei documenti.
I documenti costituenti atti amministrativi con rilevanza interna al procedimento amministrativo sottoscritti con firma elettronica avanzata hanno l'efficacia prevista dall'art. 2702 del codice civile.
Sono inclusi i documenti soggetti a registrazione particolare, che comunque devono contenere al proprio interno o avere associati l'insieme minimo dei metadati previsti per il documento amministrativo informatico.
In applicazione dell'art.23-ter comma 5-bis del CAD16, i documenti amministrativi informatici devono essere accessibili secondo le regole previste dall'art. 11 della legge n. 4/2004".

2.2 Il documento amministrativo informatico

Al documento amministrativo informatico si applicano le stesse regole valide per il documento informatico, salvo quanto specificato nel presente paragrafo. Il documento amministrativo informatico assume le caratteristiche di immodificabilità e di integrità, oltre che con le modalità di cui al paragrafo 2.1, anche con la sua registrazione nel registro di protocollo, negli ulteriori registri, nei repertori, negli albi, negli elenchi, negli archivi o nelle raccolte di dati contenute nel sistema di gestione informatica dei documenti con le modalità descritte nel manuale di gestione documentale. Al documento amministrativo informatico viene associato l'insieme dei metadati previsti per la registrazione di protocollo ai sensi dell'art 53 del TUDA, nonché i metadati relativi alla classificazione, ai sensi dell'articolo 56 del TUDA, e ai tempi di conservazione, in coerenza con il piano di conservazione, e quelli relativi alla relazione con l'aggregazione documentale informatica d'appartenenza. Al documento amministrativo informatico sono associati ulteriori metadati rilevanti ai fini amministrativi o per finalità gestionali o conservative, definiti, per ogni tipologia di documento, nell'ambito del contesto a cui esso si riferisce, secondo quanto previsto dall'Allegato 5 delle Linee guida Agid. In applicazione dell'art.23-ter comma 5-bis del CAD, i documenti amministrativi informatici devono essere accessibili secondo le regole previste dall'art. 11 della legge n. 4/2004.

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.

2.3 Il documento analogico – cartaceo amministrativo

Per documento analogico s'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), come le immagini su film (esempio: pellicole mediche, microfilm), come le magnetizzazioni su nastro (esempio: cassette e nastri magnetici audio e video) su supporto non digitale". Di seguito faremo riferimento a un documento amministrativo cartaceo predisposto con strumenti informatici (ad esempio, una lettera prodotta tramite un software di office automation) e poi stampato.
In quest'ultimo caso si definisce "originale" il documento cartaceo nella sua redazione definitiva, perfetta ed autentica negli elementi sostanziali e formali, comprendente tutti gli elementi di garanzia e di informazione del mittente e del destinatario, stampato su carta intestata e dotato di firma autografa.

2.4 Copia informatica di documento analogico

La copia informatica di documento analogico è formata mediante copia per immagine (scansione di documento amministrativo cartaceo o altra modalità) che genera un documento informatico con contenuto e forma identici a quelli dell'originale analogico.
La copia ha la stessa efficacia probatoria dell'originale da cui è tratta se la conformità all'originale non è espressamente disconosciuta.
La dichiarazione di conformità all'originale:
- Certifica il processo di formazione della copia che garantisce la corrispondenza di forma e contenuto di originale e copia
- E' attestata dal Direttore o dal funzionario dell'Ente delegato ad autenticare le copie
- E' sottoscritta con firma digitale del Direttore o del funzionario delegato (in quanto sostituisce anche il timbro)

- Può essere inserita nel documento informatico contenente la copia informatica, oppure può essere prodotta come documento informatico separato contenente un riferimento temporale e l'impronta di ogni copia.

Formule

Il sottoscritto, nella sua qualità di Direttore/funzionario delegato dal Direttore, attesta che la presente copia del sopra-riportato documento è stata prodotta mediante l'utilizzo di un sistema di gestione documentale conforme alle regole tecniche vigenti che garantisce la corrispondenza di forma e contenuto all'originale. Il Funzionario Incaricato Firmato digitalmente

La distruzione degli originali analogici potrà essere effettuata in accordo con le previsioni di cui all'art. 22, commi 4 e 5 del CAD.

2.5 Copia analogica di documento informatico

La copia analogica (cartacea) di documento informatico formata mediante il sistema di gestione documentale, conforme alle regole tecniche vigenti in materia di formazione, copia, duplicazione, riproduzione e validazione, conservazione dei documenti informatici amministrativi (D.P.C.M. 14 novembre 2014) ha la stessa efficacia probatoria dell'originale da cui è tratta se la conformità all'originale non è espressamente disconosciuta.
La copia riporta in calce l'indicazione della conformità del sistema alle regole tecniche vigenti.

Formula

Copia analogica di documento informatico prodotta con sistema di gestione documentale conforme alle regole tecniche vigenti (D.P.C.M. 14 novembre 2014)

Se la copia analogica (cartacea) di documento informatico è formata al di fuori del sistema di gestione documentale, la conformità viene attestata con apposita dichiarazione in calce alla copia, sottoscritta con firma autografa dal Direttore o dal funzionario da questi delegato ad autenticare le copie.

Formula

Il sottoscritto, nella sua qualità di Direttore/funzionario delegato dal Direttore, attesta che la presente copia del sopraripportato documento informatico è conforme all'originale. Il Funzionario Incaricato Firma autografa

2.6 Duplicati, copie ed estratti informatici di documenti informatici

Un duplicato informatico ha lo stesso valore giuridico del documento informatico da cui è tratto se è ottenuto mediante la memorizzazione della medesima evidenza informatica, sullo stesso dispositivo o su dispositivi diversi; ad esempio, effettuando una copia da un PC ad una pen-drive di un documento nel medesimo formato.
La copia di un documento informatico è un documento il cui contenuto è il medesimo dell'originale ma con una diversa evidenza informatica rispetto al documento da cui è tratto, come quando si trasforma un documento con estensione ".doc" in un documento ".pdf". L'estratto di un documento informatico è una parte del documento con una diversa evidenza informatica rispetto al documento da cui è tratto.
Tali documenti hanno lo stesso valore probatorio dell'originale da cui hanno origine se la stessa conformità non viene espressamente disconosciuta. In particolare, la validità del documento informatico per le copie e/o estratti di documenti informatici è consentita mediante uno dei due metodi:

- raffronto dei documenti;
- certificazione di processo.

I requisiti tecnici per la certificazione di processo sono individuati nell'allegato 3 "Certificazione di Processo" delle Linee Guida .Il ricorso ad uno dei due metodi sopracitati assicura la conformità del contenuto della copia o dell'estratto informatico alle informazioni del documento informatico di origine Fatto salvo quanto previsto dall'art. 23bis comma 2 del CAD nel caso in cui non vi è l'attestazione di un pubblico ufficiale, la conformità della copia o dell'estratto informatico ad un documento informatico è garantita mediante l'apposizione della firma digitale o firma elettronica qualificata o firma elettronica avanzata, nonché del sigillo elettronico qualificato e avanzato da parte di chi effettua il raffronto.

Laddove richiesta dalla natura dell'attività, l'attestazione di conformità delle copie o estratti informatici di documenti informatici può essere inserita nel documento informatico contenente la copia o l'estratto. Il documento informatico contenente l'attestazione è sottoscritto con firma digitale o con firma elettronica qualificata

Il sottoscritto, nella sua qualità di Direttore/funzionario delegato dal Direttore, attesta che il duplicato allegato è conforme all'originale. Il Funzionario Incaricato Firma digitale

2.7 Formazione del documento informatico

I documenti dell'amministrazione sono prodotti con sistemi informatici come previsto dalla vigente normativa, mediante una delle seguenti modalità:

a) creazione tramite l'utilizzo di strumenti software o servizi cloud qualificati che assicurino la produzione di documenti nei formati e nel rispetto delle regole di interoperabilità;
b) acquisizione di un documento informatico per via telematica o su supporto informatico, acquisizione della copia per immagine su supporto informatico di un documento analogico, acquisizione della copia informatica di un documento analogico;
c) memorizzazione su supporto informatico in formato digitale delle informazioni risultanti da transazioni o processi informatici o dalla presentazione telematica di dati attraverso moduli o formulari resi disponibili all'utente;
d) generazione o raggruppamento anche in via automatica di un insieme di dati o registrazioni, provenienti da una o più banche dati, anche appartenenti a più soggetti interoperanti, secondo una struttura logica predeterminata e memorizzata in forma statica

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;
- fare riferimento, in via principale, ad un solo fascicolo.

Le firme necessarie alla redazione e perfezione giuridica del documento in partenza devono essere apposte prima della sua protocollazione.
Il documento informatico è immodificabile se la sua memorizzazione su supporto informatico in formato digitale non può essere alterata nel suo accesso, gestione e conservazione.
Nel caso di documento informatico formato secondo la sopracitata lettera a), l'immodificabilità e l'integrità sono garantite da una o più delle seguenti operazioni:
● apposizione di una firma elettronica qualificata, di una firma digitale o di un sigillo elettronico qualificato o firma elettronica avanzata;
● memorizzazione su sistemi di gestione documentale che adottino idonee misure di sicurezza in accordo con quanto riportato al § 3.9;
● il trasferimento a soggetti terzi attraverso un servizio di posta elettronica certificata o un servizio elettronico di recapito certificato qualificato, come definito dal regolamento (UE) 23 luglio 2014 n. 910 del Parlamento europeo e del Consiglio in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno (regolamento eIDAS), valido ai fini delle comunicazioni
elettroniche aventi valore legale;
● versamento ad un sistema di conservazione.

Nel caso di documento informatico formato secondo la sopracitata lettera b) l'immodificabilità ed integrità sono garantite da una o più delle seguenti operazioni mediante:
● apposizione di una firma elettronica qualificata, di una firma digitale o di un sigillo elettronico qualificato o firma elettronica avanzata;
● memorizzazione su sistemi di gestione documentale che adottino idonee misure di sicurezza in accordo con quanto riportato al § 3.9;
● versamento ad un sistema di conservazione.

Nel caso di documento informatico formato secondo le sopracitate lettere c) e d) le caratteristiche di immodificabilità e di integrità sono garantite da una o più delle seguenti operazioni:

● apposizione di una firma elettronica qualificata, di una firma digitale o di un sigillo elettronico qualificato o firma elettronica avanzata
● registrazione nei log di sistema dell'esito dell'operazione di formazione del documento informatico, compresa l'applicazione di misure per la protezione dell'integrità delle basi di dati e per la produzione e conservazione dei log di sistema;
● produzione di una estrazione statica dei dati e il trasferimento della stessa nel sistema di conservazione.

Al momento della formazione del documento informatico immodificabile, devono essere generati e associati permanentemente ad esso i relativi metadati. L'insieme dei metadati del documento informatico è definito nell'allegato 5 "Metadati" alle presenti linee guida. Potranno essere individuati ulteriori metadati da associare a particolari tipologie di documenti informatici. Devono essere riportati i metadati definiti per ogni tipologia di documento.
Eventuali ulteriori metadati sono definiti in funzione del contesto e delle necessità gestionali e conservative.
Per agevolare il processo di formazione dei documenti informatici e consentire, al tempo stesso, la trattazione automatica dei dati in essi contenuti, l'AOO rende disponibili per via telematica, in primo luogo avvalendosi del sistema di gestione documentale e del portale dell'Ente, moduli e formulari standardizzati validi ad ogni effetto di legge.

2.8 Documento ricevuto

La corrispondenza in ingresso può essere acquisita dalla AOO con diversi mezzi e modalità in base alla tecnologia di trasporto utilizzata dal mittente.

Un documento informatico può essere recapitato, a titolo esemplificativo:

- a mezzo posta elettronica convenzionale o certificata;
- su supporto rimovibile quale, ad esempio, CD ROM, DVD, floppy disk, pen drive, hard disk esterni, etc, consegnato direttamente o inviato per posta convenzionale o corriere;
- 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 CAD, 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".

2.9 Documento inviato

I documenti informatici, con gli eventuali allegati, anch'essi informatici, sono inviati di norma per mezzo della posta elettronica convenzionale o 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 prioritariamente mediante l'utilizzo della posta elettronica certificata o in cooperazione applicativa.

2.10 Documento interno formale

I documenti interni sono formati con tecnologie informatiche avvalendosi del sistema di scrivania e gestione documentale.
Il documento informatico di rilevanza amministrativa giuridico-probatoria scambiato tra unità organizzative mediante il sistema di gestione documentale viene preventivamente sottoscritto con firma digitale o altra firma elettronica. Il sistema in uso è in grado di tracciare in modo immodificabile tutte le operazioni relative a una registrazione, con un meccanismo di attribuzione alla singola persona di documenti o annotazioni che configura i requisiti per l'identificazione informatica.

2.11 Documento interno informale

Per questa tipologia di corrispondenza vale quanto illustrato nel paragrafo precedente, ad eccezione della obbligatorietà dell'operazione di sottoscrizione elettronica.

2.12 La firma

Nell'ambito del sistema di gestione documentale questo Ente utilizza le seguenti tipologie di firma:
Semplice: insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo d'identificazione informatica in forma di PIN o insieme di Username e Password.
La firma semplice viene utilizzata per l'autenticazione a fini di consultazione e accesso all'erogazione di servizi:

- all'interno dell'Ente per l'utilizzo delle procedure documentali dei software applicativi secondo i diversi livelli di autorizzazione (amministratore, operatore, abilitato alla consultazione)
- per la consultazione di fascicoli informatici sul sito dell'Ente in quanto soggetto interessato al procedimento;
- per il download di documentazione dal sito dell'Ente
- per procedimenti semplici sul sito dell'Ente ad esempio pagamenti.

Non ha valore di sottoscrizione.
La firma semplice viene rilasciata a tutti gli operatori del sistema di gestione documentale.
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 Naz. Servizi.
Nei rapporti con i soggetti esterni, segnatamente in caso di ricezione dei documenti la firma avanzata per così dire "sostitutiva" rappresentata dalla ricevuta completa della PEC, costituisce legittimazione per l'inserimento all'interno di un'istruttoria procedimentale di documentazione prodotta dal mittente interessato al procedimento.
All'interno dell'Ente la firma avanzata viene utilizzata come sistema di validazione di fasi procedimentali, di comunicazione interna, di abilitazione allo svolgimento di attività specifiche.
Non ha valore di sottoscrizione con rilevanza esterna.
La firma avanzata viene rilasciata a tutti gli operatori del sistema di gestione documentale.
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.
La firma avanzata viene rilasciata a tutti i Responsabili di procedimento e tutti gli operatori legittimati alla sottoscrizione di documenti aventi rilevanza esterna.
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.
In relazione al valore legale di firma autografa e sottoscrizione, garantisce, oltre alla provenienza, anche l'integrità e l'autenticità del documento sottoscritto, inoltre sostituisce l'apposizione di timbri e sigilli.
Viene utilizzata per la firma di provvedimenti con effetto costitutivo, modificativo o estintivo di rapporti giuridici, sia di natura pubblicistica (delibere, decreti, determinazioni, ordinanze, buoni di ordinazione, ordinativi di incasso e pagamento, documenti finanziari e contabili, pareri etc) che privatistica e contrattuale (contratti, ordini, contabilizzazioni di lavori pubblici) che verranno versati nel sistema di conservazione.
La firma digitale è rilasciata a tutti i Responsabili di procedimento anche con delega all'adozione di provvedimenti, ai Responsabili di Servizio e tutti gli operatori legittimati alla sottoscrizione di documenti aventi rilevanza esterna.
Firma autografa: su documenti analogici e copie analogiche di documenti informatici.

2.13 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 (Direttore dell'Ente o funzionario delegato dal Direttore) che attesta, firmando con firma digitale, che

a) la firma è stata apposta in sua presenza dal titolare, previo accertamento della sua identità personale,
b) l'eventuale certificato elettronico utilizzato è valido
c) Il documento sottoscritto non è in contrasto con l'ordinamento giuridico.

L'autenticazione avviene anche mediante l'acquisizione digitale della sottoscrizione autografa, o di qualsiasi altro tipo di firma elettronica avanzata.

Se al documento informatico autenticato deve essere allegato altro documento formato in originale su altro tipo di supporto, il pubblico ufficiale può allegare copia informatica autenticata.

2.14 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.

2.15 Trasmissione documenti con il sistema pubblico di connettività

Lo scambio dei documenti informatici tra le varie amministrazioni, e con i cittadini, avviene attraverso meccanismi di "interoperabilità" e "cooperazione applicativa". L'articolo 72 del CAD, 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;
- 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;
- 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.

Il rispetto degli standard di protocollazione e di scambio dei messaggi garantisce l'interoperabilità dei sistemi di protocollo.

L'interoperabilità e la cooperazione applicativa tra le Amministrazioni Pubbliche sono attuate attraverso una infrastruttura condivisa a livello nazionale, operante sul Sistema Pubblico di Connettività (SPC), che si colloca nel contesto definito dal CAD. Quest'ultimo definisce il SPC come "insieme di infrastrutture tecnologiche e di regole tecniche, per lo sviluppo, la condivisione, l'integrazione e la diffusione del patrimonio informativo e dei dati della pubblica amministrazione, necessarie per assicurare l'interoperabilità di base ed evoluta e la cooperazione applicativa dei sistemi informatici e dei flussi informativi, garantendo la sicurezza, la riservatezza delle informazioni, nonché la salvaguardia e l'autonomia del patrimonio informativo di ciascuna pubblica amministrazione."

2.16 Uso della Posta Elettronica Certificata

Le comunicazioni di documenti tra le pubbliche amministrazioni e i privati cittadini e professionisti avvengono di norma mediante l'utilizzo della posta elettronica o della postaelettronica certificata; esse sono valide ai fini del procedimento amministrativo una volta che ne sia verificata la provenienza.

Ai fini della verifica della provenienza le comunicazioni sono valide se:

a) sono sottoscritte con firma digitale o altro tipo di firma elettronica qualificata;
b) ovvero sono dotate di protocollo informatizzato;

c) ovvero è comunque possibile accertarne altrimenti la provenienza, secondo quanto preisto dalla normativa vigente;
d) ovvero trasmesse attraverso sistemi di posta elettronica certificata di cui aldecreto del Presidente della Repubblica 11 febbraio 2005, n. 68.

La trasmissione telematica di comunicazioni che necessitano di una ricevuta di invio e diuna ricevuta di consegna avviene mediante la posta elettronica certificata ai sensi del decreto del Presidente della Repubblica 11 febbraio 2005, n. 68.

La trasmissione del documento informatico per via telematica, effettuata mediante la posta elettronica certificata, equivale, nei casi consentiti dalla legge, alla notificazione per mezzo della posta.

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;
- interoperare e cooperare dal punto di vista applicativo con altre AOO.

Il documento informatico trasmesso per via telematica si intende inviato e pervenuto al destinatario se trasmesso all'indirizzo elettronico da questi dichiarato. 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.

L'AOO dispone almeno di una casella di Posta Elettronica Certificata istituzionale per la corrispondenza, sia in ingresso che in uscita, pubblicata sull'Indice delle Pubbliche Amministrazioni (IPA). Tale casella costituisce l'indirizzo virtuale della AOO e di tutti gli uffici che ad essa fanno riferimento.

All'interno dell'Indice delle Pubbliche Amministrazioni (IPA) sono resi disponibili i riferimenti (PEC) per comunicare con le Pubbliche Amministrazioni e i Gestori di Pubblici Servizi.

In IPA trovi i riferimenti necessari per la fatturazione elettronica e per gli ordini elettronici.

Per quanto riguarda utilizzo della posta elettronica per le comunicazioni tra Pubbliche Amministrazioni è da intendersi quale modalità transitoria nelle more dell'applicazione delle comunicazioni tra AOO tramite cooperazione applicativa" come previsto dall'allegato 6 delle Linee Guida.

2.17 Interoperabilità dei sistemi di protocollo informatico

Per interoperabilità dei sistemi di protocollo informatico s'intende la possibilità di trattamento automatico, da parte di un sistema di protocollo ricevente, delle informazioni trasmesse da un sistema di protocollo mittente, allo scopo di automatizzare anche le attività ed i processi amministrativi conseguenti.
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 e all'efficienza interna, si collocano in una dimensione più ampia nell'ottica della interconnessione e interoperabilità dei sistemi informativi pubblici.

Per interoperabilità dei sistemi di gestione documentale e protocollo informatico s'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 e 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 gestione documentale e protocollo informatico gestito dalle pubbliche amministrazioni distribuite sul territorio è necessario, in primo luogo, stabilire una modalità di comunicazione comune, che consenta la trasmissione telematica dei documenti sulla rete.
Alla luce del decreto Legislativo 7 marzo 2005, n. 82, (di seguito CAD), i mezzi di comunicazione telematica di base, sono costituiti dalla:

- posta elettronica e posta elettronica certificata, con l'impiego del protocollo SMTP e del formato MIME per la codifica dei messaggi secondo quanto indicato nelle regole tecniche per il protocollo informatico previste dal CAD (di seguito regole tecniche);
- cooperazione applicativa basata sul Sistema Pubblico di Connettività (di seguito SPC) e Sistema Pubblico di Cooperazione (di seguito SPCoop). In tale caso i messaggi scambiati tra Enti e PA attraverso le Porte di Dominio, secondo gli standard definiti nell'ambito dell'SPCoop, sono racchiusi in una busta (di seguito Busta di e-Gov) costituita da un uso della struttura SOAP 1.1 con estensioni (come indicato nelle regole tecniche del SPC di cui al D.P.C.M. 1 aprile 2008).

Oltre ad una modalità di comunicazione comune, l'interoperabilità dei sistemi di protocollo richiede anche una efficace interazione dei sistemi di gestione documentale. In questo senso, le regole tecniche stabiliscono che ogni messaggio protocollato debba riportare alcune informazioni archivistiche fondamentali, per facilitare il trattamento dei documenti da parte del ricevente. Tali informazioni sono incluse nella segnatura informatica di ciascun messaggio protocollato.
Secondo quanto previsto nelle regole tecniche, con il presente documento, reso disponibile anche sul sito web dell'Agenzia per l'Italia Digitale, sono indicate le modalità di trasmissione dei documenti informatici, il tipo ed il formato delle informazioni archivistiche di protocollo minime ed accessorie comunemente scambiate tra le pubbliche amministrazioni e associate ai messaggi protocollati.
Le modalità tecniche ed il formato definiti verranno adeguati in relazione all'evoluzione tecnologica e alle eventuali ulteriori esigenze che le amministrazioni dovessero manifestare a seguito della loro applicazione.

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, in partenza nell'ambito di un sistema di gestione documentale aggiornato alle Linee Guida sullaformazione, gestione e conservazione dei documenti informatici (Maggio 2021)
Il registro 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.
I responsabili dei procedimenti amministrativi dei singoli uffici provvedono alla implementazione della fascicolazione della corrispondenza in arrivo ed alla protocollazionee fascicolazione della corrispondenza in partenza. Gestiscono e custodiscono i documenti dell'archivio corrente (e, in alcuni casi, dell'archivio di deposito).

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

- risorse archivistiche: piano di classificazione o titolario del presente manuale di gestione documentale
- risorse informatiche: software applicativo dedicato (Allegato 7), piattaforma documentale, PEC e posta elettronica ordinaria, cooperazione applicativa tra Pubbliche Amministrazioni, piattaforme di interscambio;
- risorse umane: operatori del servizio, responsabile della gestione documentale, coordinatore della gestione documentale (Allegato 2)
- risorse normative: D.Lsg 82/2005, Linee Guida sulla formazione, gestione e conservazione dei documenti informatici (Maggio 2021), il presente manuale.

In particolare, il sistema di protocollo informatico garantisce:

- a) l'univoca identificazione ed autenticazione degli utenti;
- b) la garanzia di accesso alle risorse esclusivamente agli utenti abilitati e/o a gruppi di utenti secondo la definizione di appositi profili;
- c) il tracciamento permanente di qualsiasi evento di modifica delle informazioni trattate e l'individuazione del suo autore.

Il protocollo informatico assicura il tracciamento e la storicizzazione di ogni operazione, comprese le operazioni di annullamento, e la loro attribuzione all'operatore. Il sistema di protocollo informatico assicura che:

● le informazioni relative all'oggetto, al mittente e al destinatario di una registrazione di protocollo, non possano essere modificate, ma solo annullate con la procedura prevista dall'art. 54 del TUDA27;
● le uniche informazioni modificabili di una registrazione di protocollo siano l'assegnazione interna all'amministrazione e la classificazione;
● le azioni di annullamento provvedano alla storicizzazione dei dati annullati attraverso le informazioni oggetto della stessa;
● per ognuno di questi eventi, anche nel caso di modifica di una delle informazioni di cui al punto precedente, il sistema storicizza tutte le informazioni annullate e modificate rendendole entrambe visibili e comparabili, nel rispetto di quanto previsto dall'art. 54, comma 2 del TUDA.

3.2 Aree Organizzative Omogenee e modelli organizzativi

L'amministrazione individua un'unica Area Organizzativa Omogenea (AOO) che è composta dall'insieme di tutte le unità organizzative (settori, servizi, uffici). All'interno della AOO il sistema di protocollazione è 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 per la corrispondenza in entrata e per la corrispondenza in uscita.
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.

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 tutti i dati. Per maggiori dettagli si rimanda alla sezione 3.3 del presente Manuale di Gestione Documentale

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

Nell'ambito degli adempimenti previsti, l'Ente si è accreditato 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 l'amministrazione;
- l'indirizzo della sede principale dell'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 d'istituzione;
  - – dell'eventuale data di soppressione;
- l'elenco degli UOR e degli UU dell'AOO.
- i dati relativi alla fatturazione elettronica

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.

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

Nell'AOO precedentemente individuata 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 della gestione documentale e del Servizio di Protocollo informatico (RSP). La nomina è riportata nell'allegato 2 del presente manuale gestione documentale.

Il Responsabile è funzionalmente individuato nella figura del Responsabile dell'Area amministrativa. In caso di assenza del Responsabile, le sue funzioni sono demandate al vicario formalmente delegato.

E' compito del Responsabile:

- provvedere all'aggiornamento e all'eventuale revisione del Manuale della gestione documentale e del Servizio di Protocollo informatico;
- 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;
- supervisionare la leggibilità nel tempo di tutti i documenti trasmessi o ricevuti dalla AOO attraverso l'adozione dei formati standard ammessi dalla normativa vigente;
- la supervisione dell'invio del pacchetto di versamento che sarà formato dai delegati di ogni unità organizzativa dell'AOO e quindi del transito del pacchetto al sistema di conservazione. Il documento, il fascicolo o l'aggregazione per poter essere correttamente versati in conservazione devono essere stati formati e gestiti in ottemperanza alle regole tecniche sulla formazione, protocollazione e firma secondo le regole tecniche e secondo quanto esplicitato nel presente manuale.
- proporre eventuali modifiche al Titolario di classificazione;
- curare le funzionalità del sistema affinché, in caso di guasti o anomalie, siano ripristinate nel più breve tempo possibile e comunque in conformità a quanto stabilito nel Piano di continuità operativa/DR e relativi allegati;
- conservare le copie di salvataggio delle informazioni del sistema di protocollo e del registro di emergenza in luoghi sicuri e diversi da quello in cui viene custodito il suddetto sistema;
- 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 e le attività di gestione degli archivi;
- autorizzare le operazioni di annullamento della registrazione di protocollo;
- aprire e chiudere il registro di protocollazione di emergenza.

3.5 La classificazione dei documenti

La classificazione è un'attività di organizzazione logica di tutti i documenti correnti, protocollati e non (spediti, ricevuti, interni) secondo uno schema di voci che identificano attività e materie specifiche del soggetto produttore.
La classificazione ha il fine di organizzare logicamente tutti i documenti amministrativi informatici prodotti o ricevuti da un ente nell'esercizio delle sue funzioni. L'attività di classificazione si avvale del piano di classificazione che mappa, su più livelli gerarchici, tutte le funzioni dell'ente.
La classificazione è un'attività obbligatoria nel sistema di gestione informatica dei documenti dell'Ente e si applica a tutti i documenti prodotti e acquisiti

Il sistema complessivo di organizzazione dei documenti è definito nel titolario di classificazione.
Lo scopo del titolario di classificazione è di guidare la sedimentazione dei documenti secondo le funzioni del soggetto. La classificazione collega ciascun documento in maniera univoca ad una precisa unità archivistica, il fascicolo

3.6 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 entro la giornata lavorativa successiva al sistema di conservazione, garantendone l'immodificabilità del contenuto.

3.7 Tutela dei dati personali

L'amministrazione, titolare dei dati di protocollo e dei dati personali contenuti nella documentazione amministrativa di propria pertinenza, dà attuazione al dettato del decreto legislativo 30 giugno 2003 n. 196 e del REG. UE 679/2016 e s.m.i. con atti formali aventi rilevanza interna ed esterna.

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

Riguardo agli adempimenti esterni, l'Amministrazione si è organizzata 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. Inoltre l'amministrazione certificante, in caso di accesso diretto ai propri archivi, rilascia all'amministrazione procedente apposita autorizzazione in cui vengono indicati i limiti e le condizioni di accesso volti ad assicurare la riservatezza dei dati personali ai sensi della normativa vigente. Di norma l'interfaccia di accesso è configurata in modo da inglobare tali limitazioni, prevenendo così alla fonte eventuali accessi illeciti o eccedenti le effettive necessità.
Viene quindi 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.

3.8 Formazione del personale

Nell'ambito delle attività di attivazione ed applicazione del sistema di gestione documentale e di workflow, l'Ente organizza 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'unità organizzativa all'interno dell'AOO sia gli strumenti informatici e le norme di base per la tutela dei dati personali, la raccolta, la registrazione e l'archiviazione delle informazioni, vengono effettuati percorsi formativi e di aggiornamento volti ad assicurare l'operatività del personale stesso.

3.9 Misure di sicurezza

Nell'attuazione delle presenti Linee Guida, 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. In tale ottica, il responsabile della gestione documentale ovvero, ove nominato, il coordinatore della gestione documentale, in accordo con il responsabile della conservazione di cui al paragrafo 4.6, con il responsabile per la transizione digitale e acquisito il parere del responsabile della protezione dei dati personali, predispone il piano della sicurezza del sistema di gestione informatica dei documenti, prevedendo opportune misure tecniche e organizzative per garantire un livello di sicurezza adeguato al rischio in materia di protezione dei dati personali, ai

sensi dell'art. 32 del Regolamento UE 679/2016 (GDPR)39, anche in funzione delle tipologie di dati trattati, quali quelli riferibili alle categorie particolari di cui agli artt. 9-10 del Regolamento stesso.
L'adozione delle predette misure è in capo al titolare o, in caso di trattamento effettuato per suo conto, al responsabile del trattamento, individuato sulla base dell'art. 28 "Responsabile del trattamento" del Regolamento.
Il piano conterrà altresì la descrizione della proceduta da adottarsi in caso di violazione dei dati personali ai sensi degli artt. 33-34 del Regolamento UE 679/201640, e sarà redatto nell'ambito del piano generale della sicurezza, in coerenza con quanto previsto dal Piano Triennale per l'Informatica nella Pubblica Amministrazione vigente.
In conformità all'art. 28 del Regolamento UE 679/2016, i soggetti esterni a cui è eventualmente delegata la tenuta del sistema di gestione informatica dei documenti sono individuati come Responsabili del trattamento dei dati e devono presentare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del Regolamento e garantisca la tutela dei diritti dell'interessato.
I soggetti privati appartenenti ad organizzazioni che applicano particolari regole di settore per la sicurezza dei propri sistemi informatici possono adottare misure di sicurezza per garantire la tenuta del documento informatico. Le citate misure di sicurezza ICT emanate dall'AGID possono costituire, a tal fine, un modello di riferimento, fermo restando gli obblighi previsti dal citato Regolamento Reg. UE 679/2016.
I servizi devono sempre organizzati nel rispetto dei principi e dei requisiti previsti in materia di sicurezza dei dati e dei sistemi dagli artt.32 e 34 del Regolamento, avuto riguardo anche alla notifica delle violazioni dei dati personali di cui all'art.33 del Regolamento 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

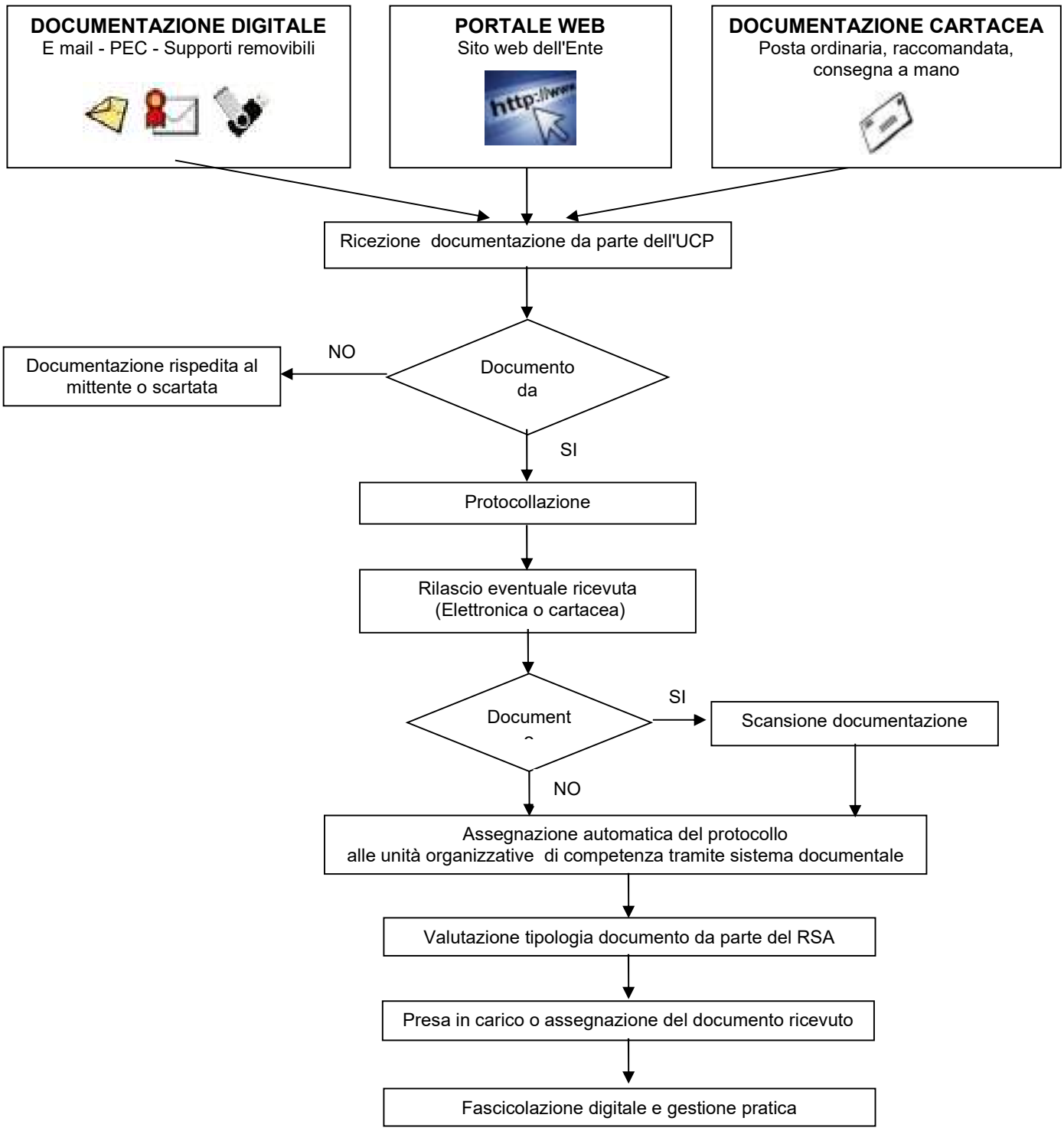
Per descrivere i flussi di lavorazione dei documenti all'interno della AOO si fa riferimento ai diagrammi di flussi riportati nelle pagine seguenti.
Essi si riferiscono, in particolare, ai documenti:

- ricevuti dalla AOO, dall'esterno
- inviati dalla AOO, all'esterno

La schematizzazione riguardante i documenti ricevuti si riferisce a un flusso di lavoro ove la maggior parte delle operazioni sono gestite dall'ufficio protocollo.
L'avvio effettivo del procedimento collegato alla documentazione protocollata viene gestita dalle singole unità organizzative competenti

La schematizzazione riguardante i documenti inviati si riferisce ad un flusso di lavoro svolto prevalentemente dall'unità organizzativa competente.

