REGIONE AUTÒNOMA DE SARDIGNA
REGIONE AUTONOMA DELLA SARDEGNA

AGENTZIA REGIONALE PRO S'AMPARU DE S'AMBIENTE DE SARDIGNA
AGENZIA REGIONALE PER LA PROTEZIONE DELL'AMBIENTE DELLA SARDEGNA

ARPAS

MANUALE DI GESTIONE DOCUMENTALE

(Aggiornamento Ottobre 2023)

SOMMARIO

ALLEGATI

Allegato 1. Organigramma con indicazione delle UUOO
Allegato 2. Provvedimenti di nomina del Responsabile della gestione documentale e della conservazione
Allegato 3. Manuale software di gestione documentale
Allegato 4. Formato dei documenti degli uffici
Allegato 5. Guida alla formazione del documento accessibile
Allegato 6. Titolario e Piano di fascicolazione
Allegato 7. Manuale tecnico e Guida per la fascicolazione dei documenti
Allegato 8. Informativa sulla classificazione e fascicolazione
Allegato 9. Manuale di conservazione
Allegato 10. Circolare annullamento registrazione di protocollo
Allegato 11. Piano di conservazione/massimario di scarto (da predisporre)
Allegato 12. Circolare protocollazione documenti riservati
Allegato 13. Modello di registro di emergenza
Allegato 14. Indicazioni operative registrazione documenti di dimensioni elevate
Allegato 15. Sicurezza dei dati – Servizi SaaS PA Digitale (confidenziale)
Allegato 16. Linee guida per la creazione e l'aggiornamento delle anagrafiche corrispondenti
Allegato 17. Utenti: Profili e abilitazioni di accesso

PARTE PRIMA – DISPOSIZIONI PRELIMINARI

1. Riferimenti normativi

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

Le Linee guida, entrate in vigore dal giorno successivo alla data di pubblicazione, divengono applicabili, come da recente modifica, a partire dal 1° gennaio 2022.

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

1) Glossario dei termini e degli acronimi;
2) Formati di file e riversamento;
3) Certificazione di processo;
4) Standard e specifiche tecniche;

5) Metadati;
6) Comunicazione tra AOO di Documenti Amministrativi Protocollati, che sostituisce la circolare 60/2013 dell'AgID.

Ulteriori norme rilevanti ai fini della gestione documentale sono:

- le disposizioni in materia di formazione dei documenti informatici, anche di natura amministrativa, e di digitalizzazione dell'attività amministrativa di cui al d.lgs. 7 marzo 2005, n. 82 "*Codice dell'Amministrazione Digitale*" (di seguito anche solo "CAD")
- le disposizioni in materia di documentazione amministrativa di cui al D.P.R. 28 dicembre 2000, n. 445 *"Disposizioni legislative in materia di documentazione amministrativa"* (di seguito anche solo "TUDA");
- le norme sul procedimento amministrativo di cui alla l. 7 agosto 1990, n. 241 "*Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi*";
- le disposizioni sulla trasparenza di cui al d.lgs. 14 marzo 2013, n. 33 "*Riordino della disciplina riguardante gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni"*;
- le disposizioni in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno di cui al Regolamento (UE) 2014/910 del Parlamento europeo e del Consiglio del 24 luglio 2014 (Regolamento "eIDAS");
- le disposizioni sulla tutela della riservatezza dei dati personali di cui al regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 *"Regolamento generale sulla protezione dei dati"* ("GDPR") e d.lgs. 30 giugno 2003 n. 196 "*Codice in materia di protezione dei dati personali*".

2. Finalità, contenuti e metodologia del documento

Il presente Manuale, ai sensi del paragrafo 3.5. delle Linee guida, descrive il sistema di gestione informatica dei documenti dell'Agenzia Regionale per la Protezione dell'Ambiente della Sardegna (d'ora in avanti anche solo "ARPAS" o "Agenzia") e fornisce le istruzioni per la formazione dei documenti informatici, per il corretto funzionamento del servizio per la tenuta del protocollo informatico, per la gestione dei flussi documentali e degli archivi, ivi compresa la conservazione dei documenti informatici.

Il Manuale è un documento interno di contenuto sia organizzativo che operativo, utile quale strumento di supporto ai processi decisionali e operativi e, pertanto, è destinato alla più ampia diffusione presso tutto il personale dell'ente.

Con la pubblicazione nella sezione "Amministrazione Trasparente" del sito internet istituzionale (sottosezione "Atti Generali"), il Manuale è reso noto anche esternamente

all'ente. In quest'ottica, il Manuale costituisce altresì un documento pubblico funzionale al perseguimento del principio di trasparenza dell'azione amministrativa.

3. Approvazione e modalità di aggiornamento del Manuale

Il presente Manuale e i suoi allegati sono approvati con determina del Direttore Generale, su proposta del Responsabile della gestione documentale e della conservazione, d'intesa con il Responsabile della Transizione Digitale dell'Agenzia, successivamente all'acquisizione del parere del Responsabile della Protezione dei Dati Personali, così come previsto dal punto 3.4 delle linee Guida Agid.

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

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

PARTE SECONDA – ORGANIZZAZIONE

4. Area organizzativa omogenea e Unità Organizzative

ARPAS si configura come un'unica Area Organizzativa Omogenea (AOO) denominata "Agenzia Regionale per la Protezione dell'Ambiente della Sardegna" (codice univoco: A059266). L'AOO e gli indirizzi di posta elettronica a essa associati sono indicati nell'Indice PA.
Le Unità Operative (UUOO) che afferiscono alla AOO sono riportate nell'Allegato 1 (Organigramma e UUOO), che potrà essere oggetto di modifiche e integrazioni per effetto di successivi interventi sulla struttura organizzativa dell'Agenzia. Le UUOO sono individuate in modo da rispecchiare l'organigramma dell'ente.

5. Responsabile della gestione documentale e vicari

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

Il Responsabile della gestione documentale dell'Agenzia è stato individuato con determinazione D.G. n. 203/2023, nella persona dell'Ing. Giampiero Mugheddu, già Direttore del Servizio Affari Generali, altresì individuato quale Responsabile della conservazione con det. D.G. n. 1850/2022. In caso di vacanza o assenza, il vicario del Responsabile della gestione documentale è stato individuato nella persona dell'Ing. Marcello Atzeni, mentre il vicario del Responsabile della Conservazione è il dott. Carmine Sau (Allegato 2 - Provvedimenti di nomina).

I compiti del Responsabile della gestione documentale (d'ora in avanti anche solo "Responsabile") sono definiti nelle Linee guida. In particolare, il Responsabile:

a) è preposto, ai sensi dell'art. 61 TUDA, al servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi della AOO unica dell'Agenzia;
b) provvede, d'intesa con il Responsabile per la Transizione Digitale (RTD), previo parere del Responsabile per la Protezione dei Dati personali (RPD), alla predisposizione e al costante aggiornamento del presente Manuale e dei relativi allegati;
c) monitora i processi e le attività che governano le fasi di formazione, gestione e versamento in conservazione dei documenti informatici;

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

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

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

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

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

Il Responsabile della gestione documentale opera d'intesa con il Responsabile della Transizione Digitale (RTD) dell'Agenzia, individuato nella figura del Direttore del Servizio Sistema informativo e informatico dell'Agenzia.

6. Sistema informatico di gestione documentale di ARPAS

Il Sistema informatico di gestione documentale di ARPAS si basa sulla soluzione SaaS, qualificata Agid, *Urbi Smart* della PA Digitale S.p.A., comprendente una suite di applicativi, integrati tra loro, che consentono la gestione del protocollo informatico, la formazione e gestione di atti amministrativi, contratti e altri documenti, nonché la pubblicazione degli stessi nell'albo pretorio online e nella sezione "Amministrazione trasparente" del sito web istituzionale.

