Autorità di Bacino Distrettuale dell'Appennino Meridionale

Decreto n. 96 **del** 5 AGO. 2022

Oggetto: approvazione del Manuale di gestione documentale del protocollo informatico.

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

VISTO il paragrafo 3.1.2 delle Linee Guida sulla formazione, gestione e conservazione dei documenti informatici adottate da AgID (Agenzia dell'Italia Digitale) con la determinazione n. 407/2020 e successivamente modificate con determinazione n. 371/2021, nel quale si prevede che *"Le Pubbliche Amministrazioni, nell'ambito del proprio ordinamento, provvedono a nominare, in ciascuna delle AOO, il responsabile della gestione documentale e un suo vicario, in possesso di idonee competenze giuridiche, informatiche ed archivistiche"*;

CONSIDERATO che questa Amministrazione individua una sola Area Organizzativa Omogenea (AOO) denominata Autorità di bacino distrettuale dell'Appennino Meridionale;

DATO ATTO che si rende necessario provvedere all'individuazione del Responsabile della Gestione Documentale e del vicario;

DATO ATTO che il Responsabile della Gestione Documentale è preposto al Servizio per la gestione informatica dei documenti dei flussi documentali e degli archivi ed ha il compito di predisporre 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;

RITENUTO che il Responsabile della Gestione Documentale debba essere individuato all'interno dell'Ente a livello apicale;

VISTI, altresì, gli artt. 20, commi 3 e 5-bis, 23-ter, comma 4, 43, commi 1 e 3, 44, 44-bis e 71, comma 1 del D.Lgs. n. 82/2005 (Codice dell'Amministrazione Digitale) che disciplinano il sistema di conservazione dei documenti informatici;

ATTESO che l'art. 40, comma 1, capo III *"Formazione, gestione e conservazione dei documenti informatici"* del predetto Decreto così recita: *"Le Pubbliche Amministrazioni formano gli originali dei propri documenti con mezzi informatici secondo le disposizioni di cui al presente codice e le regole tecniche di cui all'articolo 71"*;

VISTO l'art. 44, comma 1-bis, del D.Lgs. n. 82/2005, secondo cui il sistema di conservazione dei documenti informatici è gestito da un Responsabile;

RICHIAMATO l'art. 43, comma 3, del medesimo Decreto;

RICHIAMATO il decreto del S.G. n 249 del 22 aprile 2022 con il quale sono stati nominati:

- quale responsabile della gestione documentale la dottoressa Antonietta Napolitano, dirigente del Settore Legislazione, Contenzioso Norme e Direttive, alla quale è stato assegnato il Servizio per la Tenuta del Protocollo Informatico e vicario il sig. Gennaro Carrino dipendente di questo Ente, addetto al Servizio di Protocollo Informatico;
- quale responsabile della conservazione dei documenti informatici l'Ing. Filippo Pengue dirigente del Settore Compatibilità Idrogeologica Strutture ed Infrastrutture e Pianificazione Sottordinata;

VISTO il DPR 445/00 recante "Testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa" ed in particolare l'articolo 50 comma 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 del 3 dicembre 2013 contenente le regole tecniche per il protocollo informatico ed in particolare l'articolo 3, c.1, lett. d) e l'articolo 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 istruzione per il corretto funzionamento del servizio del protocollo informatico, della gestione dei flussi documentali e degli archivi;

CONSIDERATE le linee guida AGID sulla formazione, gestione e conservazione dei documenti informatici la cui applicazione è prevista a partire dal 1 gennaio 2022;

CONSIDERATO che il manuale di gestione documentale presente in allegato è uno strumento operativo che riflette le modalità organizzative di gestione dei flussi documentali;

RITENUTO, quindi, opportuno, procedere all'approvazione del manuale di gestione comprensivo degli allegati quali parte integrante e sostanziale del presente provvedimento;

VISTI:

- il Codice dell'Amministrazione Digitale approvato con il D.Lgs. n. 82/2005;
- le Linee Guida sulla formazione, gestione e conservazione dei documenti informatici adottateda AgID con la determinazione n. 407/2020 e successivamentemodificate con determinazione n. 371/2021;
- il decreto del Segretario Generale n. 610 del 28 maggio 2021 con il quale è stato affidato a PA DIGITALE S.P.A. il servizio di transizione al digitale ivi compreso tra l'altro il servizio di conservazione digitale, la redazione del manuale di gestione, la redazione del manuale di conservazione etc.

DECRETA

1) Di richiamare ed approvare le motivazioni in fatto e diritto del presente decreto quale parte integrante e sostanziale del presente dispositivo.

2) Di approvare il Manuale di gestione del protocollo informatico corredato da n.11 allegati facenti parte integrante e sostanziale del presente atto e più precisamente:
   - Allegato 1: Glossario dei termini e degli acronimi
   - Allegato 2: Elenco degli uffici abilitati all'utilizzo del sistema di gestione documentale
   - Allegato 3: Elenco registrazioni particolari
   - Allegato 4: Linee guida per l'inserimento e l'aggiornamento dei dati nel protocollo informatico
   - Allegato 5: Titolario di classificazione
   - Allegato 6: Norme di sicurezza e di adeguamento
   - Allegato 7: Elenco trasmissioni telematiche
   - Allegato 8: Guida per l'attivazione del registro di emergenza
   - Allegato 9: Modelli per la riproduzione cartacea di documenti informatici
   - Allegato 10: Decreto del SG. n. 249 del 22.aprile 2022
   - Allegato 11: Manuale di conservazione

3) Di pubblicare il presente decreto nella sezione Amministrazione Trasparente sottosezione "Provvedimenti" e "Atti generali".

Il Segretario Generale f.f
Vera Corbelli

Manuale di gestione documentale

Dell'Autorità di Bacino Distrettuale dell'Appennino Meridionale

INDICE

Sezione 1 *Disposizioni generali*

Sezione 2 *Formazione dei documenti*

Sezione 3 *Ricezione dei documenti*

Sezione 4 *Registrazione dei documenti*

Sezione 5 *Documentazione particolare*

1 *Disposizioni generali*

1.1 *Ambito di applicazione*

Il presente manuale è adottato ai sensi del Codice dell'Amministrazione digitale Dlgs 82/2005 e delle Linee Guida sulla formazione, gestione e conservazione dei documenti informatici (di seguito indicate come Linee Guida di Agid), Determinazioni Agid 407/2020 e 371/2021, in vigore dal 10 settembre 2020 e con adozione obbligatoria dal 1 gennaio 2022.
Il manuale di gestione documentale costituisce lo strumento operativo che descrive e disciplina il sistema di produzione e di gestione documenti.
Il sistema documentale dell'Ente è composto da:

- archivio corrente, documentazione relativa ad affari in corso di trattazione;
- archivio di deposito, documentazione relativa ad affari esauriti, non più occorrente alla trattazione degli affari in corso, che riveste comunque una valenza giuridico–amministrativa, non ancora destinata, previe le opportune operazioni di selezione e scarto, alla conservazione permanente;
- archivio storico, il complesso di documenti relativi ad affari esauriti da almeno quaranta anni, che rivestono una valenza storico-culturale, destinati alla conservazione permanente e consultabili da parte del pubblico.

Le Autorità di Bacino Distrettuale sono state istituite nel 2006 a seguito della soppressione delle Autorità di Bacino, dal 2016 esercitano le funzioni e i compiti in precedenza in capo alle soppresse Autorità di Bacino Nazionali, Interregionali e Regionali. Dal 2018 è stata infine data definitiva operatività al processo di riordino delle funzioni di competenza. L'ente ha acquisito pertanto gli archivi storici e di deposito degli enti soppressi.
Il manuale sovraintende alla gestione dell'archivio corrente.
Il manuale è costituito dall'insieme delle regole tecniche ed organizzative per l'attuazione del protocollo informatico e la gestione del flusso documentale e, in particolare, disciplina le attività di formazione, protocollazione, registrazione, classificazione, fascicolazione, gestione, archiviazione e conservazione dei documenti su qualsiasi supporto formati, considerate come flusso di lavorazione degli stessi.
Regolamenta inoltre le fasi operative per la gestione informatica dei documenti, nel rispetto della normativa vigente in materia di trasparenza degli atti amministrativi, di tutela della privacy e delle politiche di sicurezza.
Il manuale è adottato con decreto del Segretario Generale, su proposta del responsabile della gestione documentale.
Il Manuale di gestione è reso pubblico tramite la sua diffusione sul sito internet dell'Amministrazione
L'Amministrazione ha adottato un sistema di gestione documentale avanzato di protocollazione informatica sicuro, certificato e con piena validità giuridica, che consente di avviare progressivamente processi di dematerializzazione della documentazione.
Sono state intraprese le iniziative necessarie all'attuazione delle disposizioni normative in materia di gestione informatica dei documenti e dematerializzazione, perseguendo gli obiettivi di ammodernamento della pubblica amministrazione, miglioramento dei servizi, trasparenza, contenimento dei costi secondo i criteri di economicità, efficacia e pubblicità dell'azione amministrativa, coordinamento dei flussi documentali con il protocollo informatico e i procedimenti amministrativi.
Il manuale di gestione documentale fornisce le indicazioni per realizzare i processi di innovazione, che porteranno ad attuare, tramite le nuove tecnologie, la gestione documentale in modalità esclusivamente informatiche.
Al fine di garantire lo sviluppo del processo di digitalizzazione previsto dalla normativa vigente l'Ente provvede a razionalizzare e semplificare i procedimenti amministrativi, le attività gestionali, i documenti, la modulistica, le modalità di accesso e di presentazione delle istanze da parte dei cittadini e delle imprese.

Le Linee Guida sulla formazione, gestione e conservazione dei documenti informatici di Agid, entrate in vigore il 10 settembre 2020, sono applicabili dal 1° gennaio 2022 e comportano l'abrogazione delle Regole tecniche per il protocollo informatico DPCM 3/12/2013, Regole tecniche in materia di sistema di conservazione DPCM 3/12/2013 e Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici DPCM 13/11/2014.

1.2 *Definizioni dei termini*

Per quanto riguarda la definizione dei termini, che costituisce la corretta interpretazione del dettato del presente manuale, si rimanda al Glossario dei termini e degli acronimi allegato alle Linee guida di Agid (Documento n. 1), all'articolo 1 Definizioni del Codice dell'Amministrazione digitale Dlgs 82/2005 come modificato dal Dlgs 217/2017 e all'articolo 3 Definizioni del Regolamento (UE) N. 910/2014 del Parlamento europeo e del Consiglio in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno.

1.3 *Storia delle versioni del documento*

Prima versione del Manuale di gestione documentale.

1.4 *Area organizzativa omogenea*

Ai fini della gestione dei documenti è individuata una sola area organizzativa omogenea denominata Autorità di Bacino Distrettuale dell'Appennino Meridionale composta dall'insieme di tutte le sue unità organizzative come da elenco allegato (Documento n. 2). L'Ente è accreditato all'Indice dei domicili digitali delle Pubbliche Amministrazioni e dei gestori di pubblici servizi (IPA), contenente informazioni dettagliate sugli enti e le relative strutture organizzative; i codici che identificano l'Ente sono:

- codice IPA abdam
- codice univoco AOO AJ3MJ3Y

Per qualsiasi informazione relativa all'Amministrazione si rimanda alle pagine del sito istituzionale.

1.5 *Servizio per la gestione documentale e i suoi responsabili*

Il Servizio per la gestione documentale è attribuito alla struttura denominata Protocollo Generale.
Il servizio, in accordo e nel rispetto della normativa vigente, nonché della struttura organizzativa dell'Ente e delle disposizioni che lo regolano:

- garantisce il buon funzionamento degli strumenti e dell'organizzazione delle attività di registrazione di protocollo, di gestione dei documenti e dei flussi documentali, compreso il sistema dei livelli di autorizzazione e delle abilitazioni adottato (Documento n. 2);
- garantisce che le operazioni di registrazione, di segnatura, la produzione e conservazione del registro di protocollo si svolgano nel rispetto della normativa vigente e autorizza le operazioni di annullamento delle registrazioni di protocollo;
- verifica e cura l'osservanza delle disposizioni del presente manuale;
- cura, per quanto di competenza, i processi di dematerializzazione dei flussi documentali e della digitalizzazione dei documenti;
- autorizza, con appositi provvedimenti, le operazioni di annullamento delle registrazioni di protocollo;
- cura il costante aggiornamento del presente manuale di gestione e di tutti i suoi allegati.

Sono nominati il responsabile della gestione documentale e un suo vicario, per casi di vacanza, assenza o impedimento (Documento n. 10). Allo scopo di agevolare l'assolvimento dei compiti assegnatigli, il responsabile della gestione documentale può individuare un delegato, definendone le funzioni meramente operative. Allo scopo di agevolare l'assolvimento dei compiti assegnatigli, il responsabile della gestione documentale può individuare un delegato, definendone le funzioni meramente operative.
È nominato il responsabile della conservazione (Documento n. 10), che d'intesa con il responsabile della gestione documentale svolge le funzioni definite dal paragrafo 4.7 delle Linee guida di Agid, tra cui la predisposizione e l'aggiornamento del Manuale di conservazione (Documento n. 11), garantendo la conservazione integrata dei documenti e delle informazioni di contesto generale, prodotte sia nelle fasi di gestione sia in quelle di conservazione degli stessi, come strumenti di descrizione, ricerca, gestione e conservazione dei documenti.
Come previsto dall'articolo 17 del Codice dell'Amministrazione digitale Dlgs 82/2005 come modificato dal Dlgs 217/2017, è individuato il dirigente dottore Gennaro Capasso che sovraintende la transizione alla modalità operativa digitale e i conseguenti processi di riorganizzazione finalizzati alla realizzazione di un'amministrazione digitale e aperta, di servizi facilmente utilizzabili e di qualità.

1.6 *Unicità del protocollo informatico*

La numerazione delle registrazioni di protocollo è unica, progressiva, corrisponde all'anno solare ed è composta da almeno sette numeri, tuttavia a norma dell'articolo 53, comma 5 del DPR 445/2000 sono possibili registrazioni particolari. L'Ente non riconosce validità a registrazioni particolari che non siano quelle individuate nell'elenco allegato (Documento n. 3). Il sistema informatico di gestione del protocollo è sincronizzato per il calcolo dell'ora con un orologio atomico, tramite server NTP Network time protocol, che garantisce data e ora certe.
A ogni documento è dato un solo numero, che non può essere utilizzato per la registrazione di altri documenti anche se correlati allo stesso.

1.7 *Modello operativo adottato per la gestione dei documenti*

Per la gestione dei documenti è adottato un modello operativo decentrato che prevede la partecipazione attiva di più soggetti e uffici utenti abilitati a svolgere soltanto le operazioni di loro competenza di cui all'elenco allegato (Documento n. 2), le abilitazioni sono definite dal responsabile della gestione documentale.
I dirigenti sono responsabili, secondo i principi stabiliti dalla normativa vigente, della corretta applicazione delle disposizioni contenute nel presente manuale in relazione all'attività della struttura cui sono preposti, con particolare riguardo alle operazioni di protocollazione, classificazione, fascicolazione, conservazione e gestione dei documenti.
Il sistema di gestione documentale e il protocollo informatico sono condotti in modalità Cloud computing definita anche SaaS (Software as a Service), che consente all'Ente di usufruire dei servizi di protocollazione e gestione documentale messi a disposizione dall'applicativo attraverso browser ed erogati da PA Digitale SpA, La sicurezza informatica è demandata all'erogatore dei servizi, PA Digitale SpA, come descritto nel Piano di sicurezza dei documenti informatici (Documento n. 6).