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 la casella di posta elettronica certificata.
Tale regola rappresenta la norma anche per la ricezione dei documenti per i quali è richiesta la pubblicazione all'Albo Pretorio on line dell'Ente.
Ogni messaggio deve riferirsi a una sola questione. Anche nel caso in cui vengano inviati contestualmente più documenti, deve essere possibile attribuire all'invio una unica protocollazione, e una unica classificazione.
Quando i documenti informatici pervengono all'ufficio protocollo (o ad altro servizio tramite la propria casella di posta elettronica certificata) la stessa unità, previa verifica della validità della firma apposta e della leggibilità del documento, procede alla registrazione di protocollo.
Essa comprende anche i processi di verifica dell'autenticità, della provenienza e dell'integrità dei documenti stessi. 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 comunemente scambiate tra le AOO e associate ai documenti protocollati.
Le caselle PEC sono controllate quotidianamente, nei giorni di apertura degli uffici, dall'UCP o dai singoli servizi.
I documenti ricevuti per via telematica sono resi disponibili agli uffici attraverso il sistema di gestione documentale adottato dall'Ente subito dopo l'operazione di classificazione e smistamento.

4.2.2 Ricezione di documenti informatici sulla casella di posta elettronica tradizionale

Nel caso in cui il messaggio venga ricevuto su una casella di posta elettronica non destinata specificamente al servizio di protocollazione e non PEC o similare, spettano al titolare della casella le valutazioni e le incombenze in merito alla ricevibilità, all'invio all'ufficio predisposto alla protocollazione e classificazione dello stesso con inserimento nel sistema di gestione documentale. I documenti pervenuti tramite fax server da indirizzi diversi da quello assegnato alla UCP sono trattati con gli stessi criteri indicati per la posta elettronica tradizionale. A ogni messaggio di posta elettronica corrisponde un'unica operazione di registrazione di protocollo. Quest'ultima si può riferire sia al corpo del messaggio, sia a uno o più file allegati.
Le comunicazioni pervenute da altre amministrazioni, attraverso gli stessi canali, sono considerate valide ai fini del procedimento amministrativo se è possibile accertarne la provenienza, in conformità a quanto previsto dall'art. 47 del CAD.

4.2.3 Ricezione di documenti informatici tra PA tramite cooperazione applicata

Come previsto dall'allegato 6 delle Linee Guida, per dare seguito alla comunicazione tra AOO mittente e AOO destinataria della P.A., dal 01/01/2022 è possibile utilizzare lamodalità di trasmissione dei protocolli in cooperazione applicativa utilizzando il Simple Object Access Protocol (SOAP)

Per assicurare la comunicazione tra AOO in cooperazione applicativa, le Amministrazioni DEVONO registrare e mantenere aggiornato, per ogni AOO individuata nella propriaorganizzazione, l'Indice dei domicili digitali delle pubbliche amministrazioni e dei gestori di pubblici servizi (IPA) con il prefisso condiviso dagli endpoint di esposizione dei servizi indicati nell'Appendice B dell'Allegato 6 delle Linee Guida.

Le AOO mittente e AOO destinataria assicurano il non ripudio della comunicazione,provvedendo alla firma dei messaggi scambiati ed al loro trasposto su canale TLS tramite SOAP coerentemente alla specifica WS-Security.

4.2.4 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 che riesce a verificare, decodificare e interpretare con le tecnologie a sua disposizione.
Superata questa fase, il documento viene inserito nel flusso di lavorazione e sottoposto a tutti i controlli e gli adempimenti del caso.

4.2.5 Ricezione di documenti informatici da portale web dell'Ente

I documenti digitali possono anche essere ricevuti dall'Ente dal sito internet istituzionale, tramite apposito servizio web. Il cittadino, dopo essersi registrato al servizio, può avviare on line la procedura di erogazione dei servizi messi a disposizione dall'Ente. Al termine dell'operazione, verrà rilasciata all'utente una ricevuta attestante l'avvenuta presa in carico della sua richiesta.

4.2.6 Ricezione di documenti cartacei a mezzo servizio postale, corriere o consegnati a mano

I documenti pervenuti a mezzo posta convenzionale o tramite corriere sono consegnati all'ufficio protocollo. I documenti consegnati a mano agli uffici comunali sono verificati ed eventualmente consegnati all'ufficio protocollo che provvede alla protocollazione e correttamente inseriti nel sistema di gestione documentale.
Le buste o contenitori sono inizialmente esaminati per una preliminare verifica dell'indirizzo e del destinatario sugli stessi apposti.
La corrispondenza cartacea relativa a bandi di gara è registrata (con scansione della busta, e annotazione dell'orario preciso di ricezione ove richiesto) e in seguito consegnata chiusa all'ufficio responsabile della gara.
La corrispondenza personale non deve essere aperta, né protocollata: dev'essere consegnata al destinatario che ne valuterà il contenuto ed eventualmente, nel caso dovesse riguardare l'istituzione, consegnata all'ufficio protocollo per la registrazione e le operazioni complementari alla stessa. Quando la corrispondenza non rientra nelle categorie da ultimo indicate, si procede all'apertura delle buste e si eseguono i successivi controlli preliminari alla registrazione. La corrispondenza in arrivo è aperta il giorno lavorativo in cui è pervenuta, e contestualmente protocollata.
Le ricevute di ritorno della posta raccomandata potranno essere scansionate e inserite nel sistema di gestione documentale collegate al relativo fascicolo/procedimento.

4.2.7 Corrispondenza di particolare rilevanza e documenti esclusi

Quando un documento pervenuto appare di particolare rilevanza o delicatezza, indipendentemente dal supporto utilizzato, è preventivamente inviato in visione al Segretario Generale, che individua l'unità organizzativa o i singoli soggetti competenti a trattare il documento, fornendo eventuali indicazioni riguardo alla gestione del documento stesso.
Sono esclusi dalla registrazione di protocollo:

- bollettini ufficiali, notiziari della pubblica amministrazione;
- note di ricezione delle circolari e altre disposizioni;
- materiale statistico e certificazioni anagrafiche;
- 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.

4.2.8 Errata ricezione di documenti digitali

Nel caso in cui pervengano alle caselle e-mail dell'AOO messaggi istituzionali dal cui contenuto si rileva che sono stati erroneamente ricevuti, l'addetto rispedisce il messaggio al mittente con la dicitura "Messaggio pervenuto per errore - non di competenza di questa Amministrazione".
Se il messaggio è pervenuto tramite cooperazione applicativa da un'altra pubblica amministrazione, l'addetto inoltra la richiesta di annullamento di un messaggio di protocollo precedentemente ricevuto.

4.2.9 Errata ricezione di documenti cartacei

Nel caso in cui pervengano erroneamente all'Ente documenti indirizzati ad altre Amministrazioni o soggetti, possono verificarsi le seguenti eventualità:

- si restituiscono al servizio postale;
- se si tratta di documento cartaceo e la busta viene aperta per errore, il documento è protocollato in entrata e successivamente in uscita inserendo nel campo oggetto una nota del tipo "documento pervenuto per errore", provvedendo quindi al rinvio al mittente.

4.2.10 Rilascio di ricevute attestanti la ricezione di documenti informatici

La ricezione di documenti attraverso la casella di posta certificata comporta automaticamente la notifica al mittente dell'avvenuto recapito al destinatario, assicurata dallo stesso servizio di posta certificata.
Nel caso d'invio documentazione tramite servizi on line sul portale dell'Ente è automaticamente rilasciata dal sistema una ricevuta attestante l'invio della documentazione.
Nel caso di documenti inviati via posta elettronica certificata per la pubblicazione all'Albo pretorio Comunale, la conferma di pubblicazione (se richiesta) potrà essere trasmessa al mittente attraverso lo stesso canale, immediatamente dopo la scadenza della pubblicazione richiesta.
Nessuna ricevuta viene di norma rilasciata o trasmessa in caso di ricezione di documenti tramite posta elettronica tradizionale, salvo specifica richiesta.

4.2.11 Rilascio di ricevute attestanti la ricezione di documenti cartacei

Gli addetti alla protocollazione in arrivo non rilasciano, di regola, ricevute per i documenti che non sono soggetti a regolare protocollazione. Sono di regola esclusi dalla protocollazione i documenti non indirizzati all'Ente, per i quali lo stesso funge unicamente da tramite tra il mittente e il destinatario finale.
Quando il documento cartaceo è consegnato direttamente dal mittente o da altra persona incaricata all'ufficio protocollo ed è richiesto il rilascio di una ricevuta attestante l'avvenuta consegna, l'ufficio rilascia una ricevuta generata automaticamente dal sistema di protocollo oppure può essere rilasciata copia della prima pagina del documento (o fotocopia della busta chiusa) riportante il timbro o l'etichetta con gli estremi della segnatura.
Nel caso di istanze che diano avvio a un procedimento, in luogo del suddetto documento viene rilasciata una "ricevuta di presentazione/comunicazione di avvio del procedimento", riportante tutte le indicazioni richieste dalla normativa vigente.

4.2.12 Classificazione, assegnazione e presa in carico dei documenti

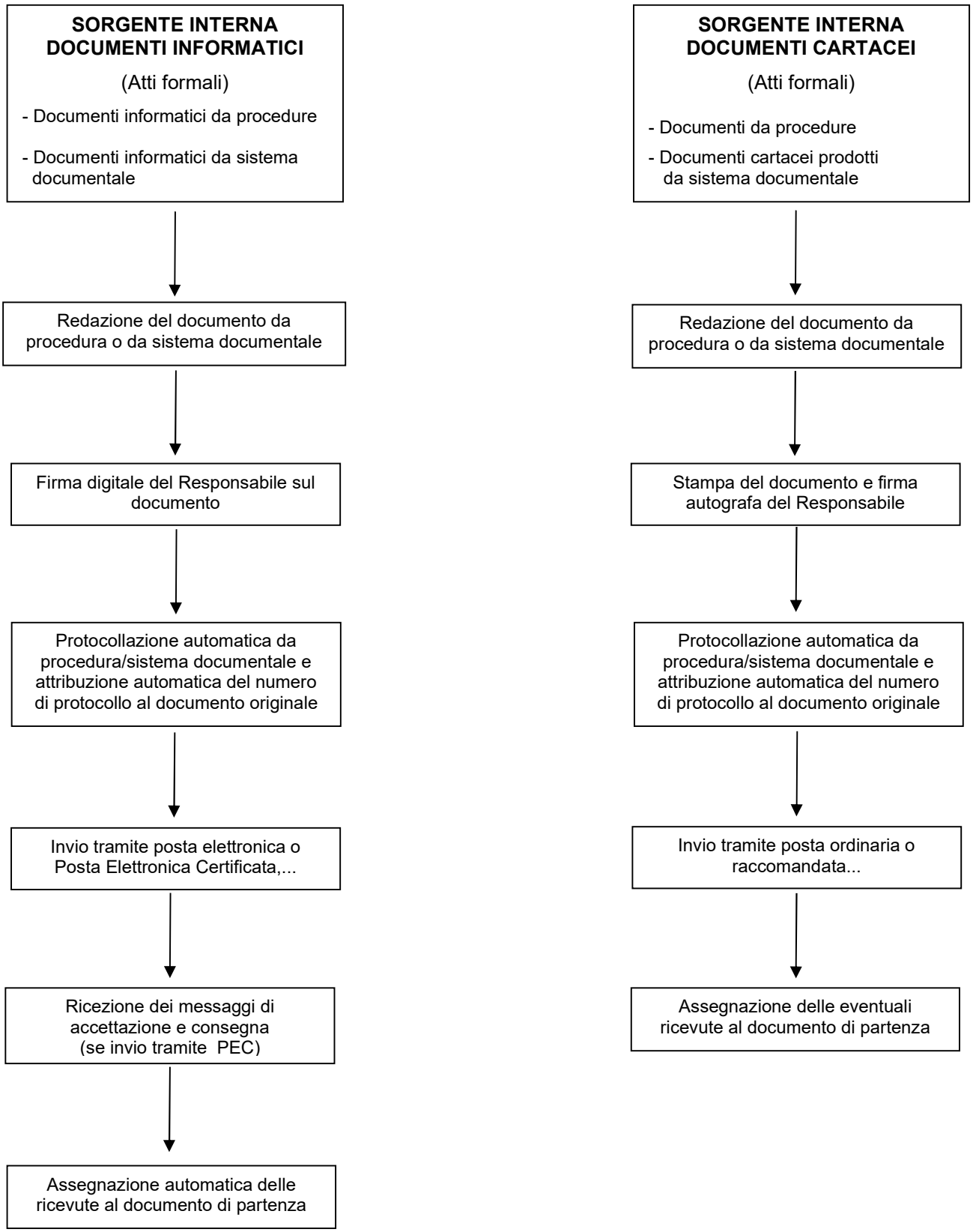
Gli addetti alla protocollazione, per i documenti da loro trattati, eseguono di norma la classificazione sulla base del Titolario di classificazione adottato presso l'AOO e provvedono ad inviarli tramite il sistema documentale all'unità organizzativa di destinazione che:

- esegue una verifica di congruità in base alle proprie competenze;
- in caso di errore, ritrasmette il documento all'ufficio protocollo;
- in caso di verifica positiva, esegue l'operazione di presa in carico e fascicolazione digitale;
- assegna le eventuali visibilità ulteriori rispetto a quelle attribuite automaticamente in base alla classificazione;
- gestisce il documento

Terminata la fase di protocollazione, i documenti sono portati automaticamente nella disponibilità dei soggetti competenti alla loro trattazione grazie al sistema documentale adottato dall'Ente. Il sistema consente comunque di assegnare la visibilità dei documenti ad altri soggetti singoli, uffici o gruppi trasversali di addetti configurati sul sistema. Questa modalità operativa consente di portare il documento all'attenzione di tutti i soggetti interessati, attraverso la condivisione interna del sistema documentale. Si tratta di una modalità particolarmente utile per favorire la conoscenza, e la disponibilità diffusa, di tipologie documentali quali circolari, manualistica, disposizioni operative, documenti di interesse generale ecc.
Viceversa, i documenti sono inesistenti per i soggetti ai quali non è stata assegnata, automaticamente o no, la visibilità specifica. Si tratta di un meccanismo semplice e affidabile per garantire la corretta gestione dei documenti riservati, contenenti dati sensibili o giudiziari, o comunque particolarmente delicati.
Nel caso di assegnazione errata, l'unità organizzativa che riceve il documento comunica l'errore all'ufficio protocollo che ha assegnato il documento, affinché proceda ad una nuova assegnazione

Tutti i documenti ricevuti dall'AOO per via telematica, o comunque disponibili in formato digitale, sono assegnati all'unità organizzativa competente attraverso il sistema di gestione documentale al termine delle operazioni di registrazione, segnatura di protocollo e memorizzazione.
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. L'originale cartaceo viene anch'esso trasmesso alla struttura di competenza, mediante collocazione nell'apposita cartella presso l'Ufficio Protocollo.
L'unità organizzativa competente ha notizia dell'arrivo del documento tramite apposita "notifica" generata automaticamente dal sistema documentale.

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'Amministrazione.
Il documento è predisposto in formato digitale, secondo gli standard illustrati nei precedenti capitoli, e recapito prioritariamente tramite posta elettronica certificata.
I documenti sono prodotti con il sistema documentale in dotazione all'Ente con le modalità descritte nell'allegato 7.
Durante la fase transitoria di migrazione verso l'utilizzo di un sistema di gestione documentale interamente digitale, il documento può essere riprodotto in formato analogico. Il mezzo di recapito della corrispondenza, in quest'ultimo caso, è tipicamente costituito dal servizio postale, nelle sue diverse forme.

4.3.2 Verifica formale dei documenti

Ogni unità organizzativa è autorizzata dal Responsabile della gestione documentale e del Servizio di Protocollo informatico; a svolgere attività di registrazione di protocollo e apposizione della segnatura per la corrispondenza in uscita. Le unità organizzative provvedono quindi ad eseguire al loro interno le verifiche di conformità della documentazione predisposta per essere trasmessa.

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 dalle singole unità organizzative abilitate, in quanto collegate al sistema di protocollo informatico della AOO a cui appartengono.

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 prioritariamente 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 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.
E' ammesso il recapito tramite posta elettronica tradizionale, qualora si disponga dei necessari riferimenti relativi al destinatario.
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.

4.3.5 Trasmissione di documenti cartacei a mezzo posta

L'ufficio protocollo gestisce le operazioni di spedizione della corrispondenza predisposta dagli uffici dell'Ente.
Gli uffici dell'Ente recapitano al protocollo i plichi da spedire, in tempo utile per consentire di organizzare al meglio la gestione.

4.3.6 Conteggi e spedizione corrispondenza cartacea

L'ufficio protocollo effettua i conteggi relativi alle spese giornaliere e mensili sostenute per le operazioni di invio della corrispondenza cartacea e cura il costante monitoraggio della spesa e verifica la disponibilità delle necessarie risorse economiche, informando con congruo anticipo il RSP dell'imminente esaurimento dei fondi a disposizione.
Il Responsabile della gestione documentale e del Servizio di Protocollo informatico promuove l'utilizzo di strumenti alternativi al servizio postale (e-mail, e-mail certificata ecc.) presso gli uffici dell'Ente.

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 SISTEMA DI CLASSIFICAZIONE, FASCICOLAZIONE DIGITALE E ARCHIVIAZIONE

Il presente capitolo illustra il sistema di classificazione dei documenti, di formazione del fascicolo digitale e di corretta gestione e formazione dell'archivio corrente e di deposito.

5.1 Titolario o piano di classificazione

La classificazione dei documenti, destinata a realizzare una corretta organizzazione dei documenti nell'archivio, è obbligatoria per legge e si avvale del piano di classificazione (Titolario), cioè di quello che si definisce "sistema precostituito di partizioni astratte gerarchicamente ordinate, individuato sulla base dell'analisi delle funzioni dell'ente, al quale è ricondotta la molteplicità dei documenti gestiti".
Il piano di classificazione è lo schema logico utilizzato per organizzare i documenti d'archivio in base alle funzioni e alle materie di competenza dell'ente.
Il Titolario è uno strumento soggetto di aggiornamento: esso deve, infatti, descrivere le funzioni e le competenze dell'ente, soggette a modifiche in forza di leggi o regolamenti.
Le modifiche al Titolario sono apportate con provvedimento esplicito.
La revisione anche parziale del Titolario viene proposta dal RSP quando è necessaria ed opportuna.
Dopo ogni modifica del Titolario, il RSP informa tutti i soggetti abilitati all'operazione di classificazione dei documenti e a fornire loro le istruzioni per il corretto utilizzo delle nuove classifiche.
Il Titolario non è retroattivo: non si applica, cioè, ai documenti protocollati prima della sua introduzione.
Viene garantita la storicizzazione delle variazioni di Titolario e la possibilità di ricostruire le diverse voci nel tempo, mantenendo stabili i legami dei fascicoli digitali e dei documenti con la struttura del Titolario vigente al momento della produzione degli stessi.
Per ogni modifica di una voce, è riportata la data d'introduzione e la data di variazione. Le variazioni sono di norma introdotte dal 1° gennaio dell'anno successivo a quello di approvazione del nuovo Titolario, e valgono almeno per l'intero anno.

5.2 La classificazione dei documenti

La classificazione è l'operazione finalizzata all'organizzazione dei documenti, secondo un ordinamento logico, in relazione alle funzioni e alle competenze della AOO.
Essa è generalmente strutturata a livelli che si articolano gerarchicamente tra loro.
Le voci di primo e secondo livello del titolario (titoli e classi) individuano le funzioni primarie e di organizzazione dell'Ente.
I successivi livelli di classificazione (macro-fascicoli, fascicoli, sotto-fascicoli…) corrispondono a specifiche competenze che rientrano concettualmente nelle macrofunzioni descritte dai primi livelli.
I primi due livelli di classificazione (*titolo-classe*) vengono attribuiti nella fase di protocollazione; l'individuazione dei successivi livelli (*macro-fascicolo,* fascicolo, sotto-fascicolo digitale...) è invece generalmente demandata al Responsabile del procedimento o suo incaricato.
Tutti i documenti ricevuti e prodotti dall'Ente, indipendentemente dal supporto sul quale sono formati, sono classificati in base al sopra citato titolario.

5.3 La fascicolazione dei documenti

Nelle Pubbliche Amministrazioni l'AOO gestisce i flussi documentali mediante fascicoli informatici predisposti secondo il piano di classificazione e relativo piano di organizzazione delle aggregazioni documentali ai sensi dell'art. 64 del TUDA.
La produzione, il mantenimento e l'uso dei fascicoli informatici sono conformi a quanto stabilito dall'art. 65 del TUDA e dell'art 41 del CAD

I documenti ricevuti e prodotti dall'Ente sono raccolti in fascicoli costituiti in modo che ciascuno rappresenti l'insieme ordinato dei documenti riferiti ad uno stesso procedimento amministrativo o, comunque, ad una stessa pratica.

I fascicoli possono essere:

- **Fascicoli cartacei**: laddove tutta la documentazione originale della pratica è prodotta in formato cartaceo;
- **Fascicoli informatici**: laddove tutta la documentazione originale della pratica è prodotta in formato elettronico;
- **Fascicoli ibridi**: nel caso in cui la documentazione riguardante la pratica sia stata formata da documenti prodotti, in originale, sia in formato cartaceo che in formato elettronico. In questi casi vengono prodotti due fascicoli distinti:
  - un fascicolo cartaceo nel quale viene raccolta la documentazione cartacea
  - un fascicolo informatico, archiviato nel sistema di gestione documentale, nel quale sono raccolti tutti i documenti prodotti in formato elettronico e i riferimenti di protocollo dei documenti prodotti in formato cartaceo.

I due fascicoli sono collegati tra loro e i riferimenti al fascicolo collegato sono riportati sia nella copertina del fascicolo cartaceo che nei dati d'identificazione del fascicolo informatico.
Oltre ai fascicoli informatici possono essere costituiti fascicoli per serie documentale, in cui vengono aggregati documenti della stessa tipologia.
I Responsabili dei singoli uffici interni dell'AOO forniscono le indicazioni operative per la gestione dei fascicoli e assicurano che la costituzione dei fascicoli avvenga secondo regole uniformi, sia per quanto riguarda i criteri da adottare per la denominazione della pratica al fine di identificare il fascicolo in modo univoco che di quelli adottati per la descrizione del fascicolo.
I fascicoli possono anche essere distinti in annuali e non annuali, con riferimento alla durata e alla tipologia delle pratiche.

5.4 La fascicolazione digitale

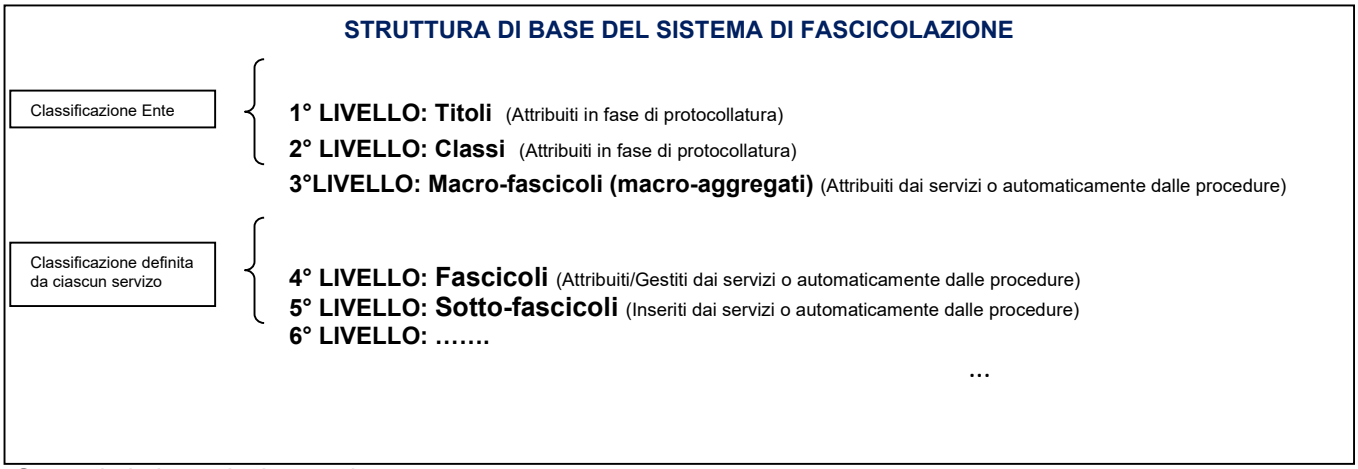
Il fascicolo digitale corrisponde generalmente ad una "Aggregazione strutturata e univocamente identificata di atti, documenti o dati informatici, prodotti e funzionali all'esercizio di una specifica attività o di uno specifico procedimento.
La formazione dei fascicoli tiene conto di come sia opportuno allocare le risorse umane addette alle pratiche in modo da razionalizzare l'impiego delle specifiche competenze degli appartenenti ai diversi settori di attività.
La formazione di un nuovo fascicolo/sotto-fascicolo avviene attraverso l'operazione di apertura che comprende la registrazione di alcune informazioni essenziali (metadati) così come previsto nell'allegato 5 delle Linee guida AgID

Le informazioni (metadati) che possono essere valorizzate sul fascicolo sono:

Descrizione del fascicolo	Data di apertura	Tipologia di aggregazione (fascicolo, serie documentale o serie di Fascicoli)
Ufficio di *riferimento*		Tipologia di fascicolo (affare, attività, persona fisica, persona giuridica, procedimento amministrativo
Ruolo	Collegamento al Titolario	Fase (se il fascicolo è legato ad un procedimento amministrativo)

Tipo di assegnazione Data di chiusura ……..

Ogni unità organizzativa è responsabile per la creazione e la gestione dei fascicoli nell'ambito dei servizi di competenza e delle prestazioni effettuate. I documenti contenuti in un fascicolo hanno di norma identica classificazione, e sono facilmente ricercabili sia attraverso quest'ultima che attraverso metadati.
I criteri di visibilità dei fascicoli digitali e dei loro relativi sottofascicoli all'interno dell'AOO sono definiti dai vari Responsabili dei Procedimenti Amministrativi in accordo con il Responsabile del Servizio per la tenuta del Protocollo informatico, la gestione dei flussi documentali e degli archivi.
I fascicoli possono anche essere distinti in annuali e non annuali, con riferimento alla durata e alla tipologia delle pratiche.
Si riporta di seguito la struttura di base del sistema di fascicolazione.



Secondo le ipotesi, si procede come segue:

- Se il documento dà avvio a un *NUOVO PROCEDIMENTO*, il soggetto preposto:
  - esegue l'operazione di apertura del fascicolo/sottofascicolo collegato al macro-fascicolo;
  - collega il documento al nuovo fascicolo aperto;
  - si occupa della gestione del documento o assegna il documento al collaboratore che dovrà istruire la pratica.
- Se il documento si ricollega a un *affare o procedimento in corso*, l'addetto:
  - seleziona il relativo fascicolo utente collegato al macro-fascicolo;
  - collega il documento al fascicolo selezionato;
  - si occupa della gestione del documento o assegna il documento al collaboratore che dovrà gestire la pratica.

5.5 Modifica delle assegnazioni dei fascicoli digitali

Quando si verifica un errore nell'assegnazione di un fascicolo, l'ufficio abilitato all'operazione di fascicolazione provvede a correggere le informazioni inserite nel sistema informatico.
Il sistema di gestione informatizzata dei documenti tiene traccia di questi passaggi, memorizzando per ciascuno di essi l'identificativo dell'operatore che effettua la modifica con la data e l'ora dell'operazione.

5.6 Chiusura dei fascicoli digitali

Il fascicolo digitale viene chiuso generalmente al termine del procedimento amministrativo o all'esaurimento dell'affare.

5.7 Serie archivistiche e repertori

I documenti soggetti a registrazione particolare, come i verbali, le delibere degli organi di governo dell'amministrazione, o i contratti, costituiscono una serie archivistica. Tali documenti sono organizzati nel registro di repertorio.

Per quanto concerne la gestione dei documenti informatici, ogni verbale, delibera, determinazione, decreto, ordinanza e contratto è, di norma, associato:

- al registro di repertorio con il numero progressivo di repertorio;
- al fascicolo, insieme ai documenti che afferiscono al medesimo affare o procedimento amministrativo.

Nel repertorio generale sono riportati gli elementi obbligatori del documento (data, classifica e numero di repertorio) che identificano il documento all'interno del repertorio stesso.
Il repertorio è costantemente aggiornato.

5.8 Archiviazione dei documenti - Tempi, criteri e regole di selezione del sistema di classificazione

L'Archivio è il complesso dei documenti prodotti o acquisiti dall'Ente durante lo svolgimento della propria attività.
I documenti amministrativi prodotti e detenuti da questo Ente sono oggetto di tutela ai sensi dell'art.10 del Codice dei beni culturali di cui al decreto legislativo 42/2004 pertanto tutti i soggetti che agiscono nell'ambito del sistema di gestione documentale dell'Ente svolgono attività archivistica.
L'Ente, ai sensi dell'art. 30 del predetto Codice, assolve all'obbligo di conservazione e ordinamento degli archivi.
Ai fini di un corretto esercizio dell'azione amministrativa, i fascicoli prodotti dagli uffici dell'Ente sono raccolti in archivi che possono essere distinti in:

- ***archivio corrente***, la parte di documentazione relativa agli affari ed ai procedimenti in corso di trattazione, riguarda i documenti necessari alle attività correnti.
  L'archiviazione corrente s'identifica per i documenti e i fascicoli informatici con l'archiviazione all'interno del sistema di gestione documentale.
- ***archivio di deposito***, la parte di documentazione di affari esauriti, non più occorrenti quindi alla trattazione degli affari in corso, riguarda i documenti ancora utili per finalità amministrative o giuridiche, ma non più indispensabili per la trattazione delle attività correnti;
- **archivio storico**, riguarda i documenti storici selezionati per la conservazione permanente

La coesistenza, nell'ambito di uno stesso procedimento, di documenti di natura mista (digitali e cartacei) costruisce il cosiddetto "archivio ibrido".
Nel sistema documentale informatico basta chiudere un fascicolo per farlo passare all'archivio di deposito.
I fascicoli cartacei chiusi fanno parte dell'archivio di deposito tradizionale. Tutti i fascicoli cartacei chiusi, che non servono più per la consultazione, possono essere spostati anche fisicamente nell'archivio di deposito dell'Ente.
La gestione dei processi di selezione dei documenti dell'archivio di deposito può condurre a due esiti tra di loro contrastanti: la conservazione permanente dei documenti che rivestono significativo valore di testimonianza storica, oltre che rilevanza giuridico probatoria, oppure lo scarto, cioè l'eliminazione irreversibile dei documenti ritenuti di valore transitorio e strumentale, da effettuare con l'autorizzazione del soprintendente archivistico competente per territorio.
Secondo le diverse tipologie documentali gestite dall'Ente sono definiti criteri e regole di selezione al fine di individuare i documenti da scartare e quelli da conservare.
1) L'elenco delle tipologie di documenti soggetti a conservazione permanente sono:

a) i "verbali", ovvero documenti "contenenti la descrizione di un fatto" quali ad es. i verbali di seduta di Giunta o di Consiglio, ovvero i verbali di una seduta di gara, di una commissione di esami, etc;
b) Statuti, Regolamenti, Decreti, Ordinanze, Interpellanze, interrogazioni, mozioni, Verbali Nucleo di Valutazione, Provvedimenti dirigenziali, Registro di protocollo, Registro albo pretorio, Registro notifiche, Atti relativi a partecipazione societarie - Documentazione relativa alle elezioni amministrative, Atti e documenti del contenzioso legale, Schedari, rubriche e repertori dell'archivio, Atti relativi a riordinamenti e scarti archivistici
c) Provvedimenti costitutivi, modificativi od estintivi di posizioni giuridiche e quindi anche determinazioni, concessioni, autorizzazioni, nulla osta etc;
d) Documenti riguardanti l'attività contrattuale: Contratti - Verbali di gara - Bandi di gara - Offerta dell'impresa aggiudicataria - Capitolati di gara - Documentazione riguardante la qualificazione.
e) Documenti prodotti da terzi ma con efficacia costitutiva di diritti soggettivi o abilitativi all'esercizio di attività quali ad esempio dichiarazioni d'inizio attività;

f) i "registri", ovvero quei documenti "sui quali vengono annotati in sequenza, secondo criteri predefiniti (tendenzialmente cronologici), una pluralità di fatti o atti giuridici" (es. il registro delle notifiche, il registro del protocollo, il registro degli infortuni, il repertorio dei contratti);
g) tutti i documenti sottoscritti con firma digitale;
h) tutti i documenti inviati e ricevuti con posta elettronica certificata;
i) studi e relazioni tecniche, ricerche, pubblicazioni, documentazione fotografica, che siano propedeutici a piani, programmi e delibere di carattere generale.

2) Documenti da conservare 40 anni

Mandati di pagamento e reversali di riscossione

3) Documenti da conservare per 15 anni

Strumenti urbanistici e documenti correlati

4) Documenti da conservare per 10 anni

a) i processi verbali relativi a sanzioni elevate nella materia di competenza dell'Ente (polizia amministrativa, polizia giudiziaria, polizia ambientale, etc.); offerte delle ditte non aggiudicatarie, libri contabili etc;
b) Concorsi (domande di partecipazione, elaborati scritti/pratici conservando eventualmente campionatura) - Gestione fiscale e assicurativa dei dipendenti e collaboratori (CUD,modello 730/4, denunce contributive annuali, autoliquidazione Inail, modelli di versamento ai fini contributivi previdenziali e fiscali, cedolini buste paga mensili, denuncia Statistiche sul personale

5) Documenti soggetti a conservazione per 5 anni sono:

a) le richieste e la documentazione allegata, le pezze giustificative, i rendiconti relativi ai "contributi" ovvero le elargizioni di denaro - comunque denominate - erogate dall'Ente;
b) la corrispondenza di carattere occasionale (le cosiddette "carte varie") ovvero "il complesso delle lettere e delle note scritte, inviate e ricevute dall'Ente" con riferimento ad un affare individuato ma che, per la loro scarsa importanza non siano sfociate in una delibera o provvedimento di altro genere, rimaste per così dire senza seguito;
c) i certificati o le dichiarazioni attestanti qualità o stati personali con validità temporale limitata (art. 41 DPR 445);
d) i dati statistici non relativi ad attività dell'Ente;
e) la documentazione fiscale per la quale la legge prevede tale termine di conservazione;
f) documenti relativi alla gestione ordinaria del personale.

5.9 Procedure di scarto

Per quanto riguarda le procedure di scarto dovrà farsi riferimento alle procedure previste dalla Sovrintendenze archivistica regionali.

In ogni caso si dovrà procedere a:

- Predisposizione della proposta di scarto indicando la documentazione che s'intende scartare;
- Presentazione di apposita istanza di autorizzazione alla Soprintendenza archivistica competente per territorio;
- Rilascio dell'autorizzazione da parte della Soprintendenza con approvazione dell'elenco di scaro con apposito provvedimento
- Distruzione della documentazione scartata con verbalizzazione delle operazioni.

6 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.