La suite Urbi Smart è nativamente integrata con il sistema di conservazione a norma della medesima società, denominato CDAN – Conservazione Digitale a Norma, che garantisce l'invio automatico in conservazione di tutte le registrazioni di protocollo e dei fascicoli chiusi.

La puntuale descrizione delle componenti e delle funzionalità del software è contenuta nei manuali operativi di gestione del software in uso.

Il Manuale del sistema in uso costituisce l'allegato n. 3.

7. Abilitazioni di accesso

Le abilitazioni di accesso degli utenti alle componenti del Sistema informatico di gestione documentale dell'Agenzia sono assegnate personalmente a ciascun dipendente dal Responsabile della gestione documentale, su indicazione del dirigente preposto all'UO in cui è inquadrato il dipendente. A ciascun utente del Sistema,

pertanto, sono attribuite specifiche funzioni, diversificate in ragione dell'appartenenza a una determinata struttura dell'organizzazione e degli specifici ruoli e compiti ad esso attribuiti.

Quanto sopra anche nel caso di nuove assunzioni presso l'Agenzia o di trasferimenti interni presso altre strutture Agenziali, dove i profili sono richiesti dal Dirigente, in base alle classi di abilitazione disponibili, mediante procedura telematica interna di Help Desk che veicola la richiesta al Responsabile della gestione documentale per opportuna valutazione e autorizzazione.

I profili di accesso, con le relative abilitazioni, sono riportati nell'allegato 17.

In via eccezionale e residuale, su richiesta del Dirigente, ad utenti appartenenti ad uno specifico profilo possono essere assegnati dei permessi aggiuntivi per svolgere determinate funzioni all'interno del sistema documentale.

8. Utenti delegati alle attività di protocollazione

I dipendenti a cui è assegnata un'utenza "Operatore" sul Sistema informatico di gestione documentale dell'Agenzia sono abilitati alla protocollazione informatica dei documenti interni ed in uscita.

La protocollazione dei documenti informatici in entrata, invece, è affidata ad un ristretto numero di utenti con specifiche abilitazioni:

- al Responsabile della gestione documentale e agli operatori del Servizio Affari Generali a ciò autorizzati è attribuita l'abilitazione alla protocollazione in entrata di tutti i documenti informatici acquisiti dall'Agenzia;
- nell'ambito di ciascuna direzione o dipartimento, inoltre, sono individuati uno o più operatori a cui è attribuita l'abilitazione alla protocollazione in entrata di tutti i documenti informatici pervenuti o assegnati alla UO di appartenenza. Le utenze abilitate alla protocollazione in entrata sono assegnate dal Responsabile della gestione documentale su richiesta del dirigente preposto all'UO di appartenenza dell'operatore.

Il responsabile della gestione documentale cura il costante aggiornamento dell'elenco dei dipendenti abilitati alla protocollazione e delle relative specifiche.

PARTE TERZA – FORMAZIONE DEI DOCUMENTI

Sezione prima – Modalità di formazione

9. Modalità di formazione dei documenti informatici

Tutti i documenti di ARPAS sono formati in originale come documenti informatici, secondo le modalità individuate nella presente Parte del Manuale.

I documenti informatici di ARPAS sono formati mediante una delle seguenti modalità:

a) creazione e redazione tramite l'utilizzo di strumenti di software o servizi cloud qualificati (ad esempio, mediante programmi di scrittura delle suite *Microsoft Office* o *Libre Office*, o mediante l'utilizzo delle funzioni dei sistemi di gestione documentale);
b) acquisizione:
   - della copia per immagine di un documento analogico su supporto informatico (ad esempio, mediante scansione di documento cartaceo);
   - della copia informatica di un documento analogico (ad esempio, acquisizione del documento tramite lettore OCR);
   - del duplicato di un documento informatico per via telematica o da supporto informatico (ad esempio, mediante download da posta elettronica o da chiave usb);
c) memorizzazione su supporto informatico delle informazioni risultanti da transazioni o processi informatici, oppure delle informazioni risultanti dall'acquisizione telematica di dati attraverso moduli o formulari resi disponibili all'utente (ad esempio, memorizzazione dei dati immessi in un *form* reso disponibile online agli utenti);
d) generazione o raggruppamento anche in via automatica di un insieme di dati o registrazioni secondo una struttura logica predeterminata e memorizzata in forma statica (ad esempio, generazione del registro di protocollo giornaliero).

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

9.1. Creazione e redazione tramite software di documenti informatici

Gli uffici dell'Agenzia dispongono dei seguenti strumenti software per la creazione dei documenti informatici mediante redazione:

- programmi della suite *Microsoft Office: Word, Excel, Access, Powerpoint, ecc.;*
- software suite Microsoft Office 365 erogati in modalità *SaaS*;

- altri strumenti individuati dal Responsabile della Transizione Digitale.

Il testo del documento informatico creato dagli uffici dell'Agenzia deve essere redatto utilizzando esclusivamente il font indicato dall'Agenzia con formale comunicazione.

Elementi essenziali del documento amministrativo informatico

Ogni documento amministrativo informatico creato e redatto dall'Agenzia deve recare obbligatoriamente i seguenti elementi:

1. denominazione dell'Amministrazione;
2. autore e ufficio responsabile;
3. numero e data di protocollo o di registrazione (se soggetto a registrazione particolare);
4. oggetto del documento;
5. riferimenti a procedimento o fascicolo;
6. sottoscrizione;
7. data e luogo;
8. numeri di pagina;
9. indicazione degli allegati (se presenti);
10. identificazione e dati dei destinatari (se si tratta di documento in uscita);
11. dati dell'Amministrazione (compresi indirizzo e recapiti, se si tratta di documento in uscita);
12. mezzo di spedizione (se documento in uscita).

Scelta del formato e modalità di sottoscrizione

Il formato del documento informatico creato dall'Agenzia viene scelto tra quelli indicati dall'Agenzia e secondo i criteri dalla stessa stabiliti (Allegato 4 – Formato Documenti Uffici). Eventuali formati differenti possono essere utilizzati in relazione a specifiche e comprovate esigenze.

Il formato del documento informatico, se diverso da quelli indicati nel citato allegato per esigenze specifiche, deve essere individuato tra quelli previsti nell'Allegato 2 alle Linee guida dell'AgID.

Le versioni di lavoro del documento, precedenti alla versione definitiva (bozze, minute, ecc.), possono essere salvate in un formato che ne consente la modificabilità (ad esempio .docx o .odt). La versione definitiva del documento, invece, è sempre preferibile sia in formato PDF.

In base a quanto sopra detto, una volta giunto alla sua versione definitiva e prima della sottoscrizione, il documento informatico è convertito in formato PDF. I documenti di maggiore rilevanza giuridico-amministrativa (ad esempio, gli atti del Direttore Generale, i contratti, le determine a contenuto provvedimentale, ecc.), prima della firma, devono essere convertiti in formato PDF/A (PDF non modificabile). I documenti in formato PDF e PDF/A sono sottoscritti con firma PADES.

Nel caso il documento definitivo assuma un formato diverso dal PDF, la sottoscrizione avviene con firma CADES (P7M).

9.2. Acquisizione di documenti informatici

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

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

b) acquisizione della copia per immagine su supporto informatico di un documento analogico (ciò avviene, ad esempio, quando si effettua la scansione di un documento cartaceo, memorizzandolo in un formato digitale);

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

In caso di acquisizione di copia informatica del documento originale (analogico o informatico), quando occorre assicurarne l'efficacia giuridico-probatoria, è necessario attestare la conformità della copia all'originale da cui è estratta, con le modalità indicate nelle disposizioni successive.