Gli archivi storici e di deposito acquisiti dagli enti soppressi sono conservati presso sedi dell'ente sul territorio di competenza.
L'Archivio corrente analogico è conservato presso le unità organizzative. La documentazione informatica è gestita secondo le modalità descritte nel Piano di sicurezza dei documenti informatici (Documento n. 6), per la conservazione l'Ente si avvale del servizio di conservazione digitale a norma erogato da PA Digitale SpA, conservatore iscritto all'elenco presso l'Agenzia per l'Italia digitale, e adotta il Manuale di conservazione (Documento n. 11).

2 *Formazione dei documenti*

2.1 *Requisiti minimi del documento*

Le modalità di formazione dei documenti, del loro contenuto e della loro struttura sono determinate dal responsabile della gestione documentale e da quanto previsto dal presente manuale; per quanto riguarda i documenti informatici, la loro produzione è regolata come descritto nel Piano di sicurezza dei documenti informatici (Documento n. 6), sulla base di modelli standard presenti nel sistema informatico di gestione documentale. I documenti prodotti e con rilevanza giuridico-amministrativa, indipendentemente dal supporto sul quale sono formati, contengono i seguenti dati ed elementi formali o l'associazione permanente ad essi:

- denominazione dell'Amministrazione, comprensiva del codice fiscale e del codice identificativo di cui all'articolo 1.4; per quanto riguarda i documenti su supporto cartaceo si utilizza il formato predisposto dall'Amministrazione (carta intestata);
- indicazione del settore, servizio o ufficio che ha prodotto il documento;
- indirizzo completo (via, numero civico, codice avviamento postale, città, sigla della provincia, numero di telefono, indirizzo di posta elettronica certificata e posta elettronica ordinaria);
- data: luogo, giorno, mese, anno;
- destinatario/i, per i documenti in partenza;
- oggetto del documento, sufficientemente esaustivo (ogni documento deve trattare un solo oggetto);
- classificazione;
- fascicolo;
- numero degli allegati, se presenti;
- numero di protocollo;
- testo;
- indicazione dello scrittore del documento (nome e cognome anche abbreviato);
- estremi identificativi del responsabile del procedimento (L. 241/1990);
- sottoscrizione autografa o elettronico/digitale.

Per i documenti informatici il numero di protocollo è associato al documento. Il sistema crea una copia del documento principale sul quale appone i dati di registrazione, numero e data di protocollazione.

2.2 *Formazione dei documenti informatici*

L'Ente forma gli originali dei propri documenti con mezzi informatici secondo le regole tecniche di cui all'articolo 71 del Codice dell'Amministrazione digitale Dlgs 82/2005 come modificato dal Dlgs 217/2017, mediante l'utilizzo di appositi strumenti software. Le tipologie particolari di documenti per i quali si stabiliscono modalità di trattamento specifiche e/o prodotti mediante modelli standard sono indicati nella Sezione 5.

2.3 *Formato dei documenti informatici*

I documenti informatici prodotti dall'Ente, indipendentemente dal software utilizzato, prima della loro sottoscrizione con firma elettronica/digitale, sono convertiti in uno dei formati standard previsti dalla normativa vigente in materia di documenti informatici (Linee Guida di Agid, Allegato 2 Formati di file e riversamento), al fine di garantire la loro inalterabilità durante le fasi di accesso e conservazione e l'immutabilità nel tempo del contenuto e della struttura. Il formato prescelto e utilizzato è pdf/A, che garantisce staticità e immodificabilità, ma al contempo assicura la leggibilità dei documenti.

2.4 *Metadati dei documenti informatici*

Al documento informatico è associato l'insieme dei metadati, come definito dalla normativa vigente in materia di documenti informatici (articolo 53 del DPR 445/2000; articolo 9 del DPCM 3/12/2013 Regole tecniche per il protocollo informatico e Allegato 5 Metadati sino al 1° gennaio 2022 e successivamente Linee guida di Agid, Allegato 5 I metadati).
Per metadati si intendono i dati associati a un documento informatico per identificarlo e descriverne il contesto, il contenuto e la struttura, nonché per permetterne la gestione nel tempo nel sistema di conservazione.
I metadati aggiuntivi e i metadati dei documenti informatici soggetti a registrazione particolare (Documento n. 3) sono individuati nel Manuale di conservazione (Documento n. 11).

2.5 *Sottoscrizione dei documenti informatici*

La sottoscrizione dei documenti informatici è ottenuta con un processo di firma elettronico/digitale conforme alle disposizioni di legge.
L'Ente utilizza:

- firme elettroniche semplici (come la posta elettronica);
- firme elettroniche avanzata (come l'accreditamento per le procedure telematiche e sistema di validazione delle fasi procedimentali, di comunicazione interna e abilitazione allo svolgimento di attività specifiche);
- firme digitali o di altro tipo di firma elettronica qualificata.

L'Ente ha stipulato un contratto di fornitura di servizio di firme digitali con un certificatore accreditato. Gli strumenti tecnologici utilizzati sono: smart card / tokien / firma remota.
I responsabili di Servizio e alcuni dipendenti con specifiche mansioni e ruoli con rilevanza esterna, in base all'organigramma dell'Ente, sono dotati di firma digitale.
Il dispositivo per la generazione della firma digitale è usato esclusivamente dal titolare designato dall'Ente; ai sensi della normativa vigente tale utilizzo si presume comunque riconducibile al titolare, salvo che questi dia prova contraria.
Il responsabile dei Sistemi informativi dell'Ente provvede al controllo della scadenza dei certificati di firma e al loro eventuale rinnovo.

3 *Ricezione dei documenti*

3.1 *Ricezione dei documenti su supporto cartaceo*

I documenti su supporto cartaceo possono arrivare all'Ente attraverso:

- il servizio postale e corrieri;
- la consegna diretta agli uffici, ai funzionari, agli sportelli abilitati presso l'Amministrazione al ricevimento della documentazione;

I documenti, esclusi quelli non soggetti a registrazione di protocollo, devono pervenire al protocollo per la loro registrazione.
La corrispondenza indirizzata alla cortese attenzione del personale dell'Ente è regolarmente aperta e registrata a protocollo. Non è ammessa la ricezione di corrispondenza di carattere personale; l'ufficio che provvede alla protocollazione è in ogni caso tenuto a verificare il contenuto della corrispondenza pervenuta.

3.2 *Ricezione dei documenti informatici*

La ricezione di comunicazioni, documenti e dati informatici è assicurata tramite:

- caselle di posta elettronica certificata elette a domicilio digitale e integrate con il sistema informatico di protocollazione, accessibile solo dall'Ufficio Protocollo, che effettua la protocollazione. Il responsabile della gestione documentale provvede a rendere pubblico e a trasmettere all'Indice dei domicili digitali delle Pubbliche Amministrazioni e dei gestori di pubblici servizi IPA (ai sensi delle Linee guida Agid, versione 1.0 del 27 febbraio 2019) gli indirizzi delle caselle di posta elettronica certificata.
- servizi on line resi disponibili dal sito istituzionale dell'Ente, tramite accesso con autenticazione elettronica dell'utente. I servizi on line consentono il conferimento controllato di documenti, in particolare legati a specifici procedimenti amministrativi, assolvendo anche il compito di verifica formale di accettabilità degli stessi. I servizi on line sono integrati con il sistema di protocollo informatico, che effettua la registrazione automatica dei documenti conferiti.

Non è possibile ricevere messaggi di posta elettronica ordinaria sulle caselle di posta elettronica certificata dell'Ente. Per le comunicazioni provenienti da indirizzi di posta elettronica ordinaria, si rendono pubblici e disponibili gli indirizzi di posta elettronica degli uffici pubblicati sul sito istituzionale dell'Ente.
Per la gestione della posta elettronica si veda quanto previsto alla Sezione 6.
L'Amministrazione riceve e trasmette documenti informatici mediante flussi telematici di dati (si veda l'articolo 5.12 Trasmissioni telematiche e procedimenti amministrativi on line).

3.3 *Formato e firma dei documenti informatici ricevuti*

L'Ente assicura l'accettazione dei documenti elettronici ricevuti tramite la casella di posta elettronica certificata, i servizi telematici o consegnati su supporto informatico quando prodotti in uno dei formati indicati dalle Linee Guida di Agid, Allegato 2 Formati di file e riversamento.
Nel caso il documento ricevuto non risulti leggibile, l'Ente ne darà comunicazione al mittente richiedendo contestualmente la ripetizione dell'invio.
In ogni caso i documenti elettronici inviati o consegnati all'Ente non dovranno contenere elementi attivi, tra cui macro e campi variabili.
Le verifiche dei documenti sono effettuate dall'Ufficio Protocollo e dai servizi che provvedono alla protocollazione. Il certificato di firma è verificato da parte delle postazioni abilitate alla registrazione dei documenti in ingresso e/o dal responsabile del procedimento. In caso di certificati scaduti o revocati si rimanda alla Sezione 5.

3.4 Acquisizione dei documenti analogici tramite copia informatica

L'Ente può acquisire i documenti analogici originali attraverso la copia per immagine su supporto informatico o la copia informatica.
Dei documenti analogici ricevuti viene effettuata copia immagine e il documento originale viene consegnato all'ufficio competente. Le immagini digitali dei documenti cartacei acquisite con lo scanner sono rese disponibili agli uffici, o ai responsabili di procedimento, tramite il sistema informatico di gestione documentale. Il processo di scansione della documentazione cartacea è descritto nella Sezione 10.

Le copie informatiche di documenti analogici sono acquisite nel sistema mediante processi e strumenti che assicurino che il documento informatico abbia contenuto identico a quello del documento analogico da cui è tratto.
Le copie per immagine e le copie informatiche di uno o più documenti analogici possono essere sottoscritte con firma digitale o firma elettronica qualificata da chi effettua la copia. Affinché le copie non siano disconoscibili, esse devono essere firmate da un pubblico ufficiale.
L'attestazione di conformità della copia informatica e della copia per immagine di un documento analogico può essere inserita nel documento informatico contenente la copia, oppure può essere prodotta come documento informatico separato contenente un riferimento temporale e l'impronta della copia. Il documento informatico prodotto è sottoscritto con firma digitale o con firma elettronica qualificata del funzionario delegato.
Le copie immagine e le copie informatiche di documenti analogici vengono prodotte secondo quanto previsto dalle Linee Guida di Agid.
L'unitarietà è garantita dal sistema mediante il numero di protocollo, l'indice di classificazione e il numero di fascicolo.

3.5 *Ricevute attestanti la ricezione dei documenti*

La ricevuta della consegna di un documento analogico può essere costituita dalla fotocopia del primo foglio del documento stesso con un timbro che attesti il giorno della consegna. Compatibilmente con le esigenze del servizio, si procederà alla protocollazione del documento: in tal caso verrà consegnata la ricevuta prodotta automaticamente del sistema di protocollo informatico.
Nel caso di ricezione dei documenti informatici, la notifica al mittente dell'avvenuto ricevimento è assicurata dal sistema elettronico.
Per istanze, segnalazioni o comunicazioni è rilasciata immediata ricevuta ai sensi dell'articolo 18 bis della L. 241/1990. La data di protocollazione non può comunque essere diversa da quella di effettiva presentazione, in seguito alla protocollazione del documento il sistema genera in automatico una ricevuta che riporta anche il numero di protocollo assegnato.

3.6 *Apertura della posta*

L'Ufficio Protocollo apre tutta la corrispondenza pervenuta all'Ente, salvo i casi particolari specificati nella Sezione 5, compresa la posta elettronica certificata.

3.7 *Conservazione delle buste o altri contenitori di documentazione analogica*

Le buste dei documenti analogici pervenuti si inoltrano agli uffici destinatari.

3.8 *Conservazione delle ricevute attestanti la consegna dei documenti spediti tramite posta elettronica certificata*

Le ricevute relative alla trasmissione di documenti informatici tramite casella di posta elettronica certificata, in quanto documenti informatici, sono soggette alle operazioni di conservazione.
Il sistema di protocollo informatico associa in automatico le ricevute pec alla registrazione di protocollo.

3.9 *Orari di apertura per il ricevimento della documentazione cartacea*

L'Ufficio protocollo riceve la documentazione negli orari di apertura al pubblico, pubblicati sul sito internet istituzionale.

4 *Registrazione dei documenti*

4.1 *Documenti soggetti a registrazione di protocollo*

Tutti i documenti prodotti e ricevuti dall'Amministrazione, indipendentemente dal supporto sul quale sono formati, a eccezione di quelli indicati nel successivo articolo, sono registrati al protocollo.
I documenti ai fini della gestione documentale si distinguono in:

- documenti in arrivo, cioè documenti ricevuti dall'esterno dall'Ente;
- documenti in partenza, cioè i documenti prodotti e spediti all'esterno dall'Ente;
- documenti interni, cioè documenti prodotti all'interno dell'Ente, che siano o meno scambiati tra strutture.

4.2 *Documenti non soggetti a registrazione di protocollo*

Sono esclusi dalla registrazione di protocollo: gazzette ufficiali, bollettini ufficiali, notiziari della pubblica amministrazione, note di ricezione delle circolari e di altre disposizioni, materiale statistico ricevuto, atti preparatori interni, giornali, riviste, materiale pubblicitario, inviti a manifestazioni, stampe varie, plichi di libri e tutti quei documenti già soggetti a registrazione particolare da parte dell'Ente il cui elenco è allegato al presente manuale (Documento n. 3).
Inoltre, sono escluse dalla protocollazione le seguenti categorie di documenti:

- pubblicità conoscitiva di convegni;
- pubblicità in generale;
- offerte, i listini prezzi e i preventivi di terzi non richiesti;
- ricevute di ritorno delle raccomandate A.R.;
- tutti i documenti che, per loro natura, non rivestono alcuna rilevanza giuridico amministrativa presente o futura.

4.3 *Registrazione di protocollo dei documenti ricevuti e spediti*

La registrazione dei documenti ricevuti o spediti è effettuata in un'unica operazione. I requisiti necessari di ciascuna registrazione di protocollo sono:

- numero di protocollo, generato automaticamente dal sistema e registrato in forma non modificabile;
- data di registrazione di protocollo, assegnata automaticamente dal sistema e registrata in forma non modificabile;
- mittente o destinatario dei documenti ricevuti o spediti, registrato in forma non modificabile;
- oggetto del documento, registrato in forma non modificabile;
- data e numero di protocollo dei documenti ricevuti, se disponibili;
- impronta del documento informatico, se trasmesso per via telematica, registrato in forma non modificabile;
- classificazione (si veda titolario allegato Documento n. 5);
- assegnazione.