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

6.1 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 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 è considerata giuridicamente inesistente presso l'amministrazione. Non è consentita la protocollazione di un documento già protocollato. Qualora ciò avvenisse per errore, la seconda protocollazione va annullata.
Il registro di protocollo è un atto pubblico originario che fa fede della tempestività e dell'effettivo ricevimento e spedizione di un documento, indipendentemente dalla regolarità del documento stesso, ed è idoneo a produrre effetti giuridici.
Il registro di protocollo è soggetto alle forme di pubblicità e di tutela di situazioni giuridicamente rilevanti previste dalla normativa vigente.
Il registro giornaliero di protocollo è trasmesso entro la giornata lavorativa successiva al sistema di conservazione, garantendone l'immodificabilità del contenuto**.**

6.2 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 viene 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;
- la classificazione;
- l'impronta del documento informatico.

Le registrazioni di protocollo, in armonia con la normativa vigente, prevedono inoltre elementi accessori, rilevanti sul piano amministrativo, organizzativo e gestionale, sempre che le rispettive informazioni siano disponibili.

6.3 Elementi facoltativi delle registrazioni di protocollo

Il 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.
La registrazione degli elementi facoltativi del protocollo, previa autorizzazione del Responsabile della gestione documentale e del Servizio di Protocollo informatico, può essere modificata, integrata e cancellata in base alle effettive esigenze delle unità organizzative o del servizio protocollo. I dati facoltativi sono modificabili senza necessità di annullare la registrazione di protocollo, fermo restando che il sistema informatico di protocollo registra tali modifiche.

6.4 Segnatura di protocollo dei documenti

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 dell'area organizzativa omogenea;
- il codice identificativo del registro di protocollo;
- l'anno solare di riferimento del protocollo;
- titolo e classe di riferimento;
- il numero progressivo di protocollo, costituito da almeno sette cifre numeriche
- la data di protocollo
- sigla della unità/settore a cui il documento è assegnato per competenza e responsabilità
- sigle delle unità/settori in copia conoscenza

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

6.5 Annullamento delle registrazioni di protocollo

La necessità di modificare anche un solo campo tra quelli obbligatori e immodificabili della registrazione di protocollo per correggere errori verificatisi in sede d'immissione manuale di dati o attraverso l'interoperabilità dei sistemi di protocollo mittente e destinatario, comporta l'obbligo di annullare la registrazione di protocollo.
Le informazioni concernenti la registrazione di protocollo 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 rilasciata dal RSP.
In tale ipotesi la procedura riporta l'annotazione di annullamento. Il sistema inoltre registra l'avvenuta rettifica, la data e il soggetto che è intervenuto.
Solo il Responsabile della gestione documentale e del Servizio di Protocollo informatico è autorizzato ad annullare, direttamente o delegando gli addetti, una registrazione di protocollo.
L'annullamento di una registrazione di protocollo generale deve essere richiesto con specifica nota, adeguatamente motivata, indirizzata al Responsabile della gestione documentale e del Servizio di Protocollo informatico.

6.6 Protocollazione documenti interni formali

I documenti formali prodotti e scambiati internamente sono soggetti a protocollazione e indicati come protocolli interni. Sono inseriti nel sistema di gestione documentale con opportuna classificazione, assegnazione di visibilità, collegamento ai documenti o procedimenti correlati, fascicolazione e archiviazione.

6.7 Oggetti ricorrenti

Ciascun Servizio può individuare tipologie di documenti per i quali concordare con il Protocollo generale l'indicazione esatta dell'oggetto, la titolazione, la tipologia e l'assegnazione a predeterminati soggetti o ambiti organizzativi.
È compito di ciascun Servizio provvedere a verificare il permanere dell'attualità di ciascun oggetto individuato e del relativo smistamento.

6.8 Registrazione differita di protocollo

Per "protocollo differito" s'intende la registrazione di un 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.

È possibile eseguire la registrazione differita di protocollo, qualora dalla mancata registrazione di un documento nell'ambito del sistema nel medesimo giorno lavorativo di ricezione, possa venire meno un diritto di terzi.
La registrazione differita di un documento in arrivo nel sistema va richiesta e deve essere autorizzata dal Responsabile della gestione documentale e del Servizio di Protocollo informatico o suo delegato.

6.9 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”.
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.

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

Il sistema di gestione documentale e di protocollazione adottato dall’Ente è basato sulla piattaforma della soluzione software **OLIMPO – archiviazione documentale e scrivania digitale della SISCOM spa**. La soluzione per la protocollazione prevede un modulo specifico denominato Egisto che gestisce tutte le fasi di protocollazione in arrivo/partenza nonché di protocolli interni in modo totalmente integrato con il sistema documentale.
La soluzione gestisce la ricezione e trasmissione delle pec e mail con la protocollazione e l’archiviazione nel sistema documentale in modo sicuro e non modificabile. I documenti pervenuti sono condivisi agli uffici e operatori destinatari e sono tracciati nell’iter burocratico.
I documenti prodotti dall’Ente sono gestiti nell’ambito del sistema documentale sia nella fase di redazione sia in quella di archiviazione, di protocollazione e di trasmissione. Il tutto il modo integrato.

7.1 Descrizione funzionale e operativa

Il presente capitolo contiene la descrizione funzionale e operativa del sistema di protocollo informatico, gestione documentale e dei procedimenti adottato dall'Ente, con particolare riferimento alle modalità di utilizzo dello stesso.
La descrizione funzionale e operativa del sistema di protocollo informatico è specificata in dettaglio all'interno dell'allegato 7.

8 CONSERVAZIONE DEI DOCUMENTI INFORMATICI

La conservazione può riguardare sia documenti informatici all'origine sia documenti analogici convertiti in formato digitale.
Nella Pubblica Amministrazione, il sistema di gestione informatica dei documenti trasferisce al sistema di conservazione, ai sensi dell’art. 44, comma 1-bis, del CAD

8.1 Principi sulla conservazione dei documenti informatici

La conservazione digitale è l’insieme delle attività e dei processi che, tramite l’adozione di regole, procedure e tecnologie, garantiscono l’accessibilità, l’utilizzabilità (leggibilità e intelligibilità), l’autenticità (identificabilità univoca e integrità) e la reperibilità dei documenti e dei fascicoli informatici con i metadati ad essi associati nel medio e nel lungo periodo, in un ambiente tecnologico presumibilmente diverso da quello originario.
Il valore legale dell'attività di conservazione è subordinato all'organizzazione del servizio e allo svolgimento dell'attività secondo le regole tecniche vigenti.

Il sistema di conservazione opera trattando dei Pacchetti informativi, contenitori che racchiudono uno o più oggetti da conservare (documenti informatici, fascicoli informatici, aggregazioni documentali informatiche) o anche i soli metadati riferiti agli oggetti da conservare.
I pacchetti informativi possono avere varia natura:

- di versamento: pacchetto inviato dal produttore del documento al sistema di conservazione secondo il formato predefinito e concordato, descritto nel manuale di conservazione. Con il versamento effettuato dal Responsabile della gestione documentale o del Protocollo il documento, il fascicolo informatico o l'aggregazione transitano dal sistema di gestione documentale al sistema di conservazione.
- di archiviazione: pacchetto informativo composto dalla trasformazione di uno o più pacchetti di versamento
- di distribuzione: pacchetto informativo inviato dal sistema di conservazione all'utente in risposta ad una sua richiesta.

Il processo di conservazione si articola nelle seguenti fasi:
1) acquisizione da parte del sistema di conservazione del pacchetto di versamento per la sua presa in carico;
2) verifica che il pacchetto di versamento e gli oggetti contenuti siano coerenti con le modalità previste dal manuale di conservazione e con quanto indicato dalle Linee Guida
NB: nel caso in cui la verifica evidenzi anomalie il pacchetto di versamento viene rifiutato;
3) trasmissione del pacchetto di versamento in modalità sicura;
4) preparazione, sottoscrizione con firma digitale o firma elettronica qualificata del Responsabile della conservazione e gestione del pacchetto di archiviazione;
5) preparazione e sottoscrizione del pacchetto di distribuzione ai fini dell'esibizione richiesta dall'utente;
6) ai fini dell'interoperabilità tra sistemi di conservazione, produzione dei pacchetti di distribuzione coincidenti con i pacchetti di archiviazione;
7) eventuale produzione di duplicati informatici o di copie informatiche effettuati su richiesta degli utenti in conformità a quanto previsto dalle regole tecniche in materia di formazione del documento informatico;
8) eventuale produzione delle copie informatiche al fine di adeguare il formato, in conformità a quanto previsto dalle regole tecniche in materia di formazione del documento informatico;
9) scarto del pacchetto di archiviazione dal sistema di conservazione alla scadenza dei termini di conservazione previsti dalla norma, dandone informativa al produttore;

8.2 La conservazione dei documenti informatici dell'Ente

L'Ente decide di affidare la gestione della conservazione ad outsourcer esterno che possiede i requisiti di qualità, sicurezza e organizzazione individuati nelle Linee Guida.
Il "ciclo di gestione della conservazione" ed il servizio adottato dall'Ente vengono descritti in dettaglio nell'allegato 8.

9 REGISTRO DI EMERGENZA

9.1 Utilizzo del registro di emergenza

Il responsabile del servizio di protocollo informatico autorizza lo svolgimento delle operazioni di registrazione di protocollo sull'apposito registro di emergenza, ogni qualvolta per cause tecniche non sia possibile utilizzare il sistema.
Il registro di emergenza è unico ed è gestito dall'Ufficio Protocollo. Tutti i servizi dell'Ente, in caso di necessità, fanno quindi riferimento a questo ufficio per ottenere l'assegnazione di un numero di protocollo di emergenza, in entrata o in uscita.
Il registro di emergenza si rinnova ogni anno solare, pertanto inizia il primo gennaio e termina il 31 dicembre di ogni anno.
Si applicano le seguenti modalità di registrazione e di recupero dei dati:

- sul registro di emergenza sono riportate le cause, la data e l'ora di inizio dell'interruzione nonché la data e l'ora del ripristino della funzionalità del sistema;

- per ogni giornata di registrazione in emergenza è riportato sul registro il numero totale di operazioni registrate;
- la sequenza numerica utilizzata su un registro di emergenza, anche a seguito di successive interruzioni, garantisce comunque l'identificazione univoca dei documenti registrati nell'ambito del sistema documentario dell'AOO;
- le informazioni relative ai documenti protocollati in emergenza sono inserite immediatamente nel sistema di protocollo informatico ripristinato;
- durante la fase di ripristino, a ciascun documento registrato in emergenza viene attribuito un numero di protocollo del sistema informatico ordinario, annotando nella scheda di protocollo gli elementi necessari a mantenere stabilmente la correlazione univoca con il numero attribuito in emergenza.

10 SICUREZZA

La sicurezza e l'integrità dei dati di protocollo e dei documenti elettronici archiviati sono garantite 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 riguardo alle norme sulla protezione dei dati personali.

10.1 Obiettivi

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

- i documenti e le informazioni trattati dall'amministrazione/AOO siano resi disponibili, integri e riservati;
- i dati personali comuni, sensibili e/o giudiziari vengano custoditi in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta, 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 decreto legislativo 30 giugno 2003, n. 196 - Codice 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 della gestione documentale ha adottato 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 acceso 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 il PdP;

- gestione delle situazioni di emergenza informatica attraverso la costituzione di un gruppo di risorse interne qualificate (o ricorrendo a strutture esterne qualificate);
- 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;
- archiviazione giornaliera, in modo non modificabile, delle copie del registro di protocollo, 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 RSP e dal titolare dei dati.

10.2 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 a 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 workflow effettuabili alle sole funzioni necessarie.

Altre modalità di accesso possono essere definite dall'organizzazione dell'ente.

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 responsabile della pratica o del procedimento.
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.
I diversi livelli di autorizzazione sono assegnati agli utenti dal RSP, in base alle indicazioni fornite dai Responsabili dei servizi di appartenenza.
Gli accessi esterni a documenti, dati e informazioni non divulgabili sono subordinati alla registrazione sul sistema e al possesso di apposite credenziali, rilasciate previa identificazione diretta da parte di un dipendente abilitato.
Gli accessi esterni a documenti, dati e informazioni divulgabili sono consentiti anche senza autenticazione all'accesso, garantendo comunque il diritto alla riservatezza e all'oblio, e la tutela dei dati personali in conformità alle disposizioni vigenti.
Gli accessi esterni vengono, di norma, gestiti attraverso il sito web dell'Ente. I dati in libera consultazione sono esposti in formato aperto (con dovute eccezioni, indotte anche da considerazioni di carattere tecnico, organizzativo o gestionale) che ne consentano il riutilizzo.

10.3 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 l'amministrazione/AOO 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 della stessa AOO e con AOO diverse.

I documenti sono prodotti con l'ausilio dell'applicativo specificato nell'allegato 7 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 di una 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 a un controllo antivirus per eliminare qualunque forma di contagio che possa arrecare danno diretto o indiretto all'amministrazione/AOO.

10.4 Trasmissione e 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 d'informazioni che, per loro natura o per espressa indicazione del mittente, sono destinate a essere rese pubbliche.
Come previsto dalla normativa vigente, i dati e i documenti trasmessi per via telematica sono di proprietà del mittente sino a che non sia avvenuta la consegna al destinatario.
Al fine di tutelare la riservatezza dei dati personali, i dati, i certificati e i documenti trasmessi all'interno dell'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'amministrazione, (o, in alternativa, del servizio disponibile all'interno dell'amministrazione/AOO) 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 decreto legislativo del 30 giugno 2003, n. 196 e s.m.i.
Per garantire alla AOO ricevente la possibilità di verificare l'autenticità della provenienza, l'integrità del messaggio e la riservatezza del medesimo, viene utilizzata la tecnologia di firma digitale a disposizione delle amministrazioni coinvolte nello scambio dei messaggi.

10.5 Accesso ai documenti informatici

Il controllo degli accessi è assicurato utilizzando le credenziali di accesso e un sistema di autorizzazione basato sulla profilazione degli utenti in via preventiva.
La profilazione preventiva consente di definire le abilitazioni/autorizzazioni che possono essere eseguite/rilasciate a un utente del servizio di protocollo e gestione documentale.
Ciascun utente del PdP può accedere solamente ai documenti che sono stati assegnati al suo UOR, o agli Uffici Utente (UU) a esso subordinati.

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

11 NORME TRANSITORIE E FINALI

11.1 Modalità di approvazione e aggiornamento del manuale

L'amministrazione adotta il "Manuale di gestione documentale del protocollo" su proposta del responsabile del servizio per la tenuta del protocollo informatico, la gestione dei flussi documentali e degli archivi (RSP).
Il Manuale 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 è approvato e modificato con deliberazione del Consiglio.
Gli allegati sono modificati, di norma e fatte salve le eccezioni esplicitamente dichiarate, con provvedimenti del Responsabile del Servizio per la tenuta del Protocollo informatico, la gestione dei flussi documentali e degli archivi.

11.2 Pubblicità del manuale di gestione documentale del protocollo informatico

Il Manuale di gestione documentale del protocollo informatico, 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:
• resa disponibile a tutto il personale dell'AOO tramite il sistema di gestione documentale;
• inviata all'organo di controllo;
• pubblicata sul sito internet dell'Amministrazione.

11.3 Entrata in vigore

Il presente documento diviene efficace al conseguimento dell'eseguibilità della deliberazione di approvazione.

ENTE DI GESTIONE DELLE AREE PROTETTE DEL PO PIEMONTESE

ALLEGATO 1

AL MANUALE DI GESTIONE DOCUMENTALE DEL PROTOCOLLO INFORMATICO, DEI FLUSSI DOCUMENTALI E DEGLI ARCHIVI

NORME DI RIFERIMENTO

Norme di riferimento

1. D.P.R. n. 513 del 10 novembre 1997
2. D.P.R. n. 445 del 28 dicembre 2000
3. Deliberazione AIPA n. 42 del 2001
4. Decreto Legislativo 23 gennaio 2002, n. 10
5. Decreto del Presidente della Repubblica 07 aprile 2003, n. 137
6. D.P.C.M. del 13 gennaio 2004
7. Deliberazione CNIPA n. 11/2004 del 19 febbraio 2004
8. D.P.R. del 11 febbraio 2005
9. Decreto legislativo 07 marzo 2005 n. 82 – Codice dell'amministrazione digitale
10. D.P.C.M. del 30 marzo 2009
11. Deliberazione CNIPA 21 maggio 2009, n. 45
12. Decreto Legge n. 5 del 09 febbraio 2012
13. D.P.C.M. del 22 febbraio 2013 pubblicato in GU n. 117 del 21-05-2013
14. D.P.C.M. del 21 marzo 2013 pubblicato in GU n. 131 del 06-06-2013
15. Decreto del Presidente del Consiglio dei Ministri 03 dicembre 2013 – Regole tecniche per il protocollo informatico ai sensi degli artt. 2 (comma1) Oggetto e Ambito di applicazione, 6 Funzionalità, 9 Formato della segnatura di protocollo, 18 (commi 1 e 5) Modalità di registrazione dei documenti informatici, 20 Segnatura di protocollo dei documenti trasmessi, 21 Informazioni da includere nella segnatura, del C.A.D. di cui D.L. 82/2005 art. 71
16. Circolare AgID n. 65 del 10 aprile 2014 pubblicata in GU n. 89 del 16 aprile 2014
17. D.P.C.M. 14 novembre 2014
18. Regolamento UE n. 679/2016
19. Circolare AgID n. 2 del 18 aprile 2017
20. Linee guida AgID 17 maggio 2021

ENTE DI GESTIONE DELLE AREE PROTETTE DEL PO PIEMONTESE

ALLEGATO 2

AL MANUALE DI GESTIONE DEL PROTOCOLLO INFORMATICO, DEI FLUSSI DOCUMENTALI E DEGLI ARCHIVI

ATTO DI NOMINA DEL RESPONSABILE DEL SERVIZIO PER LA TENUTA DEL PROTOCOLLO INFORMATICO, DELLA GESTIONE DEI FLUSSI DOCUMENTALI E DEGLI ARCHIVI

DECRETO DEL PRESIDENTE N. DEL

vista la legge regionale 29 giugno 2009, n. 19 “Testo unico sulla tutela delle aree naturali e della biodiversità” e s.m.i.;

Visto l’art. 14 (il Presidente) della L.R. n. 19/2009 e s.m.i.;

premesso che l’Ente di gestione delle Aree protette del Po Piemontese si articola in un’unica Area Organizzativa Omogenea;

atteso che in attuazione

- del Codice dell’Amministrazione Digitale recato dal D.Lgs 82/2005 nel testo vigente
- dell’art. 3, comma 1, lettera b) delle Regole tecniche per il protocollo informatico ai sensi degli articoli 40 bis, 41, 47, 57bis e 71, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005 e ai sensi delle linee guida Agid 17 maggio 2021

considerato che si rende necessario provvedere ad individuare il Responsabile della gestione documentale per l’unica area organizzativa omogenea;

dato atto che il Responsabile della gestione documentale è preposto al servizio di cui all'articolo 61 del TUDA e, d’intesa con il responsabile della conservazione, il responsabile per la transizione digitale di cui all’art.17 del CAD e acquisito il parere del responsabile della protezione dei dati personali, di cui agli artt. 37 “Designazione del responsabile della protezione dei dati” e 39 “Compiti del responsabile della protezione dei dati” del Regolamento UE 679/2016, predispone:
● il manuale di gestione documentale relativo alla formazione, alla gestione, alla trasmissione, all’interscambio, all’accesso ai documenti informatici nel rispetto della normativa in materia di trattamenti dei dati personali ed in coerenza con quanto previsto nel manuale di conservazione;
Considerato che il manuale dovrà contenere inoltre, come parte integrante dello stesso, il piano per la sicurezza informatica, per la quota parte di competenza, nel rispetto delle:
○ misure di sicurezza predisposte dall’AgID e dagli altri organismi preposti;
○ delle disposizioni in materia di protezione dei dati personali in linea con l’analisi del rischio fatta;
○ indicazioni in materia di continuità operativa dei sistemi informatici predisposti dall’AGID.

rilevato che è compito del Responsabile:

- provvedere all’aggiornamento e all’eventuale revisione del Manuale della gestione documentale e del Servizio di Protocollo informatico;
- 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;
- supervisionare la leggibilità nel tempo di tutti i documenti trasmessi o ricevuti dalla AOO attraverso l’adozione dei formati standard ammessi dalla normativa vigente;

- la supervisione dell'invio del pacchetto di versamento che sarà formato dai delegati di ogni unità organizzativa dell'AOO e quindi del transito del pacchetto al sistema di conservazione. Il documento, il fascicolo o l'aggregazione per poter essere correttamente versati in conservazione devono essere stati formati e gestiti in ottemperanza alle regole tecniche sulla formazione, protocollazione e firma secondo le regole tecniche e secondo quanto esplicitato nel presente manuale.
- proporre eventuali modifiche al Titolario di classificazione;
- curare le funzionalità del sistema affinché, in caso di guasti o anomalie, siano ripristinate nel più breve tempo possibile e comunque in conformità a quanto stabilito nel Piano di continuità operativa/DR e relativi allegati;
- conservare le copie di salvataggio delle informazioni del sistema di protocollo e del registro di emergenza in luoghi sicuri e diversi da quello in cui viene custodito il suddetto sistema;
- 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 e le attività di gestione degli archivi;
- autorizzare le operazioni di annullamento della registrazione di protocollo;
- aprire e chiudere il registro di protocollazione di emergenza.

ritenuto che il responsabile della gestione documentale debba essere individuato all'interno dell'Ente, potendo eventualmente avvalersi, per quanto concerne gli aspetti eminentemente tecnico informatici, di un supporto esterno;

ritenuto pertanto di nominare quale Responsabile della gestione documentale di questo Ente XXXXX dipendente inquadrata quale XXXXXX , profilo professionale ;

rilevato che la normativa sopra richiamata dispone l'obbligo di individuare, al fine di garantire la continuità dello svolgimento delle funzioni rimesse al Responsabile della gestione documentale, un vicario;

ritenuto di individuare il vicario del Responsabile della gestione documentale il Dipendente XXXXX nella categoria D, profilo professionale Funzionario Amministrativo;

dato atto che il Responsabile della gestione documentale non dispone di autonomo potere di spesa né di assegnazione di risorse del bilancio dell'Ente e che la presente nomina non dà luogo alla percezione di compensi accessori;

visto il Codice dell'Amministrazione Digitale recato dal D.lgs. 82/2005 nel testo vigente;

viste le Regole tecniche per il protocollo informatico ai sensi degli articoli 40 bis, 41, 47, 57bis e 71, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005 e ai sensi delle linee guida 17 maggio 2021

considerato che il presente atto non comporta assunzione di impegni di spesa;

dato atto che è stato espresso il parere favorevole della Direttrice, Monica Perroni, in ordine alla regolarità tecnico-amministrativa;

per le motivazioni citate in premessa e che si intendono qui integralmente richiamate

DECRETA

1. di nominare , per le motivazioni esposte in premessa, quale Responsabile della gestione documentale di questo Ente XXXXXX dipendente dell'Ente inquadrata quale XXXXX ,con profilo professionale di XXXXX;
2. di designare, con decorrenza dalla data di ricezione del presente provvedimento, il summenzionato soggetto che opera sotta la diretta autorità del Titolare, quale persona fisica a cui attribuire specifici compiti e funzioni connessi al trattamento di dati personali e relativi ai trattamenti conseguenti alla ricezione delle segnalazioni pervenute in applicazione della normativa in materia di conservazione dei documenti amministrativi;
3. di delegare, per effetto di quanto sopra indicato e con decorrenza dalla data di ricezione del presente provvedimento al summenzionato l'esercizio e lo svolgimento di tutti i compiti e di tutte le funzioni attribuite dal Titolare, ed analiticamente elencate nel presente provvedimento, con facoltà di successiva integrazione e/o modificazione;
4. di dare atto che il summenzionato, assume, con decorrenza dalla data di ricezione del presente atto di designazione, attribuzione e delega, il ruolo di soggetto autorizzato e designato per il trattamento dei dati personali con delega a svolgere i compiti e le funzioni attribuiti dal Titolare medesimo, di dare atto altresì che:
   - tale ruolo ha validità per l'intera durata dell'incarico;
   - tale ruolo viene a cessare al modificarsi dell'incarico;
   - tale ruolo viene a cessare in caso di revoca espressa;
   - al cessare di tale ruolo, rimane inibito e comunque non autorizzato ogni ulteriore esercizio dei compiti e delle funzioni trattamento dei dati personali oggetto del presente provvedimento, salvo che ciò sia imposto o consentito da una norma di legge o da un provvedimento dell'autorità ovvero sia necessario ad esercitare o difendere un diritto."
5. di nominare quale vicario del Responsabile della gestione documentale la dipendente inquadrata nella categoria D, profilo professionale Funzionario amministrativo, XXXXXX;
6. di attribuire ai sunnominati le incombenze previste dal Codice dell'Amministrazione Digitale recato dal D.lgs. 82/2005 nel testo vigente e dalle 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, con aggiornamenti delle linee guida Agid 17 maggio 2021
7. di dare atto che il Responsabile della gestione documentale non dispone di autonomo potere di spesa né di assegnazione di risorse del bilancio dell'Ente e che la presente nomina non dà luogo alla percezione di compensi accessori.

IL PRESIDENTE

Letto, confermato e sottoscritto (*con firma digitale, ai sensi degli artt. 20 e 21 del D.Lgs. 2/2005*)

IL PRESIDENTE	IL SEGRETARIO
ROBERTO SAINI	MONICA PERRONI

ENTE DI GESTIONE DELLE AREE PROTETTE DEL PO PIEMONTESE

ALLEGATO 3

AL MANUALE DI GESTIONE DOCUMENTALE DEL PROTOCOLLO INFORMATICO, DEI FLUSSI DOCUMENTALI E DEGLI ARCHIVI

CERTIFICAZIONE DI PROCESSO

Ai sensi delle linee guida Agid 2021– 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

Questo allegato è parte integrante al testo delle linee guida sulla *Formazione, gestione e conservazione dei documenti informatici*.

CAPITOLO 1

1.1. Certificazione di processo: principi generali

Per assicurare l'efficacia probatoria dei documenti informatici e delle copie, la *certificazione di processo,* è stata introdotta ai sensi del Decreto Legislativo 13 dicembre 2017 comma 1bis art. 22, per favorire la dematerializzazione di grosse quantità di documenti analogici. Si tratta di una delle due modalità previste per assicurare che il documento informatico abbia contenuto e forma identici a quelli del documento analogico da cui è tratto, insieme a quella tradizionalmente nota come *raffronto dei documenti*. Il legislatore ha previsto l'adozione di tecniche in grado di garantire la corrispondenza della forma e del contenuto dell'originale e della copia, come si legge all'art. 22 comma 1bis del CAD:

> *«la copia per immagine su supporto informatico di un documento analogico è prodotta mediante processi e strumenti che assicurano che il documento informatico abbia contenuto e forma identici a quelli del documento analogico da cui è tratto, previo raffronto dei documenti o attraverso certificazione di processo nei casi in cui siano adottate tecniche in grado di garantire la corrispondenza della forma e del contenuto dell'originale e della copia»*

Nel modello di certificazione di processo devono concorrere due elementi fondamentali:

- la presenza di una procedura tecnologica in grado di garantire la corrispondenza della forma e del contenuto dell'originale e della copia;
- la previa descrizione e certificazione di questo processo, al fine di conferire ai documenti risultanti dal processo di scansione l'efficacia probatoria prevista:

  *«Le copie per immagine su supporto informatico di documenti originali formati in origine su supporto analogico hanno la stessa efficacia probatoria degli originali da cui sono estratte, se la loro conformità è attestata da un notaio o da altro pubblico ufficiale a ciò autorizzato, secondo le regole tecniche stabilite ai sensi dell'articolo 71». (*art. 22 comma 2 del CAD)

La procedura tecnologica in grado di garantire tali certezze è stata tradotta in termini di efficienza gestionale dell'organizzazione preposta alla scansione massiva dei documenti e in termini di diligenza di comportamento dei soggetti preposti alla certificazione di processo.

Capitolo 2

REGOLE DI UTILIZZO DELLA CERTIFICAZIONE DI PROCESSO

2.1. Conformità allo standard ISO

La "certificazione di processo" richiama le certificazioni in materia di qualità, sicurezza, ambiente (ecc.), nel cui ambito si assiste alla presenza di due tipologie possibili di certificazione: la certificazione di prodotto e la certificazione di processo (detta anche "di sistema"), con le seguenti accezioni:

- "certificazione di prodotto/servizio" intesa come una forma di "assicurazione diretta", con cui una terza parte indipendente accerta la rispondenza di un determinato prodotto o servizio ai requisiti di legge applicabili o a procedure regolamentari autonomamente individuate;
- "certificazione di sistema o di processo" intesa come una forma di "assicurazione indiretta", in quanto assicura la capacità di un'organizzazione di strutturarsi e gestire le proprie risorse ed i propri processi produttivi in modo tale da identificare e soddisfare i requisiti stabiliti dalle parti interessate[2].

La certificazione in generale attesta che una determinata attività, o uno specifico prodotto, rispetta i requisiti che l'organizzazione si è data oppure i requisiti di una norma specifica. La certificazione è sempre ed in ogni caso una procedura con cui con cui una terza parte indipendente dà assicurazione scritta che un prodotto, un servizio, un processo è conforme ai requisiti specificati.

Pertanto, partendo dalla sopradetta assunzione, la "certificazione di processo" prevista dal comma 1-bis dagli artt. 22 e 23-ter del CAD, di fatto, è più propriamente una *certificazione di un risultato* ottenuto attraverso un determinato risultato, infatti, ovvero il prodotto, consiste in una copia informatica di documento analogico, e la certificazione di processo produce sostanzialmente una *certificazione di conformità di una copia ad un originale*; purché essa risulti corredata da una completa descrizione del processo attraverso il quale una simile copia è stata ottenuta.

La certificazione di processo mira a conseguire il medesimo risultato della "certificazione tradizionale", rappresentato dal tradizionale metodo di raffronto fra originale e copia. Pertanto, detto "processo" dovrà caratterizzarsi non solo dal punto di vista *oggettivo* (strumenti tecnologici, procedure, organizzazione,…) ma anche da quello *soggettivo* per attestare l'efficacia probatoria della certificazione di processo. Quindi, nella certificazione di processo non ci si potrà limitare a descrivere il processo con il quale è stata creata la copia digitale, ma occorrerà anche, necessariamente, certificare la copia *risultato*. Di conseguenza, due sono gli effetti che si determinano:

- per l'ambito *oggettivo*: il ciclo di dematerializzazione massiva dovrà essere certificato da organismo terzo in accordo agli standard ISO 9001 e ISO 27001[3], con campo di applicazione specifico per i servizi di progettazione e dematerializzazione massiva di documenti;

- per l'ambito *soggettivo*: il ciclo di dematerializzazione dovrà concludersi con il metodo del raffronto a campione dei documenti, generando una certificazione ovvero un risultato probatorio differente a seconda che il rapporto di verificazione sia firmato da un pubblico ufficiale o da un soggetto privato.

2.2. Efficacia probatoria della certificazione di processo

L'efficacia probatoria di un documento-copia, in tutta la normativa vigente, varia se rimessa all'intervento di un pubblico ufficiale o a quello di un soggetto privato. Il CAD, infatti, ai commi 2 e 3 dell'art. 22 e comma 3 dell'art. 23-ter distingue il valore probatorio "privilegiato" che fa piena prova fino a querela di falso (ex art. 2700 del c.c.) se la conformità all'originale è assicurata da un notaio o Pubblico Ufficiale a ciò autorizzato, dal valore probatorio "semplice" che fa piena prova fino a disconoscimento se la conformità all'originale è data da un soggetto privato. Si veda, al riguardo, la seguente tabella:

Soggetto firmatario	**Valore probatorio ex artt. 22 e 23-ter del CAD**
Notaio o PU a ciò autorizzato □	L'atto pubblico ovvero l'*attestazione di conformità* fa piena prova fino a querela di falso (ex art. 2700 del c.c.).
Privato □	Una copia fatta da chiunque fa piena prova fino a disconoscimento.

Ne consegue che si parla propriamente di certificazione di processo solo qualora l'attestazione di conformità venga rilasciata da notaio o Pubblico Ufficiale a ciò autorizzato e sottoscritta per mezzo della firma digitale o di altra firma elettronica qualificata (ex artt. 22 comma 2 e 23-ter comma 3 del CAD). Nel caso di soggetto privato, non si produrrà una certificazione di processo ma unicamente un rapporto di verificazione sottoscritto dallo stesso che fa piena prova fino a disconoscimento.

2.3. Ciclo di dematerializzazione: requisiti, fasi e controlli

La descrizione del processo di dematerializzazione va eseguita non solo per dare sostanza all'intero impianto della certificazione di processo ma, anche, per estendere in maniera massiva il processo di conversione dall'analogico al digitale a tutto il lotto di documenti sottoposti a scansione. Specificare quali debbano essere i requisiti tecnici cui attenersi, le fasi ed i controlli da seguire permetterà di avere una sorta di "presunzione" di efficacia probatoria delle copie realizzate anche in periodi di scansione diversi purché afferenti allo stesso progetto o lotto di copie digitalizzate. Il notaio/PU o privato descrivono l'intero processo e ne certificano il funzionamento verbalizzando, prima ancora che l'attività di scansione massiva venga avviata sull'intero lotto di documenti, la conformità di alcune copie campione agli originali analogici ricorrendo al tradizionale raffronto dell'originale con la copia, in modo da "congelare" i criteri di qualità e sicurezza da adottare alle successive copie informatiche.

Allo scopo di assicurare la riconducibilità della copia realizzata a quello specifico procedimento di scansione, la "certificazione iniziale" dovrà generare un codice univoco da inserire tra i metadati di ciascun documento copia o, in alternativa, riportare l'elenco dei valori di hash relativi a ciascuna copia informatica frutto della scansione effettuata. In questo modo si eviterà che copie

realizzate con altri procedimenti possano essere “inserite” fraudolentemente tra quelle prodotte dal processo certificato, acquisendo la relativa efficacia probatoria. Laddove richiesta dalla natura dell’attività, il singolo documento estratto dal procedimento di scansione o l’intero lotto potrà successivamente essere “certificato” da notaio o PU a ciò autorizzato attraverso la verifica di corrispondenza del codice oppure della variabile di hash calcolata su ciascun documento a valle della scansione massiva fatta.

In particolare, la descrizione del procedimento di dematerializzazione presente nell’attestazione di conformità[4] o rapporto di verificazione contiene le seguenti minime informazioni:

- Anagrafica Committente;
- Nominativo e ruolo del verbalizzante (privato, notaio o PU a ciò autorizzato);
- Codice identificativo univoco presente tra i metadati del documento copia (in alternativa al listato dei valori di hash calcolati sulle copie informatiche);
- Identificativo (tipologia e numero) del campione di documenti copia utilizzati per la certificazione iniziale;
- Numero, tipologia e quantità del lotto di documenti analogici sottoposti a scansione;
- Tipologia e quantità del lotto di documenti cui il campione appartiene;
- Requisiti tecnici e/o vincoli di progetto di scansione massiva;
- Finalità della scansione (es.: statistico, storico, probatorio,…);
- Riferimento contratto tra fornitore e committente (in caso di *outsourcing*);
- Luogo, data e orario inizio e fine della scansione a cui si è assistito;
- Nomi referenti presenti al processo di scansione (opzionale);
- Riferimento documentazione di analisi, di progetto o di sistema utilizzata a supporto del processo di dematerializzazione;
- Nome e versione del sw di elaborazione digitale delle immagini utilizzato;
- Segnalazione di eventuali criticità, anomalie riscontrate;
- Indicazione delle fasi e dei controlli o della procedura ISO 9001 di riferimento, che a titolo esemplificativo possono essere rappresentate da:
    - Sanificazione, fascicolazione e normalizzazione (despillatura) dei documenti analogici,
    - Settaggio (selezione dei parametri di acquisizione) del sw di image processing;
    - Scansione batch dei documenti,
    - Indicizzazione (metadatazione),
    - Verifica qualità immagini digitalizzate,
    - Segnalazione incongruenze.