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

9.3. Copie per immagine di documenti analogici

La copia per immagine su supporto informatico di un documento analogico viene prodotta mediante processi e strumenti che assicurino che il documento informatico abbia contenuto e forma identici a quelli del documento analogico da cui è tratto, previo raffronto dei documenti.

Al fine di assicurare la medesima efficacia giuridico-probatoria riconosciuta al documento analogico originale, il funzionario a tale scopo delegato, che agisce in veste di pubblico ufficiale, deve apporre sulla copia informatica del documento, quale risultante dal processo di scansione, l'attestazione di conformità all'originale da cui essa è stata estratta. Il funzionario, quindi, dovrà apporre la propria firma digitale (o altra tipologia di firma forte) o il sigillo elettronico qualificato dell'ufficio, previa iscrizione sul documento (a margine o in calce) o in foglio elettronico a esso congiunto della seguente dicitura:

"*Io sottoscritto/a* [nome e cognome – nome ente e ufficio], *ai sensi dell'art. 22, comma 2, d.lgs. n. 82/2005, attesto che la presente copia per immagine è conforme in ogni sua parte al documento originale analogico dal quale è stata estratta.* [indicazione di data e luogo]."

Nel caso sia necessario attestare la conformità all'originale di più copie per immagine da versare in conservazione, in alternativa alla procedura sopradescritta, il funzionario delegato, al fine di attestare la conformità delle copie ai documenti originali, una volta effettuato il raffronto, potrà sottoscrivere un'unica attestazione di conformità, su foglio separato ma collegato alle copie tramite apposizione dell'impronta *hash*, precisando gli elementi identificativi di ciascun documento originale scansionato.

9.4. 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 (così avviene, ad esempio, quando si duplica un documento trasferendolo dall'hard disk del proprio personal computer a un dispositivo di archiviazione esterno quale una chiave usb). Tale modalità di formazione della copia del documento informatico non richiede alcuna attestazione di conformità all'originale, perché vi è perfetta coincidenza tra le due evidenze informatiche.

La copia di un documento informatico, invece, 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 in formato PDF. in un documento in diverso formato, ad esempio .docx). Tale operazione è altrimenti detta riversamento da un formato digitale verso un altro. Affinché la copia conservi la medesima efficacia giuridico-probatoria del documento informatico originale, è necessario attestarne la conformità all'originale. Come per le copie per immagine, dunque, il funzionario, che agisce in veste di pubblico ufficiale, dovrà apporre la propria firma digitale (o altra tipologia di firma forte) o il sigillo elettronico qualificato dell'ufficio, previa iscrizione sul documento (a margine o in calce) o in foglio elettronico a esso congiunto della seguente dicitura:

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

9.5. Soggetti delegati ad attestare la conformità delle copie

Ciascun Dirigente può attestare la conformità delle copie di documenti originali formati o acquisiti dall'Agenzia. In aggiunta, altro personale indicato dal responsabile della gestione documentale, di concerto con il Dirigente competente, può essere delegato ad attestare la conformità delle copie ai documenti originali formati o acquisiti nell'ambito della propria struttura di appartenenza.

9.6. Formazione di registri e repertori

I registri e repertori tenuti dall'Agenzia, ivi compreso il registro giornaliero di protocollo e il repertorio contratti, sono formati mediante la generazione/raggruppamento in via automatica e memorizzazione in forma statica dell'insieme delle registrazioni effettuate dal sistema di gestione documentale.

Sezione seconda – Disposizioni comuni a tutte le modalità di formazione

10. Dispositivi di firma elettronica

ARPAS garantisce che tutti i dipendenti e i titolari di cariche che firmano documenti, per conto dell'Agenzia, siano dotati di dispositivi di firma elettronica. A tal fine, il Sistema di gestione documentale in dotazione all'Agenzia consente ai dipendenti in possesso di profilo utente l'apposizione della firma digitale, secondo le indicazioni fornite dal competente Servizio Arpas.

L'utilizzo del dispositivo di firma è strettamente personale e riconducibile al suo titolare. Pertanto, il dispositivo e/o le credenziali non devono essere ceduti, né devono essere diffuse le chiavi dei certificati.

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

Nel caso dei dispositivi di firma rilasciati dall'Agenzia (Firma remota), quando il proprio certificato è prossimo alla scadenza, il titolare ne dà avviso al Responsabile del Servizio sistemi informativi, affinché provveda al rinnovo dello stesso attraverso il fornitore selezionato.

In generale, al fine di costituire un riferimento temporale giuridicamente valido tale da attestare che la firma sia stata apposta in un momento in cui il certificato era valido sono possibili le seguenti attività sul documento firmato:

- apposizione di marca temporale (attualmente non in uso);
- apposizione della segnatura di protocollo;
- versamento in conservazione.

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

11. Identificazione univoca del documento informatico

Ogni documento informatico deve essere identificato in modo univoco e persistente.

L'identificazione univoca dei documenti è effettuata con l'associazione al documento dell'impronta digitale o crittografica (*hash)*. Per i documenti soggetti a registrazione di protocollo, l'associazione è effettuata tramite le apposite funzioni della componente Sistema di protocollo informatico del Sistema di gestione documentale. Per i documenti non protocollati, l'associazione è effettuata tramite le apposite funzioni degli strumenti software in uso per la formazione degli atti. In ogni caso l'impronta crittografica deve essere basata su una funzione di hash conforme alle tipologie di algoritmi previste nell'allegato 6 alle Linee guida (cfr. p. 2.2, tab. 1).

12. Associazione degli allegati al documento principale

Gli allegati sono congiunti in modo univoco al documento informatico principale tramite l'associazione tra le impronte hash effettuata dal Sistema di gestione documentale in dotazione all'Agenzia.

Al documento principale, inoltre, devono essere associati i seguenti metadati:

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

A ciascun allegato, invece, deve essere associato il metadato identificativo del documento principale (IdDoc).

13. Accessibilità del documento informatico

Per garantire l'accessibilità dei documenti informatici ai soggetti portatori di disabilità, anche ai fini della pubblicazione e dell'accesso documentale, i soggetti responsabili della formazione del documento seguono le indicazioni contenute nella "Guida pratica per la creazione di un documento accessibile" di cui all'allegato 5 (guida al documento informatico accessibile) al presente Manuale.

14. Metadati del documento informatico

Al documento informatico e al documento amministrativo informatico sono associati i metadati obbligatori previsti dall'Allegato 5 alle Linee guida dell'AgID. Ulteriori metadati facoltativi sono associati secondo le indicazioni fornite dal Servizio Informatico dell'Agenzia.

I metadati sono associati prima che il documento informatico acquisisca le caratteristiche di immodificabilità e integrità, dunque prima della sottoscrizione, della memorizzazione nel sistema o del versamento in conservazione.

15. Immodificabilità e integrità del documento informatico

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

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

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

- per i documenti di cui è richiesta la sottoscrizione, dall'apposizione di una firma elettronica qualificata, di una firma digitale, di un sigillo elettronico qualificato o di una firma elettronica avanzata;
- per i documenti di cui non è richiesta la sottoscrizione, dalla memorizzazione nel sistema di gestione documentale, purché sia garantito il rispetto delle misure di sicurezza previste (cfr. Parte sesta del presente Manuale);
- per tutte le tipologie documentali, dal versamento nel sistema di conservazione.

In ogni caso, il versamento nel sistema di conservazione è il metodo che offre le maggiori garanzie di immodificabilità e integrità dei documenti informatici nel tempo. Pertanto, è essenziale che tutti i documenti siano versati in conservazione, secondo i tempi e le modalità descritte nel presente Manuale e nell'allegato 9 relativo al vigente manuale di conservazione.