Inoltre possono essere aggiunti:

- data di arrivo;
- allegati (numero e descrizione);
- estremi del provvedimento differimento dei termini di registrazione;
- mezzo di ricezione/spedizione;
- tipo di documento;
- livello di riservatezza;
- elementi identificativi del procedimento amministrativo;
- classificazione e fascicolazione del documento ricevuto.

La fascicolazione dei documenti ricevuti è effettuata successivamente alla registrazione di protocollo, da parte dell'ufficio assegnatario del documento.

Per il corretto inserimento dei dati relativi a mittenti e destinatari nella banca dati dei soggetti si applicano le Linee guida per l'inserimento e l'aggiornamento dei dati nel protocollo informatico (Documento n. 4).

4.4 *Registrazione dei documenti interni*

I documenti prodotti dall'Ente a solo uso interno, che non costituiscono atti preparatori e non rientrano in quelli esclusi da protocollazione, indipendentemente dal supporto sul quale sono formati, sono protocollati.

4.5 *Formazione di registri e repertori informatici particolari*

L'Ente forma i propri registri e repertori informatici particolari (Documento n. 3) mediante la generazione o raggruppamento anche in via automatica di un insieme di dati o registrazioni, provenienti da una o più basi dati, secondo una struttura logica predeterminata e memorizzata in forma statica.
Ogni registrazione deve riportare necessariamente:

- dati identificativi di ciascun atto (autore, destinatario, oggetto, data: generati in modo non modificabile);
- numero di repertorio progressivo e annuale (generato in modo non modificabile).

4.6 *Registrazione degli allegati*

Il numero e la descrizione degli allegati sono elementi essenziali per l'efficacia di una registrazione. Nella registrazione di protocollo/particolare si riporta la descrizione della tipologia degli allegati e, se significativi, anche dei loro estremi (data, numero, ecc).
Tutti gli allegati devono pervenire con il documento principale alle postazioni abilitate alla protocollazione al fine di essere inseriti nel sistema di gestione documentale. In presenza di allegati analogici su ciascuno è riportata la segnatura di protocollo.

4.7 *Segnatura di protocollo*

La segnatura di protocollo è l'associazione ai documenti in forma permanente e non modificabile di informazioni riguardanti i documenti stessi, utile alla sua identificazione univoca e certa.
In merito l'articolo 55, comma 1, del DPR 445/2000 individua le informazioni che caratterizzano la segnatura di protocollo.
Le operazioni di segnatura e registrazione di protocollo sono effettuate contemporaneamente.
Gli standard, le modalità di trasmissione, il formato e le definizioni dei tipi di informazioni minime e accessorie comunemente scambiate tra le Pubbliche Amministrazioni e associate ai documenti protocollati sono definiti dalle Linee Guida di Agid, Allegato 6 Comunicazione tra AOO di Documenti Amministrativi Protocollati.
Per i documenti informatici trasmessi i dati relativi alla segnatura di protocollo sono contenuti, un'unica volta nell'ambito dello stesso messaggio, in un file conforme alle specifiche dell'Extensible Markup Language (XML); per i documenti cartacei la segnatura di protocollo è apposta al documento mediate timbro.

4.8 *Annullamento delle registrazioni di protocollo*

Le registrazioni di protocollo possono essere annullate e/o modificate con una specifica funzione del sistema di gestione informatica dei documenti, a seguito di motivata richiesta scritta al responsabile della gestione documentale o per iniziativa dello stesso. Le registrazioni annullate rimangono memorizzate nella base di dati e sono evidenziate dal sistema. Il sistema durante la fase di annullamento registra le motivazioni che hanno comportato l'annullamento. Le richieste di annullamento dei numeri di protocollo devono pervenire all'Ufficio Protocollo. Sui documenti cartacei è apposto il timbro di annullamento; il documento è conservato, anche fotoriprodotto, a cura dell'Ufficio Protocollo.
Le modifiche effettuate direttamente dal responsabile della gestione documentale o dai suoi sostituti equivalgono implicitamente ad autorizzazione.
Non è possibile annullare il solo numero di protocollo e mantenere valide le altre informazioni della registrazione.

4.9 *Differimento dei termini di protocollazione*

La registrazione della documentazione pervenuta avviene nell'arco della giornata o nella successiva giornata lavorativa. Il responsabile della gestione documentale, con apposito provvedimento motivato, può autorizzare la registrazione in tempi successivi, fissando un limite di tempo entro il quale i documenti devono essere protocollati. Ai fini giuridici i termini decorrono dalla data di ricezione riportata sul documento analogico tramite un apposito timbro e dalla data di consegna telematica (tramite pec o servizi on line) per i documenti informatici.

4.10 *Registro giornaliero e registro delle modifiche*

Il registro giornaliero di protocollo comprende tutte le registrazioni effettuate nell'arco dello stesso giorno; ciascuna registrazione include le informazioni minime previste dal DPR 445/2000, articolo 53.
Il registro delle modifiche comprende le registrazioni annullate e modificate; viene creato solo se nella giornata sono stati effettuati annullamenti o modifiche a protocolli precedentemente acquisiti.
Il registro giornaliero e il registro delle modifiche sono trasmessi entro la giornata lavorativa successiva al sistema di conservazione, garantendone l'immodificabilità del contenuto. Si tratta di documenti informatici creati in PDF/A, formato adeguato (Linee Guida di Agid, Allegato 2 Formati di file e riversamento) che assicura staticità e immodificabilità, ma al contempo ne consente la leggibilità. Il registro giornaliero e il registro delle modifiche sono integrati con i relativi metadati di identificazione, di profilo generali e specifici, che ne definiscono contesto, contenuto e struttura. La produzione del registro giornaliero e del registro delle modifiche è effettuata automaticamente dal sistema dopo lo scattare della mezzanotte della giornata di riferimento.
Il trasferimento nel sistema di conservazione avviene generando un pacchetto di versamento secondo le modalità concordate con il responsabile della conservazione. Il sistema di conservazione produce un rapporto dell'esito del versamento.
La conservazione del Registro giornaliero di protocollo è affidata a PA Digitale SpA, conservatore iscritto nell'elenco presso l'Agenzia per l'Italia digitale.
Il sistema di conservazione è descritto nel Manuale di conservazione (Documento n. 11); le iniziative di prevenzione e gestione degli incidenti di sicurezza informatica sono illustrate nel Piano di sicurezza dei documenti informatici (Documento n. 6).
Per quanto riguarda le procedure di conservazione della memoria informatica si veda anche la Sezione 11.

4.11 *Registro di emergenza*

Il responsabile della gestione documentale autorizza lo svolgimento delle operazioni di protocollo su un registro di emergenza a norma dell'articolo 63 del DPR 445/2000 e provvede successivamente a impartire le disposizioni per il riversamento dei dati nel protocollo informatico (Documento n. 8). All'inizio di ogni anno il responsabile della gestione documentale provvede a istituire il registro di emergenza su supporto cartaceo.

5 *Documentazione particolare*

5.1 *Deliberazioni della Conferenza Istituzionale Permanente e della Conferenza operativa, decreti del Segretario Generale, contratti e altri tipi di verbalizzazioni previsti dalla legge o da regolamenti*

Le deliberazioni della Conferenza Istituzionale Permanente e della Conferenza operativa, i decreti del Segretario Generale, i contratti, e altri tipi di verbalizzazioni previsti dalla legge o da regolamenti, se sono documenti già soggetti a registrazione particolare da parte dell'Ente possono non essere registrati al protocollo.
L'elenco dettagliato delle registrazioni particolari è fornito in allegato (Documento n. 3).
Il sistema di produzione e conservazione di queste tipologie particolari di documenti deve consentire di eseguire su di essa tutte le operazioni previste nell'ambito della gestione dei documenti e del sistema adottato per il protocollo informatico. Ogni registrazione deve riportare necessariamente:

- dati identificativi di ciascun atto (autore, destinatario, oggetto, data, generati in modo non modificabile);
- numero di repertorio progressivo e annuale (generato in modo non modificabile).

5.2 *Documentazione di gare d'appalto*

L'Ente si avvale del Mercato della Pubblica Amministrazione (Me.Pa) e di piattaforma telematica di e-procurement per attivare e gestire gare telematiche. Per procedure nel mercato elettronico o acquisti effettuati mediante piattaforme informatiche, tutta la documentazione è ricevuta telematicamente direttamente nel sistema, che ne garantisce la sicurezza e riservatezza, acquisita nel sistema di gestione documentale e registrata nel protocollo informatico dell'Ente.

5.3 *Documenti con mittente non identificabile, posta personale*

I documenti, sia analogici che digitali, indirizzati nominalmente al personale dell'Ente sono regolarmente aperti e registrati al protocollo.
Non è ammessa la ricezione di corrispondenza di carattere personale; nel caso in cui risulti esplicita l'attribuzione "personale" o "riservata personale", il documento sarà trasmesso al destinatario, che potrà chiederne la protocollazione. L'ufficio che provvede alla protocollazione è in ogni caso tenuto a verificare il contenuto della corrispondenza pervenuta.
I documenti di cui non sia identificabile il mittente vengono protocollati con indicazione di mittente "anonimo".

5.4 *Protocollo riservato*

Sono previste particolari forme di riservatezza per la registrazione e l'accesso a:

- documenti legati a vicende di persone o a fatti privati o particolari;
- documenti di carattere politico e di indirizzo che, se resi noti, possono ostacolare il raggiungimento degli obiettivi prefissati;
- documenti dalla cui conoscenza, anche da parte del personale dell'Ente, possa derivare pregiudizio a terzi o al buon andamento dell'attività amministrativa;

Il responsabile della gestione documentale dispone la registrazione riservata informatica dei documenti. La registrazione è effettuata nel registro del protocollo generale da personale al tal fine autorizzato. Tali documenti se cartacei, dopo le operazioni di protocollo, vengono reinseriti nella busta opportunamente chiusa ed inviati agli uffici di competenza.

5.5 *Documenti informatici con certificato di firma scaduto o revocato*

Nel caso in cui l'Ente riceva documenti informatici firmati digitalmente il cui certificato di firma risulta scaduto o revocato, questi verranno protocollati, il responsabile di procedimento effettuerà le necessarie verifiche e darà opportuna comunicazione al mittente.

5.6 *Corrispondenza con più destinatari*

Tutte le comunicazioni che abbiano più destinatari si registrano con un solo numero di protocollo.

5.7 *Allegati*

Tutti gli allegati devono essere trasmessi con i documenti a cui afferiscono all'ufficio/postazioni decentrate di protocollo per la registrazione. Il sistema informatico provvede automaticamente a registrare gli allegati come parte integrante di un documento informatico. Nel caso in cui allegati illeggibili pervengano tramite posta elettronica certificata, si dovrà chiedere chiarimenti al mittente in merito al documento. Su ogni allegato analogico è riportato il timbro della segnatura di protocollo.

5.8 *Documenti di competenza di altre amministrazioni*

Qualora pervengano all'Ente documenti di competenza di altre amministrazioni, questi vanno rimandati al mittente.

5.9 *Oggetti plurimi*

Qualora un documento in entrata presenti più oggetti, relativi a procedimenti diversi, il documento dovrà essere assegnato agli uffici competenti e verrà classificato e fascicolato in base all'argomento o affare trattato, pertanto potrà essere inserito in più fascicoli diversi. Nel caso in cui l'individuazione di più oggetti venga effettuata successivamente da parte dell'ufficio assegnatario, questi deve inviare all'Ufficio Protocollo apposita comunicazione affinché si provveda alle ulteriori assegnazioni necessarie.
Ciascun documento in uscita avrà un unico oggetto.

5.10 *Documentazione prodotta e registrata in appositi gestionali*

Il Servizio Ragioneria è responsabile della gestione delle fatture attraverso un sistema informatico di gestione della contabilità. Le fatture pervenute vengono registrate automaticamente dal sistema di protocollo informatico.
I mandati di pagamento e le riversali d'incasso sono gestiti tramite ordinativi informatici; i movimenti sono gestiti e inviati alla Tesoreria attraverso flusso informatico dei relativi tracciati. L'Ente, con credenziali di accesso fornite dalla banca della Tesoreria stessa, accede direttamente alla piattaforma di scambio dei flussi.

5.11 *Modelli pubblicati di documenti*

Tutti i modelli sono pubblicati sul sito internet o sulla rete intranet dell'Ente nei formati indicati nelle Linee Guida di Agid, Allegato 2 Formati di file e riversamento e sono classificati secondo il piano di classificazione in uso (Documento n. 5).

5.12 *Trasmissioni telematiche e procedimenti amministrativi on line*

I documenti di cui all'allegato Documento n. 7 sono trasmessi dall'Ente con immissione diretta dei dati nel sistema dell'ente destinatario. I documenti possono essere privi di firma digitale in quanto inviati tramite linee di comunicazione sicure, riservate e a identificazione univoca, attivate con i singoli enti destinatari. Gli invii telematici sostituiscono integralmente gli invii cartacei della medesima documentazione.
L'Ente tramite i servizi on line, disponibili dal sito istituzionale, riceve e protocolla documenti relativi a specifici procedimenti amministrativi. Il sistema effettua la verifica formale di accettabilità e identifica i mittenti in modo certo tramite autenticazione e identità digitale. I servizi on line sono integrati con il sistema di protocollo informatico, che effettua la registrazione automatica dei documenti conferiti.

5.13 *Produzione di copie cartacee di documenti informatici e di copie informatiche di documenti cartacei*

Nel caso di produzione di copie cartacee di documenti informatici dovranno essere obbligatoriamente redatte attestazioni che riportino dati e indicazioni previsti dai modelli predisposti (Documento n. 10).
Per gli atti amministrativi e i documenti informatici sottoscritti con firma digitale e protocollati l'Ente può avvalersi del contrassegno digitale.
Dei documenti analogici prodotti/pervenuti, per i quali è necessaria la distribuzione interna all'Ente, si faranno copie informatiche degli stessi.

5.14 *Amministrazione trasparente*

Sul sito internet istituzionale dell'Ente è stata attivata la "Sezione Amministrazione trasparente", recante i dati e le informazioni di pubblica evidenza che l'Amministrazione deve rendere disponibili on-line in applicazione del Dlgs 33/2013. Ciascuna unita operativa cura la pubblicazione dei dati di propria competenza così come indicato nel Piano triennale di prevenzione della corruzione e della trasparenza.