Per l’acquisizione massiva dei documenti si ricorre a scanner professionali che devono essere dotati di sistemi di lettura ottica ovvero di algoritmi di elaborazione digitale delle immagini in grado di migliorare la qualità delle immagini medesime e correggere automaticamente i più comuni errori. Di seguito, le funzionalità minime da assicurare per un software di elaborazione digitale delle immagini:

- Auto orientamento,
- Bilanciamento della luce e del colore,
- Correzione della deformazione,

- Correzione della curvatura,
- Rotazione e ribaltamento,
- Controllo qualità (proprietà delle immagini, come luminosità, contrasto, varianza, colore dominante, dimensioni, colori, inclinazione,...).

I suddetti requisiti tecnologici sono accompagnati dai vincoli di progetto rappresentati – ad esempio - dall'utilizzo o finalità che si vuole fare dell'immagine (memorizzazione storica a lungo termine, probatorio, distribuzione via web,...), dalla tipologia di documento sottoposto a scansione, dalla numerosità del lotto di documenti da scansionare, dalla percentuale di errore ritenuta tollerabile nel controllo visivo di qualità o ancora dagli obblighi di visualizzazione e ricerca imposti dalla normativa vigente (Ag. Entrate del 15 giugno 2009, n. 158/E),, che impongono di settare i software di *image processing* a valle dell'analisi dell'archivio analogico fatta. Le certificazioni di sistema ISO 9001 e 27001 rappresentano pertanto - lato organizzazione – una ragionevole garanzia di qualità e sicurezza a fronte delle variabili tecnologiche individuate.

Le Pubbliche Amministrazioni che vogliono svolgere in autonomia la dematerializzazione massiva di documenti analogici possono non ricorrere alle certificazioni ISO assumendo in toto la responsabilità della qualità del processo.

2.4. Validazione della certificazione di processo

Come detto, la certificazione di processo si caratterizza, sia dal punto di vista oggettivo sia da quello soggettivo, per attestare l'efficacia probatoria della certificazione di processo (§1.2). Pertanto, è indispensabile validare la conformità di un documento-copia rispetto ad un documento-originale di partenza.

A valle del processo di scansione massiva, la riconducibilità del documento copia alla certificazione iniziale è validata dal notaio/PU o soggetto privato che rilascia un verbale di "certificazione di chiusura" attraverso la verifica di corrispondenza del codice univoco presente tra i metadati o del valore di hash su un campione di documenti individuato[6].

Trattandosi di attività ovviamente non "delegabile", essa sarà rimessa all'apprezzamento esclusivo e diretto del pubblico ufficiale o soggetto privato autorizzato.

Il controllo visivo si sostanzia nell'attestare i requisiti tecnici essenziali di leggibilità del documento immagine risultato della scansione, di garanzia dell'integrità del contenuto e di completezza del processo di scansione.

Evidentemente, l'attestazione di conformità o rapporto di verificazione è sottoscritto con firma digitale o altra firma elettronica qualificata, come stabilito ai sensi dagli artt. 22 comma 2 e 23-ter comma 3 del CAD.

ENTE DI GESTIONE DELLE AREE PROTETTE DEL PO PIEMONTESE

ALLEGATO 4

AL MANUALE DI GESTIONE DOCUMENTALE DEL PROTOCOLLO INFORMATICO, DEI FLUSSI DOCUMENTALI E DEGLI ARCHIVI

STANDARD E SPECIFICHE TECNICHE

(estratto dell'allegato 4 ai sensi delle linee guida Agid maggio 2021)

1. Standard e Specifiche tecniche

Di seguito sono riportati i principali standard e specifiche tecniche di riferimento nell'ambito della formazione, gestione e conservazione di documenti informatici e documenti amministrativi informatici. In particolare:

1.1. per la gestione documentale

UNI ISO 15489-1 - Informazione e documentazione - Gestione dei documenti di archivio - Principi generali sul record management.

UNI ISO 15489-2 -Informazione e documentazione - Gestione dei documenti di archivio – Linee Guida sul record management.

ISO/TS 23081-1 - Information and documentation - Records management processes – Metadata for records – Part 1 – Principles, Quadro di riferimento per lo sviluppo di un sistema di metadati per la gestione documentale.

ISO/TS 23081-2 - Information and documentation - Records management processes – Metadata for records – Part 2 – Conceptual and implementation issues, Guida pratica per l'implementazione.

ISO 16175-1 - (ICA) Information and documentation -- Principles and functional requirements for records in electronic office environments -- Part 1: Overview and statement of principles.

ISO 16175-2 - (ICA) Information and documentation -- Principles and functional requirements for records in electronic office environments -- Part 2: Guidelines and functional requirements for digital records management systems.

ISO 16175-3 - (ICA) Information and documentation -- Principles and functional requirements for records in electronic office environments -- Part 3: Guidelines and functional requirements for records in business system.

ISO 15836 - Information and documentation - The Dublin Core metadata element set, Sistema di metadata del Dublin Core.

ISO 9001 – Sistemi di gestione per la qualità – Requisiti.

ISO 30300:2011 Information and documentation - Management systems for records - Fundamentals and vocabulary;

ISO 30301:2011 Information and documentation - Management systems for records – Requirements.

ISO 30302:2015 Information and documentation - Management systems for records - Guidelines for implementation.

ISO/TR 23081-3 - Information and documentation — Managing metadata for records — Part 3: Self-assessment method

MoReq 2001 Model requirements for the management of electronic records.

MoReq 2 Specification 2008 Model requirements for the management of electronic records – che individua i requisiti funzionali della gestione documentale.

MoReq2010 Modular requirements for records systems.

1.2. per la conservazione digitale

UNI 11386 - Standard SInCRO - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali.

ISO 14721 - OAIS (Open Archival Information System), Sistema informativo aperto per l'archiviazione.

ISO 15836 - Information and documentation - The Dublin Core metadata element set, Sistema di metadata del Dublin Core

ISO/TR 18492 - Long-term preservation of electronic document-based information.

ISO 20652 - Space data and information transfer systems - Producer-Archive interface - Methodology abstract standard.

ISO 20104 - Space data and information transfer systems — Producer-Archive Interface Specification (PAIS).

ISO/CD TR 26102 - Requirements for long-term preservation of electronic records.

SIARD Software Independent Archiving of Relational Databases 2.0

Ministère de la culture et de la communication, Service interministériel des Archives de France, Standard d'échange de donnéès pour l'archivage. Transfert – Communication – Élimination – Restitution - Modification, ver. 2.1, 2018

METS - Metadata Encoding and Transmission Standard

PREMIS – PREservation Metadata: Implementation Strategies.

EAD (3)/ISAD (G)

EAC (CPF)/ISAAR (CPF)/NIERA (CPF)

SCONS2/EAG/ISDIAH

1.3. Per affidabilità (certificazione/valutazione-autovalutazione)

ISO 16363 - Space data and information transfer systems -- Audit and certification of trustworthy digital repositories

ISO 16919 - Space data and information trans:fer systems -- Requirements for bodies providing audit and certification of candidate trustworthy digital repositories

ISO 17068 - Information and documentation -- Trusted third party repository for digital records

2.1 per Sicurezza informatica

ISO/IEC 27001 - Information technology - Security techniques - Information security management systems – Requirements, Requisiti di un ISMS (Information Security Management System);

ISO/IEC 27017 - Information technology -- Security techniques -- Code of practice for information security controls based on ISO/IEC 27002 for cloud services;

ISO/IEC 27018 - Information technology -- Security techniques -- Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors;

ETSI TS 101 533-1 V1.2.1 - Technical Specification, Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part 1: Requirements for Implementation and Management, Requisiti per realizzare e gestire sistemi sicuri e affidabili per la conservazione elettronica delle informazioni;

ETSI TR 101 533-2 V1.2.1 - Technical Report, Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part 2: Guidelines for Assessors, Linee guida per valutare sistemi sicuri e affidabili per la conservazione elettronica delle informazioni.

ENTE DI GESTIONE DELLE AREE PROTETTE DEL PO PIEMONTESE

ALLEGATO 5

AL MANUALE DI GESTIONE DOCUMENTALE DEL PROTOCOLLO INFORMATICO, DEI FLUSSI DOCUMENTALI E DEGLI ARCHIVI

METADATI MINIMI DEL DOCUMENTO INFORMATICO

(Estratto dell'allegato 5 alle linee guida Agid 2021)

1. INTRODUZIONE

Il presente allegato illustra i metadati relativi al documento informatico, al documento amministrativo informatico e all'aggregazione documentale informatica, intendendo, con quest'ultima, sia il fascicolo informatico, che la serie documentale.

Gli schemi sotto riportati sono organizzati in modo da indicare per ogni metadato:

- **Informazione**: il nome;
- **Sottocampi**: l'eventuale sottostruttura del metadato complesso;
- **Valori ammessi**: valori accettati all'interno del campo;
- **Tipo dato**: numerici o alfanumerici;
- **Obbligatorietà**: l'indicazione di obbligatorietà, eventualmente condizionata;
- **Nuova definizione**: metadati nuovi o ridefiniti rispetto all'allegato alla normativa precedente;
- **Definizione**: indicazione sulla modalità di utilizzo del metadato.

L'attività di **indicizzazione, individuazione e ricerca** è significativamente agevolata dalla definizione di metadati legati:

- **alla tipologia** – "Tipologia documentale" o "Tipologia fascicolo";
- **alla registrazione** – "Dati registrazione";
- **all'Oggetto** – "Chiave descrittiva";
- **alla Classificazione** – "Classificazione"

Particolarmente rilevante è il metadato complesso "*Assegnazione*" dell'aggregazione documentale informatica. Tale metadato, strutturato in vari sottocampi opportunamente valorizzati, consente di tracciare ogni passaggio dell'aggregazione per competenza o per conoscenza, al fine di garantire la massima trasparenza nell'ambito di qualsiasi procedimento amministrativo della PA.

2. METADATI DEL DOCUMENTO INFORMATICO

Definizione del metadato IdDoc (element xsd: IdDoc)

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

Inoltre, rappresenta le informazioni necessarie per verificare l'integrità del documento.

Il metadato è costituito da:

- Impronta: sottocampo in cui viene memorizzato l'hash del documento
- Algoritmo: sottocampo nel quale deve essere indicata la tipologia dell'algoritmo applicato riportati nell'Allegato 6 delle Linee Guida nella tabella 1 del paragrafo 2.2 "Regole di processamento"
- Identificativo: come da sistema di identificazione formalmente definito

Campi	Sottocampi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
Impronta crittografica del documento					NO, ma ridefinito
	Impronta	Rappresenta l'hash del documento	Binary	SI	
	Algoritmo	Rappresenta l'algoritmo applicato Default = SHA-256	Alfanumerico	SI	
Identificativo		Come da sistema di identificazione formalmente definito	Alfanumerico	SI	NO, ma ridefinito

Definizione del metadato Modalità di formazione (element xsd: ModalitaDiFormazione)

Indica la modalità di generazione del documento informatico.

Sono previste le seguenti modalità secondo quanto riportato nelle Linee guida:

a) creazione tramite l'utilizzo di strumenti software che assicurino la produzione di documenti nei formati dalle Linee Guida;

b) acquisizione di un documento informatico per via telematica o su supporto informatico, acquisizione della copia per immagine su supporto informatico di un documento analogico, acquisizione della copia informatica di un documento analogico;

c) memorizzazione su supporto informatico in formato digitale delle informazioni risultanti da transazioni o processi informatici o dalla presentazione telematica di dati attraverso moduli o formulari resi disponibili all'utente;

d) generazione o raggruppamento anche in via automatica di un insieme di dati o registrazioni, provenienti da una o più banche dati, anche appartenenti a più soggetti interoperanti, secondo una struttura logica predeterminata e memorizzata in forma statica

Campi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
NON Applicabile	Indicare: a) creazione tramite l'utilizzo di strumenti software che assicurino la produzione di documenti nei formati previsti nell'Allegato 2 delle Linee Guida; b) acquisizione di un documento informatico per via telematica o su supporto informatico, acquisizione della copia per immagine su supporto informatico di un documento analogico, acquisizione della copia informatica di un documento analogico; c) memorizzazione su supporto informatico in formato digitale delle informazioni risultanti da transazioni o processi informatici o dalla presentazione telematica di dati attraverso moduli o formulari resi disponibili all'utente; d) generazione o raggruppamento anche in via automatica di un insieme di dati o registrazioni, provenienti da una o più banche dati, anche appartenenti a più soggetti interoperanti, secondo una struttura logica predeterminata e memorizzata in forma statica.	Alfanumerico	SI	SI

Definizione del metadato Tipologia documentale (element xsd: TipologiaDocumentale)

Metadato funzionale che indica la tipologia del documento tra quelle trattate per lo svolgimento delle attività.

Campi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
NON Applicabile	Metadato testuale libero per indicare le tipologie documentali trattate (ad esempio, fatture, delibere, determine, etc)	Alfanumerico	SI	SI

Definizione del metadato Dati di registrazione (element xsd: DatiDiRegistrazione)

Metadato che comprende i dati di registrazione del documento sia nel caso di documento protocollato che non protocollato. Si intende per registrazione l'operazione che, in senso lato, associa ad un documento una data e un numero. In tale ottica, quindi potrebbe non essere identificabile uno specifico registro, ma sono sempre identificabili una data di registrazione e un numero di registrazione del documento.

Sono previsti i seguenti campi:

- Tipologia di flusso: indica se si tratta di un documento in uscita, in entrata o interno.
- Tipo registro: indica il sistema di registrazione adottato: protocollo ordinario/protocollo emergenza, o Repertorio/Registro.
- Data: è la data associata al documento all'atto della registrazione
- Numero documento: Numero identificativo del documento nel caso di documento non protocollato (ad esempio, numero fattura), numero di protocollo nel caso di documento protocollato.
- Codice Registro: Identificativo del registro nel caso in cui il tipo registro sia protocollo ordinario/ protocollo emergenza, o Repertorio/Registro.

Campi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
Tipologia di flusso	• "U" = In uscita • "E" = In entrata • "I" = Interno	Alfanumerico	SI	SI
Tipo registro	• Nessuno, • Protocollo Ordinario/Protocollo Emergenza • Repertorio/Registro	Alfanumerico	SI	SI

Campi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
Data registrazione	nel caso di documento non protocollato: • Data di registrazione del Documento/Ora di registrazione del Documento nel caso di documento protocollato: • Data di registrazione di protocollo/Ora di protocollazione del Documento	Date/Time	SI	NO, ma ridefinito
Numero Documento	nel caso di documento non protocollato: • Numero di registrazione del documento nel caso di documento protocollato: • Numero di protocollo	Alfanumerico	SI	SI
Codice Registro	Codice identificativo del registro in cui il documento viene registrato.	Alfanumerico	SI, nel caso in cui il tipo registro sia protocollo ordinario/protocollo emergenza, o Repertorio/Registro	SI

Definizione del metadato Soggetti (element xsd: Soggetti)

Indica il metadato che consente di individuare le informazioni relative a tutti i soggetti coinvolti e competenti sul documento a vario titolo e definiti dal campo Ruolo. Sono definiti quindi i seguenti attributi:

- Ruolo: consente di indicare, a seconda delle necessità, l'autore del documento, il mittente, il destinatario, l'assegnatario. Al fine di renderei dati di registrazione univoci deve essere sempre indicato il Soggetto che effettua la registrazione del documento (tipicamente l'Organizzazione che protocolla). Obbligatorio inoltre indicare almeno l'autore o il mittente. Nel caso di documento protocollato deve essere obbligatoriamente indicato il mittente.
- Per "Operatore" si intende il soggetto autorizzato ad apportare modifiche/integrazioni al documento, la cui definizione si renderà obbligatoria nel caso in cui venga compilato il metadato "Tracciature modifiche documento".
- Tipo soggetto: consente di tipizzare i soggetti come persone fisiche, giuridiche, amministrazioni pubbliche (italiane ed estere). Il Tipo Soggetto = SW è indicabile solo se si è indicato il ruolo = "Produttore". Per ogni Tipo Soggetto sono indicati i metadati di riferimento.

Il metadato ha una struttura ricorsiva.

Campi	Sottocampi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
Ruolo		• Assegnatario • Autore • Destinatario • Mittente • Operatore • Produttore • RGD (Responsabile della Gestione Documentale) • RSP (Responsabile del Servizio di Protocollo) • Soggetto che effettua la registrazione • Altro	Alfanumerico	SI, al fine di rendere i dati di registrazione univoci deve essere sempre indicato il soggetto che effettua la registrazione del documento. Obbligatorio indicare inoltre almeno l'autore o il mittente. Nel caso di documento protocollato deve essere obbligatoriamente indicato il mittente. Per "Operatore" si intende il soggetto autorizzato ad	NO, ma ridefinito

Campi	Sottocampi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
				apportare modifiche/ integrazioni al documento, la cui definizione si renderà obbligatoria nel caso in cui venga compilato il metadato “Tracciature modifiche documento”.	
Tipo soggetto		Se Ruolo = Assegnatario ✓ AS Se Ruolo = Soggetto che effettua la registrazione ✓ PF per Persona Fisica ✓ PG per Organizzazione Se Ruolo = Mittente o Destinatario o Altro ✓ PF per Persona Fisica ✓ PG per Organizzazione ✓ PAI per le Amministrazioni Pubbliche italiane (valido solo come mittente nei flussi in entrata, come destinatario nei flussi in uscita) ✓ PAE per le Amministrazioni Pubbliche estere (valido solo come mittente nei flussi in entrata, come destinatario nei flussi in uscita) Se Ruolo = Autore ✓ PF per Persona Fisica ✓ PG per Organizzazione ✓ PAI per le Amministrazioni Pubbliche italiane (valido solo nei flussi in entrata)	Alfanumerico	SI	SI

Campi	Sottocampi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
		✓ PAE per le Amministrazioni Pubbliche estere (valido solo nei flussi in entrata) Se Ruolo = Operatore o Responsabile della Gestione Documentale o Responsabile del Servizio Protocollo ✓ PF per Persona Fisica Se Ruolo = Produttore ✓ SW per i documenti prodotti automaticamente			
	PF	Cognome	Alfanumerico	SI	SI
		Nome	Alfanumerico	SI	
		Codice Fiscale	Alfanumerico	NO	
		Indirizzi Digitali Di Riferimento	Alfanumerico	NO	
	PG	Denominazione Organizzazione	Alfanumerico	SI	SI
		Codice fiscale\Partita Iva	Alfanumerico	NO	
		Denominazione Ufficio	Alfanumerico	NO	
		Indirizzi Digitali Di Riferimento	Alfanumerico	NO	
	PAI	Denominazione Amministrazione \ Codice IPA	Alfanumerico	SI	SI
		Denominazione Amministrazione AOO \ Codice IPA AOO	Alfanumerico	NO	
		Denominazione Amministrazione UOR \ Codice IPA UOR	Alfanumerico	NO	
		Indirizzi Digitali Di Riferimento	Alfanumerico	NO	
	PAE	Denominazione Amministrazione	Alfanumerico	SI	SI

Campi	Sottocampi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
		Denominazione Ufficio	Alfanumerico	NO	
		Indirizzi Digitali Di Riferimento	Alfanumerico	NO	
	AS	Cognome	Alfanumerico	NO	SI
		Nome	Alfanumerico	NO	
		Codice Fiscale	Alfanumerico	NO	
		Denominazione Organizzazione	Alfanumerico	SI	
		Denominazione Ufficio	Alfanumerico	SI	
		Indirizzi Digitali Di Riferimento	Alfanumerico	NO	
	SW	Denominazione Sistema	Alfanumerico	SI	SI

Definizione del metadato Allegati (element xsd: Allegati)

Indica il numero di allegati al documento e, nell'eventualità che il numero di allegati indicati sia maggiore di zero, devono essere compilati, in modalità ricorsiva, i dati:

- IdDoc: Identificativo del documento relativo all'allegato
- Descrizione: Titolo dell'Allegato

Campi	Sottocampi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
Numero allegati		Inserire un numero intero compreso tra 0 e 9999	Numerico	SI	SI
Indice allegati		Da indicare per ogni allegato se Numero allegati > 0			
	IdDoc	Identificativo del documento relativo all'allegato		SI, se numero allegati > 0	SI
	Descrizione	Testo libero	Alfanumerico	SI, se numero allegati > 0	SI

Definizione del metadato Classificazione (element xsd: Classificazione)

Classificazione del documento secondo il Piano di classificazione utilizzato da indicare sia nel caso di documento protocollato che nel caso di documento non protocollato:

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

Campi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
Indice di classificazione	Codifica del documento secondo il Piano di classificazione utilizzato	Alfanumerico	NO	SI
Descrizione	Descrizione per esteso dell'Indice di classificazione indicato.	Alfanumerico	NO	SI
Piano di classificazione	URI del Piano di classificazione pubblicato	Alfanumerico	NO	SI

Definizione del metadato Riservato (element xsd: Riservato)

Rappresenta il livello di sicurezza di accesso al documento:

- Vero: se il documento è considerato riservato
- Falso: se il documento non è considerato riservato

Consente di gestire gli accessi al documento al solo personale autorizzato.

Campi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
NON Applicabile	• Vero: se il documento è considerato riservato • Falso: se il documento non è considerato riservato	Boolean	SI	SI

Definizione del metadato Identificativo del formato (element xsd: IdentificativoDelFormato)

Indica il formato del documento e la versione del software utilizzato per la creazione del documento stesso. É costituito da:

- Formato: secondo quanto previsto dall'Allegato 2 delle Linee Guida.
- Prodotto software: prodotto software utilizzato per la creazione del documento e relativa versione, suddiviso a sua volta in tre sottocampi:
  - Nome prodotto
  - Versione prodotto
  - Produttore

Campi	Sottocampi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
Formato		Previsti dall'Allegato 2 delle Linee Guida	Alfanumerico	SI	SI
Prodotto software		Prodotto software utilizzato per la creazione del documento e relativa versione			SI
	Nome prodotto		Alfanumerico	SI, quando rilevabile	SI
	Versione prodotto		Alfanumerico	SI, quando rilevabile	SI
	Produttore		Alfanumerico	SI, quando rilevabile	SI

Definizione del metadato Tracciature modifiche documento (element xsd: TracciatureModificheDocumento)

Metadato volto a tracciare la presenza di operazioni di modifica effettuate sul documento e la data in cui esse sono state effettuate. L'autore delle modifiche è tracciato nel metadato "Soggetti" con il ruolo "Operatore".

Campi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
Tipo modifica	• Annullamento • Rettifica • Integrazione • Annotazione	Alfanumerico	SI, nel caso di versione > 1 o in caso di annullamento	SI
Soggetto autore della modifica	Come da ruolo = Operatore definito nel metadato Soggetti	Alfanumerico	SI, nel caso di versione > 1 o in caso di annullamento	SI
Data modifica/Ora modifica		Date/Time	SI, nel caso di versione > 1 o in caso di annullamento	SI
IdDoc versione precedente	Identificativo documento versione precedente		SI, nel caso di versione > 1 o in caso di annullamento	SI

XSD METADATI DEL DOCUMENTO INFORMATICO

Schema xsd:

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" elementFormDefault="qualified">
<xs:element name="DocumentoInformatico" type="DocumentoInformaticoType"/>
<xs:complexType name="DocumentoInformaticoType">
<xs:sequence>
<xs:element name="IdDoc" type="IdDocType"/>
<xs:element name="ModalitaDiFormazione" type="ModalitaDiFormazioneType"/>
<xs:element name="TipologiaDocumentale" type="xs:string" />
<xs:element name="DatiDiRegistrazione" type="DatiDiRegistrazioneType"/>
<xs:element name="Soggetti" type="SoggettiType"/>
<xs:element name="ChiaveDescrittiva" type="ChiaveDescrittivaType"/>
<xs:element name="Allegati" type="AllegatiType"/>
<xs:element name="Classificazione" type="ClassificazioneType" minOccurs="0"/>
<xs:element name="Riservato" type="xs:boolean" />
<xs:element name="IdentificativoDelFormato" type="IdentificativoDelFormatoType"/>
<xs:element name="Verifica" type="VerificaType"/>
<xs:element name="Agg" type="AggType"/>
<xs:element name="IdIdentificativoDocumentoPrimario" type="IdDocType" minOccurs="0"/>
<xs:element name="NomeDelDocumento" type="xs:string" />
<xs:element name="VersioneDelDocumento" type="xs:string" />
<xs:element                                          name="TracciatureModificheDocumento"
type="TracciatureModificheDocumentoType"
minOccurs="0" />
                        <xs:element name="TempoDiConservazione" type="TempoDiConservazioneType" minOccurs="0"/>
                        <xs:element name="Note" type="xs:string" minOccurs="0" />
                        </xs:sequence>
[Digitare qui]
```

```
</xs:complexType>
```

```
<xs:complexType name="IdDocType">
<xs:sequence>
<xs:element name="ImprontaCrittograficaDelDocumento" type="ImprontaCrittograficaDelDocumentoType" />
<xs:element name="Identificativo" type="xs:string" />
</xs:sequence>
</xs:complexType>
<xs:complexType name="ImprontaCrittograficaDelDocumentoType">
<xs:sequence>
<xs:element name="Impronta" type="xs:base64Binary" />
<xs:element name="Algoritmo" type="xs:string" default="SHA-256"/>
</xs:sequence>
</xs:complexType>

<xs:simpleType name="ModalitaDiFormazioneType">
<xs:restriction base="xs:string">
<xs:enumeration value="creazione tramite utilizzo di strumenti software che assicurino la produzione di documenti nei formati previsti in allegato 2"/>
<xs:enumeration value="acquisizione di un documento informatico per via telematica o su supporto informatico, acquisizione della copia per immagine su supporto informatico di un documento analogico, acquisizione della copia informatica di un documento analogico"/>
<xs:enumeration value="memorizzazione su supporto informatico in formato digitale delle informazioni risultanti da transazioni o processi informatici o dalla presentazione telematica di dati attraverso moduli o formulari resi disponibili ad utente"/>
<xs:enumeration value="generazione o raggruppamento anche in via automatica di un insieme di dati o registrazioni, provenienti da una o più banche dati, anche appartenenti a più soggetti interoperanti, secondo una struttura logica predeterminatae memorizzata in forma statica"/>
</xs:restriction>
</xs:simpleType>

<xs:complexType name="DatiDiRegistrazioneType">
```

```
<xs:sequence>
<xs:element name="TipologiaDiFlusso" type="TipologiaDiFlussoType"/>
<xs:element name="TipoRegistro" type="TipoRegistroType"/>
</xs:sequence>
</xs:complexType>

<xs:simpleType name="TipologiaDiFlussoType">
<xs:restriction base="xs:string">
<xs:enumeration value="E"/>
<xs:enumeration value="U"/>
<xs:enumeration value="I"/>
</xs:restriction>
</xs:simpleType>

                                <xs:complexType name="TipoRegistroType">
                                <xs:sequence>
                                <xs:choice>
                                <xs:element name="Nessuno" type="NoRegistroType"/>
                                <xs:element                                                    name="ProtocolloOrdinario_ProtocolloEmergenza"
type="ProtocolloType"/>
                                <xs:element name="Repertorio_Registro" type="NoProtocolloType"/>
                                </xs:choice>
                                </xs:sequence>
                                </xs:complexType>

                                        <xs:complexType name="NoRegistroType">
                                                <xs:sequence>
                                            <xs:element name="TipoRegistro" type="xs:string" fixed = 'Nessuno'/>
                                                    <xs:element name="DataDocumento" type="xs:date"/>
                                                <xs:element name="OraDocumento" type="xs:time" minOccurs="0"/>
```

```
                                        <xs:element name="NumeroDocumento" type="xs:string" />
                                                </xs:sequence>
                                            </xs:complexType>

                                            <xs:complexType name="ProtocolloType">
                                            <xs:sequence>
                                            <xs:element name="TipoRegistro" type="xs:string" fixed =
'ProtocolloOrdinario\ProtocolloEmergenza'/>
                                            <xs:element name="DataProtocollazioneDocumento" type="xs:date"/>
                                            <xs:element name="OraProtocollazioneDocumento" type="xs:time"
minOccurs="0"/>
                                            <xs:element name="NumeroProtocolloDocumento" type="NumProtType"/>
                                            <xs:element name="CodiceRegistro" type="CodiceRegistroType"/>
                                            </xs:sequence>
                                            </xs:complexType>

        <xs:complexType name="NoProtocolloType">
                                                    <xs:sequence>
<xs:element name="TipoRegistro" type="xs:string" fixed = 'Repertorio\Registro'/>
<xs:element name="DataRegistrazioneDocumento" type="xs:date"/>
<xs:element name="OraRegistrazioneDocumento" type="xs:time"
minOccurs="0"/>
                                        <xs:element name="NumeroRegistrazioneDocumento" type="xs:string"/>
                                        <xs:element name="CodiceRegistro" type="CodiceRegistroType"/>
                                        </xs:sequence>
                                        </xs:complexType>

                                        <xs:simpleType name="NumProtType">
                                        <xs:restriction base="xs:string">
                                        <xs:pattern value="[0-9]{7,}"/>
```

```
                                                    </xs:restriction>
                                                   </xs:simpleType>

<xs:simpleType name="CodiceRegistroType">
<xs:restriction base="xs:string">
<xs:pattern value="[A-Za-z0-9_\.\-]{1,16}"/>
</xs:restriction>
</xs:simpleType>

<xs:complexType name="SoggettiType">
<xs:sequence>
<xs:element name="Ruolo" type="RuoloType" minOccurs="1" maxOccurs="unbounded"/>
</xs:sequence>
</xs:complexType>

<xs:complexType name="RuoloType">
<xs:choice>
<xs:element name="SoggettoCheEffettuaLaRegistrazione" type="TipoSoggetto21Type"/>
<xs:element name="Assegnatario" type="TipoSoggetto22Type"/>
<xs:element name="Destinatario" type="TipoSoggetto11Type"/>
<xs:element name="Mittente"                                    type="TipoSoggetto12Type"/>
<xs:element name="Autore" type="TipoSoggetto31Type"/>
<xs:element name="Operatore" type="TipoSoggetto32Type"/>
<xs:element name="ResponsabileGestioneDocumentale" type="TipoSoggetto33Type"/>
<xs:element name="ResponsabileServizioProtocollo" type="TipoSoggetto34Type"/>
<xs:element name="Produttore" type="TipoSoggetto4Type"/>
<xs:element name="Altro" type="TipoSoggetto13Type"/>
</xs:choice>
</xs:complexType>
```

```
<xs:complexType name="TipoSoggetto11Type">
<xs:sequence>
<xs:element name="TipoRuolo" type="xs:string" fixed = 'Destinatario'/>
<xs:choice>
<xs:element name="PF" type="PFType"/>
<xs:element name="PG" type="PGType"/>
<xs:element name="PAI" type="PAIType"/>
<xs:element name="PAE" type="PAEType"/>
</xs:choice>
</xs:sequence>
</xs:complexType>

<xs:complexType name="TipoSoggetto12Type">
<xs:sequence>
<xs:element name="TipoRuolo" type="xs:string" fixed = 'Mittente'/>
<xs:choice>
<xs:element name="PF" type="PFType"/>
<xs:element name="PG" type="PGType"/>
<xs:element name="PAI" type="PAIType"/>
<xs:element name="PAE" type="PAEType"/>
</xs:choice>
</xs:sequence>
</xs:complexType>

                                        <xs:complexType name="TipoSoggetto13Type">
<xs:sequence>
                <xs:element name="TipoRuolo" type="xs:string" fixed = 'Altro'/>
                                                                    <xs:choice>
<xs:element name="PF" type="PFType"/>
<xs:element name="PG" type="PGType"/>
```

```
                                                    <xs:element name="PAI" type="PAIType"/>
                                                    <xs:element name="PAE" type="PAEType"/>
                                                        </xs:choice>
                                                    </xs:sequence>
                                                </xs:complexType>

                                            <xs:complexType name="TipoSoggetto21Type">
                                                    <xs:sequence>
        <xs:element name="TipoRuolo" type="xs:string" fixed = 'Soggetto Che Effettua La Registrazione'/>
                                                        <xs:choice>
                                                    <xs:element name="PF" type="PFType"/>
                                                    <xs:element name="PG" type="PGType"/>
                                                        </xs:choice>
                                                    </xs:sequence>
                                                </xs:complexType>

<xs:complexType name="TipoSoggetto22Type">
<xs:sequence>
<xs:element name="TipoRuolo" type="xs:string" fixed = 'Assegnatario'/>
<xs:element name="AS" type="ASType"/>
</xs:sequence>
</xs:complexType>

<xs:complexType name="ASType" >
<xs:sequence>
<xs:element name="Cognome" type="xs:string" minOccurs="0"/>
<xs:element name="Nome" type="xs:string" minOccurs="0" />
<xs:element name="CodiceFiscale" type="CFType" minOccurs="0"/>
<xs:element name="DenominazioneOrganizzazione" type="xs:string" />
<xs:element name="DenominazioneUfficio" type="xs:string" />
```

```
                                                                    <xs:element  name="IndirizziDigitaliDiRiferimento"  type="xs:string"
minOccurs="0" maxOccurs="unbounded"/>
</xs:sequence>
                                                </xs:complexType>


<xs:complexType name="TipoSoggetto31Type">
<xs:sequence>
<xs:element name="TipoRuolo" type="xs:string" fixed = 'Autore'/>
<xs:choice>
<xs:element name="PF" type="PFType"/>
<xs:element name="PG" type="PGType"/>
<xs:element name="PAI" type="PAIType"/>
<xs:element name="PAE" type="PAEType"/>
</xs:choice>
</xs:sequence>
</xs:complexType>

                                        <xs:complexType name="TipoSoggetto32Type">
                                                    <xs:sequence>
                <xs:element name="TipoRuolo" type="xs:string" fixed = 'Operatore'/>
                                                    <xs:element name="PF" type="PFType"/>
                                                     </xs:sequence>
                                                </xs:complexType>

<xs:complexType name="TipoSoggetto33Type">
<xs:sequence>
<xs:element name="TipoRuolo" type="xs:string" fixed = 'Responsabile della Gestione Documentale'/>
<xs:element name="PF" type="PFType"/>
                                                    </xs:sequence>
                                                </xs:complexType>
```

```
<xs:complexType name="TipoSoggetto34Type">
<xs:sequence>
<xs:element name="TipoRuolo" type="xs:string" fixed = 'Responsabile del Servizio di Protocollo'/>
<xs:element name="PF" type="PFType"/>
                                                    </xs:sequence>
                                                </xs:complexType>

                                            <xs:complexType name="TipoSoggetto4Type">
                                                    <xs:sequence>
            <xs:element name="TipoRuolo" type="xs:string" fixed = 'Produttore'/>
                                                <xs:element name="SW" type="SWType"/>
                                                    </xs:sequence>
                                                </xs:complexType>

                                                    <xs:complexType name="PFType">
                                                    <xs:sequence>
                                                    <xs:element name="Cognome" type="xs:string" />
                                                    <xs:element name="Nome" type="xs:string" />
                                                    <xs:element name="CodiceFiscale" type="CFType" minOccurs="0"/>
                                                    <xs:element  name="IndirizziDigitaliDiRiferimento"  type="xs:string"
minOccurs="0" maxOccurs="unbounded"/>
                                                    </xs:sequence>
                                                    </xs:complexType>

                                                    <xs:complexType name="PGType">
                                                    <xs:sequence>
                                                    <xs:element                                                 name="DenominazioneOrganizzazione"
type="xs:string" />
```