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

Sezione terza - Disposizioni sulla formazione di documenti analogici

16. Copie analogiche di documenti informatici

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

Quando è necessario che al destinatario giunga un documento avente la medesima efficacia giuridico probatoria del documento originale, ai sensi dell'art. 3, d.lgs. n. 39/1993, la copia analogica dovrà essere accompagnata dall'indicazione della fonte del documento originale e del soggetto responsabile dell'immissione, riproduzione, trasmissione o emanazione del documento stesso. Quando il documento originale

informatico è sottoscritto con firma digitale o altra firma elettronica qualificata, la firma è sostituita dall'indicazione a stampa del nominativo del soggetto responsabile.

La copia analogica inviata, inoltre, deve contenere apposita dicitura che specifichi che il documento informatico da cui la copia è tratta è stato predisposto come documento nativo digitale ed è disponibile presso l'amministrazione (ad es.: "*La presente copia è tratta da documento informatico, predisposto come documento nativo digitale da* [nome responsabile]*, Responsabile dell'Ufficio* [indicazione UO]*. Il documento originale informatico è archiviato nel sistema informatico dell'Agenzia regionale per la protezione dell'ambiente della Sardegna, presso cui è disponibile per l'accesso*").

Quando possibile, la dicitura deve essere integrata con indicazioni sulle modalità per effettuare l'accesso online al documento informatico.

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

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

- ai sensi dell'art. 2, comma 6, CAD, esclusivamente nell'ambito dell'esercizio di attività e funzioni di ordine e sicurezza pubblica, difesa e sicurezza nazionale, polizia giudiziaria e polizia economico-finanziaria e consultazioni elettorali, nonché alle comunicazioni di emergenza e di allerta in ambito di protezione civile;
- in tutti i casi in cui il documento è consegnato a sportello e il richiedente è un soggetto privato che non agisce in qualità di professionista.

PARTE QUARTA - GESTIONE DOCUMENTALE

Sezione prima - Flussi documentali esterni

18. Ricezione di documenti in entrata

I documenti in entrata, pervenuti tramite i canali di ricezione previsti al successivo paragrafo, dopo averne accertata la provenienza, l'integrità e l'assenza di virus[1], sono oggetto di registrazione di protocollo da parte degli operatori individuati a livello di singola struttura (cfr. Sezione seconda par. 8). Da tale momento i documenti sono validi ai fini del procedimento amministrativo.

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

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

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

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

d) sono trasmesse da un domicilio digitale PEC ai sensi dell'art. 3-bis, comma 4-quinquies del CAD ed è possibile accertare la provenienza della trasmissione. Tale modalità di trasmissione costituisce elezione di domicilio digitale speciale per quel singolo procedimento o affare;

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

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

19. Canali di ricezione

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

1. Via PEC, attraverso le seguenti caselle:

Struttura	PEC
Direzione Generale	arpas@pec.arpa.sardegna.it
Direzione Area Amministrativa	da@pec.arpa.sardegna.it
Direzione Area Tecnico Scientifica	dts@pec.arpa.sardegna.it

[1] Si rinvia alla lettura del Regolamento interno sull'utilizzo delle risorse e degli strumenti informatici dell'ARPAS, approvato con DDG n. 968/2020

Dipartimento di Cagliari e Medio Campidano	dipartimento.ca@pec.arpa.sardegna.it
Dipartimento Sulcis	dipartimento.ci@pec.arpa.sardegna.it
Dipartimento Nuoro e Ogliastra	dipartimento.nu@pec.arpa.sardegna.it
Dipartimento Oristano	dipartimento.or@pec.arpa.sardegna.it
Dipartimento Sassari e Gallura	dipartimento.ss@pec.arpa.sardegna.it
Dipartimento Meteoclimatico	dipartimento.imc@pec.arpa.sardegna.it
Dipartimento Geologico	dipartimento.geo@pec.arpa.sardegna.it

2. Cooperazione applicativa tra pubbliche amministrazioni;
3. Altri canali di trasmissione, anche di posta elettronica ordinaria, indicati per specifici procedimenti;
4. Posta ordinaria o consegna a mano.

Gli indirizzi di posta elettronica certificata, configurati sul sistema, sono abilitati alla ricezione dei documenti provenienti da indirizzi di posta elettronica ordinaria.

Nel caso in cui un soggetto tenuto a effettuare comunicazioni esclusivamente in via telematica (imprese, professionisti, altre PP.AA., salvi i casi di cui all'art. 2, comma 6, CAD) faccia pervenire agli uffici dell'Agenzia comunicazioni e documenti in modalità analogica, questi non saranno ritenuti validamente trasmessi. In tali casi, la circostanza è segnalata in nota alla registrazione di protocollo. Il responsabile dell'UO assegnataria della comunicazione, o comunque il soggetto individuato quale responsabile del procedimento ai sensi dell'art. 5, comma 3, l. n. 241/1990, provvede a comunicare al mittente il motivo della mancata accettazione dei documenti e a indicare modalità di trasmissione valide. La comunicazione, quando possibile, è trasmessa al domicilio digitale del mittente estratto dagli indici di cui agli articoli 6-*bis* e 6-*ter* del CAD.

20. Formati accettati

Sono accettati, e conseguentemente registrati al protocollo, documenti informatici esclusivamente nei formati previsti dall'allegato 2 alle Linee guida.

Il controllo sulla conformità del formato dei documenti in entrata è effettuato dal personale addetto alla protocollazione prima della registrazione di protocollo. Qualora pervengano documenti in formati non ammessi, la circostanza deve essere indicata in nota al momento della registrazione di protocollo e segnalata al responsabile del procedimento, affinché ne dia comunicazione al mittente.

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

21. Controllo dei certificati di firma

Il Responsabile del procedimento verifica la validità dei certificati di firma e, in caso di certificato scaduto o revocato, lo segnala al personale addetto alla protocollazione, affinché indichi la circostanza in nota alla registrazione di protocollo (v. procedura di modifica di cui al punto 33 del presente Manuale). Il Responsabile, inoltre, valuta le azioni da intraprendere a seconda della tipologia di procedimento.

22. Trasmissione telematica di documenti informatici in uscita

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

Per la trasmissione telematica di documenti a imprese e professionisti tenuti obbligatoriamente all'iscrizione in albi o elenchi, il domicilio digitale è estratto dall'indice INI-PEC (www.inipec.gov.it).

Le comunicazioni agli indirizzi estratti da INI-PEC sono valide esclusivamente nell'ambito di rapporti professionali intercorrenti tra ARPAS e il destinatario (quindi, non sarà valida la comunicazione effettuata all'indirizzo PEC del professionista che abbia ad oggetto un rapporto che si pone al di fuori dell'attività professionale).

Quando l'indirizzo PEC del soggetto destinatario (professionista o impresa) non risulti attivo, la circostanza deve essere segnalata alla Camera di Commercio competente per la registrazione nel registro delle imprese o al soggetto competente per la tenuta dell'albo o registro presso cui il professionista è tenuto all'iscrizione.

I documenti informatici in uscita sono trasmessi a mezzo PEC solo dopo essere stati classificati, fascicolati e protocollati secondo le disposizioni della presente Parte del Manuale.

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

23. Comunicazioni e trasmissione di documenti con altre Pubbliche Amministrazioni

La trasmissione di comunicazioni e documenti verso altre pubbliche amministrazioni avviene sempre per via telematica agli indirizzi di posta elettronica, anche ordinaria, dei singoli uffici. Gli indirizzi di spedizione sono rilevati tramite la consultazione dell'Indice delle Pubbliche Amministrazioni (indicepa.gov.it) di cui all'art. 6-*ter* del CAD.