6 *Posta elettronica*

6.1 Posta elettronica certificata

La casella istituzionale di posta elettronica certificata dell'Amministrazione, integrata con il sistema di protocollo informatico, è adeguata allo scambio di messaggi con altre pubbliche amministrazione e rappresenta l'indirizzo ufficiale anche per cittadini, imprese, professionisti e altri soggetti dotati di analoghi strumenti di trasmissione. L'Amministrazione accetta dunque le istanze e le dichiarazioni trasmesse attraverso la casella di posta elettronica certificata. Vengono protocollati i documenti-file allegati e anche il solo corpo del messaggio, se privo di allegati. Qualora i file non siano corredati di firma digitale, verranno protocollati e assegnati all'ufficio competente, successivamente il responsabile del procedimento provvederà alla valutazione del contenuto del documento e della sua ammissibilità ai fini del procedimento amministrativo a cui si riferisce.
L'Ente ha adempiuto agli obblighi normativi dotandosi di un indirizzo di posta elettronica certificata, pubblicando tale indirizzo sulla home page del sito internet istituzionale e comunicandolo all'Indice dei domicili digitali delle Pubbliche Amministrazioni e dei gestori di pubblici servizi (IPA).
Non è possibile ricevere messaggi di posta elettronica ordinaria sulle caselle di posta elettronica certificata dell'Ente. Per le comunicazioni provenienti da indirizzi di posta elettronica ordinaria, si rendono pubblici e disponibili gli indirizzi di posta elettronica degli uffici pubblicati sul sito istituzionale dell'Ente

6.2 Gestione della posta elettronica

La posta elettronica viene utilizzata per l'invio di comunicazioni, informazioni e documenti sia all'interno dell'Ente, che nei rapporti con i cittadini e altri soggetti privati e con altre pubbliche amministrazioni.
La trasmissione di documenti tramite la posta elettronica deve attenersi alle norme e alle regole vigenti al fine di garantirne la validità legale e amministrativa, nonché la corretta gestione nel protocollo informatico, nel sistema di gestione documentale e nel sistema di conservazione dell'Ente.
Le comunicazioni formali e la trasmissione di documenti informatici, il cui contenuto impegni l'Ente verso terzi, avvengono tramite la casella di posta elettronica certificata istituzionale, eletta come domicilio digitale e le caselle di posta elettronica certificata attribuite ai servizi.
Le semplici comunicazioni informali ricevute o trasmesse per posta elettronica, che consistano in scambio di informazioni, possono non essere protocollate.
Qualora risulti necessario attribuire efficacia probatoria a documenti informatici e messaggi pervenuti alle caselle di posta degli uffici, questi dovranno essere acquisiti tramite il sistema di protocollo informatico.
Non è possibile inviare messaggi dalla casella di posta elettronica personale quando il contenuto di questi impegni l'Amministrazione verso terzi. Per quanto riguarda la gestione della posta elettronica nelle pubbliche amministrazioni, si rimanda agli articoli 45-49 del Codice dell'Amministrazione digitale Dlgs 82/2005 come modificato dal Dlgs 217/2017.
La posta elettronica nominativa non può essere utilizzata per la ricezione o la spedizione di documenti a firma digitale, per i quali è prevista apposita casella istituzionale.

6.3 Posta elettronica per le comunicazioni interne

Le comunicazioni tra l'Ente e i propri dipendenti, nonché tra le varie strutture, avvengono di norma mediante l'utilizzo della casella di posta elettronica ordinaria dei rispettivi uffici o nominative, nel rispetto delle norme in materia di protezione dei dati personali, nonché previa informativa agli interessati circa il grado di riservatezza degli strumenti utilizzati.
Nell'ambito dell'attività amministrativa interna è sufficiente un semplice messaggio di posta elettronica per:

- convocare riunioni interne all'Ente;
- inviare comunicazioni di servizio o notizie, dirette ai dipendenti in merito a informazioni generali di organizzazione;
- diffondere circolari, ordini di servizio, copie di documenti (gli originali si conservano nel fascicolo specifico debitamente registrati).

6.4 *Posta elettronica ricevuta da cittadini o altri soggetti privati*

Le istanze e le dichiarazioni trasmesse per via telematica all'indirizzo istituzionale devono ritenersi valide a tutti gli effetti di legge qualora:

- sono trasmesse via posta elettronica o via posta elettronica certificata, regolarmente sottoscritte con firma elettronica/digitale dotata di certificato valido rilasciato da un certificatore accreditato;
- l'autore del documento è identificato attraverso il sistema pubblico di identità digitale (SPID), la carta di identità elettronica o la carta nazionale dei servizi;
- sono formate tramite il punto di accesso telematico per i dispositivi mobili, IO APP, definito dall'articolo 64-bis del Codice dell'Amministrazione digitale Dlgs 82/2005;
- siano sottoscritte e presentate unitamente alla copia del documento d'identità;
- sono trasmesse da domicilio digitale oppure da un indirizzo elettronico eletto presso un servizio di posta elettronica certificata o un servizio elettronico di recapito certificato qualificato

Al di fuori delle predette ipotesi, le comunicazioni di posta elettronica che pervengono all'indirizzo istituzionale, dei singoli servizi o a quelli nominativi, sono valutate in ragione della loro rispondenza a ragionevoli criteri di attendibilità e riconducibilità al mittente dichiarato, e successivamente soggette, se del caso, a protocollazione. Spetterà al responsabile del procedimento, ove ne rilevi la necessità, richiedere al mittente la regolarizzazione dell'istanza o della dichiarazione, acquisendo ogni utile documentazione integrativa.

6.5 Posta elettronica ricevuta da altre pubbliche amministrazioni

Le comunicazioni e i documenti ricevuti da altre pubbliche amministrazioni sono valide ai fini del procedimento una volta che ne sia verificata la provenienza, ovvero quando:

- sono trasmessi attraverso sistemi di posta elettronica certificata o altro servizio elettronico di recapito certificato;
- sono sottoscritti con firma elettronica/digitale;
- sono dotati di segnatura di protocollo.

7 *Assegnazione dei documenti*

7.1 *Assegnazione*

L'assegnazione dei documenti agli uffici è effettuata dagli operatori dell'Ufficio Protocollo, delegati dal responsabile della gestione documentale sulla base delle indicazioni del Segretario Generale, tramite il sistema di gestione documentale. Le abilitazioni all'assegnazione dei documenti, effettuate da altri uffici, sono rilasciate dal responsabile della gestione documentale.
Anche le assegnazioni per conoscenza devono essere effettuate tramite il sistema di gestione documentale.
Spettano al responsabile del procedimento amministrativo le incombenze relative alla gestione del documento, l'inserimento nel fascicolo di competenza.
I documenti ricevuti dall'Ente, al termine delle operazioni di registrazione, classificazione, segnatura e assegnazione, sono fatti pervenire in originale agli uffici competenti.

7.2 *Modifica delle assegnazioni*

Nel caso di assegnazione errata dei documenti, l'ufficio che ha ricevuto il documento è tenuto a restituirlo all'Ufficio protocollo, che provvederà alla riassegnazione al corretto assegnatario, sulla base delle indicazioni del segretario Generale.
Il sistema di gestione informatica dei documenti tiene traccia delle rassegnazioni e dei movimenti dei documenti.

7.3 *Consegna dei documenti*

I documenti informatici e le immagini digitali dei documenti cartacei acquisite con lo scanner sono resi disponibili agli uffici tramite il sistema informatico di gestione documentale. Si veda anche la Sezione 10.
I documenti analogici protocollati e assegnati sono resi disponibili ai destinatari mediante l'uso di apposite cartelle per ufficio per la posta in arrivo; ciascun ufficio provvede a ritirare la corrispondenza depositata nelle cartelle.

8 *Classificazione e fascicolazione dei documenti*

8.1 *Classificazione dei documenti*

Tutti i documenti ricevuti o prodotti, indipendentemente dal supporto sul quale sono formati, sono classificati in base al titolario (Documento n. 5). I documenti prodotti dall'Ente sono classificati da chi li scrive pertanto perverranno alle postazioni di protocollo già classificati, i dati di classificazione sono riportati sui documenti. Il programma di protocollo informatico non permette la registrazione di documenti non classificati. I documenti in arrivo sono classificati dall'Ufficio Protocollo, i documenti prodotti dall'Ente sono classificati dalle postazioni di protocollo in uscita.
Il sistema in fase di protocollazione classifica in automatico le fatture elettroniche.

8.2 *Formazione e identificazione dei fascicoli*

Tutti i documenti, indipendentemente dal supporto sul quale vengono formati, sono riuniti in fascicoli o serie documentarie. L'apertura dei fascicoli è effettuata dai responsabili di servizio o di procedimento, o dai collaboratori abilitati a questa funzione (Documento n. 2). La formazione di un nuovo fascicolo avviene attraverso l'operazione di apertura, che prevede la registrazione nel sistema informatico delle seguenti informazioni:

- classificazione;
- numero del fascicolo (la numerazione dei fascicoli è annuale e indipendente per classificazione);
- oggetto del fascicolo;
- data di apertura;
- ufficio assegnatario;
- responsabile del procedimento, se informazione disponibile.

Il sistema di protocollo informatico aggiorna automaticamente il repertorio/elenco dei fascicoli.

8.3 *Processo di fascicolazione*

In presenza di un documento da inserire in un fascicolo, i responsabili di servizio e procedimento o i collaboratori stabiliscono, consultando le funzioni del protocollo informatico, se esso si colloca nell'ambito di un affare o procedimento in corso oppure se da avvio a un nuovo procedimento, in quest'ultimo caso aprono un nuovo fascicolo (seguendo le procedure descritte nell'articolo precedente).
I responsabili di servizio e procedimento o i collaboratori, hanno cura di inserire nei fascicoli i documenti in arrivo, già protocollati e classificati dall'Ufficio Protocollo/uffici protocollo decentrati presso i servizi. I documenti prodotti dall'Ente sono fascicolati da chi li scrive, pertanto perverranno alle postazioni di protocollo già con l'indicazione dell'identificativo di fascicolo.
Nel caso di documenti informatici il sistema provvede automaticamente, dopo l'assegnazione del numero di fascicolo, a inserire il documento nel fascicolo informatico stesso. I documenti analogici sono fisicamente inseriti nei fascicoli cartacei dal responsabile di servizio/procedimento.
Ai documenti informatici prodotti tramite gli applicativi gestionali e l'utilizzo di modelli standard o creati dall'utente attraverso moduli e formulari, resi disponibili mediante servizi on line, sono associati automaticamente dal sistema di gestione documentale i metadati minimi del fascicolo informatico o aggregazione documentale informatica cui appartengono o a cui danno avvio.
Il sistema in fase di protocollazione fascicola in automatico le fatture elettroniche.

8.4 *Modifica delle assegnazioni dei fascicoli*

La riassegnazione di un fascicolo è effettuata, su istanza scritta dell'ufficio che ha in carico il fascicolo dal responsabile di procedimento che provvede a modificare le informazioni del sistema informatico e del repertorio dei fascicoli e inviare il fascicolo all'ufficio del responsabile del procedimento di nuova assegnazione. Delle operazioni di riassegnazione è conservata traccia nel sistema informatico di gestione dei documenti.

8.5 *Fascicolo ibrido*

Il fascicolo ibrido è composto da documenti formati su due supporti, quello cartaceo e quello informatico, afferenti a un affare o procedimento amministrativo che dà origine a due unità archivistiche di conservazione differenti. L'unitarietà del fascicolo è garantita dal sistema di gestione documentale mediante il codice del fascicolo (formato da indice di classificazione, anno di apertura e numero del fascicolo).

8.6 *Fascicolo informatico*

Il fascicolo informatico costituisce un'aggregazione strutturata e univocamente identificata di atti, documenti o dati informatici, prodotti e funzionali all'esercizio di una specifica attività o di uno specifico procedimento. Nella pubblica amministrazione il fascicolo informatico collegato al procedimento amministrativo è creato e trattato secondo le disposizioni stabilite dall'articolo 41 del Codice dell'Amministrazione digitale Dlgs 82/2005 come modificato dal Dlgs 217/2017.
Il fascicolo informatico è gestito tramite il sistema di gestione documentale e protocollo informatico.
Il fascicolo informatico può contenere sia documenti digitali che copie immagine e copie informatiche di documenti analogici.

8.7 *Metadati dei fascicoli informatici*

Al fascicolo informatico è associato l'insieme dei metadati, come definito dalla normativa vigente in materia di documenti informatici (sino al 1° gennaio 2022 DPCM 13/11/2014, Allegato 5 Metadati e successivamente Linee Guida di Agid, Allegato 5 I metadati).

8.8 *Tenuta dei fascicoli dell'archivio corrente*

I fascicoli dell'archivio corrente, relativi agli affari in corso di trattazione o comunque necessari allo svolgimento delle attività correnti, sono formati e gestiti a cura dei responsabili di procedimento e conservati, fino al trasferimento nell'archivio di deposito, presso gli uffici di competenza.
I documenti e i fascicoli informatici sono gestiti e conservati nei sistemi messi a disposizione ed erogati da PA Digitale SpA in modalità Cloud computing
La sicurezza e la conservazione dei documenti e dei fascicoli informatici sono descritte e garantite dal Manuale di conservazione (Documento n. 11) e dal Piano di sicurezza dei documenti informatici (Documento n. 6). Si veda anche la Sezione 11.

9 *Invio dei documenti destinati all'esterno*

9.1 *Invio dei documenti informatici*

La spedizione dei documenti informatici avviene tramite il sistema informatico di gestione dei documenti, dopo che sono stati classificati e protocollati, secondo i seguenti criteri generali:

- i documenti informatici sono trasmessi all'indirizzo elettronico dichiarato dai destinatari abilitato alla ricezione della posta per via telematica;
- per la spedizione, l'Amministrazione si avvale di casella di posta elettronica certificata istituzionale;
- l'Ufficio Protocollo/le postazioni decentrate di protocollo provvedono a
  - effettuare l'invio telematico utilizzando i servizi di autenticazione
  - verificare l'avvenuto recapito dei documenti spediti per via telematica
- le ricevute elettroniche si collegano automaticamente alle registrazioni di protocollo.

I soggetti corrispondenti dell'Ente sono inseriti e descritti nell'anagrafica unica del sistema, secondo le prescrizioni contenute nelle Linee guida per l'inserimento e l'aggiornamento dei dati nel protocollo informatico e per la compilazione della banca dati dei soggetti (Documento n. 4).
Per la riservatezza delle informazioni contenute nei documenti elettronici, chi spedisce si attiene a quanto prescritto dall'articolo 49 del Codice dell'Amministrazione digitale Dlgs 82/2005.
Per l'uso della posta elettronica si rimanda alla Sezione 6.
La spedizione di documenti informatici al di fuori dei canali istituzionali descritti è considerata una mera trasmissione di informazioni senza che a questa l'Amministrazione riconosca un carattere giuridico-amministrativo che la impegni verso terzi.

9.2 *Spedizione dei documenti analogici*

Qualora sia necessario spedire documenti analogici originali questi devono essere completi della firma autografa del responsabile del procedimento, della classificazione e del riferimento al fascicolo nonché delle eventuali indicazioni necessarie a individuare il procedimento amministrativo di cui fanno parte.
Nel caso in cui vengano inviate copie cartacee di documenti informatici si utilizzano i modelli preposti (Documento n. 10), che ne attestano la conformità all'originale informatico oppure il contrassegno digitale.
I documenti da spedire sono trasmessi in busta chiusa all'Ufficio Economato che provvederà alla spedizione.
Nel caso di spedizione che utilizzi pezze di accompagnamento (raccomandate, posta celere, corriere o altro mezzo di spedizione), queste devono essere compilate a cura dell'ufficio produttore.
Eventuali situazioni di urgenza che modifichino la procedura descritta devono essere valutate e autorizzate dal responsabile del Servizio per la gestione documentale.