```
                                        <xs:element                                 name="CodiceFiscale_PartitaIva"      type="PIType"
minOccurs="0"/>
                                        <xs:element                                 name="DenominazioneUfficio"      type="xs:string"
minOccurs="0" />
                                        <xs:element  name="IndirizziDigitaliDiRiferimento"  type="xs:string"
minOccurs="0" maxOccurs="unbounded"/>
                                        </xs:sequence>
                                        </xs:complexType>


                                        <xs:complexType name="PAIType" >
                                        <xs:sequence>
                                        <xs:element name="IPAAmm" type="CodiceIPAType" />
                                        <xs:element name="IPAAOO" type="CodiceIPAType" minOccurs="0"
/> minOccurs="0"/>
                                        <xs:element                                 name="IPAUOR"          type="CodiceIPAType"
minOccurs="0" maxOccurs="unbounded"/>
                                        <xs:element  name="IndirizziDigitaliDiRiferimento"  type="xs:string"

                                        </xs:sequence>
                                        </xs:complexType>


                                        <xs:complexType name="PAEType" >
                                        <xs:sequence>
                                                <xs:element                                 name="DenominazioneAmministrazione"
type="xs:string"/>minOccurs="0"/>
                                                <xs:element                 name="DenominazioneUfficio"      type="xs:string"
minOccurs="0" maxOccurs="unbounded"/>
                                                <xs:element  name="IndirizziDigitaliDiRiferimento"  type="xs:string"
</xs:complexType>
                                                </xs:sequence>
```

```
<xs:complexType name="CodiceIPAType" >
<xs:sequence>
<xs:element name="Denominazione" type="xs:string" />
<xs:element name="CodiceIPA" type="xs:string" />
</xs:sequence>
</xs:complexType>

                                        <xs:complexType name="SWType">
                                            <xs:sequence>
                                        <xs:element name="DenominazioneSistema" type="xs:string" />
                                            </xs:sequence>
                                        </xs:complexType>

<xs:complexType name="ChiaveDescrittivaType">
<xs:sequence>
<xs:element name="Oggetto" type="xs:string" />
<xs:element name="ParoleChiave" type="xs:string" minOccurs="0" maxOccurs="5" />
</xs:sequence>
</xs:complexType>

<xs:complexType name="AllegatiType">
<xs:sequence>
<xs:element name="NumeroAllegati" type="NumeroAllegatiType" />
<xs:element name="IndiceAllegati" type="IndiceAllegatiType" minOccurs="0" maxOccurs="9999" />
</xs:sequence>
</xs:complexType>

<xs:simpleType name="NumeroAllegatiType">
<xs:restriction base="xs:integer">
```

```
<xs:minInclusive value="0"/>
<xs:maxInclusive value="9999"/>
</xs:restriction>
</xs:simpleType>

<xs:complexType name="IndiceAllegatiType">
<xs:sequence>
<xs:element name="IdDoc" type="IdDocType" />
<xs:element name="Descrizione" type="xs:string" />
</xs:sequence>
</xs:complexType>

<xs:complexType name="ClassificazioneType">
<xs:sequence>
<xs:element name="IndiceDiClassificazione" type="xs:string"  minOccurs="0" />
<xs:element name="Descrizione" type="xs:string"  minOccurs="0" />
<xs:element name="PianoDiClassificazione" type="xs:string" minOccurs="0" />
</xs:sequence>
</xs:complexType>

<xs:complexType name="IdentificativoDelFormatoType">
<xs:sequence>
<xs:element name="Formato" type="xs:string" />
<xs:element name="ProdottoSoftware" type="ProdottoSoftwareType" minOccurs="0"/>
</xs:sequence>
</xs:complexType>

<xs:complexType name="ProdottoSoftwareType">
<xs:sequence>
<xs:element name="NomeProdotto" type="xs:string" minOccurs="0" />
```

```
<xs:element name="VersioneProdotto" type="xs:string" minOccurs="0" />
<xs:element name="Produttore" type="xs:string" minOccurs="0" />
</xs:sequence>
</xs:complexType>

<xs:complexType name="VerificaType">
<xs:sequence>
<xs:element name="FirmatoDigitalmente" type="xs:boolean" />
<xs:element name="SigillatoElettronicamente" type="xs:boolean" />
<xs:element name="MarcaturaTemporale" type="xs:boolean" />
<xs:element name="ConformitaCopieImmagineSuSupportoInformatico" type="xs:boolean" />
</xs:sequence>
</xs:complexType>

<xs:complexType name="AggType">
<xs:sequence>
<xs:element name="TipoAgg" type="IdAggType" minOccurs="0" maxOccurs="unbounded"/>
</xs:sequence>
</xs:complexType>

<xs:complexType name="IdAggType">
<xs:sequence>
<xs:element name="TipoAggregazione" type="TipoAggregazioneType"/>
<xs:element name="IdAggregazione" type="xs:string" />
</xs:sequence>
</xs:complexType>

<xs:simpleType name="TipoAggregazioneType">
<xs:restriction base="xs:string">
<xs:enumeration value="Fascicolo"/>
```

```
<xs:enumeration value="Serie Documentale"/>
<xs:enumeration value="Serie Di Fascicoli"/>
</xs:restriction>
</xs:simpleType>

<xs:complexType name="TracciatureModificheDocumentoType">
<xs:sequence>
<xs:element name="TipoModifica" type="TipoModificaType"/>
<xs:element name="SoggettoAutoreDellaModifica" type="PFType" />
<xs:element name="DataModifica" type="xs:date"/>
<xs:element name="OraModifica" type="xs:time" minOccurs="0"/>
<xs:element name="IdDocVersionePrecedente" type="IdDocType"/>
</xs:sequence>
</xs:complexType>

<xs:simpleType name="TipoModificaType">
<xs:restriction base="xs:string">
<xs:enumeration value="Annullamento"/>
<xs:enumeration value="Rettifica"/>
<xs:enumeration value="Integrazione"/>
<xs:enumeration value="Annotazione"/>
</xs:restriction>
</xs:simpleType>

<xs:simpleType name="CFType">
<xs:restriction base="xs:string" >
<xs:pattern                                                                    value="[A-Z]{6}[0-9LMNPQRSTUV]{2}[ABCDEHLMPRST][0-
9LMNPQRSTUV]{2}[A-Z][0-9LMNPQRSTUV]{3}[A-Z]"/>
</xs:restriction>
</xs:simpleType>
```

```
                <xs:simpleType name="PIType">
                        <xs:restriction base="xs:string">
                                <xs:pattern value="\d{11}"/>
                        </xs:restriction>
                                </xs:simpleType>

<xs:simpleType name="TempoDiConservazioneType">
<xs:restriction base="xs:integer">
<xs:minInclusive value="1"/>
<xs:maxInclusive value="9999"/>
</xs:restriction>
</xs:simpleType>
</xs:schema>
```

3. METADATI DEL DOCUMENTO AMMINISTRATIVO INFORMATICO

Definizione del metadato IdDoc (element xsd: IdDoc)

Identificativo univoco e persistente associato in modo univoco e permanente al documento amministrativo informatico in modo da consentirne l'identificazione. Inoltre, rappresenta le informazioni necessarie per verificare l'integrità del documento. Il metadato è costituito dai campi:

- Impronta crittografica del documento: a sua volta suddiviso in:

o Impronta: sottocampo in cui viene memorizzato l'hash del documento

o Algoritmo: sottocampo nel quale deve essere indicata la tipologia dell'algoritmo applicato secondo quanto riportato nell'Allegato 6 delleLinee Guida nella tabella 1 del paragrafo 2.2 "Regole di processamento"

- Identificativo: come da sistema di identificazione formalmente definito
- Segnatura: segnatura di protocollo, da indicare obbligatoriamente nel caso di documento amministrativo protocollato, a sua volta strutturato come da Allegato 6 delle Linee Guida.

Campi	Sottocampi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
Impronta crittografica del documento					
	Impronta	Rappresenta l'hash del documento	Binary	SI	NO, ridefinito.
	Algoritmo	Rappresenta l'algoritmo applicato Default = SHA-256	Alfanumerico	SI	SI
Identificativo		Come da sistema di identificazione formalmente definito	Alfanumerico	SI	
Segnatura		Segnatura del protocollo	Alfanumerico	SI, nel caso di documento protocollato	

Definizione del metadato Modalità di formazione (element xsd: ModalitaDiFormazione)

Indica la modalità di generazione del documento amministrativo informatico. Sono

previste le seguenti modalità secondo quanto riportato nelle Linee guida:

a) creazione tramite l'utilizzo di strumenti software che assicurino la produzione di documenti nei formati previsti dalle Linee Guida;

b) acquisizione di un documento informatico per via telematica o su supporto informatico, acquisizione della copia per immagine su supporto informatico di un documento analogico, acquisizione della copia informatica di un documento analogico;

c) memorizzazione su supporto informatico in formato digitale delle informazioni risultanti da transazioni o processi informatici o dalla presentazione telematica di dati attraverso moduli o formulari resi disponibili all'utente;

d) generazione o raggruppamento anche in via automatica di un insieme di dati o registrazioni, provenienti da una o più banche dati, anche appartenenti a più soggetti interoperanti, secondo una struttura logica predeterminata e memorizzata in forma statica.

Campi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
NON Applicabile	Indicare a) creazione tramite l'utilizzo di strumenti software che assicurino la produzione di documenti nei formati previsti nell'Allegato 2 delle Linee; b) acquisizione di un documento informatico per via telematica o su supporto informatico, acquisizione della copia per immagine su supporto informatico di un documento analogico, acquisizione della copia informatica di un documento analogico; c) memorizzazione su supporto informatico in formato digitale delle informazioni risultanti da transazioni o processi informatici o dalla presentazione telematica di dati attraverso moduli o formulari resi disponibili all'utente; d) generazione o raggruppamento anche in via automatica di un insieme di dati o registrazioni, provenienti da una o più banche dati, anche appartenenti a più soggetti interoperanti, secondo una struttura logica predeterminata e memorizzata in forma statica	Alfanumerico	SI	SI

Definizione del metadato Tipologia documentale (element xsd: TipologiaDocumentale)

Metadato funzionale che indica la tipologia del documento tra quelle trattate per lo svolgimento delle attività.

Campi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
NON Applicabile	Metadato testuale libero per indicare le tipologie documentali trattate (ad esempio, fatture, delibere, determine, etc)	Alfanumerico	SI	SI

Definizione del metadato Dati di registrazione (element xsd: DatiDiRegistrazione)

Metadato che comprende i dati di registrazione del documento sia nel caso di documento protocollato che non protocollato.

Sono previsti i seguenti campi:

- Tipologia di flusso: indica se si tratta di un documento in uscita, in entrata o interno. Per documento interno si intende un documento scambiato tra le diverse UOR afferenti alla stessa AOO
- Tipo registro: indica il sistema di registrazione adottato: protocollo ordinario/protocollo emergenza, o Repertorio/Registro.
- Data: è la data associata al documento all'atto della registrazione
- Numero documento: Numero identificativo del documento nel caso di documento non protocollato (ad esempio, numero fattura), numero di protocollo nel caso di documento protocollato.
- Codice Registro: Identificativo del registro in cui il documento viene registrato.

Campi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
Tipologia di flusso	• "U" = In uscita • "E" = In entrata • "I" = Interno Per documenti interni si intende i documenti scambiati all'interno della medesima AOO	Alfanumerico	SI	SI
Tipo registro	• Protocollo Ordinario /Protocollo Emergenza • Repertorio/Registro	Alfanumerico	SI	SI
Data registrazione	nel caso di documento non protocollato: • Data di registrazione del Documento/Ora di registrazione del Documento nel caso di documento protocollato: • Data di registrazione di protocollo/Ora di protocollazione del Documento	Date/Time	SI	NO, ma ridefinito

Campi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
Numero Documento	nel caso di documento non protocollato: • Numero di registrazione del documento nel caso di documento protocollato: • Numero di protocollo	Alfanumerico	SI	NO, ma ridefinito
Codice Registro	Codice identificativo del registro in cui il documento viene registrato.	Alfanumerico	SI	SI

Definizione del metadato Soggetti (element xsd: Soggetti)

Indica il metadato che consente di individuare le informazioni relative a tutti i Soggetti coinvolti e competenti sul documento a vario titolo e definiti dal campo Ruolo. Sono definiti quindi i seguenti attributi:

- Ruolo: consente di indicare, a seconda delle necessità, l'autore del documento, il mittente, il destinatario, l'assegnatario. Al fine di renderei dati di registrazione univoci deve essere sempre indicata l'Amministrazione che effettua la registrazione del documento. Obbligatorio inoltre indicare almeno l'autore o il mittente. Nel caso di documento protocollato deve essere obbligatoriamente indicato il mittente. Per "Operatore" si intende il soggetto autorizzato ad apportare modifiche/integrazioni al documento, la cui definizione si renderà obbligatoria nel caso in cui venga compilato il metadato "Tracciature modifiche documento". Nel caso di ruolo Assegnatario si prevede l'indicazione della UOR di riferimento con l'indicazione, a completamento, della persona fisica. Nel caso di ruolo RUP le informazioni relative alla persona fisica e alla UOR di appartenenza diventano obbligatorie.
- Tipo soggetto: consente di tipizzare i soggetti come persone fisiche, giuridiche, amministrazioni pubbliche (italiane ed estere). Il Tipo Soggetto = SW è indicabile solo se si è indicato il ruolo = "Produttore". Per ogni Tipo Soggetto sono indicati i metadati di riferimento.

Il metadato ha una struttura ricorsiva.

Campi	Sottocampi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
Ruolo		• Amministrazione che effettua la registrazione • Assegnatario • Autore • Destinatario • Mittente • Operatore • Produttore • RGD (Responsabile della Gestione Documentale) • RSP (Responsabile del Servizio di Protocollo) • RUP	Alfanumerico	SI, al fine di rendere i dati di registrazione univoci deve essere sempre indicata l'Amministrazione che effettua la registrazione del documento. Obbligatorio indicare inoltre almeno l'autore o il mittente. Nel caso di documento protocollato deve essere obbligatoriamente indicato il mittente. Per "Operatore" si intende il	NO ma ridefinito

Campi	Sottocampi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
				soggetto autorizzato ad apportare modifiche/integrazioni al documento, la cui definizione si renderà obbligatoria nel caso in cui venga compilato il metadato “Tracciature modifiche documento”. Nel caso di ruolo Assegnatario si prevede l’indicazione sia della persona fisica che, a complemento o in alternativa, della relativa UOR di riferimento. Nel caso di ruolo = RUP le informazioni relative alla persona fisica e alla UOR di appartenenza diventano obbligatorie.	
Tipo soggetto		Se Ruolo = Assegnatario ✓ AS Se Ruolo = Amministrazione che effettua la registrazione ✓ PAI per le Amministrazioni Pubbliche italiane Se Ruolo = Mittente o Destinatario ✓ PF per Persona Fisica ✓ PG per Organizzazione ✓ PAI per le Amministrazioni Pubbliche Italiane	Alfanumerico	SI	SI

Campi	Sottocampi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
		✓ PAE per le Amministrazioni Pubbliche Estere Se Ruolo = Autore ✓ PF per Persona Fisica ✓ PG per Organizzazione (valido solo nei flussi in entrata) ✓ PAI per le Amministrazioni Pubbliche italiane ✓ PAE per le Amministrazioni Pubbliche Estere (valido solo nei flussi in entrata) Se Operatore o Responsabile della Gestione Documentale o Responsabile del Servizio Protocollo ✓ PF per Persona Fisica Se Ruolo = RUP ✓ RUP Se Ruolo = Produttore ✓ SW per i documenti prodotti automaticamente			
	PF	Cognome	Alfanumerico	SI	SI
		Nome	Alfanumerico	SI	
		Codice Fiscale	Alfanumerico	NO	
		Denominazione Amministrazione\ Codice IPA	Alfanumerico	Obbligatorio solo se si è indicato l'AOO o l'UOR	
		Denominazione Amministrazione AOO \ Codice IPA AOO	Alfanumerico	Obbligatorio solo se si è indicato l'Amministrazione o l'UOR	
		Denominazione Amministrazione UOR \ Codice IPA UOR	Alfanumerico	NO	

Campi	Sottocampi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
		Indirizzi Digitali Di Riferimento	Alfanumerico	NO	
	PG	Denominazione Organizzazione	Alfanumerico	SI	SI
		Codice fiscale\Partita Iva	Alfanumerico	NO	
		Denominazione Ufficio	Alfanumerico	NO	
		Indirizzi Digitali Di Riferimento	Alfanumerico	NO	
	PAI	Denominazione Amministrazione\ Codice IPA	Alfanumerico	SI	SI
		Denominazione Amministrazione AOO \ Codice IPA AOO	Alfanumerico	SI	
		Denominazione Amministrazione UOR \ Codice IPA UOR	Alfanumerico	NO	
		Indirizzi Digitali Di Riferimento	Alfanumerico	SI	
	PAE	Denominazione Amministrazione	Alfanumerico	SI	SI
		Denominazione Ufficio	Alfanumerico	NO	
		Indirizzi Digitali Di Riferimento	Alfanumerico	SI	
	AS	Cognome	Alfanumerico	NO	SI
		Nome	Alfanumerico	NO	
		Codice Fiscale	Alfanumerico	NO	
		Denominazione Amministrazione\ Codice IPA	Alfanumerico	SI	
		Denominazione Amministrazione AOO \ Codice IPA AOO	Alfanumerico	SI	
		Denominazione Amministrazione UOR \ Codice IPA UOR	Alfanumerico	SI	

Campi	Sottocampi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
		Indirizzi Digitali Di Riferimento	Alfanumerico	SI	
	RUP	Cognome	Alfanumerico	SI	SI
		Nome	Alfanumerico	SI	
		Codice Fiscale	Alfanumerico	NO	
		Denominazione Amministrazione\ Codice IPA	Alfanumerico	SI	
		Denominazione Amministrazione AOO \ Codice IPA AOO	Alfanumerico	SI	
		Denominazione Amministrazione UOR \ Codice IPA UOR	Alfanumerico	SI	
		Indirizzi Digitali Di Riferimento	Alfanumerico	SI	
	SW	Denominazione Sistema	Alfanumerico	SI	SI

Definizione del metadato Chiave descrittiva (element xsd: ChiaveDescrittiva)

Metadato funzionale volto a riassumere il contenuto del documento o comunque a chiarirne la natura. È costituito da seguenti campi:

- Oggetto: testo libero;
- Parole Chiave: da compilare facoltativamente attingendo da thesauri o da vocabolari controllati, per evitare ambiguità terminologiche e avere la possibilità di utilizzare il metadato come chiave di ricerca del documento. Il metadato è ricorsivo fino ad un massimo di 5 occorrenze.

Campi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
Oggetto	Testo libero	Alfanumerico	SI	SI
Parole chiave	Testo libero	Alfanumerico	NO	SI

Definizione del metadato Allegati (element xsd: Allegati)

Indica il numero di allegati al documento e, nell'eventualità che il numero di allegati indicati sia maggiore di zero, devono essere compilati, in modalità ricorsiva, i dati:

- IdDoc: Identificativo del documento relativo all'allegato
- Descrizione: Titolo dell'allegato

Campi	Sottocampi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
Numero allegati		Inserire un numero intero compreso tra 0 e 9999	Numerico	SI	SI
Indice allegati		Da indicare per ogni allegato se Numero allegati > 0			
	IdDoc	Identificativo del documento relativo all'allegato		SI, se numero allegati > 0	SI
	Descrizione	Testo libero	Alfanumerico	SI, se numero allegati > 0	SI

Definizione del metadato Classificazione (element xsd: Classificazione)

Classificazione del documento secondo il Piano di classificazione utilizzato, da indicare sia nel caso di documento protocollato che nel caso di documento non protocollato:

- Indice di classificazione: Codifica del documento secondo il Piano di classificazione utilizzato
- Descrizione: Descrizione per esteso dell'Indice di classificazione indicato.
- Piano di classificazione: riportare l'URI di pubblicazione del Piano di classificazione

Campi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
Indice di classificazione	Codifica del documento secondo il Piano di classificazione utilizzato	Alfanumerico	SI	SI
Descrizione	Descrizione per esteso dell'Indice di classificazione indicato.	Alfanumerico	SI	SI
Piano di classificazione	URI del Piano di classificazione pubblicato	Alfanumerico	NO	SI

Definizione del metadato Riservato (element xsd: Riservato)

Rappresenta il livello di sicurezza di accesso al documento:

- Vero: se il documento è considerato riservato
- Falso: se il documento non è considerato riservato

Consente di gestire gli accessi al documento al solo personale autorizzato.

Campi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
NON Applicabile	• Vero: se il documento è considerato riservato • Falso: se il documento non è considerato riservato	Boolean	SI	SI

Definizione del metadato Identificativo del formato (element xsd: IdentificativoDelFormato)

Indica il formato del documento e la versione del software utilizzato per la creazione del documento stesso. É costituito dai seguenti campi:

- Formato: secondo quanto previsto dalle Linee Guida.
- Prodotto software: Prodotto software utilizzato per la creazione del documento e relativa versione, suddiviso a sua volta in tre sottocampi:
  - Nome prodotto
  - Versione prodotto
  - Produttore

Campi	Sottocampi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
Formato		Previsti dall'Allegato 2 delle Linee guida	Alfanumerico	SI	SI
Prodotto software		Prodotto software utilizzato per la creazione del documento e relativa versione			SI
	Nome prodotto		Alfanumerico	SI, quando rilevabile	SI
	Versione prodotto		Alfanumerico	SI, quando rilevabile	SI
	Produttore		Alfanumerico	SI, quando rilevabile	SI

Definizione del metadato Verifica (element xsd: Verifica)

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

Campi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
Firmato Digitalmente	• Vero • Falso	Boolean	SI, obbligatorio nel caso di modalità di formazione doc = a/b	SI
Sigillato Elettronicamente	• Vero • Falso	Boolean	SI, obbligatorio nel caso di modalità di formazione doc = a/b	SI
Marcatura Temporale	• Vero • Falso	Boolean	SI, obbligatorio nel caso di modalità di formazione doc = a/b	SI
Conformità copie immagine su supporto informatico	• Vero • Falso	Boolean	SI, obbligatorio nel caso di modalità di formazione doc = b	SI

Definizione del metadato Identificativo dell'Aggregazione documentale (element xsd: Agg)

Identificativo univoco dell'Aggregazione come definito nel successivo paragrafo dei METADATI DELLE AGGREGAZIONI DOCUMENTALI INFORMATICHE. Metadato ricorsivo.

Campi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
NON Applicabile	Identificativo del fascicolo o della serie come definito nel successivo paragrafo dei METADATI DELLE AGGREGAZIONI DOCUMENTALI INFORMATICHE.	Alfanumerico	SI	SI

Definizione del metadato Identificativo del Documento Primario (element xsd: IdIdentificativoDocumentoPrimario)

Identificativo univoco e persistente del Documento primario.

Campi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
NON Applicabile	IdDoc del documento primario		SI, nel caso in cui sia presente un documento primario	SI

Definizione del metadato Nome del documento\file (element xsd: NomeDelDocumento)

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

Campi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
NON Applicabile		Alfanumerico	SI	SI

Definizione del metadato Versione del documento (element xsd: VersioneDelDocumento)

Versione del documento

Campi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
NON Applicabile	Indicare la versione del documento	Alfanumerico	SI	SI

Definizione del metadato Tracciature modifiche documento (element xsd: TracciatureModificheDocumento)

Metadato volto a tracciare la presenza di operazioni di modifica effettuate sul documento e la data in cui esse sono state effettuate. L'autore delle modifiche è tracciato nel metadato "Soggetti" con il ruolo "Operatore".

Campi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
Tipo modifica	• Annullamento • Rettifica • Integrazione • Annotazione	Alfanumerico	SI, nel caso di versione > 1 o in caso di annullamento	SI
Soggetto autore della modifica	Come da ruolo = Operatore definito nel metadato Soggetti	Alfanumerico	SI, nel caso di versione > 1 o in caso di annullamento	SI
Data modifica/Ora modifica		Date/Time	SI, nel caso di versione > 1 o in caso di annullamento	SI
IdDoc versione precedente	Identificativo documento versione precedente		SI, nel caso di versione > 1 o in caso di annullamento	SI

Definizione del metadato Tempo di conservazione (element xsd: TempoDiConservazione)

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

Campi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
NON Applicabile	Indicare il numero di anni come da Piano di classificazione; indicare 9999 per un tempo di conservazione perenne	Numerico	NO	SI

Definizione del metadato Note (element xsd: Note)

Eventuali indicazioni aggiuntive utili ad indicare situazioni particolari.

Campi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
NON Applicabile	Testo Libero	Alfanumerico	NO	SI

XSD METADATI DEL DOCUMENTO AMMINISTRATIVO INFORMATICO

Schema xsd:

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" elementFormDefault="qualified">
<xs:element name="DocumentoAmministrativoInformatico" type="DocumentoAmministrativoInformaticoType"/>
<xs:complexType name="DocumentoAmministrativoInformaticoType">
<xs:sequence>
<xs:element name="IdDoc" type="IdDocType"/>
<xs:element name="ModalitaDiFormazione" type="ModalitaDiFormazioneType"/>
<xs:element name="TipologiaDocumentale" type="xs:string" />
<xs:element name="DatiDiRegistrazione" type="DatiDiRegistrazioneType"/>
<xs:element name="Soggetti" type="SoggettiType"/>
<xs:element name="ChiaveDescrittiva" type="ChiaveDescrittivaType"/>
<xs:element name="Allegati" type="AllegatiType"/>
<xs:element name="Classificazione" type="ClassificazioneType"/>
<xs:element name="Riservato" type="xs:boolean" />
<xs:element name="IdentificativoDelFormato" type="IdentificativoDelFormatoType"/>
<xs:element name="Verifica" type="VerificaType"/>
<xs:element name="Agg" type="AggType"/>
<xs:element name="IdIdentificativoDocumentoPrimario" type="IdDocType" minOccurs="0"/>
<xs:element name="NomeDelDocumento" type="xs:string" />
<xs:element name="VersioneDelDocumento" type="xs:string" />
<xs:element                                                    name="TracciatureModificheDocumento"      type="TracciatureModificheDocumentoType"
minOccurs="0" />
                        <xs:element name="TempoDiConservazione" type="TempoDiConservazioneType" minOccurs="0"/>
                        <xs:element name="Note" type="xs:string" minOccurs="0" />
                        </xs:sequence>
```

```
</xs:complexType>
<xs:complexType name="IdDocType">
<xs:sequence>
<xs:element name="ImprontaCrittograficaDelDocumento" type="ImprontaCrittograficaDelDocumentoType" />
<xs:element name="Identificativo" type="xs:string" />
<xs:element name="Segnatura" type="xs:string" minOccurs="0" />
</xs:sequence>
</xs:complexType>
<xs:complexType name="ImprontaCrittograficaDelDocumentoType">
<xs:sequence>
<xs:element name="Impronta" type="xs:base64Binary" />
<xs:element name="Algoritmo" type="xs:string" default="SHA-256"/>
</xs:sequence>
</xs:complexType>
<xs:simpleType name="ModalitaDiFormazioneType">
<xs:restriction base="xs:string">
<xs:enumeration value="creazione tramite utilizzo di strumenti software che assicurino la produzione di documentinei formati previsti in allegato 2"/>
<xs:enumeration value="acquisizione di un documento informatico per via telematica o su supporto informatico, acquisizione della copia per immagine su supporto informatico di un documento analogico, acquisizione della copia informatica di un documentoanalogico"/>
<xs:enumeration value="memorizzazione su supporto informatico in formato digitale delle informazioni risultanti datransazioni o processi informatici o dalla presentazione telematica di dati attraverso moduli o formulari resi disponibili ad utente"/>
<xs:enumeration value="generazione o raggruppamento anche in via automatica di un insieme di dati o registrazioni, provenienti da una o più banche dati, anche appartenenti a più soggetti interoperanti, secondo una struttura logica predeterminatae memorizzata in forma statica"/>
</xs:restriction>
</xs:simpleType>
<xs:complexType name="DatiDiRegistrazioneType">
<xs:sequence>
```

```
<xs:element name="TipologiaDiFlusso" type="TipologiaDiFlussoType"/>
<xs:element name="TipoRegistro" type="TipoRegistroType"/>
</xs:sequence>
</xs:complexType>
                                    <xs:simpleType name="TipologiaDiFlussoType">
                                    <xs:restriction base="xs:string">
                                    <xs:enumeration value="E"/>
                                    <xs:enumeration value="U"/>
                                    <xs:enumeration value="I"/>
                                    </xs:restriction>
                                    </xs:simpleType>
                                    <xs:complexType name="TipoRegistroType">
                                    <xs:sequence>
                                    <xs:choice>
                                    <xs:element                                                    name="ProtocolloOrdinario_ProtocolloEmergenza"
type="ProtocolloType"/>
                                    <xs:element name="Repertorio_Registro" type="NoProtocolloType"/>
                                    </xs:choice>
                                    </xs:sequence>
                                    </xs:complexType>
                                    <xs:complexType name="ProtocolloType">
                                    <xs:sequence>
                                    <xs:element                                name="TipoRegistro"          type="xs:string"          fixed          =
'ProtocolloOrdinario\ProtocolloEmergenza'/>
                                                <xs:element name="DataProtocollazioneDocumento" type="xs:date"/>
                                                <xs:element                        name="OraProtocollazioneDocumento"        type="xs:time"
minOccurs="0"/>
                                                <xs:element name="NumeroProtocolloDocumento" type="NumProtType"/>
                                                <xs:element name="CodiceRegistro" type="CodiceRegistroType"/>
                                                </xs:sequence>
```

```
                                        </xs:complexType>
                                        <xs:complexType name="NoProtocolloType">
                                        <xs:sequence>
                                        <xs:element name="TipoRegistro" type="xs:string" fixed = 'Repertorio\Registro'/>
                                        <xs:element name="DataRegistrazioneDocumento" type="xs:date"/>
                                        <xs:element                                    name="OraRegistrazioneDocumento"        type="xs:time"
minOccurs="0"/>
                                        <xs:element name="NumeroRegistrazioneDocumento" type="xs:string"/>
                                        <xs:element name="CodiceRegistro" type="CodiceRegistroType"/>
                                        </xs:sequence>
                                        </xs:complexType>
                                        <xs:simpleType name="NumProtType">
                                        <xs:restriction base="xs:string">
                                        <xs:pattern value="[0-9]{7,}"/>
                                                    </xs:restriction>
                                                </xs:simpleType>
                                <xs:simpleType name="CodiceRegistroType">
                                            <xs:restriction base="xs:string">
                                        <xs:pattern value="[A-Za-z0-9_\.\-]{1,16}"/>
                                            </xs:restriction>
                                </xs:simpleType>

<xs:complexType name="SoggettiType">
<xs:sequence>
<xs:element name="Ruolo" type="RuoloType" minOccurs="1" maxOccurs="unbounded"/>
</xs:sequence>
</xs:complexType>

<xs:complexType name="RuoloType">
<xs:choice>
```

```
<xs:element name="AmministrazioneCheEffettuaLaRegistrazione" type="TipoSoggetto1Type"/>
<xs:element name="Assegnatario" type="TipoSoggetto2Type"/>
<xs:element name="Destinatario" type="TipoSoggetto31Type"/>
<xs:element name="Mittente"                                    type="TipoSoggetto32Type"/>
<xs:element name="Autore" type="TipoSoggetto41Type"/>
<xs:element name="Operatore" type="TipoSoggetto42Type"/>
<xs:element name="ResponsabileGestioneDocumentale" type="TipoSoggetto43Type"/>
<xs:element name="ResponsabileServizioProtocollo" type="TipoSoggetto44Type"/>
<xs:element name="Produttore" type="TipoSoggetto5Type"/>
<xs:element name="RUP" type="TipoSoggetto6Type"/>
                                                </xs:choice>
                                            </xs:complexType>

                                        <xs:complexType name="TipoSoggetto1Type">
                                        <xs:sequence>
                                        <xs:element name="TipoRuolo" type="xs:string" fixed = 'Amministrazione Che Effettua
La Registrazione'/>
                                        <xs:element name="PAI" type="PAIType"/>
                                        </xs:sequence>
                                        </xs:complexType>

                                        <xs:complexType name="TipoSoggetto2Type">
                                        <xs:sequence>
                                        <xs:element name="TipoRuolo" type="xs:string" fixed = 'Assegnatario'/>
                                        <xs:element name="AS" type="ASType"/>
                                        </xs:sequence>
                                        </xs:complexType>

                                        <xs:complexType name="TipoSoggetto31Type">
                                        <xs:sequence>
```

```
<xs:element name="TipoRuolo" type="xs:string" fixed = 'Destinatario'/>
<xs:choice>
<xs:element name="PF" type="PFType"/>
<xs:element name="PG" type="PGType"/>
<xs:element name="PAI" type="PAIType"/>
<xs:element name="PAE" type="PAEType"/>
</xs:choice>
</xs:sequence>
</xs:complexType>

<xs:complexType name="TipoSoggetto32Type">
<xs:sequence>
<xs:element name="TipoRuolo" type="xs:string" fixed = 'Mittente'/>
<xs:choice>
<xs:element name="PF" type="PFType"/>
<xs:element name="PG" type="PGType"/>
<xs:element name="PAI" type="PAIType"/>
<xs:element name="PAE" type="PAEType"/>
</xs:choice>
</xs:sequence>
</xs:complexType>

<xs:complexType name="TipoSoggetto41Type">
<xs:sequence>
<xs:element name="TipoRuolo" type="xs:string" fixed = 'Autore'/>
<xs:choice>
<xs:element name="PF" type="PFType"/>
<xs:element name="PG" type="PGType"/>
<xs:element name="PAI" type="PAIType"/>
<xs:element name="PAE" type="PAEType"/>
```

```
                                                    </xs:choice>
                                                  </xs:sequence>
                                  </xs:complexType>

<xs:complexType name="TipoSoggetto42Type">
<xs:sequence>
<xs:element name="TipoRuolo" type="xs:string" fixed = 'Operatore'/>
<xs:element name="PF" type="PFType"/>
                                                  </xs:sequence>
                                              </xs:complexType>

                                              <xs:complexType name="TipoSoggetto43Type">
                                              <xs:sequence>
                                              <xs:element name="TipoRuolo" type="xs:string" fixed = 'Responsabile della Gestione
Documentale'/>
                                              <xs:element name="PF" type="PFType"/>
                                              </xs:sequence>
                                              </xs:complexType>

                                              <xs:complexType name="TipoSoggetto44Type">
                                              <xs:sequence>
                                              <xs:element name="TipoRuolo" type="xs:string" fixed = 'Responsabile del Servizio di
Protocollo'/>
                                              <xs:element name="PF" type="PFType"/>
                                              </xs:sequence>
                                              </xs:complexType>



                                              <xs:complexType name="TipoSoggetto5Type">
                                              <xs:sequence>
```

```
<xs:element name="TipoRuolo" type="xs:string" fixed = 'Produttore'/>
<xs:element name="SW" type="SWType"/>
</xs:sequence>
</xs:complexType>

<xs:complexType name="TipoSoggetto6Type">
<xs:sequence>
<xs:element name="TipoRuolo" type="xs:string" fixed = 'RUP'/>
<xs:element name="RUP" type="RUPType"/>
</xs:sequence>
</xs:complexType>

<xs:complexType name="ASType" >
<xs:sequence>
<xs:element name="Cognome" type="xs:string" minOccurs="0"/>
<xs:element name="Nome" type="xs:string" minOccurs="0" />
<xs:element name="CodiceFiscale" type="CFType" minOccurs="0"/>
<xs:element name="IPAAmm" type="CodiceIPAType" />
<xs:element name="IPAAOO" type="CodiceIPAType" />
<xs:element name="IPAUOR" type="CodiceIPAType" />
<xs:element name="IndirizziDigitaliDiRiferimento" type="xs:string" minOccurs="1" maxOccurs="unbounded"/>
</xs:sequence>
</xs:complexType>

<xs:complexType name="RUPType" >
<xs:sequence>
<xs:element name="Cognome" type="xs:string" />
<xs:element name="Nome" type="xs:string" />
<xs:element name="CodiceFiscale" type="CFType" minOccurs="0"/>
<xs:element name="IPAAmm" type="CodiceIPAType" />
```

```
                                        <xs:element name="IPAAOO" type="CodiceIPAType"  />
                                        <xs:element name="IPAUOR" type="CodiceIPAType" />
                                        <xs:element                    name="IndirizziDigitaliDiRiferimento"       type="xs:string"
minOccurs="1"    maxOccurs="unbounded"/>
                                        </xs:sequence>
                                        </xs:complexType>

                                        <xs:complexType name="PFType" >
                                        <xs:sequence>
                                        <xs:element name="Cognome" type="xs:string" />
                                        <xs:element name="Nome" type="xs:string" />
                                        <xs:element name="CodiceFiscale" type="CFType" minOccurs="0"/>
                                        <xs:element name="IPAAmm" type="CodiceIPAType" minOccurs="0"/>
                                        <xs:element name="IPAAOO" type="CodiceIPAType" minOccurs="0" />
                                        <xs:element name="IPAUOR" type="CodiceIPAType" minOccurs="0"/>
                                        <xs:element                    name="IndirizziDigitaliDiRiferimento"       type="xs:string"
minOccurs="0"    maxOccurs="unbounded"/>
                                        </xs:sequence>
                                        </xs:complexType>

                                        <xs:complexType name="PGType">
                                        <xs:sequence>
                                        <xs:element name="DenominazioneOrganizzazione" type="xs:string"
/> minOccurs="0"/>
                                        <xs:element                              name="CodiceFiscale_PartitaIva"      type="PIType"
minOccurs="0" />
                                        <xs:element                              name="DenominazioneUfficio"      type="xs:string"
minOccurs="0" maxOccurs="unbounded"/>
                                        <xs:element  name="IndirizziDigitaliDiRiferimento"  type="xs:string"

                                        </xs:sequence>
```

```
                                        </xs:complexType>

                                        <xs:complexType name="PAIType" >
                                        <xs:sequence>
                                        <xs:element name="IPAAmm" type="CodiceIPAType" />
                                        <xs:element name="IPAAOO" type="CodiceIPAType" />
                                        <xs:element                    name="IPAUOR"          type="CodiceIPAType"
minOccurs="0"/>
                                        <xs:element  name="IndirizziDigitaliDiRiferimento"  type="xs:string"
minOccurs="1" maxOccurs="unbounded"/>
                                        </xs:sequence>
                                        </xs:complexType>

                                        <xs:complexType name="PAEType" >
                                        <xs:sequence>
                                                <xs:element                name="DenominazioneAmministrazione"
type="xs:string"/>
                                                <xs:element      name="DenominazioneUfficio"      type="xs:string"
minOccurs="0"/>
                                         <xs:element    name="IndirizziDigitaliDiRiferimento"    type="xs:string"    minOccurs="1"
maxOccurs="unbounded"/>
                                    </xs:sequence>
</xs:complexType>


<xs:complexType name="CodiceIPAType" >
<xs:sequence>
<xs:element name="Denominazione" type="xs:string" />
<xs:element name="CodiceIPA" type="xs:string" />
</xs:sequence>
</xs:complexType>
```

```
                                        <xs:complexType name="SWType">
                                            <xs:sequence>
                                        <xs:element name="DenominazioneSistema" type="xs:string" />
                                            </xs:sequence>
                                        </xs:complexType>


<xs:complexType name="ChiaveDescrittivaType">
<xs:sequence>
<xs:element name="Oggetto" type="xs:string" />
<xs:element name="ParoleChiave" type="xs:string" minOccurs="0" maxOccurs="5" />
</xs:sequence>
</xs:complexType>

<xs:complexType name="AllegatiType">
<xs:sequence>
<xs:element name="NumeroAllegati" type="NumeroAllegatiType" />
<xs:element name="IndiceAllegati" type="IndiceAllegatiType" minOccurs="0" maxOccurs="9999" />
</xs:sequence>
</xs:complexType>

<xs:simpleType name="NumeroAllegatiType">
<xs:restriction base="xs:integer">
<xs:minInclusive value="0"/>
<xs:maxInclusive value="9999"/>
</xs:restriction>
</xs:simpleType>

<xs:complexType name="IndiceAllegatiType">
```

```
<xs:sequence>
<xs:element name="IdDoc" type="IdDocType" />
<xs:element name="Descrizione" type="xs:string" />
</xs:sequence>
</xs:complexType>

<xs:complexType name="ClassificazioneType">
<xs:sequence>
<xs:element name="IndiceDiClassificazione" type="xs:string" />
<xs:element name="Descrizione" type="xs:string" />
<xs:element name="PianoDiClassificazione" type="xs:string" minOccurs="0" />
</xs:sequence>
</xs:complexType>

<xs:complexType name="IdentificativoDelFormatoType">
<xs:sequence>
<xs:element name="Formato" type="xs:string" />
<xs:element name="ProdottoSoftware" type="ProdottoSoftwareType" minOccurs="0"/>
</xs:sequence>
</xs:complexType>

<xs:complexType name="ProdottoSoftwareType">
<xs:sequence>
<xs:element name="NomeProdotto" type="xs:string" minOccurs="0" />
<xs:element name="VersioneProdotto" type="xs:string" minOccurs="0" />
<xs:element name="Produttore" type="xs:string" minOccurs="0" />
</xs:sequence>
</xs:complexType>

<xs:complexType name="VerificaType">
```

```
<xs:sequence>
<xs:element name="FirmatoDigitalmente" type="xs:boolean" />
<xs:element name="SigillatoElettronicamente" type="xs:boolean" />
<xs:element name="MarcaturaTemporale" type="xs:boolean" />
<xs:element name="ConformitaCopieImmagineSuSupportoInformatico" type="xs:boolean" />
</xs:sequence>
</xs:complexType>

<xs:complexType name="AggType">
<xs:sequence>
<xs:element name="TipoAgg" type="IdAggType" minOccurs="1" maxOccurs="unbounded"/>
</xs:sequence>
</xs:complexType>

<xs:complexType name="IdAggType">
<xs:sequence>
<xs:element name="TipoAggregazione" type="TipoAggregazioneType"/>
<xs:element name="IdAggregazione" type="xs:string" />
</xs:sequence>
</xs:complexType>

<xs:simpleType name="TipoAggregazioneType">
<xs:restriction base="xs:string">
<xs:enumeration value="Fascicolo"/>
<xs:enumeration value="Serie Documentale"/>
<xs:enumeration value="Serie Di Fascicoli"/>
</xs:restriction>
</xs:simpleType>

<xs:complexType name="TracciatureModificheDocumentoType">
```

```
<xs:sequence>
<xs:element name="TipoModifica" type="TipoModificaType"/>
<xs:element name="SoggettoAutoreDellaModifica" type="PFType" />
<xs:element name="DataModifica" type="xs:date"/>
<xs:element name="OraModifica" type="xs:time" minOccurs="0"/>
<xs:element name="IdDocVersionePrecedente" type="IdDocType"/>
</xs:sequence>
</xs:complexType>

<xs:simpleType name="TipoModificaType">
<xs:restriction base="xs:string">
<xs:enumeration value="Annullamento"/>
<xs:enumeration value="Rettifica"/>
<xs:enumeration value="Integrazione"/>
<xs:enumeration value="Annotazione"/>
</xs:restriction>
</xs:simpleType>

                                                <xs:simpleType name="CFType">
                                                <xs:restriction base="xs:string" >
        <xs:pattern                                                                                                                                value="[A-Z]{6}[0-
9LMNPQRSTUV]{2}[ABCDEHLMPRST][0-9LMNPQRSTUV]{2}[A-Z][0-9LMNPQRSTUV]{3}[A-Z]"/>
                                                        </xs:restriction>
                                                       </xs:simpleType>

                                                <xs:simpleType name="PIType">
                                                <xs:restriction base="xs:string">
                                                     <xs:pattern value="\d{11}"/>
                                                          </xs:restriction>
                                                         </xs:simpleType>
```

```
<xs:simpleType name="TempoDiConservazioneType">
<xs:restriction base="xs:integer">
<xs:minInclusive value="1"/>
<xs:maxInclusive value="9999"/>
</xs:restriction>
</xs:simpleType>

</xs:schema>
```