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

24. Disposizioni sui documenti analogici

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

- il servizio postale;
- la consegna diretta agli addetti a ricevere in presenza;
- il fax, nei soli casi di esclusione dell'applicazione della normativa previsti dall'art. 2, comma 6, D.lgs. n. 82/2005.

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

Sezione seconda - Protocollo informatico

25. Sistema di protocollo informatico

ARPAS, per la protocollazione dei documenti, utilizza la componente di Sistema di protocollo informatico del software di gestione documentale in uso presso l'ente. La puntuale descrizione funzionale e operativa del Sistema di protocollo informatico è illustrata nel manuale di utilizzo fornito dal produttore del software in uso.

26. Funzioni del Responsabile della Gestione Documentale in materia di protocollo informatico

La corretta tenuta del protocollo informatico è garantita dal Responsabile della gestione documentale. In particolare, nella sua veste di responsabile del protocollo informatico:

a. coordina la gestione del Sistema di protocollo informatico;
b. assegna al personale addetto alla protocollazione l'abilitazione all'utilizzo delle funzioni di protocollo del Sistema;
c. esercita il controllo generale sui flussi documentali esterni e interni;
d. assicura la corretta esecuzione delle attività di protocollazione;
e. autorizza l'attivazione del protocollo di emergenza;
f. autorizza con comunicazione formale le operazioni di annullamento delle registrazioni di protocollo;
g. vigila sull'osservanza della normativa e delle disposizioni del presente Manuale da parte del personale addetto.

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

27. Registro generale di protocollo

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

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

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

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

28. Registro giornaliero di protocollo

Il Registro giornaliero di protocollo è costituito dall'elenco delle informazioni inserite con l'operazione di registrazione di protocollo nell'arco di uno stesso giorno. Esso è prodotto automaticamente dal Sistema di protocollo informatico, che provvede altresì al versamento automatico al Sistema di conservazione, entro 24 ore.

29. Documenti soggetti a registrazione di protocollo e documenti esclusi

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

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

- gazzette ufficiali, bollettini ufficiali, notiziari della Pubblica Amministrazione;
- note di ricezione delle circolari e altre disposizioni;
- materiale statistico;
- atti preparatori interni;
- giornali, riviste, materiale pubblicitario, stampe varie, plichi di libri;
- biglietti augurali, inviti a manifestazioni e documenti di occasione vari che non attivino procedimenti amministrativi;
- bolle accompagnatorie;
- richiesta/invio comunicazioni informali.

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

Le ricevute di accettazione e di consegna di un messaggio inviato tramite PEC non devono essere protocollate, ma devono essere associate alla registrazione di protocollo del documento trasmesso/ricevuto a cui la ricevuta stessa si riferisce.

30. Disposizioni per particolari tipologie di documenti

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

31. Registrazione di protocollo

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

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

A suddetti metadati registrati in forma non modificabile, inoltre, sono aggiunti da parte di chi effettua la protocollazione:

g) tipologia di documento;
h) classificazione (titolo e classe) sulla base del Titolario (v. allegato 6);
i) fascicolo di appartenenza;
j) assegnazione in competenza e in copia conoscenza;
k) data e ora di arrivo (per la posta in entrata)
l) allegati;
m) flag documento riservato (Vedi allegato 12);
n) mezzo di ricezione o invio;
o) annotazioni (eventuali);
p) estremi del provvedimento di differimento della registrazione (eventuali);
q) elementi identificativi del procedimento amministrativo (eventuali).

32. Modalità di registrazione

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

Con il sistema in dotazione all'Agenzia si possono protocollare documenti:

- **in entrata**, ovvero tutta la corrispondenza ricevuta dall'esterno;
- **in uscita**, ovvero tutta la corrispondenza diretta all'esterno dell'ARPAS;
- **interni**, ovvero la documentazione diretta ad altra struttura dell'Agenzia che necessità, comunque, di essere registrata a protocollo.

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

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

I corrispondenti (mittenti e destinatari esterni) associati alle registrazioni di protocollo sono memorizzati su apposita banca dati del Sistema di gestione in uso. Per la corretta formazione dell'anagrafe si rimanda all'allegato 16 "*Linee guida per la creazione e l'aggiornamento delle anagrafiche del protocollo informatico*".

Si rimanda all'allegato 14, per i casi in cui risulta necessario protocollare documenti con allegati di dimensioni elevate.

33. Annullamento della registrazione di protocollo

La registrazione degli elementi obbligatori del protocollo non può essere modificata né integrata, né cancellata, ma soltanto annullata attraverso l'apposita procedura conforme all'art. 54 del TUDA. In particolare, i metadati indicati al par. 31 del presente Manuale, lettere da a) a f), non sono modificabili, ma eventualmente annullabili. I metadati da g) a q) del medesimo paragrafo, invece, sono modificabili.

Ogni annullamento della registrazione deve:

- essere autorizzato con provvedimento del Responsabile;
- comportare la memorizzazione di data, ora e estremi del provvedimento di annullamento;
- consentire sempre la memorizzazione e la visibilità delle informazioni oggetto di annullamento.

Le richieste di annullamento rivolte al Responsabile devono essere motivate. Le richieste sono accolte, di norma, in casi di mero errore materiale quali, ad esempio, la doppia registrazione, la registrazione di documenti che non diano seguito a procedimenti o ad attività amministrative proprie dell'ente, la registrazione errata che necessiterebbe di modifiche sostanziali dei campi obbligatori. Solo il Responsabile ha

il potere di autorizzare l'annullamento delle registrazioni di protocollo, ovvero di dare disposizioni in tal senso.

Le operazioni di modifica posso essere svolte dal personale addetto alla protocollazione, anche senza previa autorizzazione del Responsabile.

L'annullamento avviene secondo la procedura guidata descritta nella Circolare allegata (Allegato 10 - Circolare n. 4/2020).

34. Gestione degli allegati

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

Non è ammessa l'associazione al documento informatico già registrato di allegati non indicati nella registrazione di protocollo. L'associazione di allegati successivamente alla registrazione, solo nel caso della posta in ingresso, può essere effettuata in casi eccezionali attraverso la procedura definita di "storicizzazione".

35. Tempi di registrazione e casi di differimento

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

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

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

Al momento della registrazione differita devono essere indicati in nota alla registrazione gli estremi del provvedimento di differimento. In ogni caso, della ricezione del documento informatico da parte dell'Agenzia fa fede la ricevuta di consegna generata dal gestore della casella PEC.

Ai fini del computo dei termini previsti dalla legge o da altri atti (es. bandi, contratti, ecc.) resta fermo quanto previsto dall'art. 45 del CAD. In base a tale articolo il documento informatico trasmesso per via telematica si intende "spedito" dal mittente se inviato al proprio gestore e si intende "consegnato" al destinatario se reso disponibile all'indirizzo elettronico da questi dichiarato nella casella di posta elettronica del destinatario messa a disposizione dal gestore.

36. Segnatura di protocollo

Secondo quanto previsto dall'art. 55 del TUDA, la segnatura di protocollo è l'associazione al documento amministrativo informatico, in forma permanente e non modificabile, di informazioni riguardanti il documento stesso. Tale operazione avviene per tutti i documenti protocollati sia in ingresso e sia in uscita dal Sistema di protocollo informatico ed è fondamentale per la loro successiva identificazione univoca e certa.

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

I requisiti necessari di ciascuna segnatura di protocollo sono:

a. indicazione della Amministrazione mittente;
b. codice identificativo dell'AOO mittente;
c. codice identificativo del registro;
d. numero progressivo di protocollo;
e. data di registrazione;
f. oggetto del messaggio di protocollo;
g. classificazione del messaggio di protocollo;
h. indicazione del fascicolo in cui è inserito il messaggio di protocollo.