10 *Scansione dei documenti su supporto cartaceo*

10.1 *Documenti soggetti a scansione*

I documenti in arrivo e in partenza su supporto cartaceo sono acquisiti all'interno del sistema di protocollo informatico in formato immagine con l'ausilio di scanner, prima/successivamente/in fase delle operazioni di registrazione.
L'Ente adotta il seguente modello operativo:

- sono prodotti documenti informatici a firma elettronico/digitale;
- tutti i documenti sono classificati e fascicolati;
- i documenti ricevuti dall'esterno su formato cartaceo vengono registrati al protocollo e classificati, timbrati e scansionati; la copia immagine del documento è allegata alla relativa registrazione di protocollo e resa disponibile all'ufficio assegnatario/sulla postazione di lavoro del responsabile del procedimento;
- i documenti informatici sono spediti all'esterno tramite la casella di posta elettronica certificata agli indirizzi di posta elettronica dei destinatari oppure in copie cartacee tramite i servizi di posta ordinaria; per effettuare copia cartacea di documenti informatici si utilizzano i modelli preposti (Documento n. 10), che ne attestano la conformità all'originale informatico oppure il contrassegno digitale.

10.2 *Processo di scansione*

Il processo di scansione si articola di massima nelle seguenti fasi:

- acquisizione delle immagini in modo che a ogni documento, anche composto da più fogli, corrisponda un unico file in un formato standard;
- tutti i tipi di documenti in formato A4, comunque separabili o leggibili dagli scanner vengono digitalizzati. In caso di planimetrie o volumi non sperabili si potrà fare scansione del frontespizio;
- verifica della leggibilità delle immagini acquisite e della loro esatta corrispondenza con gli originali cartacei;
- collegamento delle rispettive immagini alla registrazione di protocollo, in modo non modificabile;
- memorizzazione delle immagini, in modo non modificabile.

I documenti analogici soggetti a scansione si conservano nell'archivio dell'Ente fino a procedimento legale di scarto.
In merito alla produzione di copie immagini su supporto informatico di documenti analogici si veda anche l'articolo 3.4 Acquisizione dei documenti analogici tramite copia immagine e copia informatica.

11 *Conservazione e tenuta dei documenti*

11.1 *Sistema informatico*

Il sistema informatico, le misure di sicurezza fisica e logica, le procedure comportamentali adottate per la gestione del sistema documentale e del sistema informatico sono demandati all'erogatore dei servizi, PA Digitale SpA, e descritti nel Piano di sicurezza dei documenti informatici (Documento n. 6). Il piano per la sicurezza informatica e predisposto e regolarmente aggiornato da PA Digitale SpA.

11.2 *Gestione delle password*

Il sistema garantisce la gestione e la conservazione delle password di accesso al sistema stesso e ai servizi online degli utenti interni ed esterni secondo le modalità descritte nel Piano per la sicurezza dei documenti informatici (Documento n. 6).

11.3 *Conservazione e memorizzazione dei documenti analogici, informatici e delle rappresentazioni digitali dei documenti cartacei*

I documenti dell'Ente, prodotti su supporti e nei formati previsti, sono conservati a cura del Servizio di gestione documentale.
La documentazione analogica corrente è custodita a cura del responsabile del procedimento fino al trasferimento in archivio di deposito.
I documenti informatici sono memorizzati nel sistema, in modo non modificabile, al termine delle operazioni di registrazione e segnatura di protocollo.
Le rappresentazioni digitali dei documenti originali su supporto cartaceo, acquisite con l'ausilio dello scanner, sono memorizzate nel sistema, in modo non modificabile, al termine del processo di scansione, associazione alle corrispondenti registrazioni di protocollo e fascicolazione.

11.4 *Sistema di conservazione dei documenti informatici*

La conservazione dei documenti informatici è assicurata dai requisiti funzionali del sistema di conservazione, in modo da garantire autenticità, integrità, identificazione univoca, mantenimento stabile di tutte le relazioni istituite nel contesto di produzione, gestione e tenuta del documento e leggibilità nel tempo. I requisiti adottati sono conformi agli standard internazionali e alle norme nazionali.
Al fine di dare solidità al sistema e di consentire la presunzione di autenticità, viene conservata tutta la documentazione relativa alle fasi di trattamento dei documenti. Le soluzioni di sicurezza adottate avvengono secondo le modalità specificate negli standard, nelle Linee Guida di Agid.
Il responsabile per la gestione documentale provvede altresì alla conservazione degli strumenti di descrizione, ricerca, gestione e conservazione dei documenti (inventari, indici, quadri di classificazione e relativi massimari di selezione e scarto, repertori).
Ai sensi del paragrafo 4.5 delle Linee Guida di Agid, l'Ente ha individuato il responsabile della conservazione (Documento n. 14).
Il responsabile della conservazione definisce e attua le politiche di conservazione dei documenti.
L'Ente si avvale del servizio di conservazione digitale a norma erogato da PA Digitale SpA, conservatore iscritto nell'elenco presso l'Agenzia per l'Italia digitale, e ne adotta il Manuale di conservazione (Documento n. 11).
Il Manuale di conservazione illustra l'organizzazione del sistema di conservazione, individua i soggetti coinvolti e i ruoli da essi svolti, descrive il processo di conservazione, le architetture e le infrastrutture utilizzate, le modalità di accesso ai documenti e le misure di sicurezza. Il responsabile della conservazione delega formalmente la trattazione del processo di conservazione digitale al conservatore accreditato e vigila periodicamente sullo svolgimento dell'attività.
I documenti informatici, i fascicoli informatici e le aggregazioni documentali informatiche sono versati nel sistema di conservazione, corredati dai metadati previsti sino al 1° gennaio 2022 dal DPCM 3/12/2013 Regole tecniche in materia di sistema di conservazione, Allegato 5 Metadati e successivamente dalle Linee Guida di Agid, Allegato 5 I metadati, e descritti nel Manuale di conservazione (Documento n. 11), in modo non modificabile. I formati dei documenti destinati alla conservazione sono i formati previsti per la conservazione dalla normativa vigente in materia (Linee guida di Agid, Allegato 2 Formati di file e riversamenti).
In caso di migrazione dei documenti informatici, la corrispondenza fra il formato originale e quello migrato è

garantita dal responsabile della conservazione.

11.5 *Memorizzazione e salvataggio dei dati e dei documenti informatici*

I dati e i documenti informatici sono memorizzati nel sistema di gestione documentale al termine delle operazioni di registrazione.
Il sistema di gestione documentale e il protocollo informatico sono condotti in modalità Cloud computing definita anche SaaS (Software as a Service), che consente all'Ente di usufruire dei servizi di protocollazione e gestione documentale messi a disposizione dall'applicativo attraverso browser ed erogati da PA Digitale SpA, La sicurezza informatica è demandata all'erogatore dei servizi, PA Digitale SpA, come descritto nel Piano di sicurezza dei documenti informatici (Documento n. 6).

11.6 *Pacchetti di versamento*

Il responsabile della gestione documentale assicura la trasmissione del contenuto del pacchetto di versamento al sistema di conservazione, secondo le modalità operative definite nel Manuale di conservazione (Documento n. 11)
Il responsabile del servizio di conservazione fornisce il rapporto di versamento relativo ai pacchetti di versamento generato dal sistema di conservazione, secondo le modalità descritte nel Manuale di conservazione (Documento n. 11).

11.7 *Conservazione dei documenti analogici*

L'archivio corrente analogico è conservato presso le unità organizzative.
Gli archivi storici e di deposito acquisiti dagli enti soppressi sono conservati presso sedi dell'ente sul territorio di competenza.

11.8 *Trasferimento delle unità archivistiche analogiche negli archivi di deposito e storico e conservazione dei fascicoli informatici*

Gli uffici individuano i fascicoli relativi ad affari e procedimenti conclusi, o comunque non più necessari allo svolgimento delle attività correnti, di norma all'inizio di ogni anno e comunque con cadenza periodica, dandone comunicazione al responsabile della gestione documentale, il quale provvede al loro trasferimento all'archivio di deposito e compila il relativo elenco. Il trasferimento è effettuato rispettando l'organizzazione dei fascicoli e delle serie nell'archivio corrente.
Prima di effettuare il conferimento dei fascicoli chiusi, il responsabile di procedimento verifica:

- l'effettiva conclusione della pratica;
- la trascrizione dell'esaurimento della pratica nel repertorio dei fascicoli, gestito tramite il sistema di protocollo informatico;
- il corretto aggiornamento della data di chiusura sulla camicia del fascicolo cartaceo;
- lo sfoltimento di eventuali copie e fotocopie di documentazione passibile di macero, al fine di garantire;
- la presenza di tutti e soli documenti pertinenti alla pratica.

Di norma sono versati all'archivio storico tutti i documenti anteriori all'ultimo quarantennio. E' tuttavia possibile depositare anche documentazione successiva al quarantennio purché non rivesta più un preminente carattere giuridico-amministrativo per l'Ente.
La gestione dell'archivio di deposito, la consultazione e il prelevamento dei documenti dallo stesso, l'archiviazione e la custodia dei documenti contenenti dati personali avvengono in conformità alla normativa vigente.
I fascicoli informatici, mediante specifiche funzionalità di sistema, vengono trasferiti nel sistema di conservazione adottato. Delle operazioni di trasferimento è lasciata traccia documentale.

11.9 *Selezione e conservazione dei documenti*

La procedura di selezione della documentazione da proporre allo scarto sarà realizzata attivando il procedimento amministrativo di scarto documentale, in base al Piano di conservazione da definire, con l'invio

della proposta alla competente Soprintendenza archivistica. I documenti e i fascicoli non soggetti a operazioni di scarto andranno a costituire l'archivio storico per la conservazione permanente.
Lo scarto dei documenti informatici avviene mediante le specifiche funzionalità del sistema di conservazione.

11.10 *Gestione dell'archivio storico*

L'archivio storico è costituito dal complesso dei documenti relativi ad affari esauriti e destinati, previe operazioni di selezione, alla conservazione permanente per garantirne la consultazione al pubblico. In base alla normativa vigente l'archivio storico è formato dai documenti relativi ad affari esauriti da oltre 40 anni: l'archivio storico deve essere conservato nella sua organicità e in luogo idoneo alla conservazione permanente. Ogni spostamento dell'archivio storico in altra sede deve essere comunicato e autorizzato dalla Soprintendenza archivistica. L'Ente ha inoltre l'obbligo di ordinare e inventariare l'archivio storico.
Come previsto dal Codice dei beni culturali Dlgs 42/2004, l'Ente cura la conservazione, promozione, valorizzazione e assicura la fruizione del patrimonio documentario, garantendo a tutti l'accesso gratuito.

12 *Accesso a dati, informazioni e documenti - Pubblicità legale e trasparenza amministrativa*

12.1 *Accessibilità da parte degli utenti appartenenti all'Amministrazione*

La sicurezza e la riservatezza delle registrazioni di protocollo e dei documenti informatici e il controllo degli accessi al sistema sono garantiti attraverso l'uso di profili e password, o altre tecniche e dispositivi di autenticazione sicura.
Sulla base della struttura organizzativa e funzionale dell'Ente, il responsabile della gestione documentale attribuisce i livelli di autorizzazione (consultazione, inserimento, cancellazione e modifica delle informazioni), come descritto nel Piano per la sicurezza dei documenti informatici (Documento n. 6).

12.2 *Accesso esterno*

L'accesso al sistema informatico da parte di utenti esterni può avvenire nei casi di procedimenti amministrativi attraverso il Sistema pubblico per la gestione dell'identità digitale, oppure con l'uso della carta d'identità elettronica e della carta nazionale dei servizi; sino alla data da stabilire con decreto del Presidente del Consiglio dei ministri o del Ministro per la semplificazione e la pubblica amministrazione, come previsto dall'articolo 64 del Dlgs 82/2005 come modificato dal DL 76/2020, possono essere utilizzati anche altri strumenti informatici messi a disposizione dall'Ente che consentano l'individuazione certa del soggetto richiedente.
Come previsto dal Dlgs. 33/2013, è garantito a tutti i cittadini, mediante l'istituzione dell'Accesso civico, la libera consultazione degli atti dell'Ente per i quali è prevista la pubblicazione. Sul sito istituzionale è consultabile l'apposita "Sezione Amministrazione Trasparente", a cui il cittadino ha libero accesso e nella quale sono disponibili informazioni integre e conformi all'originale, secondo quanto previsto dalla normativa e come specificato nel Piano triennale di prevenzione della corruzione e della trasparenza.
I documenti, le informazioni e i dati oggetto di pubblicazione obbligatoria sono pubblicati in formato di tipo aperto.

12.3 *Accesso da parte di altre amministrazioni*

L'accesso al sistema informatico documentale da parte di pubbliche amministrazioni è realizzato applicando le norme e i criteri tecnici emanati per la realizzazione della rete unitaria delle pubbliche amministrazioni o nell'ambito di altre convenzioni, attraverso modalità di interoperabilità.

13 *Approvazione, Revisione e Pubblicazione*

13.1 *Approvazione*

Il presente manuale è adottato con decreto del Segretario Generale, su proposta del responsabile della gestione documentale.

13.2 *Revisione*

La modifica o l'aggiornamento di uno o tutti i documenti allegati al presente manuale non comporta la revisione del manuale stesso. Qualora se ne presenti la necessità, si potrà procedere a revisione o integrazione del manuale anche prima della scadenza prevista.

13.3 *Pubblicazione e divulgazione*

Il Manuale di gestione è reso pubblico tramite la sua diffusione sul sito internet istituzionale dell'Ente nella "Sezione Amministrazione trasparente",e l'invio di copia alla Soprintendenza Archivistica e Bibliografica della Campania.

Dc 1

AGID | Agenzia per l'Italia Digitale

Glossario dei termini e degli acronimi

Allegato 1 al documento "*Linee Guida sulla formazione, gestione e conservazione dei documenti informatici*".

Indice

Sommario

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

CAPITOLO 1

Premessa

1.3 Scopo e campo di applicazione del documento

Lo scopo del presente allegato è il seguente:

- esplicitare il significato dei termini maggiormente utilizzati nel documento *linea guida sulla formazione, gestione e conservazione dei documenti informatici*, che necessitano una spiegazione.

1.4 Glossario dei termini

TERMINE	DEFINIZIONE
Accesso	Operazione che consente di prendere visione dei documenti informatici.
Affidabilità	Caratteristica che, con riferimento a un sistema di gestione documentale o conservazione, esprime il livello di fiducia che l'utente ripone nel sistema stesso, mentre con riferimento al documento informatico esprime la credibilità e l'accuratezza della rappresentazione di atti e fatti in esso contenuta.
Aggregazione documentale informatica	Insieme di documenti informatici o insieme di fascicoli informatici riuniti per caratteristiche omogenee, in relazione alla natura e alla forma dei documenti o in relazione all'oggetto e alla materia o in relazione alle funzioni dell'ente.
Archivio	Complesso dei documenti prodotti o acquisiti da un soggetto pubblico o privato durante lo svolgimento della propria attività.
Archivio informatico	Archivio costituito da documenti informatici, organizzati in aggregazioni documentali informatiche.