4. METADATI DELLE AGGREGAZIONI DOCUMENTALI INFORMATICHE

Definizione del metadato Identificativo dell'Aggregazione documentale (element xsd: IdAgg)

L' Identificativo dell'Aggregazione documentale è una sequenza di caratteri alfanumerici associata in modo univoco all'aggregazione documentale informatica in modo da consentirne l'identificazione, indica se si tratta di un Fascicolo o di una Serie Documentale o di una Serie di Fascicoli.

Il fascicolo è una aggregazione documentale informatica strutturata e univocamente identificata contenente atti, documenti o dati informatici prodotti efunzionali all'esercizio di una attività o allo svolgimento di uno specifico procedimento.

Le serie documentarie sono costituite da documenti singoli accorpati per ragioni funzionali in base alla tipologia di riferimento.

Le serie di fascicoli sono costituite da fascicoli accorpati per ragioni funzionali in base alla classe di riferimento o alla tipologia di fascicoli.

Campi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
TipoAggregazione	Indicare: • Fascicolo • Serie Documentale • Serie Di Fascicoli	Alfanumerico	SI	SI
IdAggregazione	Come da sistema di identificazione formalmente definito.	Alfanumerico	SI	NO, ma ridefinito

Definizione del metadato Tipologia fascicolo (element xsd: TipologiaFascicolo)

I fascicoli sono organizzati per:

- affare: conserva i documenti relativi a una competenza non proceduralizzata, ma che nella consuetudine amministrativa la PA deve concretamente portare a buon fine. Il fascicolo per affare ha una data di apertura e una durata circoscritta.
- attività: comprende i documenti prodotti nello svolgimento di un'attività amministrativa semplice che implica risposte obbligate o meri adempimenti, per la quale quindi non è prevista l'adozione di un provvedimento finale. Ha in genere durata annuale.
- persona fisica: comprende tutti i documenti, anche con classifiche diverse, che si riferiscono a una persona fisica. Quasi sempre i fascicoli intestati alle persone restano correnti per molti anni, costituendo serie aperte.
- persona giuridica: comprende tutti i documenti, anche con classifiche diverse, che si riferiscono a una persona giuridica. Quasi sempre i fascicoli intestati alle persone restano correnti per molti anni, costituendo serie aperte
- procedimento amministrativo: conserva una pluralità di documenti che rappresentano azioni amministrative omogenee e destinate a concludersi con un provvedimento amministrativo.

Campi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova Definizione
NON Applicabile	Solo in caso di TipoAggregazione = 'Fascicolo' Tipologia del fascicolo: • affare • attività • persona fisica • persona giuridica • procedimento amministrativo	Alfanumerico	SI, solo in caso di TipoAggregazione = 'Fascicolo'	SI

Definizione del metadato Soggetti (element xsd: Soggetti)

Indica il metadato che consente di individuare le informazioni relative a tutti i Soggetti che, a vario titolo, sono coinvolti nella costituzione dell'aggregazione. Sono definiti quindi i seguenti attributi:

- Ruolo:
  - Amministrazione titolare
  - Amministrazioni partecipanti
  - Assegnatario
  - Soggetto intestatario persona fisica
  - Soggetto intestatario persona giuridica
  - RUP: da indicare solo in caso di TipoAggregazione = 'Fascicolo'
- Tipo soggetto: consente di tipizzare i soggetti come persone fisiche, giuridiche, amministrazioni pubbliche (italiane ed estere) in funzione del Ruolo. Per ogni tipo soggetto sono indicati i metadati di riferimento. Nel caso in cui sia stato definito un Ruolo=RUP è obbligatorio indicare anche l'UOR corrispondente.

Campi	Sottocampi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
Ruolo		• Amministrazione titolare • Amministrazioni partecipanti • Assegnatario • Soggetto intestatario persona fisica • Soggetto intestatario persona giuridica • RUP Da indicare solo in caso di TipoAggregazione = 'Fascicolo'	Alfanumerico	SI	SI

Campi	Sottocampi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
Tipo soggetto		Se Ruolo = Amministrazione titolare ✓ PAI per le Amministrazioni Pubbliche italiane Se Ruolo = Amministrazioni partecipanti ✓ PAI per le Amministrazioni Pubbliche italiane ✓ PAE per le Amministrazioni Pubbliche estere Se Ruolo = Assegnatario ✓ AS Se Ruolo = Soggetto intestatario persona giuridica • PG per Organizzazione • PAI per le Amministrazioni Pubbliche Italiane • PAE per le Amministrazioni Pubbliche estere Se Ruolo = Soggetto intestatario persona fisica ✓ PF per Persona Fisica Se Ruolo = RUP ✓ RUP	Alfanumerico	SI	SI
	PF	Cognome	Alfanumerico	SI	SI
		Nome	Alfanumerico	SI	
		Codice Fiscale	Alfanumerico	NO	
		Indirizzi Digitali Di Riferimento	Alfanumerico	NO	
	PG	Denominazione Organizzazione	Alfanumerico	SI	SI
		Codice fiscale\Partita Iva	Alfanumerico	NO	
		Denominazione Ufficio	Alfanumerico	NO	

Campi	Sottocampi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
		Indirizzi Digitali Di Riferimento	Alfanumerico	NO	
	PAI	Denominazione Amministrazione \ Codice IPA	Alfanumerico	SI	SI
		Denominazione Amministrazione AOO \ Codice IPA AOO	Alfanumerico	SI	
		Denominazione Amministrazione UOR \ Codice IPA UOR	Alfanumerico	NO	
		Indirizzi Digitali Di Riferimento	Alfanumerico	SI	
	PAE	Denominazione Amministrazione	Alfanumerico	SI	SI
		Denominazione Ufficio	Alfanumerico	NO	
		Indirizzi Digitali Di Riferimento	Alfanumerico	SI	
	AS	Cognome	Alfanumerico	NO	SI
		Nome	Alfanumerico	NO	
		Codice Fiscale	Alfanumerico	NO	
		Denominazione Amministrazione\ Codice IPA	Alfanumerico	SI	
		Denominazione Amministrazione AOO \ Codice IPA AOO	Alfanumerico	SI	
		Denominazione Amministrazione UOR \ Codice IPA UOR	Alfanumerico	SI	
		Indirizzi Digitali Di Riferimento	Alfanumerico	SI	
	RUP	Cognome	Alfanumerico	SI	SI
		Nome	Alfanumerico	SI	

Campi	Sottocampi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
		Codice Fiscale	Alfanumerico	NO	
		Denominazione Amministrazione\ Codice IPA	Alfanumerico	SI	
		Denominazione Amministrazione AOO \ Codice IPA AOO	Alfanumerico	SI	
		Denominazione Amministrazione UOR \ Codice IPA UOR	Alfanumerico	SI	
		Indirizzi Digitali Di Riferimento	Alfanumerico	SI	

Definizione del metadato Assegnazione (element xsd: Assegnazione)

Indica il metadato che consente di individuare le informazioni relative all'assegnazione per conoscenza o per competenza. I Soggetti indicati in questo metadato devono essere stati dichiarati nel metadato Soggetti. Sono definiti quindi i seguenti attributi:

- Tipo assegnazione
- Soggetto assegnatario
- Data inizio assegnazione
- Data fine assegnazione

Il metadato ha una struttura ricorsiva.

Campi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
Tipo assegnazione	• Per competenza • Per conoscenza	Alfanumerico	SI, in caso di fascicolo	SI
Soggetto Assegnatario	Come da Ruolo = Assegnatario definito del metadato Soggetti.	Alfanumerico	SI, in caso di fascicolo	SI
Data inizio assegnazione / Ora inizio assegnazione	Data inizio assegnazione	Date/Time	SI, in caso di fascicolo	SI
Data fine assegnazione / Ora fine assegnazione	Data fine assegnazione	Date/Time	NO	SI

ENTE DI GESTIONE
DELLE AREE PROTETTE
DEL PO PIEMONTESE

ALLEGATO 6

Comunicazione tra AOO di Documenti Amministrativi Protocollati.

Estratto dell'Allegato 6 al documento "*Linee Guida sulla formazione, gestione e conservazione dei documenti informatici*".

Ai sensi delle linee guida Agid 2021– 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

1. Scopo ed ambito di applicazione

Il “Sistema di Gestione Informatica dei Documenti” è utilizzato da una Pubbliche Amministrazioni (di seguito *PA*) per gestire il ciclo di vita dei “Documenti Amministrativi Informatici”, a partire dalla loro formazione/ricezione per giungere alla loro archiviazione e/otrasmissione, nell’esercizio delle proprie funzioni istituzionali.

Con “Protocollo Informatico” indichiamo la componente software del sistema di “Sistema di Gestione Informatica dei Documenti” che assicura la gestione contemporanea della registrazione di protocollo e segnatura di protocollo.

Nel dettaglio il “Protocollo Informatico” assicura le seguenti azioni:

- produzione della segnatura di protocollo, cioè l'apposizione o l'associazione all'originale del documento, in forma permanente non modificabile, dei metadati riguardanti il documento stesso funzionali alla ricezione o spedizione dalle pubblicheamministrazioni;
- registrazione di protocollo, cioè l’attività di memorizzazione dei dati necessari a conservare le informazioni per ogni documento ricevuto o spedito dalle pubbliche amministrazioni.

La strategia per la digitalizzazione della PA, e non da ultimo le indicazioni riportate nel “Piano Triennale per l’Informatica nella Pubblica Amministrazione”, individuano l’esigenza di favorire l’interazione tra i sistemi informatici delle PA che, nel presente allegato, si concretizza nella comunicazione tra le Aree Organizzative Omogenee (AOO) della medesima PA o appartenenti a differenti PA.

Di seguito, quale presupposto all’esigenza di ricezione e spedizione espressa in precedenza, sono definite la tipologia e la rappresentazione (formati dati) delle informazioniassociate ai documenti amministrativi informatici protocollati che costituiscono la segnaturadi protocollo. La rappresentazione formale degli stessi è realizzata attraverso l’utilizzo degli XML Schema nel rispetto delle specifiche W3C:

- W3C XML Schema Definition Language (XSD) 1.1 Part 1: Structures[1]
- W3C XML Schema Definition Language (XSD) 1.1 Part 2: Datatypes[2]

In attuazione di quanto disposto dell’art. 47 del D.Lgs. 82/2005, relativamente alle comunicazioni tra amministrazioni, di documenti amministrativi informatici protocollati, sonoindividuate le modalità tecniche per assicurare il trasporto di documenti amministrativi informatici tra AOO della pubblica amministrazione.

I formati dati e le modalità tecniche per il trasporto indicati nel presente allegato verranno adeguati in relazione all'evoluzione tecnologica e alle eventuali ulteriori esigenze che le amministrazioni dovessero manifestare a seguito della loro applicazione.

Il presente documento abroga e sostituisce la circolare 60/2103 dell’AgID in materia di “Formato e definizione dei tipi di informazioni minime ed accessorie associate ai messaggi

---

1

scambiati tra le Pubbliche Amministrazioni", preservando, fino al completamento della comunicazione tra AOO basata su cooperazione applicativa, la modalità di inoltro tramiteposta elettronica fatta salva l'esigenza di attuare quanto indicato nell'Appendice C.

1.1. Note di lettura del documento

Nella definizione dei requisiti, delle specifiche e delle regole descritte nei documenti precedentemente indicati sono utilizzate le parole chiave DEVE, NON DEVE, OBBLIGATORIO, VIETATO, DOVREBBE, CONSIGLIATO, NON DOVREBBE, SCONSIGLIATO, POTREBBE, OPZIONALE che devono essere interpretate in conformità con RFC 2119[3] dell'Internet Engineering Task Force. In particolare:

- DEVE, OBBLIGATORIO significano che la definizione è un requisito assoluto, la specifica deve essere implementata, la consegna è inderogabile.
- DOVREBBE, CONSIGLIATO significano che in particolari circostanze possono esistere validi motivi per ignorare un requisito, non implementare una specifica, derogare alla consegna, ma che occorre esaminare e valutare con attenzione le implicazioni correlate alla scelta.
- PUÒ, OPZIONALE significano che un elemento della specifica è a implementazione facoltativa.
- NON DOVREBBE, SCONSIGLIATO significano che in particolari circostanze possono esistere validi di motivi per cui un elemento di specifica è accettabile o persino utile, ma, prima di implementarlo, le implicazioni correlate dovrebbero essereesaminate e valutate con attenzione.
- NON DEVE, VIETATO significano che c'è proibizione assoluta di implementazione di un determinato elemento di specifica.

2. Messaggio di protocollo

Lo scambio di documenti amministrativi protocollati tra AOO vede coinvolti:

- il *mittente*, l'AOO che invia i documenti amministrativi protocollati;
- il *destinatario*, l'AOO che riceve i documenti amministrativi protocollati.

Un *messaggio di protocollo*, l'elemento atomico di interesse per dare seguito allo scambio di documenti amministrativi protocollati tra AOO, è una struttura logica che:

- DEVE contenere il documento amministrativo informatico principale (di seguito *documento principale*);
- PUÒ contenere un numero qualsiasi di documenti amministrativi informatici allegati (di seguito *allegati*);
- DEVE contenere la segnatura di protocollo del messaggio protocollato (di seguito *segnatura di protocollo*).

Figure 1. Struttura logica del "messaggio di protocollo"

Il *documento principale* e gli eventuali *allegati* DEVONO essere formati nel rispetto delle regole di formazione dei documenti amministrativi informatici.

La *segnatura di protocollo* DEVE essere formata nel rispetto di quanto indicato al successivo paragrafo 2.1 Struttura segnatura di protocollo.

La *segnatura di protocollo* DEVE essere associata in forma permanente al *documento principale* e agli *allegati* che con esso formano il *messaggio di protocollo*. A tal fine sistema informatico dell'AOO mittente:

- DEVE riportare nella *segnatura di protocollo* l'impronta del *documento principale* e, se presenti, degli *allegati*;
- DEVE assicurare l'autenticità e integrità della *segnatura di protocollo* attuando le regole tecniche in materia di firma elettronica dei documenti informatici emanate dall'AgID conformemente al regolamento UE n° 910/2014, nel dettaglio applicando un "sigillo elettronico qualificato" previsti alla sezione 5 del regolamento UE n° 910/2014 utilizzando il profilo XAdES baseline B level signatures definito in ETSI EN 319 132-1 v1.1.1.

Il controllo della validità amministrativa del *documento principale*, degli *allegati* e dei dati riportati nella *segnatura di protocollo:*

- è di responsabilità della AOO mittente;
- DEVE essere effettuato prima della composizione del *messaggio di protocollo.*

Per assicurare la non ripudiabilità dello scambio tra AOO, le informazioni della *segnatura di protocollo* DEVONO essere memorizzate nel sistema di gestione dei documenti della AOO mittente e in quello delle AOO destinataria. L'indicata azione di memorizzazione è

assicurata dalla registrazione di protocollo realizzata dal "Protocollo informatico".

2.1. Struttura della segnatura di protocollo

La *segnatura di protocollo* DEVE prevedere le seguenti sezioni:

- "Intestazione", contiene i dati identificativi e le informazioni fondamentali del messaggio;
- "Descrizione", opzionalmente, contiene le informazioni relative al messaggio di protocollo ricevuto;
- "Descrizione", contiene le informazioni descrittive riguardanti il contenuto del messaggio;
- "Signature" per permettere la firma della segnatura di protocollo conformemente al profilo XAdES baseline B level signatures.

Di seguito sono indicate la natura delle informazioni presenti nelle sezioni della *segnatura di protocollo*.

Le AOO mittenti che predispongono la *segnatura di protocollo* DEVONO assicurare la conformità rispetto all'XML Schema riportato nell'Appendice A.

2.1.1. Intestazione

La sezione "Intestazione" DEVE contenere gli elementi essenziali di identificazione e caratterizzazione amministrativa del *messaggio di protocollato*.

In particolare, la sezione contiene l'*Identificatore* della registrazione relativa al messaggio protocollato in uscita. Tale identificatore riporta i seguenti dati:

a) indicazione della amministrazione mittente;
b) indicazione della AOO mittente;
c) indicazione del registro nell'ambito del quale è stata effettuata la registrazione;
d) numero progressivo di protocollo;
e) data di registrazione;
f) l'oggetto del messaggio di protocollo;
g) la classificazione del messaggio di protocollo;
h) il fascicolo del messaggio di protocollo.

In merito ai precedenti punti a) e b) si evidenzia che l'Amministrazione:

- DEVE utilizzare il codice IPA dell'amministrazione registrato nell'Indice dei domicili digitali delle pubbliche amministrazioni e dei gestori di pubblici servizi (IPA) per indicare la amministrazione mittente;
- DEVE utilizzare il codice AOO[4] registrato nell'Indice dei domicili digitali delle pubbliche amministrazioni e dei gestori di pubblici servizi (IPA) per indicare la AOOmittente.

2.1.2. Riferimento

La sezione "Riferimento" PUO' contenere i dati per permettere al mittente di indicare il messaggio di protocollo ricevuto che ha determinato la presente segnatura.

2.1.3. Descrizione

La sezione "Descrizione" DEVE contenere le informazioni che descrivono i corrispondenti (mittente e destinatario) interessati nello scambio e i riferimenti al *documento principale* e agli eventuali *allegati* del *messaggio di protocollo*.

In particolare, contiene l'impronta informatica del *documento principale* e degli eventuali *allegati* necessari per associarli in forma permanente alla *segnatura di protocollo*.

2.1.4. Signature

La sezione "Signature" DEVE contenere le informazioni per assicurare la firma della *segnatura di protocollo* da parte della AOO mittente per assicurare l'autenticità e integrità.

2.2. Regole di processamento

Il flusso di processamento che le AOO mittenti devono realizzare per assicurare la formazione del *messaggio di protocollo* è di seguito riportato:

A. Formazione del *documento principale* (*document*), ed eventuali *allegati* (*attachment*$_i$), DEVONO rispettare le regole di formazione dei documenti amministrativi elettronici, inclusa la classificazione.
B. Calcolo dell'impronta del *documento principale* (*digest(document,algorithm)*), e degli eventuali *allegati* (*digest(attachment*$_i$*,algorithm)*), che DEVONO utilizzare uno degli algoritmi indicati nella seguente tabella 1.
C. Generazione del numero di protocollo da assegnare al *messaggio di protocollo.*

D. Formazione della *segnatura di protocollo* che DEVE rispettare l'XML Schema indicato nell'Appendice A, utilizzando le impronte *digest(document,algorithm)* e *digest(attachment$_i$,algorithm)* create al passo B.
E. Apposizione di un "sigillo elettronico qualificato" alla *segnatura di protocollo per* garantire l'integrità e autenticità che DEVE applicare il profilo XAdES baseline B level signatures definito in ETSI EN 319 132-1 v1.1.1.

Tabella 1 - Digest algorithm

SIGLA	URI
SHA-224	http://www.w3.org/2001/04/xmldsig-more#sha224
SHA-256	http://www.w3.org/2001/04/xmlenc#sha256
SHA-384	http://www.w3.org/2001/04/xmldsig-more#sha384
SHA-512	http://www.w3.org/2001/04/xmlenc#sha512
HMAC-SHA-224	http://www.w3.org/2001/04/xmldsig-more#hmac-sha224
HMAC-SHA-256	http://www.w3.org/2001/04/xmldsig-more#hmac-sha256
HMAC-SHA-384	http://www.w3.org/2001/04/xmldsig-more#hmac-sha384
HMAC-SHA-512	http://www.w3.org/2001/04/xmldsig-more#hmac-sha512

3. Flussi di comunicazione

Le esigenze di comunicazione tra AOO mittente e AOO destinataria per assicurare l'inoltro di un messaggio protocollato richiedono:

- *inoltro di un messaggio protocollato* (**MessaggioInoltro**) da una AOO mittente ad una AOO destinataria e la relativa conferma se richiesta dal Mittente;
- *annullamento protocollazione mittente* (**AnnullamentoInoltroMittente**), nel caso in cui successivamente all'inoltro l'AOO mittente adotti un provvedimento per il suo annullamento;
- *annullamento protocollazione destinatario* (**AnnullamentoInoltroDestinatario**), nel caso in cui successivamente alla conferma di ricezione l'AOO destinataria adotti un provvedimento per il suo annullamento.

Le esigenze di comunicazione individuate sono sintetizzate nel seguente UML sequence diagram.

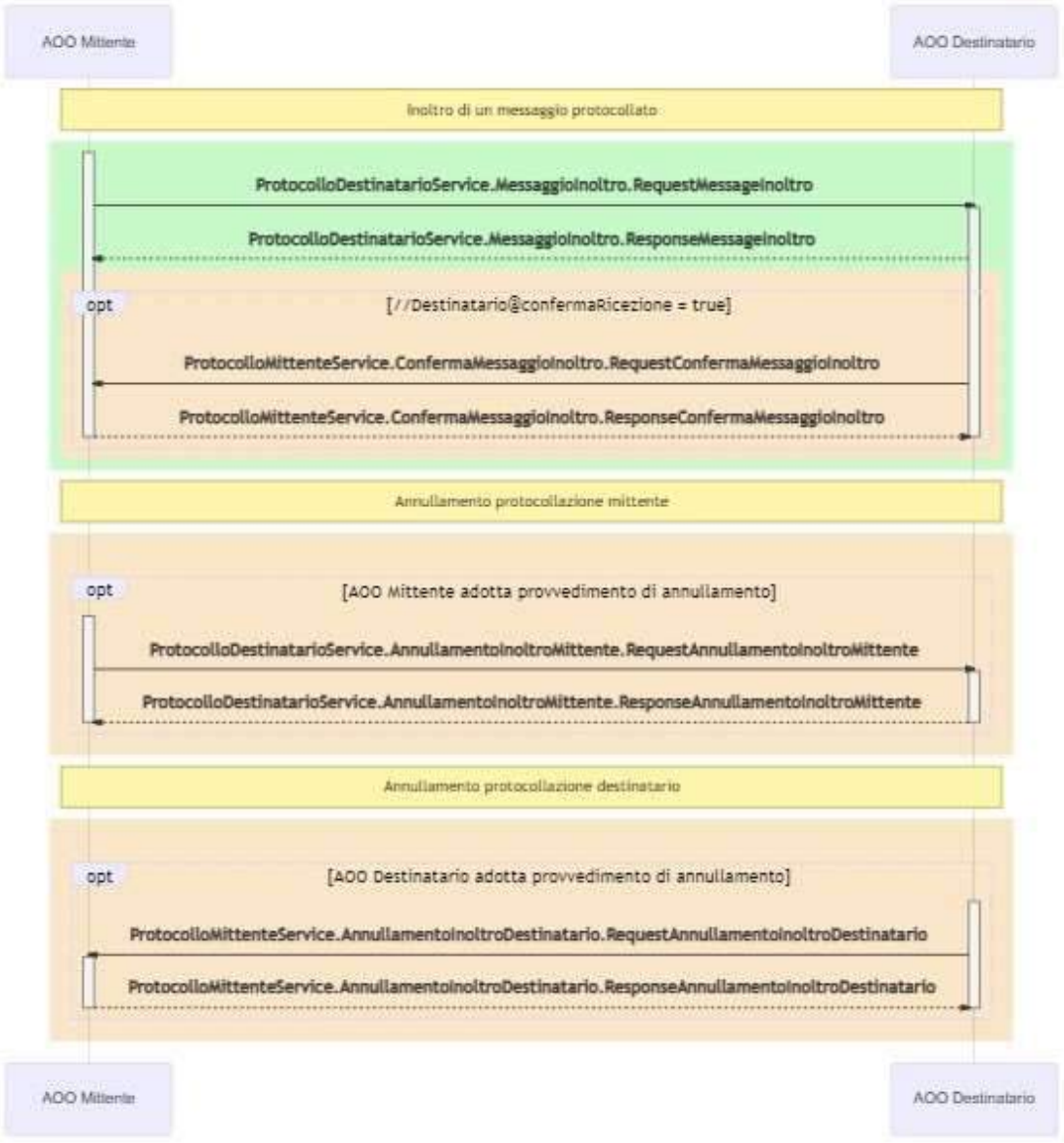


Figure 2. Comunicazioni tra AOO mittente e AOO destinatario

Per dare seguito alla comunicazione tra AOO mittente e AOO destinataria, le stesse adottano la modalità previste dalla norma basata sulla *cooperazione applicativa*, utilizzandoil Simple Object Access Protocol assicurando l'implementazione delle interfacce di servizio riportate nell'Appendice B.

Per assicurare la comunicazione tra AOO le Amministrazioni DEVONO registrare e mantenere aggiornato, per ogni AOO individuata nella propria organizzazione, l'Indice deidomicili digitali delle pubbliche amministrazioni e dei gestori di pubblici servizi (IPA) con il prefisso condiviso dagli *endpoint* di esposizione dei servizi indicati nell'Appendice B.

3.1. Regole di processamento

I flussi di processamento che le AOO mittenti e destinatari devono realizzare per assicurare l'inoltro e ricezione dei messaggi protocollati sono riportate di seguito.

3.1.1. Inoltro di un messaggio protocollato

A. AOO mittente: Inoltro messaggio di protocollo

   L'AOO mittente DEVE produrre il *messaggio di protocollo*, come indicato nel precedente paragrafo 2 e inoltrare lo stesso alla AOO destinataria.

   N.B. l'AOO mittente determina l'inoltro della conferma di ricezione da parte della AOO destinataria settando l'attributo /*SegnaturaInformatica/Descrizione/Destinatario@confermaRicezione* = true.

B. AOO destinatario: Riceve *messaggio di protocollo*

   L'AOO destinatario ricevuto il *messaggio di protocollo* DEVE verificare la *segnatura di protocollo*, nel dettaglio:

   a. DEVE verificare la correttezza della firma della *segnatura di protocollo*;
   b. DEVE verificare la corrispondenza dell'impronta del *documento principale* presente nella *segnatura di protocollo* e il documento *principale* ricevuto;
   c. se presenti *allegati*, per ogni allegato DEVE verificare la corrispondenza dell'impronta dell'*allegato* presente nella *segnatura di protocollo* e l'allegato ricevuto.

   Se l'AOO destinataria è riuscita a verificare il *messaggio di protocollo* ricevuto DEVE rispondere indicando l'Identificatore associato dalla AOO mittente.

   Se l'AOO destinataria non è riuscita a verificare il *messaggio di protocollo* ricevuto DEVE segnalare alla AOO mittente l'anomalia riscontrata è nel dettaglio:

   a. se la firma della *segnatura di protocollo* non è verificata DEVE restituire l'anomalia 001_ValidazioneFirma;

b. se almeno una delle impronte riportate nella *segnatura di protocollo* (*documento principale* e *allegati*) non è verificata DEVE restituire l'anomalia 002_AnomaliaImpronta.

I seguenti step sono realizzati se l'AOO destinatario verifica che l'APP mittente a settato a true l'attributo /*SegnaturaInformatica/Descrizione/Destinatario@confermaRicezione*.

C. AOO destinatario: Inoltro conferma di protocollazione del *messaggio di protocollo*

L'AOO destinataria DEVE inoltrare conferma di protocollazione del *messaggio di protocollo* alla AOO mittente a conclusione del processo di protocollazione in ingresso.