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

37. Protocollo riservato

La registrazione di un protocollo riservato avviene secondo le istruzioni operative descritte nella Circolare allegata (Allegato 12 - Circolare n. 2/2021).

Sono considerati documenti riservati ad accesso ristretto e controllato i seguenti:

- in generale, tutti i documenti contenenti categorie particolari di dati personali ai sensi dell'art. 9 del Regolamento UE 2016/679, che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche o l'appartenenza sindacale, dati genetici, dati biometrici intesi a identificare in modo univoco una

persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona (ad es. documenti che contengono certificati medici con diagnosi o patologie, certificati di invalidità, documenti attestanti l'adesione a partiti politici, documenti contenenti sfratti esecutivi e pignoramenti, ecc.), dati personali relativi a condanne penali e reati o a connesse misure di sicurezza (ad es. documenti provenienti dal casellario giudiziale);
- atti dei procedimenti amministrativi in relazione ai quali sussistano particolari esigenze di protezione della riservatezza di terzi, persone, gruppi, imprese ed associazioni e dalla cui contestuale pubblicità possa derivare pregiudizio a terzi o al buon andamento dell'attività amministrativa;
- documenti relativi a vicende di persone o a fatti privati o particolari;
- documenti di carattere politico e di indirizzo che, se resi di pubblico dominio, possono ostacolare il raggiungimento degli obbiettivi prefissati;
- le tipologie di documenti individuati dall'art. 24 della legge 7 agosto 1990 n. 241;
- documenti che contengano dati particolari, giudiziari o personali, come definiti dal Codice in materia di protezione dei dati personali;
- segnalazioni indirizzate al RPCT ai sensi della normativa in materia di whistleblowing.

Tutti gli utenti abilitati alla protocollazione in ingresso e in uscita hanno la possibilità di selezionare il flag "protocollo riservato" che rende la protocollazione riservata e il documento rimane visibile esclusivamente dal protocollatore e dal/i destinatario/i. L'apposizione del flag esclude che, in fase di ricerca, l'oggetto e i documenti allegati ad una registrazione riservata possano essere visualizzati da soggetti diversi da quelli precedentemente citati.
Va evidenziato che la procedura di cui sopra consente di eseguire sul documento c.d. riservato tutte le operazioni quali: la registrazione, la segnatura, la classificazione e la fascicolazione, adottate per gli altri documenti e procedimenti amministrativi. In caso di documento analogico va eseguita la scansione ai fini della conservazione dello stesso in formato pdf. Nel caso di riservatezza temporanea delle informazioni è necessario indicare, contestualmente alla registrazione di protocollo, anche la data nel quale le informazioni temporaneamente riservate divengono soggette all'accesso ordinariamente previsto.
I documenti registrati con tali forme appartengono al protocollo riservato dell'Agenzia, costituito dalle registrazioni sul Sistema di protocollo il cui accesso è consentito solamente agli utenti autorizzati.

38. Registro di emergenza

Nei casi in cui non sia possibile l'utilizzo del registro di protocollo informatico, il Responsabile provvede alla formazione del registro di emergenza su supporto analogico secondo le indicazioni fornite dal Responsabile, in coerenza con il software in uso.

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

Il registro di protocollo di emergenza, da predisporre secondo l'allegato 13, ha una numerazione progressiva propria, perciò, ai documenti protocollati su tale registro, una volta riversati, saranno associati due numeri di protocollo, quello del registro di emergenza e quello del registro di protocollo generale. Le registrazioni sul registro di emergenza avvengono, quando possibile, secondo le medesime regole e con le stesse modalità adoperate per le registrazioni sul registro generale di protocollo.

Sul registro di emergenza, inoltre, sono riportati:

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

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

39. Documenti soggetti a registrazione particolare

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

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

- Determinazioni dirigenziali;
- Contratti (sia in forma pubblica amministrativa sia soggetti a registrazione in caso d'uso);
- Circolari interne;
- Ordini di servizio.

I registri e repertori diversi dal protocollo sono tenuti tramite il Sistema di gestione documentale di cui si avvale l'Agenzia. Essi contengono almeno le seguenti informazioni:

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

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

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

40. Disposizioni sulla protocollazione di documenti analogici

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

Qualora il documento analogico sia consegnato direttamente dal mittente o da altra persona a ciò delegata e sia richiesto il rilascio di una ricevuta attestante l'avvenuta consegna del documento, è cura del personale addetto alle attività di protocollazione rilasciare la ricevuta di avvenuta protocollazione prodotta direttamente dal protocollo informatico.
La ricevuta di avvenuta protocollazione prodotta dal sistema di protocollo (dettaglio prot. in arrivo) riporta i seguenti dati:

- il numero e la data di protocollo;
- l'indicazione dell'AOO;
- il mittente;
- l'oggetto;
- numero e descrizione degli allegati se presenti;
- l'indicazione dell'Ufficio o dell'utente destinatario cui è assegnato il documento per competenza;
- l'operatore di protocollo che ha effettuato la registrazione.

Qualora per ragioni organizzative o tecniche non sia possibile protocollare immediatamente il documento, l'addetto al protocollo comunica al mittente o ad altra persona incaricata il termine entro il quale il documento verrà protocollato,

impegnandosi a far pervenire la ricevuta all'indirizzo o recapito indicato dal mittente stesso (anche tramite e-mail). La ricevuta può essere altresì ritirata dall'interessato o da persona espressamente delegata nei giorni successivi.

40.1. Registrazione, segnatura, annullamento.

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

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

Per i documenti analogici la segnatura è apposta con timbro ed etichetta riportante i dati indicati al par. 36, lett. a)..e).

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

40.2. Corrispondenza contenente dati particolari

I documenti cartacei contenenti categorie particolari di dati (prima definiti dati sensibili) o soggetti a riservatezza, pervenuti in modalità cartacea, dopo essere stati scansionati e allegati alla registrazione effettuata con protocollo riservato, devono essere inseriti in busta chiusa recante la dicitura "contiene dati particolari" e successivamente nelle apposite cassettine dedicate allo smistamento ubicate presso l'Ufficio centrale di protocollo.

40.3. Corrispondenza personale o riservata

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

40.4. Corrispondenza cartacea non di competenza dell'Amministrazione

La corrispondenza cartacea che non è evidentemente di competenza dell'Agenzia (es. altro destinatario) non va aperta e va riconsegnata al Servizio postale; in caso di errata

apertura, la busta va richiusa indicando la dicitura “aperta per errore”, apponendo timbro datario e riconsegnata al Servizio postale. La corrispondenza cartacea che invece riporta l'indirizzo corretto sulla busta, ma non è di competenza dell’Agenzia, a seguito dell'apertura e valutazione, va richiusa indicando la dicitura “aperta e non di competenza”, apponendo timbro datario e riconsegnata al Servizio postale.

Sezione terza – Classificazione e fascicolazione

41. Classificazione dei documenti

I documenti formati e acquisiti dall’Agenzia sono classificati mediante indicazione del titolo e della classe secondo i criteri previsti nel Titolario contenuto nel Piano di fascicolazione di cui all’allegato 6. I documenti devono essere classificati prima della registrazione di protocollo. Non è ammessa la registrazione di protocollo di documenti non classificati.

La classificazione dei documenti in entrata è effettuata dal personale addetto alla protocollazione, mentre la classificazione dei documenti prodotti dall’Agenzia è effettuata dal Responsabile dell’UO o dal personale dallo stesso delegato.
Per approfondimenti sulle modalità di classificazione e fascicolazione dei documenti si rimanda all’Allegato 7.