TERMINE	DEFINIZIONE
Area Organizzativa Omogenea	Un insieme di funzioni e di uffici individuati dall'ente al fine di gestire i documenti in modo unitario e coordinato, secondo quanto disposto dall'art. 50 comma 4 del D.P.R. 28 dicembre 2000, n. 445. Essa rappresenta il canale ufficiale per l'invio di istanze e l'avvio di procedimenti amministrativi.
Attestazione di conformità delle copie per immagine su supporto informatico di un documento analogico	Dichiarazione rilasciata da notaio o altro pubblico ufficiale a ciò autorizzato allegata o asseverata al documento informatico.
Autenticità	Caratteristica in virtù della quale un oggetto deve considerarsi come corrispondente a ciò che era nel momento originario della sua produzione. Pertanto un oggetto è autentico se nel contempo è integro e completo, non avendo subito nel corso del tempo o dello spazio alcuna modifica non autorizzata. L'autenticità è valutata sulla base di precise evidenze.
Certificazione	Attestazione di terza parte relativa alla conformità ai requisiti specificati di prodotti, processi, persone e sistemi.
Classificazione	Attività di organizzazione di tutti i documenti secondo uno schema costituito da un insieme di voci articolate in modo gerarchico e che individuano, in astratto, le funzioni, competenze, attività e/o materie del soggetto produttore.
Cloud della PA	Ambiente virtuale che consente alle Pubbliche Amministrazioni di erogare servizi digitali ai cittadini e alle imprese nel rispetto di requisiti minimi di sicurezza e affidabilità.
Codec	Algoritmo di codifica e decodifica che consente di generare flussi binari, eventualmente imbustarli in un file o in un *wrapper* (codifica), così come di estrarli da esso (decodifica).
Conservatore	Soggetto pubblico o privato che svolge attività di conservazione dei documenti informatici.
Conservazione	Insieme delle attività finalizzate a definire ed attuare le politiche complessive del sistema di conservazione e a governarne la gestione in relazione al modello organizzativo

TERMINE	DEFINIZIONE
	adottato, garantendo nel tempo le caratteristiche di autenticità, integrità, leggibilità, reperibilità dei documenti
Convenzioni di denominazione del file	Insieme di regole sintattiche che definisce il nome dei file all'interno di un filesystem o pacchetto.
Coordinatore della Gestione Documentale	Soggetto responsabile della definizione di criteri uniformi di classificazione ed archiviazione nonché di comunicazione interna tra le AOO ai sensi di quanto disposto dall'articolo 50 comma 4 del DPR 445/2000 nei casi di amministrazioni che abbiano istituito più AOO.
Destinatario	Soggetto o sistema al quale il documento informatico è indirizzato.
Digest	Vedi Impronta crittografica.
Documento amministrativo informatico	Ogni rappresentazione, grafica, fotocinematografica, elettromagnetica o di qualunque altra specie, del contenuto di atti, anche interni, formati dalle pubbliche amministrazioni, o, comunque, da queste ultime utilizzati ai fini dell'attività amministrativa
Documento elettronico	Qualsiasi contenuto conservato in forma elettronica, in particolare testo o registrazione sonora, visiva o audiovisiva
Documento informatico	Documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti
Duplicato informatico	Vedi art. 1, comma 1, lett) i quinquies del CAD.
eSeal	Vedi sigillo elettronico.
Esibizione	operazione che consente di visualizzare un documento conservato
eSignature	Vedi firma elettronica.
Estratto di documento informatico	Parte del documento tratto dal documento originale
Estratto per riassunto di documento informatico	Documento nel quale si attestano in maniera sintetica fatti, stati o qualità desunti da documenti informatici.

TERMINE	DEFINIZIONE
Estrazione statica dei dati	Estrazione di informazioni utili da grandi quantità di dati (es. database, datawarehouse ecc...), attraverso metodi automatici o semi-automatici
Evidenza informatica	Sequenza finita di *bit* che può essere elaborata da una procedura informatica.
Fascicolo informatico	Aggregazione documentale informatica strutturata e univocamente identificata contenente atti, documenti o dati informatici prodotti e funzionali all'esercizio di una attività o allo svolgimento di uno specifico procedimento.
File	Insieme di informazioni, dati o comandi logicamente correlati, raccolti sotto un unico nome e registrati, per mezzo di un programma di elaborazione o di scrittura, nella memoria di un computer.
File container	Vedi Formato contenitore.
File wrapper	Vedi Formato contenitore.
File-manifesto	File che contiene metadati riferiti ad un file o ad un pacchetto di file.
Filesystem	Sistema di gestione dei file, strutturato mediante una o più gerarchie ad albero, che determina le modalità di assegnazione dei nomi, memorizzazione e organizzazione all'interno di uno storage.
Firma elettronica	Vedi articolo 3 del Regolamento eIDAS.
Firma elettronica avanzata	Vedi articoli 3 e 26 del Regolamento eIDAS.
Firma elettronica qualificata	Vedi articolo 3 del Regolamento eIDAS.
Flusso (binario)	Sequenza di bit prodotta in un intervallo temporale finito e continuativo che ha un'origine precisa ma di cui potrebbe non essere predeterminato il suo istante di interruzione.
Formato contenitore	Formato di file progettato per consentire l'inclusione ("imbustamento" o *wrapping*), in uno stesso file, di una o più

TERMINE	DEFINIZIONE
	evidenze informatiche soggette a differenti tipi di codifica e al quale possono essere associati specifici metadati.
Formato del documento informatico	Modalità di rappresentazione della sequenza di bit che costituiscono il documento informatico; comunemente è identificato attraverso l'estensione del file.
Formato "deprecato"	Formato in passato considerato ufficiale il cui uso è attualmente sconsigliato a favore di una versione più recente.
Funzioni aggiuntive del protocollo informatico	Nel sistema di protocollo informatico, componenti supplementari rispetto a quelle minime, necessarie alla gestione dei flussi documentali, alla conservazione dei documenti nonché alla accessibilità delle informazioni.
Funzioni minime del protocollo informatico	Componenti del sistema di protocollo informatico che rispettano i requisiti di operazioni ed informazioni minime di cui all'articolo 56 del D.P.R. 28 dicembre 2000, n. 445.
Funzione di *hash* crittografica	Funzione matematica che genera, a partire da una evidenza informatica, una impronta crittografica o *digest* (vedi) in modo tale che risulti computazionalmente difficile (di fatto impossibile), a partire da questa, ricostruire l'evidenza informatica originaria e generare impronte uguali a partire da evidenze informatiche differenti.
Gestione Documentale	Processo finalizzato al controllo efficiente e sistematico della produzione, ricezione, tenuta, uso, selezione e conservazione dei documenti.
hash	Termine inglese usato, impropriamente, come sinonimo d'uso di "impronta crittografica" o "*digest*" (vedi).
Identificativo univoco	Sequenza di numeri o caratteri alfanumerici associata in modo univoco e persistente ad un'entità all'interno di uno specifico ambito di applicazione.
Impronta crittografica	Sequenza di bit di lunghezza predefinita, risultato dell'applicazione di una funzione di *hash* crittografica a un'evidenza informatica.

TERMINE	DEFINIZIONE
Integrità	Caratteristica di un documento informatico o di un'aggregazione documentale in virtù della quale risulta che essi non hanno subito nel tempo e nello spazio alcuna alterazione non autorizzata. La caratteristica dell'integrità, insieme a quella della completezza, concorre a determinare la caratteristica dell'autenticità.
Interoperabilità	Caratteristica di un sistema informativo, le cui interfacce sono pubbliche e aperte, e capaci di interagire in maniera automatica con altri sistemi informativi per lo scambio di informazioni e l'erogazione di servizi.
Leggibilità	Caratteristica di un documento informatico che garantisce la qualità di poter essere decodificato e interpretato da un'applicazione informatica.
Manuale di conservazione	Documento informatico che descrive il sistema di conservazione e illustra dettagliatamente l'organizzazione, i soggetti coinvolti e i ruoli svolti dagli stessi, il modello di funzionamento, la descrizione del processo, la descrizione delle architetture e delle infrastrutture.
Manuale di gestione	Documento informatico che descrive il sistema di gestione, anche ai fini della conservazione, dei documenti informatici e fornisce le istruzioni per il corretto funzionamento del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi.
Metadati	Dati associati a un o documento informatico, a un fascicolo informatico o a un'aggregazione documentale per identificarli, descrivendone il contesto, il contenuto e la struttura - così da permetterne la gestione del tempo - in conformità a quanto definito nella norma ISO 15489-1:2016 e più nello specifico dalla norma ISO 23081-1:2017.
Naming convention	Vedi Convenzioni di denominazione
Oggetto di conservazione	Oggetto digitale versato in un sistema di conservazione.
Oggetto digitale	Oggetto informativo digitale, che può assumere varie forme tra le quali quelle di documento informatico, fascicolo informatico, aggregazione documentale informatica o archivio informatico.

TERMINE	DEFINIZIONE
Pacchetto di archiviazione	Pacchetto informativo generato dalla trasformazione di uno o più pacchetti di versamento coerentemente con le modalità riportate nel manuale di conservazione.
Pacchetto di distribuzione	Pacchetto informativo inviato dal sistema di conservazione all'utente in risposta ad una sua richiesta di accesso a oggetti di conservazione.
Pacchetto di file (*file package*)	Insieme finito di più file (possibilmente organizzati in una struttura di sottoalbero all'interno di un filesystem) che costituiscono, collettivamente oltre che individualmente, un contenuto informativo unitario e auto-consistente.
Pacchetto di versamento	Pacchetto informativo inviato dal produttore al sistema di conservazione secondo il formato descritto nel manuale di conservazione.
Pacchetto informativo	Contenitore logico che racchiude uno o più oggetti di conservazione con i relativi metadati, oppure anche i soli metadati riferiti agli oggetti di conservazione.
Path	Percorso (*vedi*).
Pathname	Concatenazione ordinata del percorso di un file e del suo nome.
Percorso	Informazioni relative alla localizzazione virtuale del file all'interno del filesystem espressa come concatenazione ordinata del nome dei nodi del percorso.
Piano della sicurezza del sistema di conservazione	Documento che, nel contesto del piano generale di sicurezza, descrive e pianifica le attività volte a proteggere il sistema di conservazione dei documenti informatici da possibili rischi.
Piano della sicurezza del sistema di gestione Informatica dei documenti	Documento che, nel contesto del piano generale di sicurezza, descrive e pianifica le attività volte a proteggere il sistema di gestione informatica dei documenti da possibili rischi.
Piano di classificazione (Titolario)	Struttura logica che permette di organizzare documenti e oggetti digitali secondo uno schema desunto dalle funzioni e dalle attività dell'amministrazione interessata.

TERMINE	DEFINIZIONE
Piano di conservazione	Documento, allegato al manuale di gestione e integrato con il sistema di classificazione, in cui sono definiti i criteri di organizzazione dell'archivio, di selezione periodica e di conservazione ai sensi dell'articolo 68 del D.P.R. 28 dicembre 2000, n. 445.
Piano di organizzazione delle aggregazioni documentali	Strumento integrato con il sistema di classificazione a partire dai livelli gerarchici inferiori di quest'ultimo e finalizzato a individuare le tipologie di aggregazioni documentali (tipologie di serie e tipologie di fascicoli) che devono essere prodotte e gestite in rapporto ai procedimenti e attività in cui si declinano le funzioni svolte dall'ente
Piano generale della sicurezza	Documento che pianifica le attività volte alla realizzazione del sistema di protezione e di tutte le possibili azioni indicate dalla gestione del rischio nell'ambito dell'organizzazione di appartenenza.
Presa in carico	Accettazione da parte del sistema di conservazione di un pacchetto di versamento in quanto conforme alle modalità previste dal manuale di conservazione e, in caso di affidamento del servizio all'esterno, dagli accordi stipulati tra il titolare dell'oggetto di conservazione e il responsabile del servizio di conservazione.
Processo	Insieme di attività correlate o interagenti che trasformano elementi in ingresso in elementi in uscita.
Produttore dei PdV	Persona fisica, di norma diversa dal soggetto che ha formato il documento, che produce il pacchetto di versamento ed è responsabile del trasferimento del suo contenuto nel sistema di conservazione. Nelle pubbliche amministrazioni, tale figura si identifica con il responsabile della gestione documentale.
qSeal	Sigillo elettronico qualificato, come da art. 35 del Regolamento eIDAS.
qSignature	Firma elettronica qualificata, come da art. 25 del Regolamento eIDAS.
Rapporto di versamento	Documento informatico che attesta l'avvenuta presa in carico da parte del sistema di conservazione dei pacchetti di versamento inviati dal produttore.

TERMINE	DEFINIZIONE
Registro di protocollo	Registro informatico ove sono memorizzate le informazioni prescritte dalla normativa per tutti i documenti ricevuti e spediti da un ente e per tutti i documenti informatici dell'ente stesso.
Registro particolare	Registro informatico individuato da una pubblica amministrazione per la memorizzazione delle informazioni relative a documenti soggetti a registrazione particolare.
Regolamento eIDAS	electronic IDentification Authentication and Signature, Regolamento (UE) № 910/2014 del Parlamento Europeo e del Consiglio, del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE.
Repertorio	Registro su cui vengono annotati con un numero progressivo i fascicoli secondo l'ordine cronologico in cui si costituiscono all'interno delle suddivisioni del piano di classificazione.
Responsabile dei sistemi informativi per la conservazione	Soggetto che coordina i sistemi informativi all'interno del conservatore, in possesso dei requisiti professionali individuati da AGID.
Responsabile del servizio di conservazione	soggetto che coordina il processo di conservazione all'interno del conservatore, in possesso dei requisiti professionali individuati da AGID
Responsabile della conservazione	Soggetto che definisce e attua le politiche complessive del sistema di conservazione e ne governa la gestione con piena responsabilità ed autonomia.
Responsabile della funzione archivistica di conservazione	soggetto che coordina il processo di conservazione dal punto di vista archivistico all'interno del conservatore, in possesso dei requisiti professionali individuati da AGID
Responsabile della gestione documentale	Soggetto responsabile della gestione del sistema documentale o responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi, ai sensi dell'articolo 61 del D.P.R. 28 dicembre 2000, n. 445.