L'AOO destinataria PUO' effettuare il controllo dei file ricevuti (*documento principale* e *allegati*) ed in caso di anomalie DEVE segnalare alla AOO mittente l'anomalia riscontrata è nel dettaglio:

a. se almeno uno dei file ricevuto (*documento principale* e *allegati*) risulta non leggibile DEVE restituire l'anomalia 003_DocumentoAllegatiNonLeggibili.
b. se almeno uno dei file ricevuto (*documento principale* e *allegati*) risulta firmato e la validazione della stessa fallisce DEVE restituire l'anomalia 004_DocumentoAllegatiErrorreValidazioneFirma.
c. se almeno uno dei file ricevuto (*documento principale* e *allegati*) risulta con marca temporale e la validazione della stessa fallisce DEVE restituire l'anomalia 005_DocumentoAllegatiErroreValidazioneMarcaTemporale.
d. se almeno uno dei file ricevuto (*documento principale* e *allegati*) risulta con sigillo elettronico e la validazione dello stesso fallisce DEVE restituire l'anomalia 006_DocumentoAllegatiErroreValidazioneSigillo.

AOO destinataria DEVE verificare la ricevibilità del *messaggio di protocollo* ricevuto, ed in caso negativo DEVE restituire l'anomalia 000_Irricevibile e l'indicazione della motivazione di irricevibilità.

AOO destinatario DEVE generare il numero di protocollo per *messaggio di protocollo* ricevuto e, contemporaneamente, memorizzare lo stesso nel registro di protocollo in ingresso.

L'AOO destinatario DEVE inoltrare la conferma di protocollazione del *messaggio di protocollo* ricevuto includendo l'Identificatore associato dal AOO mittente e l'Identificatore da essa associato.

D. AOO mittente: Ricezione della conferma di protocollazione del *messaggio di protocollo*

Nel caso in cui l'AOO destinatario non segnali anomalie l'AOO mittente DEVE memorizzare la conferma di protocollazione del *messaggio di protocollo* nel registro diprotocollo per assicurare la persistenza dello stesso.

Nel caso in cui l'AOO destinatario segnali anomalie l'AOO mittente DEVE ritenere la transazione non conclusa.

3.1.2. Annullamento protocollazione mittente

A. AOO mittente: Inoltro messaggio annullamento

L'AOO mittente DEVE inoltrare la richiesta di annullamento di un *messaggio di protocollo* precedentemente inviato:

- indicando l'Identificatore associato da essa al momento dell'inoltro e l'Identificatore associato dal destinatario indicato nella ricevuta di ricezione del *messaggio di protocollo*;
- riportando il riferimento al provvedimento che determina il presupposto amministrativo per l'annullamento.

B. AOO destinatario: Inoltro ricevuta annullamento

L'AOO destinatario DEVE inoltrare la ricevuta di annullamento di un *messaggio diprotocollo* precedentemente ricevuto.

L'AOO destinataria assicura che nella ricevuta di annullamento:

- DEVE indicare l'Identificatore associato dalla AOO mittente al momento dell'inoltro e l'Identificatore associato da esso indicato nella ricevuta di ricezione del *messaggio di protocollo* inoltrata al mittente;
- nel caso di irricevibilità dell'annullamento DEVE restituire l'anomalia 000_Irricevibile indicando il motivo di irricevibilità;
- nel caso in cui non risulti il *messaggio di protocollo* DEVE restituire l'anomalia 007_ErroreIdentificatoreNonTrovato.

3.1.3. Annullamento protocollazione destinatario

1. AOO destinatario: Inoltro messaggio annullamento

L'AOO destinatario DEVE inoltrare la richiesta di annullamento di un *messaggio di protocollo* precedentemente ricevuto:

- indicando l'Identificatore associato dalla AOO mittente al momento dell'inoltro e l'Identificatore associato da esso indicato nella ricevuta di ricezione del *messaggio di protocollo* inoltrata al mittente;
- riportando il riferimento al provvedimento che determina il presupposto amministrativo per l'annullamento.

2. AOO mittente: Inoltro ricevuta annullamento

L'AOO mittente DEVE inoltrare la ricevuta di annullamento di un *messaggio di protocollo* precedentemente inviato.

L'AOO mittente assicura che nella ricevuta di annullamento:

- DEVE indicare l'Identificatore associato da essa al momento dell'inoltro l'Identificatore associato dal destinatario indicato nella ricevuta di ricezione del *messaggio di protocollo*;
- nel caso di irricevibilità dell'annullamento DEVE restituire l'anomalia 000_Irricevibile indicando il motivo di irricevibilità;

- nel caso in cui non risulti il *messaggio di protocollo* DEVE restituire l’anomalia 007_ErroreIdentificatoreNonTrovato.

ENTE DI GESTIONE
DELLE AREE PROTETTE DEL PO PIEMONTESE

ALLEGATO 7

AL MANUALE DI GESTIONE DOCUMENTALE DEL PROTOCOLLO INFORMATICO, DEI FLUSSI DOCUMENTALI E DEGLI ARCHIVI

IL SISTEMA DOCUMENTALE E DI PROTOCOLLAZIONE ADOTTATO DALL'ENTE

Ai sensi delle linee guida Agid 2021– Regole tecniche per il protocollo informatico ai sensi dell'artt. 40-bis, 41, 47, 57-bis

INDICE

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 **"OLIMPO"** che ha un modulo specifico per la protocollazione denominato "EGISTO".
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 sia 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 soli 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 denominata "*Quaderno di lavoro*", all'interno della quale ogni operatore è in grado di visionare la corrispondenza in arrivo, prenderla in carico, fascicolarla, assegnarla ed evaderla.
La corrispondenza in partenza è 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 denominata "*Quaderno di lavoro*".
Inoltre, grazie al calendario digitale integrato, ogni appuntamento, scadenze o attività lavorativa può essere registrata dall'utente e mantenuta in evidenza nell'area di monitoraggio.
Il "*Quaderno di lavoro*" supporta così passo a passo l'operatore nell'espletamento di tutte le sue incombenze.

2. Gestione accessi

Il sistema OLIMPO 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 sono continuamente monitorate e registrate in automatico in appositi file di LOG, immodificabili.
A ciascun addetto sono 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. Inserimento/Formazione di un nuovo documento

L'inserimento di un documento è la prima operazione con la quale si confrontano quotidianamente gli operatori.
Esistono diversi modi per inserire un nuovo documento in OLIMPO; di seguito saranno richiamate le principali.
Per formare un documento si parte dalla specifica funzione "NUOVO DOCUMENTO" e si redige il documento previa compilazione della maschera d'indicizzazione.

La maschera d'indicizzazione contiene le informazioni principali relative al documento, essenziali per la ricerca. Al fine di standardizzare il più possibile le metodologie di archiviazione dei documenti sono stati previsti campi con liste predefinite, utili nel prevenire errori di digitazione o impostazioni personali.

Il secondo modo di inserire un documento in OLIMPO è quello di partire da un documento simile già presente all'interno del sistema. In questo caso, dopo aver ricercato il documento di base, si procede duplicando la scheda relativa con il menù contestuale.
In alternativa, si può partire da un modello di documento già presente in OLIMPO. E' stato, infatti, predisposto sul sistema un tipo di documento denominato "*MODELLI*", con maschera d'indicizzazione semplificata che permette di memorizzare agevolmente i modelli dei documenti più usati, ottimizzandone l'utilizzo ed evitando le fasi ripetitive.

E' inoltre possibile inserire in OLIMPO un documento, acquisendolo direttamente dal file system. Questo metodo è particolarmente indicato per tipologie di file provenienti da applicazioni che non dispongono di "macro" di inserimento.

I documenti provenienti dall'esterno sono importati nel sistema in modo diretto se già in formato digitale, oppure sono importati previa digitalizzazione tramite scansione.
I documenti informatici arrivati tramite posta elettronica sono gestiti automaticamente con apposita funzione. Se si tratta di messaggi di posta elettronica certificati inviati alla caselle PEC dell'Ente, sono gestiti dalla voce "PEC in arrivo".

4. 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 è riportata in dettaglio all'interno del capitolo *"4. Sistema di classificazione, fascicolazione digitale e archiviazione"* del manuale di gestione del protocollo informatico, dei flussi documentali e degli archivi.

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

1. Documenti prodotti dall'Ente:
   - da sistema documentale
   - da procedure gestionali
   - da procedure workflow

2. Documenti pervenuti all'Ente

Quando viene prodotto un nuovo documento tramite specifica procedura gestionale del sistema integrato sarà la stessa a collocare il documento all'interno del relativo fascicolo digitale (macrofascicolo) ed a creare il fascicolo/sottofascicolo relativo all'affare o al procedimento in corso. Se esiste già il relativo sotto-fascicolo, il documento verrà automaticamente collegato ad esso.
Se il documento è prodotto invece tramite la scrivania digitale del sistema documentale OLIMPO, l'assegnazione del fascicolo e del relativo sotto-fascicolo sarà automatica se si risponde ad un documento già fascicolato, a carico del soggetto competente negli altri casi.

Per quanto riguarda invece i documenti pervenuti all'Ente, l'assegnazione del fascicolo e del relativo sotto-fascicolo è a carico del soggetto competente.

5. Ricerca dei documenti in archivio

OLIMPO possiede un efficiente sistema di ricerca e reperimento dei documenti basato sui dati inseriti nelle maschere d'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.). Il sistema di gestione documentale consente l'inserimento di modelli di ricerca e di consultazione, con maschere personalizzate, richiamabili ripetutamente nel tempo. La ricerca delle informazioni sul sistema è effettuata secondo criteri basati su tutti i tipi d'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.

6. Condivisione dei documenti

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

La peculiarità della posta OLIMPO, a differenza della posta elettronica tradizionale, consiste nel fatto che i documenti memorizzati nel sistema non sono effettivamente inviati: ciò che viene trasmesso attraverso la posta è un link al documento, che è sempre unico all'interno del sistema, e come tale si presenta sempre aggiornato agli utenti che vi accedono. Il sistema consente di assegnare le visibilità, e di spedire i documenti con o senza "notifica" di avviso.
La ricezione di un documento condiviso è segnalata su apposito nodo del quaderno di lavoro di OLIMPO accompagnata dalla specifica dell'operazione da compiere sul documento.

Grazie a questo sistema di condivisione/assegnazione interno non vi è alcuna replicazione del documento.

7. Assegnazione dei documenti

Tramite il sistema documentale è possibile assegnare un documento ad uno o più "incaricati del procedimento/collaboratori".
Il documento assegnato viene ricevuto in apposito nodo del loro quaderno di lavoro di OLIMPO.
L'assegnazione può inoltre essere accompagnata da una nota operativa con la quale si possono indicare le eventuali modalità operative da eseguire.
L'assegnatario può monitorare in qualsiasi momento lo stato di avanzamento delle operazioni sul documento.

La peculiarità dell'assegnazione di OLIMPO, a differenza della posta elettronica tradizionale, consiste nel fatto che i documenti che sono assegnati nel sistema non sono effettivamente inviati: ciò che viene trasmesso è un link al documento, che è sempre unico all'interno del sistema, e come tale si presenta sempre aggiornato agli utenti che vi accedono.

8. 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, tuttora sottoutilizzato rispetto alle sue potenzialità, rappresenta un prerequisito ineludibile per l'evoluzione della documentazione, sempre più destinata a trasformarsi da foglio di carta a file memorizzato nel sistema.
OLIMPO gestisce sia l'inserimento di documenti già firmati digitalmente, sia la firma diretta dei documenti all'interno del 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.

9. Invio di un documento a destinatari esterni

E' possibile protocollare in uscita sia un documento già presente nell'archivio interno (duplicando la relativa scheda che di norma riporta anche la tipologia documentale appropriata), sia un documento in corso di inserimento nel sistema. Dopo avere compilato gli indici, il documento sarà opportunamente fascicolato e archiviato.

10. Iter documento

Tutte le azioni effettuate su un documento all'interno del sistema documentale (visualizzazione, lettura, presa in carico, assegnazione, ecc) sono 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.

11. 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 il modulo software EGISTO.

EGISTO permette infatti di protocollare:

- E-mail Certificate/E-mail: il sistema protocolla automaticamente tutte 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 "OLIMPO" all'interno dell'area di monitoraggio denominata "Quaderno di lavoro".
Le operazioni che si possono effettuare 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 altro incaricato competente. Se il documento è rimosso dal quaderno, è sempre possibile ricercarlo in archivio documentale.
- **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 nel capitolo *"4. Fascicolazione di un documento"* del presente allegato.
- **Assegnazione di un documento ad incaricato del procedimento**
  Il Responsabile di un'unità organizzativa può assegnare un documento ricevuto a 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, E-mail certificata...)
- **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.

12. 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 OLIMPO: 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 scelga di partire da un modello predisposto);
Il testo così creato può essere redatto dall'operatore competente.
La risposta a un documento propone automaticamente l'eventuale evasione dell'istanza ricevuta.

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

- **Condivisone/assegnazione di un documento all'interno dell'AOO**
  Le modalità di gestione sono descritte nei capitoli *"6. Condivisione dei documenti"* e "*7. Assegnazione dei documenti"* del presente allegato.
- **Fascicolazione digitale del documento**
  L'operazione di fascicolazione digitale avviene con le modalità descritte nel capitolo *"4. 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 OLIMPO sfruttando la funzione di firma automatica così come specificato nel capitolo *"8. 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. Utilizzando la funzione di protocollazione automatica è visualizzata la maschera del protocollo comprensiva di tutti i dati già preventivamente caricati dall'utente sul documento e si può attribuire il numero di protocollo.
  I riferimenti del protocollo sono poi riportati automaticamente all'interno del file sul quale si stava lavorando (*se si trattava di modello di testo predisposto*).
  Se l'utente non è abilitato alla protocollazione può comunque trasmettere il documento tramite il sistema documentale all'ufficio protocollo, il quale vedrà la richiesta in uno specifico nodo sul quaderno di lavoro e potrà protocollare il documento.
- **Archiviare un documento**
  Terminate le operazioni di redazione del documento si può procedere all'archiviazione del medesimo. A ciascun documento archiviato è attribuito un codice univoco di archiviazione.
- **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, 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 tramite Posta Elettronica Certificata.

ENTE DI GESTIONE DELLE AREE PROTETTE DEL PO PIEMONTESE

ALLEGATO 8

AL MANUALE DI GESTIONE DOCUMENTALE DEL PROTOCOLLO INFORMATICO, DEI FLUSSI DOCUMENTALI E DEGLI ARCHIVI

IL SISTEMA DI CONSERVAZIONE ADOTTATO DALL'ENTE

Ai sensi delle linee guida Agid 2021– 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

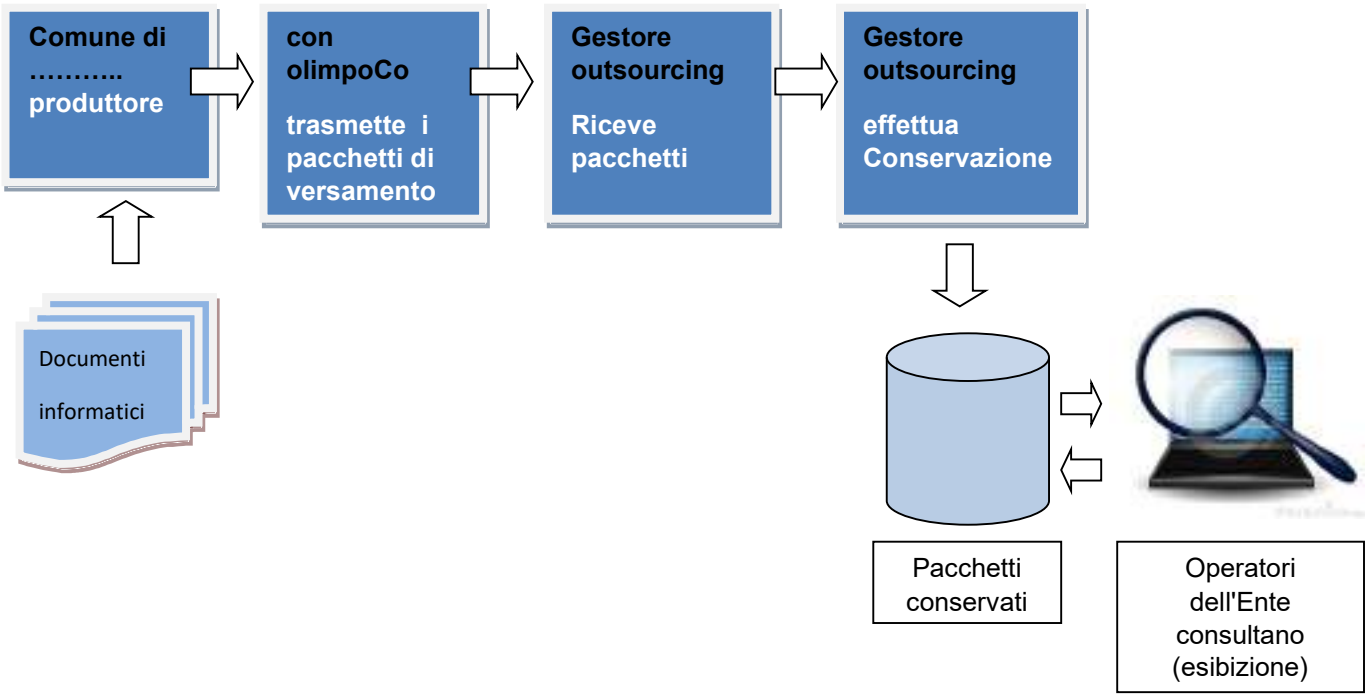
Indice

1 La conservazione dei documenti informatici dell'Ente

1.1 Il sistema di conservazione adottato dall'Ente

L'Ente affida il servizio di conservazione ad un conservatore accreditato esterno.

Il "ciclo di gestione della conservazione" in outsourcing realizzato da con conservatore accreditato



Il sistema prevede la "gestione del ciclo della conservazione" … dal reperimento dei documenti e la preparazione dei pacchetti di versamento, fino alla conservazione a **norma** effettuata **c/o outsourcer esterno accreditato** che viene nominato responsabile della conservazione.

1.2 Il sistema di versamento organizzato dall'Ente

Il sistema di versamento adottato dall'Ente è il sistema OlimpoCoOutosurcer che consente la gestione completa del flusso di versamento: creazione pacchetti, trasmissione tramite interfaccia al conservatore, archiviazione ricevute e monitoraggio operatività.

Ogni servizio produttore di documenti informatici è anche responsabile del procedimento di trasmissione dei pacchetti di versamento di propria competenza al conservatore esterno.

Modulo adottato: software OlimpoCo per produzione/trasmissione pacchetti di versamento all'outsourcer.

Le tipologie documentarie prodotte dall'Ente, da conservare, sono numerose (contratti, fatture, registri, atti, provvedimenti, etc.).

Pertanto si rende necessario avere un sistema che gestisce la conservazione di questo universo di documenti in modo programmato.

Nel contesto del ciclo di conservazione riveste particolare importanza la gestione della fase di versamento che prevede:

- Programmazione delle tipologie dei documenti da conservare
- Scadenziario per tipologia documentaria
- Preparazione dei pacchetti di versamento per il sistema di conservazione con le specifiche tecniche definite con l'outsourcer
- Registro delle avvenute conservazioni

Il modulo adottato è altamente qualificato per gestire il versamento dei documenti informatici in modo automatico, controllato con lo scadenziario ed il periodo di conservazione.
La gestione dei pacchetti di versamento avviene tramite il sistema di interscambio “OlimpoCoOutsourcer” che gestisce i pacchetti di versamento da conservare interfacciandosi con le procedure Siscom e con la piattaforma di gestionale documentale.

1.3 Il sistema di esibizione pacchetti di distribuzione

La consultazione dei documenti conservati dei pacchetti di distribuzione (esibizione) è accedibile tramite il sistema on-line messo a disposizione dall’Outsourcer con abilitazione tramite autentica degli operatori delegati dall’ente.
I soggetti abilitati alla consultazione dei pacchetti di distribuzione (esibizione) sono comunicati all’Outsourcer contestualmente alla modulistica di adesione al servizio.

2 Manuale della conservazione

Viene adottato il Manuale della conservazione dell’Outsourcer a cui viene affidato il servizio pubblicato su sito web dell' Agid.
L’Ente definisce nella gestione del manuale di gestione documentale i procedimenti di versamento e di rapporti operativi con il Conservatore esterno.

3 Responsabile della conservazione

L’ente nomina come “Responsabile della conservazione” il Responsabile della conservazione dell’Outsourcer a cui affida il servizio.
Il Responsabile della gestione documentale è anche responsabile della conservazione interna, limitatamente alle funzioni di coordinamento e supervisione del sistema realizzato dall’Ente per la gestione delle operazioni di Versamento dei pacchetti da conservare trasmessi al conservatore.
Il Responsabile della conservazione interno tiene i rapporti con il personale dei servizi per le operazioni di versamento.

4 Specificità per la conservazione del registro di protocollo informatico

L’Ente provvede ad effettuare la conservazione del registro giornaliero di protocollo utilizzando il sistema di conservazione generale dell’Ente.
L’operazione di conservazione del registro di protocollo comprende:
- l'elenco delle informazioni inserite con l'operazione di registrazione di protocollo nell'arco di uno stesso giorno
- la trasmissione entro la giornata lavorativa successiva, al sistema di conservazione OlimpoConserve, garantendo l'immodificabilità del contenuto.

Il responsabile di protocollo, direttamente o tramite suoi incaricati, provvede tramite specifica funzione programmata del sistema di protocollo, interfacciata con il software di OlimpoConserve, alla creazione del pacchetto di versamento del registro di protocollo del giorno precedente, per la verifica e la trasmissione al sistema di conservazione. Lo stesso soggetto e’ tenuto al monitoraggio dell’esito positivo delle operazioni di avvenuta conservazione.

5 Gestore del servizio in outsourcing dell’Ente

L’Ente tiene un registro nel quale vengono riportati i riferimenti ai conservatori esterni a cui e’ affidata la conservazione con le date di incarico e di inizio attività ed eventuale fine incarico. Tale registro viene mantenuto aggiornato dal Responsabile della gestione documentale.

ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI

ABSC_ID			Livello	Descrizione	Modalità di implementazione
1	1	1	M	Implementare un inventario delle risorse attive correlato a quello ABSC 1.4	In fase di sperimentazione portale wazuh
1	1	2	S	Implementare ABSC 1.1.1 attraverso uno strumento automatico	In fase di sperimentazione portale wazuh
1	1	3	A	Effettuare il discovery dei dispositivi collegati alla rete con allarmi in caso di anomalie.	In fase di sperimentazione portale wazuh
1	1	4	A	Qualificare i sistemi connessi alla rete attraverso l'analisi del loro traffico.	In fase di sperimentazione portale wazuh
1	2	1	S	Implementare il "logging" delle operazione del server DHCP.	Non attivo
1	2	2	S	Utilizzare le informazioni ricavate dal "logging" DHCP per migliorare l'inventario delle risorse e identificare le risorse non ancora censite.	Non attivo
1	3	1	M	Aggiornare l'inventario quando nuovi dispositivi approvati vengono collegati in rete.	In fase di sperimentazione portale wazuh
1	3	2	S	Aggiornare l'inventario con uno strumento automatico quando nuovi dispositivi approvati vengono collegati in rete.	In fase di sperimentazione portale wazuh
1	4	1	M	Gestire l'inventario delle risorse di tutti i sistemi collegati alla rete e dei dispositivi di rete stessi, registrando almeno l'indirizzo IP.	Non attivo
1	4	2	S	Per tutti i dispositivi che possiedono un indirizzo IP l'inventario deve indicare i nomi delle macchine, la funzione del sistema, un titolare responsabile della risorsa e l'ufficio associato. L'inventario delle risorse creato deve inoltre includere informazioni sul fatto che il dispositivo sia portatile e/o personale.	Non attivo
1	4	3	A	Dispositivi come telefoni cellulari, tablet, laptop e altri	Non attivo, per le pdl è in fase di sperimentazione portale wazuh

				dispositivi elettronici portatili che memorizzano o elaborano dati devono essere identificati, a prescindere che siano collegati o meno alla rete dell'organizzazione.	
1	5	1	A	Installare un'autenticazione a livello di rete via 802.1x per limitare e controllare quali dispositivi possono essere connessi alla rete. L'802.1x deve essere correlato ai dati dell'inventario per distinguere i sistemi autorizzati da quelli non autorizzati.	Non attivo: In fase di valutazione per costi e gestione anche in ragione delle limitate dimensioni dell'ente e della difficoltà di attuare la manutenzione rispetto ad un accesso di nuove apparecchiature.
1	6	1	A	Utilizzare i certificati lato client per validare e autenticare i sistemi prima della connessione a una rete locale.	Non attivo

ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI

ABSC_ID			Livello	Descrizione	Modalità di implementazione
2	1	1	M	Stilare un elenco di software autorizzati e relative versioni necessari per ciascun tipo di sistema, compresi server, workstation e laptop di vari tipi e per diversi usi. Non consentire l'installazione di software non compreso nell'elenco.	Non attivo
2	2	1	S	Implementare una "whitelist" delle applicazioni autorizzate, bloccando l'esecuzione del software non incluso nella lista. La "whitelist" può essere molto ampia per includere i software più diffusi.	Non attivo
2	2	2	S	Per sistemi con funzioni specifiche (che richiedono solo un piccolo numero di programmi per funzionare), la "whitelist" può essere più mirata. Quando si proteggono i sistemi con software personalizzati che può essere difficile inserire nella "whitelist", ricorrere al punto ABSC 2.4.1 (isolando il software personalizzato in un sistema operativo virtuale).	Non attivo e non esistono attualmente pdl con questi requisiti

2	2	3	A	Utilizzare strumenti di verifica dell'integrità dei file per verificare che le applicazioni nella "whitelist" non siano state modificate.	In fase di sperimentazione portale wazuh
2	3	1	M	Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato.	Le pdl sono protette dalla soluzione SOPHOS Intercept X Essentials
2	3	2	S	Mantenere un inventario del software in tutta l'organizzazione che copra tutti i tipi di sistemi operativi in uso, compresi server, workstation e laptop.	In fase di sperimentazione portale wazuh
2	3	3	A	Installare strumenti automatici d'inventario del software che registrino anche la versione del sistema operativo utilizzato nonché le applicazioni installate, le varie versioni ed il livello di patch.	In fase di sperimentazione portale wazuh
2	4	1	A	Utilizzare macchine virtuali e/o sistemi air-gapped per isolare ed eseguire applicazioni necessarie per operazioni strategiche o critiche dell'Ente, che a causa dell'elevato rischio non devono essere installate in ambienti direttamente collegati in rete.	Non applicabile perché non sono state rilevate applicazioni critiche.

ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER

ABSC_ID			Livello	Descrizione	Modalità di implementazione
3	1	1	M	Utilizzare configurazioni sicure standard per la protezione dei sistemi operativi.	Tutte le pdl sono dotate di o.s. licenziato
3	1	2	S	Le configurazioni sicure standard devono corrispondere alle versioni "hardened" del sistema operativo e delle applicazioni installate. La procedura di hardening comprende tipicamente: eliminazione degli account non necessari (compresi gli account di servizio), disattivazione o eliminazione dei servizi non	Non attivo

				necessari, configurazione di stack e heaps non eseguibili, applicazione di patch, chiusura di porte di rete aperte e non utilizzate.	
3	1	3	A	Assicurare con regolarità la validazione e l'aggiornamento delle immagini d'installazione nella loro configurazione di sicurezza anche in considerazione delle più recenti vulnerabilità e vettori di attacco.	Le applicazioni funzionali all'ente sono in cloud, non vengono più utilizzare immagini per i nuovi pc ma configurati direttamente con i link condivisi alle applicazioni
3	2	1	M	Definire ed impiegare una configurazione standard per workstation, server e altri tipi di sistemi usati dall'organizzazione.	Non attivo
3	2	2	M	Eventuali sistemi in esercizio che vengano compromessi devono essere ripristinati utilizzando la configurazione standard.	Non attivo
3	2	3	S	Le modifiche alla configurazione standard devono effettuate secondo le procedure di gestione dei cambiamenti.	Non attivo
3	3	1	M	Le immagini d'installazione devono essere memorizzate offline.	Non indispensabile le applicazioni sono prettamente in cloud
3	3	2	S	Le immagini d'installazione sono conservate in modalità protetta, garantendone l'integrità e la disponibilità solo agli utenti autorizzati.	Non indispensabile le applicazioni sono prettamente in cloud
3	4	1	M	Eseguire tutte le operazioni di amministrazione remota di server, workstation, dispositivi di rete e analoghe apparecchiature per mezzo di connessioni protette (protocolli intrinsecamente sicuri, ovvero su canali sicuri).	In fase di definizione con il nuovo appaltante
3	5	1	S	Utilizzare strumenti di verifica dell'integrità dei file per assicurare che i file critici del sistema (compresi eseguibili di sistema e delle applicazioni sensibili, librerie e configurazioni) non siano stati alterati.	Le pdl sono protette dalla soluzione SOPHOS Intercept X Essentials
3	5	2	A	Nel caso in cui la verifica di cui al punto precedente venga eseguita da uno strumento automatico, per qualunque	Le pdl sono protette dalla soluzione SOPHOS Intercept X Essentials

				alterazione di tali file deve essere generato un alert.	
3	5	3	A	Per il supporto alle analisi, il sistema di segnalazione deve essere in grado di mostrare la cronologia dei cambiamenti della configurazione nel tempo e identificare chi ha eseguito ciascuna modifica.	Non attivo
3	5	4	A	I controlli di integrità devono inoltre identificare le alterazioni sospette del sistema, delle variazioni dei permessi di file e cartelle.	Le pdl sono protette dalla soluzione SOPHOS Intercept X Essentials
3	6	1	A	Utilizzare un sistema centralizzato di controllo automatico delle configurazioni che consenta di rilevare e segnalare le modifiche non autorizzate.	Le pdl sono protette dalla soluzione SOPHOS Intercept X Essentials
3	7	1	A	Utilizzare strumenti di gestione della configurazione dei sistemi che consentano il ripristino delle impostazioni di configurazione standard.	Non attivo

ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITÀ

ABSC_ID			Livello	Descrizione	Modalità di implementazione
4	1	1	M	Ad ogni modifica significativa della configurazione eseguire la ricerca delle vulnerabilità su tutti i sistemi in rete con strumenti automatici che forniscano a ciascun amministratore di sistema report con indicazioni delle vulnerabilità più critiche.	Le pdl sono protette dalla soluzione SOPHOS Intercept X Essentials
4	1	2	S	Eseguire periodicamente la ricerca delle vulnerabilità ABSC 4.1.1 con frequenza commisurata alla complessità dell'infrastruttura.	Le pdl sono protette dalla soluzione SOPHOS Intercept X Essentials
4	1	3	A	Usare uno SCAP (Security Content Automation Protocol) di validazione della vulnerabilità che rilevi sia le vulnerabilità	Non attivo

				basate sul codice (come quelle descritte dalle voci Common Vulnerabilities ed Exposures) che quelle basate sulla configurazione (come elencate nel Common Configuration Enumeration Project).	
4	2	1	S	Correlare i log di sistema con le informazioni ottenute dalle scansioni delle vulnerabilità.	Non attivo
4	2	2	S	Verificare che i log registrino le attività dei sistemi di scanning delle vulnerabilità	In fase di sperimentazione portale wazuh
4	2	3	S	Verificare nei log la presenza di attacchi pregressi condotti contro target riconosciuto come vulnerabile.	In fase di sperimentazione portale wazuh
4	3	1	S	Eseguire le scansioni di vulnerabilità in modalità privilegiata, sia localmente, sia da remoto, utilizzando un account dedicato che non deve essere usato per nessun'altra attività di amministrazione.	Non attivo
4	3	2	S	Vincolare l'origine delle scansioni di vulnerabilità a specifiche macchine o indirizzi IP, assicurando che solo il personale autorizzato abbia accesso a tale interfaccia e la utilizzi propriamente.	In fase di sperimentazione portale wazuh
4	4	1	M	Assicurare che gli strumenti di scansione delle vulnerabilità utilizzati siano regolarmente aggiornati con tutte le più rilevanti vulnerabilità di sicurezza.	In fase di sperimentazione portale wazuh
4	4	2	S	Registrarsi ad un servizio che fornisca tempestivamente le informazioni sulle nuove minacce e vulnerabilità. Utilizzandole per aggiornare le attività di scansione	In fase di sperimentazione portale wazuh
4	5	1	M	Installare automaticamente le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni.	Non attivo
4	5	2	M	Assicurare l'aggiornamento dei sistemi separati dalla rete, in particolare di quelli air-gapped, adottando misure adeguate al	Non presenti

				loro livello di criticità.	
4	6	1	S	Verificare regolarmente che tutte le attività di scansione effettuate con gli account aventi privilegi di amministratore siano state eseguite secondo delle policy predefinite.	Non attivo
4	7	1	M	Verificare che le vulnerabilità emerse dalle scansioni siano state risolte sia per mezzo di patch, o implementando opportune contromisure oppure documentando e accettando un ragionevole rischio.	In fase di sperimentazione portale wazuh
4	7	2	S	Rivedere periodicamente l'accettazione dei rischi di vulnerabilità esistenti per determinare se misure più recenti o successive patch possono essere risolutive o se le condizioni sono cambiate, con la conseguente modifica del livello di rischio.	In fase di sperimentazione portale wazuh
4	8	1	M	Definire un piano di gestione dei rischi che tenga conto dei livelli di gravità delle vulnerabilità , del potenziale impatto e della tipologia degli apparati (e.g. server esposti, server interni, PdL, portatili, etc.).	Non attivo
4	8	2	M	Attribuire alle azioni per la risoluzione delle vulnerabilità un livello di priorità in base al rischio associato. In particolare applicare le patch per le vulnerabilità a partire da quelle più critiche.	Non attivo
4	9	1	S	Prevedere, in caso di nuove vulnerabilità, misure alternative se non sono immediatamente disponibili patch o se i tempi di distribuzione non sono compatibili con quelli fissati dall'organizzazione.	Non attivo
4	10	1	S	Valutare in un opportuno ambiente di test le patch dei prodotti non standard (es.: quelli sviluppati ad hoc) prima di installarle nei sistemi in esercizio.	Tutte le applicazioni installate sono standard di mercato diffusi

ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE

ABSC_ID			Livello	Descrizione	Modalità di implementazione
5	1	1	M	Limitare i privilegi di amministrazione ai soli utenti che abbiano le competenze adeguate e la necessità operativa di modificare la configurazione dei sistemi.	Parzialmente implementato nelle sedi in cui è presente un sistema di autenticazione a dominio
5	1	2	M	Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato.	Non attivo
5	1	3	S	Assegnare a ciascuna utenza amministrativa solo i privilegi necessari per svolgere le attività previste per essa.	Parzialmente implementato nelle sedi in cui è presente un sistema di autenticazione a dominio
5	1	4	A	Registrare le azioni compiute da un'utenza amministrativa e rilevare ogni anomalia di comportamento.	Non attivo
5	2	1	M	Mantenere l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata.	Non attivo
5	2	2	A	Gestire l'inventario delle utenze amministrative attraverso uno strumento automatico che segnali ogni variazione che intervenga.	Non attivo
5	3	1	M	Prima di collegare alla rete un nuovo dispositivo sostituire le credenziali dell'amministratore predefinito con valori coerenti con quelli delle utenze amministrative in uso.	Non attivo
5	4	1	S	Tracciare nei log l'aggiunta o la soppressione di un'utenza amministrativa.	Non attivo
5	4	2	S	Generare un'allerta quando viene aggiunta un'utenza amministrativa.	Non attivo