42. Fascicolazione informatica dei documenti

Al fine di garantire la consultazione dei documenti informatici, da parte sia di altre amministrazioni che degli utenti, questi sono raccolti in fascicoli informatici, come definiti nel Piano di fascicolazione (allegato 6), seguendo le indicazioni fornite nel Manuale tecnico e nella Guida per la fascicolazione dei documenti di cui all’allegato 7. I fascicoli eventualmente possono essere organizzati in sotto fascicoli.

I documenti soggetti a protocollazione sono inseriti nel pertinente fascicolo tramite l’apposita funzione del Sistema di gestione documentale (cfr. allegato 8). Quando è necessario aprire un nuovo fascicolo informatico, l’utente abilitato alla creazione dei fascicoli della UO che ha prodotto il documento provvede all’apertura del fascicolo in cui inserire il documento.

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

I fascicoli informatici possono essere organizzati:

a. **per affare**, quando i documenti raccolti nel fascicolo, accomunati secondo un criterio di classificazione basato sulla competenza amministrativa, non sono tutti riferibili a un singolo procedimento amministrativo. Il fascicolo per affare deve avere una data di apertura e una durata circoscritta;
b. **per attività**, quando i documenti raccolti nel fascicolo attengono allo svolgimento di un'attività amministrativa semplice, che implica risposte obbligate o meri adempimenti, per la quale quindi non è prevista l'adozione di un provvedimento finale. Ha in genere durata annuale;
c. **per persona (fisica o giuridica)**, quando i documenti raccolti nel fascicolo, anche con classificazioni diverse, sono riferibili a un medesimo soggetto. Sono fascicoli di tipo "aperto", con durata pluriennale e indeterminata;
d. **per procedimento amministrativo**, quando i documenti raccolti nel fascicolo rappresentano azioni amministrative omogenee e destinate a concludersi con un provvedimento amministrativo.

I fascicoli, una volta chiusi, sono automaticamente inviati in conservazione a norma. La chiusura, in funzione della tipologia del fascicolo, può essere impostata su base annuale con riapertura automatica nell'anno successivo per replicare ogni anno il medesimo fascicolo. Riguardo l'utilizzo di tali funzionalità si rimanda all'Allegato 7 "Manuale tecnico di fascicolazione".
I fascicoli informatici devono recare i metadati obbligatori delle aggregazioni documentali previsti nell'allegato 5 alle Linee guida AgID.

Sezione quarta – Flussi documentali interni

43. Assegnazione dei documenti in entrata agli uffici

L'assegnazione dei documenti in entrata, quando possibile, è effettuata con modalità automatizzate. I criteri di assegnazione automatica sono definiti dal Responsabile, sentite le UUOO interessate.

I documenti non assegnati automaticamente sono assegnati alle UO Responsabili dal personale addetto alla protocollazione in base all'oggetto del documento e alla classificazione (cfr. allegato 6). Quando un documento è di interesse anche per più UUOO, si provvede a più assegnazioni, sia "per competenza" che "per conoscenza". Nel caso di assegnazione errata l'ufficio/unità che riceve il documento, attraverso le funzionalità del sistema, lo rifiuta indicando il motivo in nota di esecuzione e lo re-invia all'incaricato della protocollazione che provvederà alla riassegnazione.

44. Protocollazione interna

Il sistema di gestione documentale in uso all'Agenzia consente la registrazione a protocollo "interno" delle comunicazioni tra differenti strutture a cui si vuole dare una certezza di trasmissione/ricezione e conservazione, in ragione del rilievo giuridico amministrativo assunto dal documento stesso.

Sostanzialmente, le registrazioni di protocollo interno seguono procedure analoghe alla protocollazione in partenza ma con un minor numero di metadati obbligatori e limitati mezzi di trasmissione (telematica o a mano).

45. Comunicazioni non registrate a protocollo

Lo scambio di documenti tra le UUOO dell'Agenzia può avvenire anche senza la relativa registrazione di protocollo.

Scambi di documenti tra gli uffici, infatti, possono essere effettuati anche attraverso rete intranet e cartelle condivise. In ogni caso, nelle attività di trasmissione e scambio dei documenti tutto il personale deve utilizzare esclusivamente gli strumenti di comunicazione messi a disposizione da ARPAS e osservare le disposizioni contenute nel Regolamento sull'utilizzo delle risorse e degli strumenti informatici adottato dall'Agenzia.

Le comunicazioni personali sono trasmesse a mezzo posta elettronica ordinaria. Quando la comunicazione indirizzata a più destinatari, in ragione del contenuto e degli invii multipli, potrebbe comportare la divulgazione di dati personali, il mittente provvede a invii individuali o in copia conoscenza nascosta (ccn).

In assenza di apposita regolamentazione, nell'ARPAS non è consentito l'utilizzo di servizi di messaggistica istantanea (es. Whatsapp, Telegram, ecc.) nell'ambito dell'attività lavorativa.

46. Pubblicazioni nell'Albo pretorio

Tutti gli atti prodotti dall'Agenzia che, ai sensi della normativa vigente, sono soggetti a pubblicazione nell'Albo pretorio online, sono trasmessi per la pubblicazione in modo automatizzato solo dopo che il documento sia divenuto immodificabile (cfr. par. 15 del presente Manuale).

PARTE QUINTA – CONSERVAZIONE DEI DOCUMENTI

47. Sistema di conservazione dei documenti informatici

ARPAS, per la conservazione dei documenti informatici e degli altri oggetti della conservazione, si avvale del sistema di conservazione di un conservatore esterno ai sensi dell'art. 44, comma 1-quater, CAD.

Il servizio di conservazione dei documenti informatici dell'ente è stato affidato al Conservatore PA Digitale S.p.A. (d'ora in avanti anche solo "Conservatore").

Le attività affidate al Conservatore sono puntualmente indicate nella convenzione per l'affidamento del servizio.

Per la descrizione delle attività del processo di conservazione non definite nel presente Manuale, così come consentito dal par. 4.6 delle Linee Guida, è fatto rinvio al manuale di conservazione di cui all'allegato 9 al presente Manuale, nonché agli ulteriori documenti tecnici concernenti l'affidamento del servizio di conservazione.

48. Responsabile della conservazione

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

Come stabilito nella determina di nomina (allegato 2.2), è compito del Responsabile monitorare il corretto funzionamento del processo di conservazione e il rispetto degli obblighi contrattuali assunti da parte del Conservatore, ivi compreso il rispetto delle misure di sicurezza dei dati trattati. A tal fine, il Responsabile della conservazione opera d'intesa con il Responsabile del trattamento dei dati personali e con i delegati da questo individuati e con il Responsabile IT dell'Agenzia.

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

49. Oggetti della conservazione

Gli oggetti della conservazione sono:

- i documenti informatici formati dall'Agenzia e i rispettivi metadati (conformi all'allegato 5 alle Linee guida dell'AgID);

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

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

a) pacchetti di versamento;
b) pacchetti di archiviazione;
c) pacchetti di distribuzione.

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

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

Il Responsabile firma digitalmente i pacchetti inviati in conservazione.

Le specifiche operative e le modalità di descrizione e di versamento delle singole tipologie documentarie oggetto del servizio di conservazione sono dettagliatamente descritte nel manuale utente del Sistema di gestione documentale *Urbi smart* e nel Manuale del Conservatore PA Digitale S.p.A. (allegato 9)

50. Formati ammessi per la conservazione

I formati ammessi per la conservazione sono individuati nell'allegato 2 alle Linee guida dell'AgID.

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

51. Modalità e tempi di trasmissione dei pacchetti di versamento

All'inizio di ogni anno ciascuna UO individua i fascicoli da versare all'archivio di deposito, disponendone la chiusura per il successivo invio automatico in conservazione.