TERMINE	DEFINIZIONE
Responsabile della protezione dei dati	Persona con conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, in grado di assolvere i compiti di cui all'articolo 39 del Regolamento (UE) 2016/679.
Responsabile della sicurezza dei sistemi di conservazione	soggetto che assicura il rispetto dei requisiti di sicurezza all'interno del conservatore, in possesso dei requisiti professionali individuati da AGID
Responsabile dello sviluppo e della manutenzione del sistema di conservazione	soggetto che assicura lo sviluppo e la manutenzione del sistema all'interno del conservatore, in possesso dei requisiti professionali individuati da AGID
Riferimento temporale	Insieme di dati che rappresenta una data e un'ora con riferimento al Tempo Universale Coordinato (UTC).
Riversamento	Procedura mediante la quale uno o più documenti informatici sono convertiti da un formato di file (ovvero di busta, ovvero di pacchetto di file) ad un altro, lasciandone invariato il contenuto per quanto possibilmente permesso dalle caratteristiche tecniche del formato (ovvero dei formati) dei file e delle codifiche di destinazione.
Scarto	Operazione con cui si eliminano definitivamente, secondo quanto previsto dalla normativa vigente, i documenti ritenuti non più rilevanti ai fini giuridico-amministrativo e storico-culturale.
Serie	Raggruppamento di documenti con caratteristiche omogenee (vedi anche aggregazione documentale informatica).
***Sidecar* (file)**	File-manifesto (*vedi*).
Sigillo elettronico	Dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati in forma elettronica, per garantire l'origine e l'integrità di questi ultimi.
Sistema di conservazione	Insieme di regole, procedure e tecnologie che assicurano la conservazione dei documenti informatici in attuazione a quanto previsto dall'art. 44, comma 1, del CAD.
Sistema di gestione informatica dei documenti	Insieme delle risorse di calcolo, degli apparati, delle reti di comunicazione e delle procedure informatiche utilizzati dalle organizzazioni per la gestione dei documenti. Nell'ambito

TERMINE	DEFINIZIONE
	della pubblica amministrazione è il sistema di cui all'articolo 52 del D.P.R. 28 dicembre 2000, n. 445
Timeline	Linea temporale virtuale su cui sono disposti degli eventi relativi ad un sistema informativo o a un documento informatico. Costituiscono esempi molto diversi di *timeline* un file di log di sistema, un flusso multimediale contenente essenze audio\video sincronizzate.
Titolare dell'oggetto di conservazione	Soggetto produttore degli oggetti di conservazione.
Trasferimento	Passaggio di custodia dei documenti da una persona o un ente ad un'altra persona o un altro ente.
TUDA	Testo Unico della Documentazione Amministrativa, Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, e successive modificazioni e integrazioni.
Ufficio	Riferito ad un'area organizzativa omogenea, un ufficio dell'area stessa che utilizza i servizi messi a disposizione dal sistema di protocollo informatico.
Utente abilitato	Persona, ente o sistema che interagisce con i servizi di un sistema di gestione informatica dei documenti e/o di un sistema per la conservazione dei documenti informatici, al fine di fruire delle informazioni di interesse.
Versamento	Passaggio di custodia, di proprietà e/o di responsabilità dei documenti. Nel caso di un organo giudiziario e amministrativo dello Stato operazione con la quale il responsabile della conservazione trasferisce agli Archivi di Stato o all'Archivio Centrale dello Stato della documentazione destinata ad essere ivi conservata ai sensi della normativa vigente in materia di beni culturali.

1.5 Glossario degli Acronimi

ACRONIMO	DEFINIZIONE
AGID	Agenzia per l'Italia digitale

ACRONIMO	DEFINIZIONE
AOO	Area Organizzativa Omogenea
CAD	Codice dell'Amministrazione Digitale - Decreto legislativo 7 marzo 2005, n. 82 e successive modificazioni e integrazioni.
eIDAS	Regolamento (UE) № 910/2014 del Parlamento Europeo e del Consiglio, del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE.
FEA	Vedi firma elettronica avanzata.
FEQ	Vedi firma elettronica qualifica.
GDPR	Regolamento (UE) № 679/2016 del Parlamento Europeo e del Consiglio, del 27 aprile 2016 ("*General Data Protection Regulation*"), 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.
PdA (AiP)	Pacchetto di Archiviazione.
PdD (DiP)	Pacchetto di Distribuzione.
PdV (SiP)	Pacchetto di Versamento.
UOR	Unità Organizzativa Responsabile

Elenco dei servizi e degli uffici dell'Autorità di Bacino Distrettuale dell'Appennino Meridionale abilitati all'utilizzo del sistema di gestione documentale del protocollo informatico e all'inserimento dei dati

Documento n. 2

L'Autorità di Bacino Distrettuale dell'Appennino Meridionale è articolato nelle seguenti strutture come da organigramma e funzionigramma approvato con decreto del SG n. 471 del 29 giugno 2022:

Segreteria Particolare
Ufficio accoglienza
Protocollo generale
Settore Staff Analisi Socio-economiche
Ufficio Automezzi
Uffici di Staff
Area Amministrativa
Area Tecnica
SETTORI

Abilitazioni all'utilizzo delle funzionalità del sistema di gestione documentale e protocollo informatico:

- registrazione dei documenti in arrivo e partenza : Protocollo generale,

- classificazione e fascicolazione dei documenti: tutte le postazioni dei vari uffici
- consultazione: tutte le postazioni dei vari uffici, in base all'assegnazione-competenza dei documenti
- definizione delle liste di controllo degli accessi (ACL) e del ruolo degli utenti: Protocollo generale
- assegnazione: Protocollo generale sulla base dell'assegnazione del segretario generale
- aggiornamento anagrafica mittente/destinatario sul Sistema: protocollo generale
- protocollazione dei documenti nel registro di emergenza: Protocollo generale

Postazioni abilitate: *una postazione per ogni dipendente che si occupa della trattazione di documenti*

Elenco delle registrazioni particolari

Documento n. 3

.

Per registrazioni particolari si intende: registri-repertori informatici realizzati tramite applicativi informatici e con numerazione "solida" come quella del protocollo, pertanto non modificabile.
Ciò che non è registrato in repertori-registri particolari, è registrato a protocollo.

Contratti pubblici in forma amministrativa
Contratti di lavoro individuali
Convenzioni
Atti della Conferenza Istituzionale Permanente
Atti del Segretario Generale
Atti della Conferenza operativa
Fatture emesse
Mandati di pagamento
Riversali
Verbali della delegazione trattante per la contrattazione integrativa
Verbali delle violazioni per ritardata/omessa denuncia di infortunio
Verbali della revisione dei conti

Linee guida per l'inserimento e l'aggiornamento dei dati nel protocollo informatico e per la compilazione della banca dati dei soggetti[1]

Documento n. 4

Maiuscole e minuscole

Di norma per l'inserimento dei dati si devono usare le maiuscole e le minuscole secondo l'uso attuale. Per quanto riguarda il protocollo informatico dell'ente e la banca dati dell'anagrafica unica si è scelto di usare sempre la maiuscola.

Abbreviazioni

Tutte le abbreviazione devono essere sciolte; non devono essere abbreviati i nomi degli enti, e qualora una abbreviazione facesse parte del nome ufficiale dell'istituto -e non sia possibile scioglierla- deve essere riportata così come compare nell'intestazione originale:

no AVV. ROSSI MARIO - STUDIO LEGALE ASSOCIATO;
si AVVOCATO ROSSI MARIO – STUDIO LEGALE ASSOCIATO

no CENSIS
si CENTRO STUDI INVESTIMENTI SOCIALI - CENSIS

no C.C.I.A.
si CAMERA DI COMMERCIO INDUSTRIA E ARTIGIANATO - CCIA

Segni di interpunzione

Al fine di consentire una facile interrogazione delle informazioni inserite nelle banche dati si deve limitare l'uso dei segni di interpunzione nelle intitolazioni di nomi collettivi, di enti, ditte ecc.; questi sono consentiti nel caso facciano parte integrante dell'intitolazione.
Nell'indicazione della ragione sociale (spa, srl ecc.) delle ditte (individuali o società) non si useranno i punti fermi:

no S.P.A., S.R.L, S.p.a., S.p.A., S.r.l., S.r.L.
si SPA, SRL

L'eventuale nome di una ditta o di un ente scritto fra virgolette non andrà inserito con le virgolette:

no ASSOCIAZIONE "AMICI DELLA MUSICA"
si ASSOCIAZONE AMICI DELLA MUSICA

Nell'utilizzo dei segni di interpunzione si rimanda alle regole di scrittura: non deve mai precedere al segno uno spazio; dopo il segno e prima della parola successiva uno spazio; prima e dopo la lineetta uno spazio; la lineetta quando è tra due parole che esprimono un termine composto non deve avere spazi; il segno di parentesi segue la parola preceduto da uno spazio, all'interno della parentesi la prima parola è scritta subito dopo il segno di parentesi senza essere preceduta da uno spazio:

no LUNEDÌ , MARTEDÌ; LUNEDÌ,MARTEDÌ; LUNEDÌ ,MARTEDÌ
si LUNEDÌ, MARTEDÌ

no I COLORI SONO : GIALLO, ROSSO, ECC.; I COLORI SONO:GIALLO, ROSSO, ECC.; I COLORI SONO :GIALLO, ROSSO, ecc.
si I COLORI SONO: GIALLO, ROSSO, ecc.

no REGIONE SARDEGNA-DIREZIONE GENERALE

---

[1] Per la redazione delle seguenti linee guida si veda: ARRABBITO LOREDANA - BUGGIARELLI TERESA - MAZZETTO DONATELLA, *Linee guida per l'inserimento dei dati nel protocollo informatico*, in Archivi & Computer, X, 1, Pisa 2000.

si REGIONE SARDEGNA - DIREZIONE GENERALE

no GIURIDICO - AMMINISTRATIVO
si GIURIDICO-AMMINISTRATIVO

no (GIALLO, ROSSO)
si (GIALLO, ROSSO)

Nomi di persona

Sono esclusi tutti i titoli di cortesia (eccellenza, reverendo, ecc.), di onorificenza, predicati nobiliari (N.H., N.D. ecc.), i titoli accademici (dott., ing. ecc.), quelli professionali (rag., geom. ecc.) e tutto ciò che non corrisponda al nome:

no DOTT. AVV. ROSSI MARIO;
no ROSSI AVV. MARIO;
si ROSSI MARIO.

Nomi di persona giuridica, ditte individuali, enti pubblici, società

Le denominazione delle persone giuridiche ecc. devono essere inserite come appaiono nella carta intestata facendo attenzione fra il logo e l'intestazione che spesso non corrispondono, scegliendo fra le due l'intestazione:

no AVV. ROSSI MARIO - STUDIO LEGALE ASSOCIATO;
si AVVOCATO ROSSI MARIO – STUDIO LEGALE ASSOCIATO
si STUDIO LEGALE ROSSI MARIO.

In mancanza dell'intestazione completa si preferisca il logo, oppure ricorrendo al responsabile del procedimento si rintracci la definizione originale da immettere nella banca dati. La tipologia della società (srl ecc.) va scritta non puntata (vedi sopra).
I nomi di enti o persone giuridiche nonché quelli di enti collettivi vanno scritti completi e per esteso, senza abbreviazioni; qualora l'ente o la persona giuridica sono meglio conosciuti con l'acronimo, questo va inserito dopo il nome completo in maiuscolo non puntato dopo un trattino preceduto e seguito da uno spazio:

no CENSIS
si CENTRO STUDI INVESTIMENTI SOCIALI - CENSIS

no C.C.I.A.
si CAMERA DI COMMERCIO INDUSTRIA E ARTIGIANATO - CCIA

no MIN. LAV. E PREV. SOCIALE;
si MINISTERO DEL LAVORO E DELLA PREVIDENZA SOCIALE
si MINISTERO DEL LAVORO E DELLA PREVIDENZA SOCIALE - MLPS

no INPS - IST. NAZ. PREVIDENZA SOCIALE
si ISTITUTO NAZIONALE PREVIDENZA SOCIALE - INPS

Molti enti hanno più sedi e sezioni o strutture, per l'inserimento dei dati valgono le stesse regole con l'aggiunta della denominazione della sede distaccata o sezione dopo la lineetta preceduta e seguita da uno spazio

no DIREZIONE GENERALE CULTURA REGIONE LOMBARDIA;
si REGIONE LOMBARDIA - DIREZIONE GENERALE CULTURA.

Intestazione, ufficio, firmatario

Nell'inserimento dell'intestazione di una lettera deve essere distinto il firmatario dall'ente o persona giuridica, dalla ditta individuale o società. Il firmatario o la provenienza/destinazione particolare vanno inseriti nell'apposita stringa dell'anagrafica:

no SINDACO DEL COMUNE DI SASSARI
si COMUNE DI SASSARI (nell'apposita stringa dell'anagrafica verrà inserito: IL SINDACO).

no IL MINISTRO DEL LAVORO E PREVIDENZA SOCIALE;
si MINISTERO DEL LAVORO E DELLA PREVIDENZA SOCIALE (nell'apposita stringa dell'anagrafica verrà inserito: IL MINISTRO).

no IL PRESIDENTE DELLA PROVINCIA DI MILANO;
si PROVINCIA DI CREMONA (nell'apposita stringa dell'anagrafica verrà inserito: IL PRESIDENTE).

Nomi stranieri

I nomi di persona, di città, o di qualsiasi ente straniero vanno inseriti nella versione originale, solo lo stato va scritto in lingua italiana

Indirizzo

Per quanto riguarda gli indirizzi di residenza quando devono essere inseriti quelli dichiarati nella carta intestata; per quelli degli enti pubblici andrà sempre inserito l'indirizzo giuridico dichiarato; per gli uffici decentrati quello della sede dell'ufficio; non devono essere inserite posizioni in anagrafica incomplete di parte dell'indirizzo: luogo, provincia, via, numero civico, codice avviamento postale.

Casi particolari

Tutti i casi particolari vengano discussi con il Responsabile del servizio archivio-protocollo prima dell'inserimento nella banca dati.

La banca dati dell'anagrafica non deve essere compilata con dati parziali.

PADIGITALE
INNOVAZIONE PER LA PUBBLICA AMMINISTRAZIONE
WEB TECHNOLOGY FOR A REAL INNOVATION

Titolario di classificazione

Specifiche normative e archivistiche

Il Testo unico sulla documentazione amministrativa **DPR 445/2000** (Artt. 56 e 64) e il Codice dei beni culturali e del paesaggio **DLgs 42/2004** definiscono l'**obbligo di classificazione di documenti e fascicoli per le Pubbliche Amministrazioni**.

Per classificare i documenti e i fascicoli lo strumento archivistico da impiegare è il Titolario o Piano di classificazione.

Il **Titolario o Piano di classificazione** è un **sistema precostituito di partizioni astratte** con le seguenti caratteristiche:

- insieme di **voci logiche gerarchicamente ordinate** dal generale al particolare
- individuate sulla base dell'analisi di **funzioni e materie di competenza dell'ente**
- al quale deve ricondursi la molteplicità dei documenti prodotti, ricevuti, spediti
- ha la finalità di **consentire l'organizzazione di documenti e fascicoli** secondo un ordine che rispecchi l'attività svolta e **favorire il reperimento dei documenti** in modo funzionale
- non è progettato sulla base dell'organigramma dell'ente, al fine di garantire la stabilità della classificazione e la continuità delle serie archivistiche, pur nel mutare degli uffici

TITOLARIO DI CLASSIFICAZIONE

Il titolario è articolato su due livelli; i documenti e i fascicoli saranno da classificare al secondo livello.

Il titolario comprende le funzioni amministrative-strumentali e le funzioni istituzionali.

Per l'individuazione delle funzioni istituzionali sono stati di riferimento i seguenti documenti pubblicati sul sito istituzionale dell'Ente:

- *Convenzione istitutiva*

Contenuti del sito istituzionale

1. Organizzazione Generale

1.1 Legislazione, Circolari ministeriali, Mission
1.2 Statuto, Circolari Interne, Politiche Interne
1.3 Rapporti ed attività istituzionali con altri enti (accordi,intese,patrocini,etc).