5	4	3	S	Generare un'allerta quando vengano aumentati i diritti di un'utenza amministrativa.	Non attivo
5	5	1	S	Tracciare nei log i tentativi falliti di accesso con un'utenza amministrativa.	Non attivo
5	6	1	A	Utilizzare sistemi di autenticazione a più fattori per tutti gli accessi amministrativi, inclusi gli accessi di amministrazione di dominio. L'autenticazione a più fattori può utilizzare diverse tecnologie, quali smart card, certificati digitali, one time password (OTP), token, biometria ed altri analoghi sistemi.	Non attivo – in fase di definizione con il nuovo appaltatore
5	7	1	M	Quando l'autenticazione a più fattori non è supportata, utilizzare per le utenze amministrative credenziali di elevata robustezza (e.g. almeno 14 caratteri).	Non attivo – in fase di definizione con il nuovo appaltatore
5	7	2	S	Impedire che per le utenze amministrative vengano utilizzate credenziali deboli.	Non attivo – in fase di definizione con il nuovo appaltatore
5	7	3	M	Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (password aging).	Non attivo – in fase di definizione con il nuovo appaltatore
5	7	4	M	Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history).	Non attivo – in fase di definizione con il nuovo appaltatore
5	7	5	S	Assicurare che dopo la modifica delle credenziali trascorra un sufficiente lasso di tempo per poterne effettuare una nuova.	Non attivo
5	7	6	S	Assicurare che le stesse credenziali amministrative non possano essere riutilizzate prima di sei mesi.	Non attivo
5	8	1	S	Non consentire l'accesso diretto ai sistemi con le utenze amministrative, obbligando gli amministratori ad accedere con un'utenza normale e successivamente eseguire come utente privilegiato i singoli comandi.	Non attivo
5	9	1	S	Per le operazioni che richiedono privilegi gli amministratori debbono utilizzare macchine dedicate, collocate su una rete	Non attivo

				logicamente dedicata, isolata rispetto a Internet. Tali macchine non possono essere utilizzate per altre attività.	
5	10	1	M	Assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali diverse.	Non attivo
5	10	2	M	Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona.	Non attivo – in fase di verifica con il nuovo appaltatore
5	10	3	M	Le utenze amministrative anonime, quali "root" di UNIX o "Administrator" di Windows, debbono essere utilizzate solo per le situazioni di emergenza e le relative credenziali debbono essere gestite in modo da assicurare l'imputabilità di chi ne fa uso.	Non attivo – in fase di verifica con il nuovo appaltatore
5	10	4	S	Evitare l'uso di utenze amministrative locali per le macchine quando sono disponibili utenze amministrative di livello più elevato (e.g. dominio).	Non attivo
5	11	1	M	Conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza.	Non attivo – in fase di verifica con il nuovo appaltatore
5	11	2	M	Se per l'autenticazione si utilizzano certificati digitali, garantire che le chiavi private siano adeguatamente protette.	Non attivo

ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE

ABSC_ID			Livello	Descrizione	Modalità di implementazione
8	1	1	M	Installare su tutti i sistemi connessi alla rete locale strumenti atti a rilevare la presenza e bloccare l'esecuzione di malware (antivirus locali). Tali strumenti sono mantenuti aggiornati in modo automatico.	Le pdl sono protette dalla soluzione SOPHOS Intercept X Essentials

8	1	2	M	Installare su tutti i dispositivi firewall ed IPS personali.	Le pdl sono protette dalla soluzione SOPHOS Intercept X Essentials
8	1	3	S	Gli eventi rilevati dagli strumenti sono inviati ad un repository centrale (syslog) dove sono stabilmente archiviati.	Le pdl sono protette dalla soluzione SOPHOS Intercept X Essentials
8	2	1	S	Tutti gli strumenti di cui in ABSC_8.1 sono monitorati e gestiti centralmente. Non è consentito agli utenti alterarne la configurazione.	Le pdl sono protette dalla soluzione SOPHOS Intercept X Essentials
8	2	2	S	È possibile forzare manualmente dalla console centrale l'aggiornamento dei sistemi anti-malware installati su ciascun dispositivo. La corretta esecuzione dell'aggiornamento è automaticamente verificata e riportata alla console centrale.	Non previsto dalla versione dell'ENDPOINT SOPHOS Intercept Essential
8	2	3	A	L'analisi dei potenziali malware è effettuata su di un'infrastruttura dedicata, eventualmente basata sul cloud.	Le pdl sono protette dalla soluzione SOPHOS Intercept X Essentials
8	3	1	M	Limitare l'uso di dispositivi esterni a quelli necessari per le attività aziendali.	Non previsto dalla versione dell'ENDPOINT SOPHOS Intercept Essential
8	3	2	A	Monitorare l'uso e i tentativi di utilizzo di dispositivi esterni.	Non previsto dalla versione dell'ENDPOINT SOPHOS Intercept Essential
8	4	1	S	Abilitare le funzioni atte a contrastare lo sfruttamento delle vulnerabilità, quali Data Execution Prevention (DEP), Address Space Layout Randomization (ASLR), virtualizzazione, confinamento, etc. disponibili nel software di base.	Non attivo
8	4	2	A	Installare strumenti aggiuntivi di contrasto allo sfruttamento delle vulnerabilità, ad esempio quelli forniti come opzione dai produttori di sistemi operativi.	In fase di sperimentazione portale wazuh
8	5	1	S	Usare strumenti di filtraggio che operano sull'intero flusso del traffico di rete per impedire che il codice malevolo raggiunga gli host.	Non attivo
8	5	2	A	Installare sistemi di analisi avanzata del software sospetto.	Non attivo
8	6	1	S	Monitorare, analizzare ed eventualmente bloccare gli accessi a	Le pdl sono protette dalla soluzione SOPHOS Intercept X Essentials

				indirizzi che abbiano una cattiva reputazione.	
8	7	1	M	Disattivare l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili.	Non previsto dalla versione dell'ENDPOINT SOPHOS Intercept Essential
8	7	2	M	Disattivare l'esecuzione automatica dei contenuti dinamici (e.g. macro) presenti nei file.	Non attivo
8	7	3	M	Disattivare l'apertura automatica dei messaggi di posta elettronica.	Non attivo
8	7	4	M	Disattivare l'anteprima automatica dei contenuti dei file.	Non attivo
8	8	1	M	Eseguire automaticamente una scansione anti-malware dei supporti rimuovibili al momento della loro connessione.	Le pdl sono protette dalla soluzione SOPHOS Intercept X Essentials
8	9	1	M	Filtrare il contenuto dei messaggi di posta prima che questi raggiungano la casella del destinatario, prevedendo anche l'impiego di strumenti antispam.	Non Attivo
8	9	2	M	Filtrare il contenuto del traffico web.	Le pdl sono protette dalla soluzione SOPHOS Intercept X Essentials
8	9	3	M	Bloccare nella posta elettronica e nel traffico web i file la cui tipologia non è strettamente necessaria per l'organizzazione ed è potenzialmente pericolosa (e.g. .cab).	Non Attivo
8	10	1	S	Utilizzare strumenti anti-malware che sfruttino, oltre alle firme, tecniche di rilevazione basate sulle anomalie di comportamento.	Le pdl sono protette dalla soluzione SOPHOS Intercept X Essentials
8	11	1	S	Implementare una procedura di risposta agli incidenti che preveda la trasmissione al provider di sicurezza dei campioni di software sospetto per la generazione di firme personalizzate.	Le pdl sono protette dalla soluzione SOPHOS Intercept X Essentials

ABSC 10 (CSC 10): COPIE DI SICUREZZA

ABSC_ID	Livello	Descrizione	Modalità di implementazione

10	1	1	M	Effettuare almeno settimanalmente una copia di sicurezza almeno delle informazioni strettamente necessarie per il completo ripristino del sistema.	Non previsto, le soluzioni in SAAS ci consentono di reinstallare o sostituire rapidamente una pdl
10	1	2	A	Per assicurare la capacità di recupero di un sistema dal proprio backup, le procedure di backup devono riguardare il sistema operativo, le applicazioni software e la parte dati.	Non previsto, le soluzioni in SAAS ci consentono di reinstallare o sostituire rapidamente una pdl
10	1	3	A	Effettuare backup multipli con strumenti diversi per contrastare possibili malfunzionamenti nella fase di restore.	Non Attivo – per il file server è attiva la soluzione office 365 ma attualmente non è coperta da backup
10	2	1	S	Verificare periodicamente l'utilizzabilità delle copie mediante ripristino di prova.	Non attivo
10	3	1	M	Assicurare la riservatezza delle informazioni contenute nelle copie di sicurezza mediante adeguata protezione fisica dei supporti ovvero mediante cifratura. La codifica effettuata prima della trasmissione consente la remotizzazione del backup anche nel cloud.	Non Attivo
10	4	1	M	Assicurarsi che i supporti contenenti almeno una delle copie non siano permanentemente accessibili dal sistema onde evitare che attacchi su questo possano coinvolgere anche tutte le sue copie di sicurezza.	Non Attivo – In fase di verifica con il nuovo appaltatore

ABSC 13 (CSC 13): PROTEZIONE DEI DATI

ABSC_ID			Livello	Descrizione	Modalità di implementazione
13	1	1	M	Effettuare un'analisi dei dati per individuare quelli con particolari requisiti di riservatezza (dati rilevanti) e segnatamente quelli ai quali va applicata la protezione crittografica	Non attivo

13	2	1	S	Utilizzare sistemi di cifratura per i dispositivi portatili e i sistemi che contengono informazioni rilevanti	Non attivo – in fase di valutazione soluzione alternativa di gestione endpoint con criptatura
13	3	1	A	Utilizzare sul perimetro della rete strumenti automatici per bloccare, limitare ovvero monitorare in maniera puntuale, sul traffico uscente dalla propria rete, l'impiego di crittografia non autorizzata o l'accesso a siti che consentano lo scambio e la potenziale esfiltrazione di informazioni.	Non Attivo
13	4	1	A	Effettuare periodiche scansioni, attraverso sistemi automatizzati, in grado di rilevare sui server la presenza di specifici "data pattern", significativi per l'Amministrazione, al fine di evidenziare l'esistenza di dati rilevanti in chiaro.	Non Attivo
13	5	1	A	Nel caso in cui non sia strettamente necessario l'utilizzo di dispositivi esterni, implementare sistemi/configurazioni che impediscano la scrittura di dati su tali supporti.	Non Attivo
13	5	2	A	Utilizzare strumenti software centralizzati atti a gestire il collegamento alle workstation/server dei soli dispositivi esterni autorizzati (in base a numero seriale o altre proprietà univoche) cifrando i relativi dati. Mantenere una lista aggiornata di tali dispositivi.	Non attivo
13	6	1	A	Implementare strumenti DLP (Data Loss Prevention) di rete per monitorare e controllare i flussi di dati all'interno della rete in maniera da evidenziare eventuali anomalie.	Non attivo
13	6	2	A	Qualsiasi anomalia rispetto al normale traffico di rete deve essere registrata anche per consentirne l'analisi off line.	Non attivo
13	7	1	A	Monitorare il traffico uscente rilevando le connessioni che usano la crittografia senza che ciò sia previsto.	Non attivo
13	8	1	M	Bloccare il traffico da e verso url presenti in una blacklist.	Non attivo
13	9	1	A	Assicurare che la copia di un file fatta in modo autorizzato	Non attivo

				mantenga le limitazioni di accesso della sorgente, ad esempio attraverso sistemi che implementino le regole di controllo degli accessi (e.g. Access Control List) anche quando i dati sono trasferiti al di fuori del loro repository.	

Rilevazione delle Misure di sicurezza e dell'ambiente SAAS NUVOLA Comuni di SISCOM SPA

Soluzione SAAS Conforme al catalogo ACN:	https://catalogocloud.acn.gov.it/service/143
ID Scheda:	**SA-143**
Ubicazione del server:	DataCenter Tim di Cesano Maderno (MI)
Tipologia di backup:	Backup notturno della VM retention di 10 gg, backup incrementale su sito secondario
Standard e certificazioni:	Standard di erogazione SiscCloud che viene rispettato per ogni servizio siscom. Certificazioni sul sistema di qualita' Iso9001, sistema di sicurezza informazioni : Iso27001 ed estensioni Iso27017 Iso27018 , Iso14001 su gestione ambientale

Aree protette
Po piemontese

CollinaPo

ENTE DI GESTIONE
DELLE AREE PROTETTE
DEL PO PIEMONTESE

MANUALE DELLA CONSERVAZIONE DOCUMENTALE DEL PROTOCOLLO INFORMATICO, DEI FLUSSI DOCUMENTALI E DEGLI ARCHIVI

Ai sensi delle linee guida Agid 2021–
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.

INDICE

SOMMARIO

Registro delle versioni

N°Ver	Data emissione	Codice/Nome documento
1	XXXXXX	MANUALE DI CONSERVAZIONE

1. SCOPO E AMBITO DEL DOCUMENTO

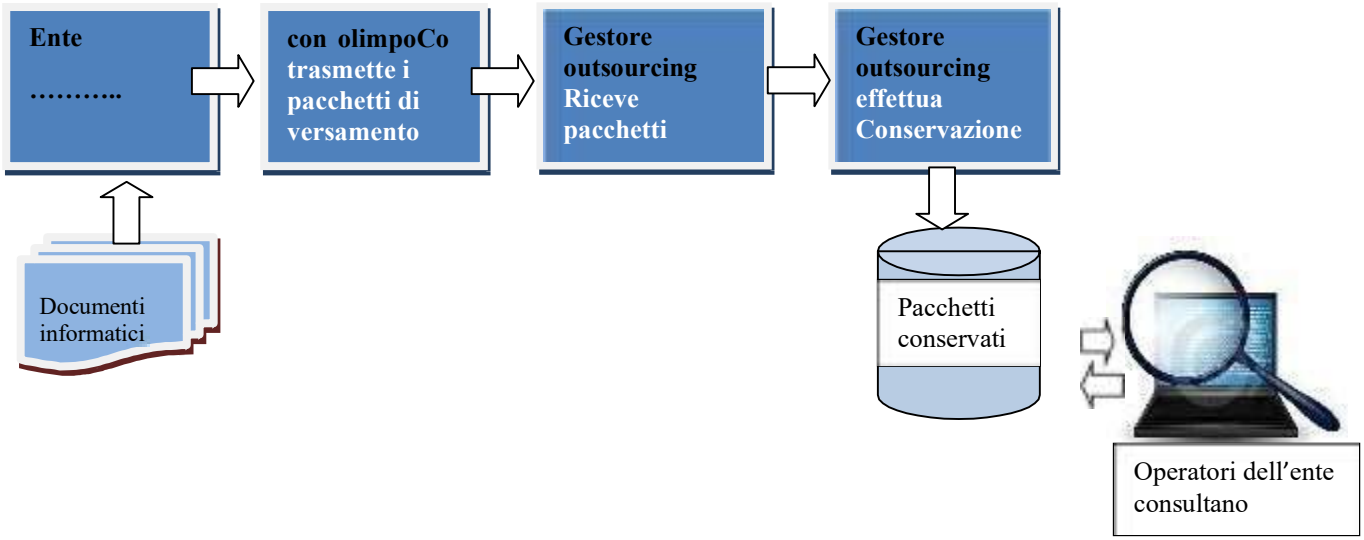
Il presente documento è il **Manuale di Conservazione** (di seguito per brevità chiamato anche "**Manuale**") di:

- **ENTE DI GESTIONE DEL SISTEMA DELLE AREE PROTETTE DEL PO PIEMONTESE**
- C.F.: 95000120063

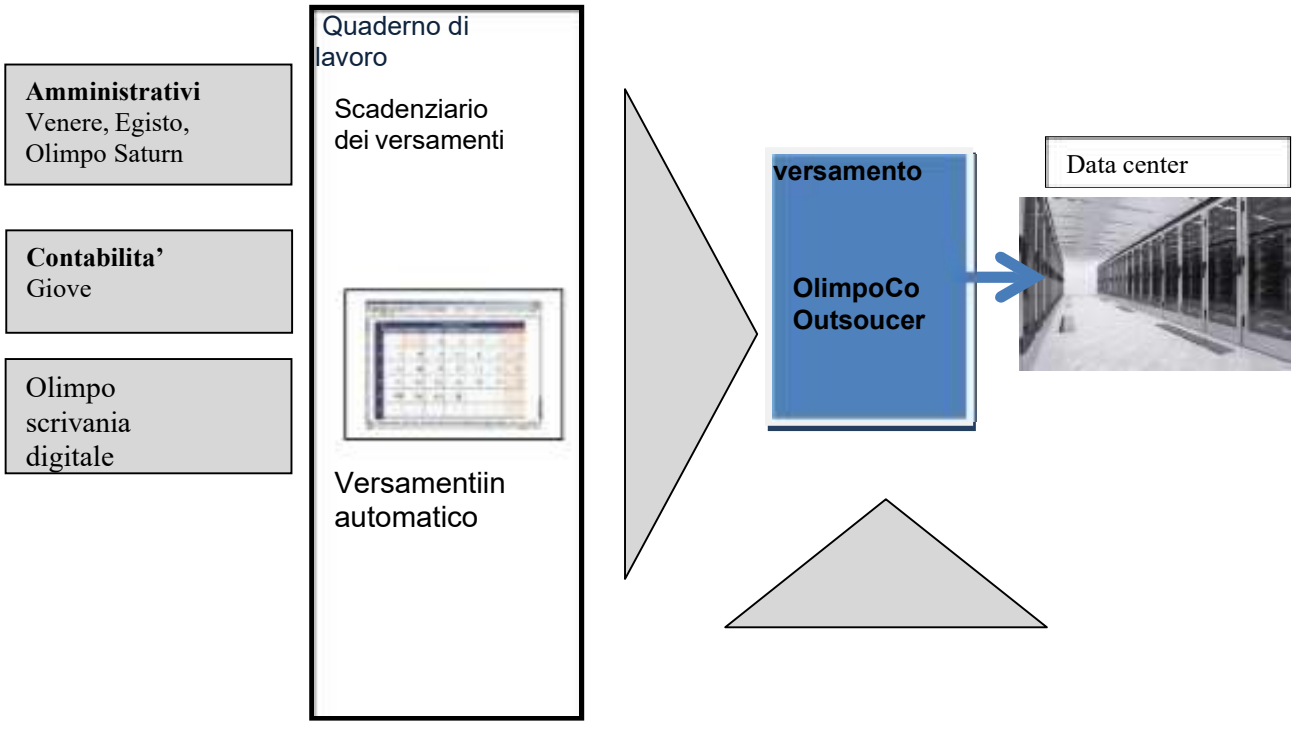
di seguito anche denominata Titolare, per tutti i documenti prodotti dalla stessa.

Il Titolare ha affidato il processo di conservazione digitale al conservatore SISCOM SpA in quanto il sistema di conservazione di quest'ultima assicura, tramite l'adozione di apposite regole, procedure e tecnologie, la conservazione dei dati e degli oggetti informatici in esso versati, garantendone le caratteristiche di autenticità, integrità, affidabilità, leggibilità e reperibilità.

La ditta SISCOM prevede la "gestione del ciclo della conservazione" dal reperimento dei documenti e la preparazione dei pacchetti di versamento fino alla conservazione a norma effettuata c/o outsourcer esterno accreditato.



Le componenti funzionali del sistema di conservazione della SISCOM SpA OlimpoCoOutsourcer sono in grado di assicurare il trattamento dell'intero ciclo di gestione degli oggetti conservati nell'ambito del processo di conservazione, attraverso il Conservatore garantendo al Titolare, al contempo, l'accesso agli oggetti conservati per il periodo prescritto dalla norma o concordato nel contratto sottoscritto con il Conservatore e ciò, indipendentemente dall'evolversi del contesto tecnologico.



Trattamento dei dati personali e degli oggetti digitali conservati

Ai sensi e per gli effetti dell'articolo 28 del Regolamento UE 2016/679, relativamente e limitatamente ai trattamenti riguardanti la conservazione degli oggetti digitali affidati in conservazione alla ditta SISCOM S.p.a. OlimpoCoOutsourcer, a partire dalla data di sottoscrizione del contratto di affidamento del servizio, il titolare dei suddetti oggetti digitali nomina SISCOM S.p.a. quale Responsabile esterno del trattamento dei dati. Tale nomina viene formalizzata con un apposito documento che contiene anche le politiche della ditta SISCOM S.p.a. in tema di privacy. La nomina a Responsabile esterno del trattamento dei dati avrà la medesima validità ed efficacia della durata del contratto sottoscritto con il Conservatore.

2. IL SISTEMA DI CONSERVAZIONE

Servizio di conservazione in outsourcing

Soggetto "outosourcer" che svolge il servizio di conservazione
La SISCOM SPA ha attivato una convenzione quadro con CONSERVATORI ACCREDITATI per lo svolgimento del servizio di conservazione ai clienti. Pertanto per il Servizio di Conservazione digitale, offerto si prevede l'affidamento ad outsourcer accreditato AGID che svolgera' il servizio di conservazione a norma in base al manuale di conservazione pubblicato su Agid. L'Outsourcer provvede alle operazioni di conservazione e di retenzione dei dati conservati.

SISCOM si fa carico delle procedure burocratiche per l'attivazione ufficiale dell'affidamento di questo servizioall'Outsourcer.

Esibizione dei documenti
L'outsourcer mette a disposizione una funzione di consultazione dei documenti processati a conservazione.
Accesso tramite login e password assegnati al cliente.
Funzioni di ricerca per chiavi valorizzate nei metadati forniti con i versamenti.

Interscambio dei documenti informatici tra Ente produttore e Outsourcer
Tramite il software OlimpoCoOutsourcer l'Ente trasmette i documenti informatici presenti su Olimpo/Egisto da sottoporre a procedimento di conservazione digitale. La trasmissione avviene tramite un "web service" programmato e collaudato siscom/OlimpoCoOutsourcer e sistema di conservazione dell'Ousourcer. Il protocollo di comunicazione e' stato definito tra Siscom ed outsourcer. Il sistema dell'outsourcer provvede a prendere in carico i pacchetti di versamento dei documenti informatici trasmessi e quindi a sottoporli a processo di conservazione per creare i pacchetti di archiviazione e di esibizione su data center certificato. In risposta viene comunicata una ricevuta di ricezione al produttore.

Il sistema di conservazione assicura, 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:

a) i documenti informatici e i documenti amministrativi informatici con i metadati ad essi associati;

b) 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, nel rispetto di quanto indicato per le Pubbliche Amministrazioni nell'articolo 67, comma 2, del DPR 445/200042 e art. 44, comma 1-bis, CAD;

c) gli archivi informatici con i metadati associati.

Il sistema di conservazione garantisce l'accesso all'oggetto conservato per il periodo previsto dal piano di conservazione del Titolare dell'oggetto della conservazione e dalla normativa vigente, o per un tempo superiore concordato tra le parti, indipendentemente dall'evoluzione del contesto tecnologico.

Gli oggetti della conservazione sono trattati dal sistema di conservazione in pacchetti informativi che si distinguono in: Pacchetti di Versamento, Pacchetti di Archiviazione, Pacchetti di Distribuzione.

3. RUOLI E RESPONSABILITA'

In sintesi, nel sistema di conservazione si possono identificare i seguenti ruoli fondamentali:

- Titolare dell'oggetto di conservazione;
- Produttore del PdV;
- Utente abilitato;
- Responsabile della Conservazione;
- Responsabile del Servizio di conservazione;
- Conservatore accreditato OlimpoCoOutsourcer

I ruoli e le responsabilità del sistema di conservazione sono descritti nel dettaglio nel Manuale del conservatore SISCOM S.p.a., al quale si rimanda.

Responsabile della conservazione

Il Responsabile della conservazione, sotto la propria responsabilità, affida alla ditta SISCOM S.p.a., il servizio di conservazione digitale dei documenti informatici, affidando le attività previste dal relativo contratto sottoscritto con il Conservatore.

Nello specifico, la ditta SISCOM S.p.a., ai fini dell'erogazione del servizio oggetto del Contratto, svolge le attività ad essa affidate attraverso il Conservatore accreditato OlimpoCoOutsourcer.

Lo spazio viene riservato per la conservazione su data center server certificato sulla sicurezza a norma Iso27001 dell'Outsourcer accreditato. Lo spazio previsto per il Vs Ente per questo affidamento e' di N. 4 GigaByte/anno

Di seguito sono riportati i dati identificativi dell'attuale Responsabile della Conservazione del Titolare e degli ulteriori soggetti che nel tempo hanno assunto tale ruolo:

Data inizio incarico	Data fine incarico	Nome e Cognome Responsabile di Conservazione	Cod.Fisc. Responsabile
31/03/2023		**SISCOM S.p.A. OlimpoCoOutsourcer**	01778000040

Conservatore

Soggetto che svolge attività di conservazione.

Di seguito sono riportati i dati di riferimento del conservatore:

Denominazione sociale: SISCOM **S.p.a.**

Sede legale in: Cervere CN, Centro Direzionale S.Rocco, Via Adua 4

Codice fiscale/P.IVA: 01778000040

N. Iscr. Reg. Imprese di Cuneo: 01778000040

PEC .....: siscom@siscom.eu

Sito web generale (informativo).....: www.siscom.eu

4. ALTRI DATI E INFORMAZIONI

In merito agli aspetti elencati di seguito si rimanda interamente o per dettagli al manuale del Conservatore SISCOM S.p.a. OlimpoCoOutsourcer, sempre disponibile sul sito istituzionale di quest'ultima e all'interno dell'applicativo del servizio di conservazione:

- i 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;
- struttura organizzativa comprensiva delle funzioni, delle responsabilità e degli obblighi dei diversi soggetti che intervengono nel processo di conservazione;
- descrizione delle tipologie degli oggetti digitali sottoposti a conservazione, comprensiva dell'indicazione dei formati gestiti, dei metadati da associare alle diverse tipologie di oggetti e delle eventuali eccezioni;
- descrizione delle modalità di presa in carico di uno o più pacchetti di versamento, comprensiva della predisposizione del rapporto di versamento;
- descrizione del processo di conservazione e del trattamento dei pacchetti di archiviazione;
- modalità di svolgimento del processo di esibizione e di esportazione dal sistema di conservazione con la produzione del pacchetto di distribuzione;
- descrizione del sistema di conservazione, comprensivo di tutte le componenti tecnologiche, fisiche e logiche, opportunamente documentate e delle procedure di gestione e di evoluzione delle medesime;
- descrizione delle procedure di monitoraggio della funzionalità del sistema di conservazione e delle verifiche sull'integrità degli archivi con l'evidenza delle soluzioni adottate in caso di anomalie;
- descrizione delle procedure per la produzione di duplicati o copie;
- tempi entro i quali le diverse tipologie di oggetti digitali devono essere trasferite in conservazione ed eventualmente scartate, qualora, nel caso delle Pubbliche Amministrazioni, non siano già indicati nel piano di conservazione allegato al manuale di gestione documentale;
- modalità con cui viene richiesta la presenza di un pubblico ufficiale, indicando anche quali sono i casi per i quali è previsto il suo intervento;
- normative in vigore nei luoghi dove sono conservati gli oggetti digitali.

ENTE DI GESTIONE DELLE AREE PROTETTE DEL PO PIEMONTESE

ESTRATTO DELLA SINTESI DEI MODELLI DI INTEROPERABILITÀ TRA SISTEMI DI CONSERVAZIONE

Allegato al documento "Manuale sulla formazione, gestione e conservazione dei documenti informatici"

Ai sensi delle linee guida Agid 2022

Il presente documento si pone l'obiettivo di individuare alcuni modelli di interoperabilità tra sistemi di conservazione partendo dalla definizione di un PdA interoperabile, in modo da garantire ai poli di conservazione lo scambio reciproco degli oggetti conservati, riducendo al minimo la perdita di informazioni

I modelli dei Pacchetti di Archiviazione

A questo punto si è in grado di descrivere e analizzare potenziali modelli di interoperabilità tra sistemi di conservazione, utilizzando lo standard e i criteri finora individuati.
I modelli di seguito elencati hanno una duplice funzione:
• descrivere una potenziale struttura e una semantica dei documenti amministrativi informatici all'interno del PdA;
• fornire un quadro comune per la rilevazione e la comprensione dei casi rinvenuti nella prassi.
Appare evidente che i modelli individuati non rappresentano e non possono rappresentare tutte le possibili soluzioni, ma forniscono una base utile per realizzare l'interoperabilità tra sistemi di conservazione.
I modelli di PdA sono individuati sulla base di quattro aspetti funzionali/organizzativi:
1. Il numero di UD che possono essere presenti all'interno di un PdA.
Quando il PDA coincide con una UD può essere necessaria una gestione diversa dal caso in cui il numero di UD contenute nel PdA sia più di una. Va anche detto che nella realtà potrebbero essere presenti casi in cui una UD è divisa in più PdA: tale casistica non è stata oggetto di analisi in quanto ritenuta di difficile gestione in un ambito di interoperabilità tra sistemi di conservazione.
2. L'organizzazione dell'UD e dei suoi metadati.
Una UD, che può essere composta da più documenti, può essere descritta con un unico file di metadati oppure ciascun documento, facente parte dell'UD, potrebbe disporre di un proprio file di metadati. Entrambe le possibilità sono coerenti con quanto previsto dall'allegato 5 alle LLGG.
3. L'elemento di *MoreInfo* dell'indice utilizzato per la memorizzazione dei metadati.
Come già segnalato, i metadati possono essere presenti nell'elemento *PVolume*, oppure *FileGroup* e *File*, con diverse ricadute funzionali.
4. L'articolazione dell'UD a livello di contenuto (e non di metadati).
L'UD può essere variamente strutturata nell'ambito del PdA. È possibile che l'elemento *FileGroup* contenga l'intera UD oppure, sempre nell'elemento *FileGroup* potrebbe essere descritto un singolo documento e quest'ultimo, in tal caso, verrebbe articolato in più elementi *File*.
Dalle possibili combinazioni dei quattro aspetti funzionali/organizzativi ora elencati, sono stati individuati sette diversi modelli possibili per l'interoperabilità tra i sistemi di conservazione.

Sintesi dell'analisi dei risultati

Nell'analisi dei modelli e nella successiva verifica rispetto alla prassi è emersa l'importanza di vincoli e regole che diano una logica coerente alla struttura delle informazioni e del pacchetto.
Si riportano tutte le precondizioni emerse:
• il PdA può contenere una o più UD.
• L'UD è composta da uno o più Documenti che a loro volta si distinguono in Documento principale (obbligatorio e sempre presente), Allegati, Annessi e Annotazioni. A sua volta il singolo Documento può essere costituito da uno o più componenti (file)[7].
• L'UD deve essere integralmente contenuta nel PdA. Non possono sussistere, quindi, UD suddivise in più PdA. Potrebbe essere possibile, invece, il caso di una UD versata nel sistema di conservazione in più PdV[8], così come è possibile che un PdV origini più PdA.
• I metadati descrittivi sono composti da due parti: una, obbligatoria, fa riferimento al set di

metadati dell'Allegato 5 alle LLGG, eventualmente integrato con metadati aggiuntivi legati a specifiche tipologie documentarie e l'altra, opzionale, che prevede i metadati descrittivi propri del sistema di conservazione. Il modello di interoperabilità si riferisce esclusivamente al primo subset.

• I metadati previsti dall'Allegato 5 alle LLGG possono essere riferiti all'intera UD o ai singoli Documenti. Non è ammessa la presenza di tali metadati sia a livello di UD che a livello di Documento.

• Il PdA può contenere anche le evidenze di conservazione, cioè documenti ricevuti e prodotti nel corso del processo di conservazione, in genere riconducibili alle operazioni di acquisizione dei PdV nel Sistema di conservazione.

• Devono essere presenti set di metadati informativi aggiuntivi finalizzati a indicare il modello applicabile e altre informazioni necessarie a garantire la massima interoperabilità.

Inoltre, per consentire la corretta rappresentazione dell'ordinamento dell'archivio nel sistema di conservazione è consigliabile che, qualora il PdA contenga più UD, tali UD costituiscano un'aggregazione o parte di essa, in modo che tali PdA possano poi essere gestiti più agevolmente nel PdA dell'aggregazione.

Infine, questo documento si è concentrato sull'interoperabilità dei PdA delle UD, tuttavia sembra doveroso segnalare alcuni aspetti generali che impattano sulle tematiche di interoperabilità tra sistemi di conservazione quali il numero di PdA costituenti l'intero archivio da trasferire e il rapporto tra PdA e le aggregazioni.

Si ipotizza per quel che riguarda i modelli di organizzazione delle UD e i modelli di organizzazione delle "Evidenze di Conservazione" di utilizzare l'elemento *Label* come da tabella sottostante.

	Pvolume - Label	Pvolume - Description	PvolumeGroup - Label	PvolumeGroup - Description	FileGroup - Label	FileGroup - Description
Modello 1	UD Singola	Descrizione del modello utilizzato	Denominazione Univoca Aggregazione Documentale	Descrizione Serie Documentale	Prove di conservazione, Rapporto di Versamento, UD, Sottoparte di UD	Descrizione di dettaglio
Modello 2	UD Singola	Descrizione del modello utilizzato	Denominazione Univoca Aggregazione Documentale	Descrizione Serie Documentale	Prove di conservazione, Rapporto di Versamento, UD, Sottoparte di UD	Descrizione di dettaglio
Modello 3	UD Singola	Descrizione del modello utilizzato	Denominazione Univoca Aggregazione Documentale	Descrizione Serie Documentale	Prove di conservazione, Rapporto di Versamento, UD, Sottoparte di UD	Descrizione di dettaglio
Modello 4	UD Singola	Descrizione del modello utilizzato	Denominazione Univoca Aggregazione Documentale	Descrizione Serie Documentale	Prove di conservazione, Rapporto di Versamento, UD, Sottoparte di UD	Descrizione di dettaglio

Modello 5	UD Singola	Descrizione del modello utilizzato	Denominazione Univoca Aggregazione Documentale	Descrizione Serie Documentale	Prove di conservazione, Rapporto di Versamento, UD	Descrizione di dettaglio
Modello 6	UD Multipla	Descrizione del modello utilizzato	Denominazione Univoca Aggregazione Documentale	Descrizione Serie Documentale	Prove di conservazione, Rapporto di Versamento, UD	Descrizione di dettaglio
Modello 7	UD Multipla	Descrizione del modello utilizzato	Denominazione Univoca Aggregazione Documentale	Descrizione Serie Documentale	Prove di conservazione, Rapporto di Versamento, UD	Descrizione di dettaglio

Nel dettaglio la proposta analizzata elemento per elemento si struttura come segue.

PVOLUME

Uso: fornire indicazioni sul modello d'interoperabilità adottato

- **Label** = stringa identificativa della tipologia di modello con la funzione di individuare se contiene 1 o n unità documentarie;
- **Description** = descrizione più dettagliata del modello impiegato;
- **MoreInfo** = informazioni più dettagliate sul volume (es. numero UD, data di apertura, data di chiusura …).

PVOLUMEGROUP

Uso: fornire indicazioni sull'aggregazione

- **Label** = stringa identificativa della tipologia di aggregazione (es. serie delibere, messaggi di posta elettronica ecc.);
- **Description** = descrizione più dettagliata del particolare insieme contenuto (es. delibere della Giunta regionale adottate nella seduta del 15/10/2022, messaggi di posta elettronica certificata pervenuti in data 01/11/2022 ecc.).

FILEGROUP

Per i modelli che prevedono il trattamento di unità documentarie raggruppate all'interno dell'elemento *FileGroup*, il FileGroup viene usato per raggruppare i seguenti tipi di insiemi di file: prove di conservazione, rapporto di versamento, unità documentaria.

Per i modelli che prevedono il trattamento di unità documentarie non raggruppate all'interno dell'elemento *FileGroup*, sono previsti i seguenti tipi di insiemi di file: prove di conservazione, rapporto di versamento, unità documentaria o documento.

- **Label** = stringa identificativa del raggruppamento (es. prove di conservazione, rapporto di versamento, unità documentaria);
- **Description** = descrizione più dettagliata del particolare raggruppamento.

Si ritiene utile una futura aggiunta degli elementi *Label* e *Description* anche all'elemento *File* al fine di andarne a identificare la natura all'interno dell'unità documentaria che potrebbe essere molteplice, come ad esempio: documento principale, allegato al documento principale, metadati.

RELATION

La parte *Relation* ai fini dell'interoperabilità può servire per mettere in relazione le prove di conservazione con le unità documentarie cui fanno riferimento.