Il Responsabile, attraverso le funzionalità del sistema, genera il rapporto di versamento relativo a uno o più pacchetti di versamento e una o più impronte relative

all'intero contenuto del pacchetto, secondo le modalità descritte nel manuale del Conservatore.

Prima del versamento in conservazione, il sistema verifica che agli oggetti della conservazione siano stati correttamente associati i rispettivi metadati e, se mancanti, viene generato un errore con richiesta, a carico del produttore dell'oggetto, di provvedere correttamente all'associazione dei metadati.

Il versamento dei documenti avviene secondo le seguenti tempistiche:

- versamento annuale, per cui ogni anno entro il mese di febbraio sono versati in conservazione tutti i documenti informatici di ARPAS, anche a fascicolo aperto;
- versamento automatizzato a determinate scadenze, che per il registro di protocollo giornaliero avviene entro le 24 ore successive al momento della produzione. Il Responsabile può individuare altre tipologie di versamento automatizzato a determinate scadenze per particolari tipologie di documenti;
- versamento anticipato, nelle particolari ipotesi che richiedono un versamento in conservazione prima del versamento a cadenza annuale (ad esempio, documenti con certificato di firma in scadenza).

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

I dati e i documenti informatici sono memorizzati nel Sistema di gestione documentale, che provvede all'archiviazione su server cloud qualificato dall'AgID ai sensi della normativa vigente. Dettagli sulle norme di sicurezza dell'infrastruttura di erogazione dei servizi di PA Digitale sono riportati nell'allegato 15 che, per questioni di riservatezza e privativa industriale, è sottratto alla pubblicazione.

Sono memorizzati sul data center di ARPAS, su apposite cartelle condivise windows, esclusivamente bozze e semilavorati dei documenti che, se del caso, saranno successivamente registrati a protocollo ed inviati in conservazione.

Tutti i documenti memorizzati nelle cartelle condivise sono salvati in copia di backup su base quotidiana. Mediante apposito job che viene eseguito a fine giornata, il Servizio Sistema Informativo e Informatico, effettua le copie di backup, che sono riversate su supporti di memorizzazione tecnologicamente avanzati e conservati secondo specifiche procedure interne dell'Agenzia.

53. Accesso al Sistema di conservazione

Gli utenti espressamente autorizzati da ARPAS possono accedere al Sistema tramite credenziali personali rilasciate da PA Digitale S.p.A. su richiesta del Responsabile e comunicate al singolo utente. L'accesso al Sistema consente di consultare i documenti digitali versati nel Sistema e le configurazioni specifiche adottate.

54. Selezione e scarto dei documenti

Periodicamente, secondo quanto sarà previsto nel Piano di conservazione/Massimario di scarto in corso di predisposizione (allegato 11), viene effettuata la procedura di selezione della documentazione da proporre allo scarto ed attivato il procedimento amministrativo di scarto documentale. Le modalità per effettuare le operazioni di selezione e scarto dei documenti informatici sono descritte nel Manuale del Conservatore (allegato 9).

55. Conservazione, selezione e scarto dei documenti analogici

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

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

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

56. Misure di sicurezza e monitoraggio

Il Manuale di conservazione dell'Agenzia (allegato 9) e il piano della sicurezza di PA Digitale S.p.A. (allegato 15) descrivono le modalità con cui il Conservatore assicura gli obiettivi di sicurezza richiesti per la conservazione a lungo termine degli archivi informatici, dettagliando i controlli di sicurezza delle diverse componenti del sistema (organizzazione, accessi, infrastruttura, gestione dell'esercizio, gestione dello sviluppo) e le procedure adottate per garantire i *backup* degli archivi e il *Disaster recovery*.

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

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

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

In caso di databreach, si applicano le disposizioni contenute nelle istruzioni operative allegate al "*Regolamento in materia di attuazione del Regolamento (UE) 2016/679 del Parlamento e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)*", approvato con Determinazione del Direttore generale n. 846/2022 del 20/06/2022.

PARTE SESTA – SICUREZZA E PROTEZIONE DEI DATI PERSONALI

57. Sicurezza dei sistemi informatici di ARPAS

Lo strumento software *Urbi Smart*, utilizzato per la formazione e gestione dei documenti informatici, è reso accessibile al personale dell'Agenzia tramite il servizio cloud (SaaS) qualificato dall'Agenzia per l'Italia Digitale fornito dalla PA Digitale S.p.A. Il servizio consente altresì l'archiviazione dei documenti, prodotti mediante l'utilizzo dei software, nel rispetto degli standard di sicurezza previsti dalla normativa, garantendone così l'integrità e l'immodificabilità ai sensi delle Linee guida (cfr. parr. 2.1.1. e 3.9).

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

58. Amministratore di sistema

L'amministratore di sistema realizza le copie di sicurezza (operazioni di backup e recovery dei dati) e assicura la custodia delle credenziali alla gestione dei sistemi di autenticazione e di autorizzazione. Adotta, inoltre, sistemi idonei alla registrazione degli accessi logici (autenticazione informatica), ai sistemi di elaborazione e agli archivi di sistema. Le registrazioni (access log) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo per cui sono richieste. Le registrazioni devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate e devono essere conservate per un congruo periodo, non inferiore a sei mesi.
Gli Amministratori di sistema dell'Agenzia, ai sensi del vigente regolamento UE 679/2016 sulla protezione dei dati personali, sono espressamente nominati Responsabili del trattamento.

59. Uso del profilo utente per l'accesso al sistema informatico

Per l'accesso al sistema informatico della gestione documentale di ARPAS è necessaria l'assegnazione di un profilo utente da parte del Responsabile. Ogni profilo è protetto da un sistema di credenziali (username e password). Al momento della creazione del profilo utente, sono attribuiti all'utente lo username e una password temporanea. Al primo accesso dell'utente, viene richiesto l'inserimento di una nuova password, mentre lo username resta invariato.

L'uso di ogni profilo utente è strettamente personale e ogni dipendente, sotto la propria responsabilità, è tenuto a custodire e non diffondere le proprie credenziali. Ciascun dipendente deve associare al proprio profilo una password di almeno 12 caratteri che dovranno essere 14 nel caso delle utenze di amministrazione. La password deve prevedere almeno una lettera maiuscola, una lettera minuscola, un numero e un segno (ad esempio: #, !, ?, -, &, ecc.). La password non deve mai coincidere con altre password associate ad altri profili o utenze (ad esempio, non si deve usare la stessa password del proprio account e-mail personale).

L'Amministratore di sistema provvede affinché, almeno a cadenza trimestrale, per ogni profilo utente sia richiesto il rinnovo della password.

Nel prossimo futuro è prevista anche l'autenticazione forte mediante SPID in funzione dei tempi di rilascio della nuova funzionalità da parte della società proprietaria del sistema in uso.

Ogni richiesta diretta al Fornitore per l'accesso – anche temporaneo – al Sistema o la modifica delle credenziali profilo utente deve essere effettuata direttamente dall'Amministratore di sistema, previa comunicazione al Responsabile.

Per la corretta tenuta delle credenziali di accesso, si rimanda anche al più generale "Regolamento sull'utilizzo delle risorse e degli strumenti informatici dell'ARPAS" approvato con Determinazione del Direttore generale n. 968/2020 del 21/07/2020.

60. Accesso alle postazioni di lavoro, ai locali e agli archivi dell'Agenzia

Ogni utente abilitato è tenuto a rispettare le disposizioni di sicurezza che sono prescritte dall'Agenzia, con particolare riferimento al complesso delle misure tecniche, informatiche, organizzative, fisiche, logistiche e procedurali che configurano i livelli di protezione necessari ad eliminare o mitigare i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.