2 Risorse umane

2.1 Legislazione generale
2.2 Organizzazione degli uffici, dotazione organica
2.3 C.C.N.L.– Sindacati- ARAN- Contrattazione integrativa
2.4 Fascicoli del personale - assunzioni, cessazioni, ordini di servizio, concorsi e mobilità, ferie e permessi, provvedimenti disciplinari
2.5 Gestione economica del personale
2.6 Tutela della salute e della sicurezza sui luoghi di lavoro
2.7 Formazione e aggiornamento professionale
2.8 Collaboratori esterni
2.9 Performance

3 Risorse finanziarie

3.1 Legislazione
3.2 Bilancio (Preventivo economico e Bilancio di esercizio) e Piano esecutivo di gestione (P.E.G.), Entrate e finanziamenti, Costi ed Uscite, Mutui e passività pregresse, Economato, Fatturazione Elettronica
3.3 Rapporti con istituti bancari - Tesoreria
Economato
3.4 Corte dei conti e organi di controllo
3.5 Patrimonio disponibile (manutenzione e acquisto aree, automezzi ed edifici)
3.6 Controllo di gestione

4 Risorse informative

4.1 Legislazione ed Agid
4.2 Sistema informativo e sito internet, sistema documentale ed archivio
4.3 Conservazione, Gestione Documentale, transizione al digitale
4.4 Responsabile della transizione al digitale

5. Gestione Tecnica Attività

5.1 Qualità e quantità delle acque (derivazioni, concessioni, acque superficiali e sotterranee)
5.2 Risorsa Suolo (geologia e geotecnica)
5.3 Risorsa Ambiente (Via-Vas-Vi ecc.)
5.4 Infrastrutture
5.5 Sistema Costiero
5.6 Pareri di compatibilità
5.7 Programmazione e Monitoraggio Interventi (RENDIS)

6. Gestione Giuridico - Amministrativa
6.1 Protocollo e URP
6.2 Gare e contratti, acquisti e affidamenti, forniture di beni e servizi
6.3 ANAC
6.4 Avvocatura e Contenzioso e Gestione extragiudiziale del contezioso
6.5 O.I.V. e organismi di valutazione

7. Oggetti Diversi
7.1 Oggetti diversi

D.46

PADIGITALE
INNOVAZIONE PER LA PUBBLICA AMMINISTRAZIONE
WEB TECHNOLOGY FOR A REAL INNOVATION

CONSERVATORE DI DOCUMENTI INFORMATICI

Norme di Sicurezza e Adeguamento

Pieve Fissiraga, 14-02-2022

Urbi Smart / WebTec / CDAN
Qualificazione dei servizi SAAS e ottemperanza al GDPR (General Data Protection Regulation Regolamento UE 2016/679), così come disposto dal Decreto Legislativo 10 agosto 2018, n. 101

Indice

1. Urbi Smart: Cloud Comuputing e licenza d'uso

Urbi Smart è il sistema informativo gestionale e direzionale integrato, web nativo, con un'unica base dati, che ha rivoluzionato la gestione delle informazioni nella Pubblica Amministrazione.

Urbi Smart è un unico strumento di supporto per il governo del Comune e degli Enti, accessibile da qualsiasi dispositivo mobile (essendo web nativo, si "muove" agevolmente in Internet) e in qualsiasi momento e luogo grazie alla modalità **CLOUD COMPUTING - di seguito Cloud -** definita anche SAAS (Software as a service) o ASP (Application Service Providing). Urbi Smart è per l'appunto disponibile nella modalità Cloud, ma può essere utilizzato anche nella tradizionale forma in licenza d'uso.

L'architettura web nativa - con accesso mediante qualsiasi PC con browser collegato a Internet o anche attraverso i più moderni strumenti mobile (come ipad Apple, tablet con Android oltre che iPhone, smartphone, palmari ecc.) - consente una naturale predisposizione verso il Cloud. Urbi Smart quindi si trova nella "nuvola informatica" (essendo in rete) e non risiede presso i server dell'ente che ne fruisce, ma in server dislocati presso un Internet Data Center (IDC) esterno sul territorio nazionale italiano. L'IDC di cui dispone PA Digitale S.p.A. (d'ora in avanti PA Digitale) risulta qualificato da AgID (Agenzia per l'Italia Digitale) come CSP - Tipo C così come imposto dalla normativa vigente.

Oltre ad essere in linea con le direttive dell'Agenzia per l'Italia Digitale (ex Digit PA, già CNIPA), tale modalità di erogazione consente di utilizzare soluzioni ad alto profilo tecnologico e costantemente aggiornate, protette e in grado di facilitare notevolmente l'interazione con i cittadini o altri soggetti esterni, senza forti investimenti infrastrutturali e pesanti costi di gestione (ad es. acquisto di software, hardware e infrastrutture di rete, costi di personale altamente specializzato per la gestione di infrastrutture complesse necessarie per usufruire della rete ecc.).

L'ente si avvale così anche **di un servizio specializzato che consente il ripristino rapido e completo dei dati in caso di interruzioni impreviste dei servizi e, quindi, la continuità operativa dei propri utenti** (in linea con quanto disposto dall'art. 50 del D. Lgs. 82/2005, Codice dell'Amministrazione Digitale - CAD).

Attualmente oltre 850 Enti utilizzano Urbi Smart in modalità Cloud e oltre 100 in modalità on premise (licenza d'uso).

La tecnologia web rende le applicazioni Urbi Smart estremamente efficaci, comunque, anche se acquisite in modalità licenza d'uso, in quanto sono tecnologicamente predisposte per essere installate in un proprio CED o presso altra server farm ed essere aperte alla rete internet. In questo contesto Urbi Smart si presta ad essere l'unica soluzione per aggregazioni di Comuni, CST, Comunità Montane che vogliono erogare i servizi direttamente dalla loro server farm o struttura CED.

2. WebTec: Cloud Comuputing

WebTec è la piattaforma **di servizi per la digitalizzazione di dati, attività e processi, sviluppata con tecnologia web**, che PA Digitale rivolge a Software House, Rivenditori, Produttori di software applicativi, Dealer, System Integrator per accompagnare i loro clienti - aziende, professionisti, associazioni di categoria, ordini professionali - verso la Digital Transformation, mantenendo una completa autonomia tecnica e di mercato nonché una gestione esclusiva del cliente.

Con WebTec, gli operatori ICT possono completare la loro offerta gestionale con nuovi **servizi perfettamente integrabili con i principali ERP e soluzioni gestionali, grazie a una ricca libreria di API rest**, per assicurare con la massima semplicità un colloquio applicativo e una gestione aziendale integrata con le soluzioni già in uso.

L'offerta dei servizi è veramente ampia, ideata per la massima semplicità e fruibilità grazie anche al pannello di gestione che consente l'attivazione di servizi e funzioni: **fattura elettronica** (*PA Digitale è soggetto accreditato SDI*), **gestore documentale e conservazione digitale a norma con workflow integrato e firma digitale, workflow processuale, servizi di integrazione con l'Agenzia delle Entrate, quadratura cassetto fiscale, gestione strutturata delle PEC, web mail, gestione pratiche, agenda mobile, prenotazioni on line degli appuntamenti, servizi di collaboration & communication per la condivisione di dati e documenti con clienti/associati, gestione corrispondenza, gestione del credito.**

Grazie al pannello di attivazione, accessibile anche in mobilità, è **sempre garantita quindi la possibilità di attivare nuove funzioni/componenti applicative e comporre così la proposta di servizi sulla base delle reali esigenze del clienti.**

WebTec è un **sistema unico** in cui le informazioni man mano si arricchiscono pur garantendo **l'unicità del dato** e dunque, senza duplicazione delle informazioni all'interno del DB dell'utente finale.

Tutti i servizi sono fruibili in totale mobilità e in cloud: il 100% delle funzioni è utilizzabile, per tutto il sistema e per qualsiasi utente, da un qualsiasi luogo e con qualsiasi device, ottenendo così una totale mobilità. I servizi WebTec sono quindi disponibili 24 ore su 24, 365 giorni all'anno e sono costantemente aggiornati prevedono aggiornamenti e backup "a caldo", senza alcun costo infrastrutturale e di gestione.
Gli oltre 300.000 utenti finali e 70.000.000 di fatture elettroniche gestite ogni anno, per esempio, testimoniano la solidità del sistema che rende i dealer veri protagonisti dell'innovazione digitale.

3. Servizio di Conservazione Digitale a Norma CDAN

Il Servizio di Conservazione Digitale a Norma **CDAN** di PA Digitale, preposto alla conservazione dei documenti informatici dei Clienti, è stato **realizzato con le tecnologie più innovative** e **in conformità alle regole tecniche di cui all'art. 71 del Codice dell'Amministrazione Digitale** (CAD), la cui rispondenza è requisito indispensabile ed essenziale per la corretta conservazione a norma dei documenti informatici.
Il servizio CDAN assicura la conservazione digitale dei documenti informatici secondo le vigenti disposizioni di legge, garantendone le caratteristiche di autenticità, integrità, affidabilità, leggibilità e reperibilità e mantenendo così inalterato nel tempo **il valore legale** dei documenti conservati.
Grazie ai numerosi automatismi e all'integrazione nativa con le applicazioni Urbi Smart e WebTec, la conservazione digitale a norma garantisce la **massima semplicità di gestione** per gli utenti, agevolati da **funzionalità immediate e da una grafica piacevole e intuitiva**. Tutti gli accessi al sistema, sia da parte degli utenti sia per le operazioni automatizzate di conservazione, avvengono in totale sicurezza tramite l'utilizzo di canali di comunicazione sicuri.
Il Servizio di Conservazione Digitale a Norma CDAN è erogato in modalità Cloud Computing come SaaS (Software as a Service) per i Clienti del Mercato Pubblico e Privato ed è conforme alle recenti *Linee guida sulla formazione, gestione e conservazione dei documenti informatici e relativi allegati* pubblicate da AgID. Il Servizio di Conservazione Digitale a Norma CDAN applica quanto previsto dal *Regolamento sui criteri per la fornitura dei servizi di conservazione dei documenti informatici* e dai relativi Allegati A e B.

4. Le Certificazioni di PA Digitale

La modalità di applicazione di quanto descritto nel presente documento è governata da Procedure Operative Interne e da Istruzioni di Lavoro previste dal Sistema di Gestione Integrato per le norme ISO adottate da PA Digitale e certificato da un ente terzo indipendente, accreditato da Accredia, per l'ambito *Analisi, progettazione, sviluppo, produzione, installazione, commercializzazione, distribuzione, manutenzione e assistenza di prodotti software per la Pubblica Amministrazione Locale e Centrale e per il Mercato Privato, erogati in modalità SaaS oppure erogati con installazione in locale (on premise). Erogazione di servizi professionali connessi ai prodotti software per la Pubblica Amministrazione. Erogazione dei servizi SaaS in cloud per la Conservazione Digitale di documenti informatici a Norma e relativo servizio di assistenza.*
Le norme a cui PA Digitale attualmente aderisce sono

- UNI EN ISO 9001:2015 - Sistemi di Gestione per la Qualità - Requisiti, i cui dettagli sono illustrati nella Politica Aziendale della Qualità, pubblicata sul sito istituzionale di PA Digitale e raggiungibile nella sua versione più aggiornata al link https://www.padigitale.it/certificazioni/
- UNI CEI EN ISO/IEC 27001:2017 - Tecnologie Informatiche - Tecniche per la Sicurezza - Sistemi di gestione per la sicurezza delle informazioni - esteso alle Linee Guida: ISO/IEC 27017:2015 e ISO/IEC 27018:2019, i cui dettagli sono illustrati nella Politica Aziendale della Sicurezza delle Informazioni, pubblicata sul sito istituzionale di PA Digitale e raggiungibile nella sua versione più aggiornata al link https://www.padigitale.it/certificazioni/

I Sistemi di Gestione sono integrati con la Politica Aziendale in Materia di Trattamento e Protezione dei Dati Personali pubblicata sul proprio sito istituzionale al link https://www.padigitale.it/privacy/.

I servizi SaaS Urbi Smart e CDAN sono conformi alle Circolari AgID n. 2 e 3 del 9 aprile 2018 e pertanto sono presenti nel *Catalogo dei servizi Cloud qualificati per la PA* ai link:

- https://catalogocloud.agid.gov.it/service/494 (Urbi Smart),
- https://catalogocloud.agid.gov.it/service/1530 (CDAN).

PA Digitale eroga il Servizio di Conservazione Digitale certificato in conformità:

- alla Norma UNI EN ISO 9001:2015 - Sistemi di Gestione per la Qualità - Requisiti.

- alla Norma UNI CEI EN ISO/IEC 27001:2017 "Tecnologie informatiche - Tecniche per la sicurezza - Sistemi di gestione per la sicurezza delle informazioni - Requisiti". Il Sistema di Gestione della sicurezza delle informazioni soddisfa i criteri contenuti nelle seguenti Linee Guida: ISO/IEC 27017:2015 e ISO/IEC 27018:2019.
- ai requisiti individuati il servizio di "Conservatore di documenti informatici ai sensi dell'art. 29, comma 1, del D.Lgs. 7 marzo 2005, n. 82" e ss.mm.ii, tra cui si citano (a titolo esemplificativo e non esaustivo) le "Linee Guida sulla formazione, gestione e conservazione dei documenti informatici" (Agid Determinazioni 407/2020 e 371/2021, con applicazione dal 1° gennaio 2022) e il "Regolamento sui criteri per la fornitura dei servizi di conservazione dei documenti informatici" (Agid Determinazione 445/2021, in vigore dal 1° gennaio 2022).

Per tali ragioni, dal 14/02/2022 il Servizio di Conservazione Digitale a Norma **CDAN risulta qualificato presso AgID** mediante l'avvenuta iscrizione al Marketplace dei servizi di conservazione della società PA Digitale S.p.A. ai sensi dell'articolo 34 comma 1-bis lettera b) del decreto legislativo 7 marzo 2005, n. 82 e s.m.i., recante il Codice dell'amministrazione digitale (CAD). La qualificazione è consultabile al link: https://conservatoriqualificati.agid.gov.it/?page_id=276.

PA Digitale adotta un Codice Etico e un Modello di Organizzazione, Gestione e Controllo ai sensi del D. Lgs. 231/01, disponibili in consultazione sul sito istituzionale www.padigitale.it.

Si aggiunge infine che PA Digitale ha ottenuto un punteggio di **++ (tra i più alti degli operatori di settore) nel rating di legalità pubblicato dall'Autorità Garante della Concorrenza e del Mercato "AGCM". L'Elenco delle imprese con rating di legalità aggiornato e consultabile è reso disponibile dall'AGCM sul proprio sito al link https://www.agcm.it/competenze/rating-di-legalita/rating-elenco-imprese.

5. Cloud: vantaggi

Oltre alla possibilità di accedere ovunque alle applicazioni, l'utilizzo delle soluzioni erogate da PA Digitale in modalità Cloud (Urbi Smart, WebTec e CDAN) consente di avere molti vantaggi:

- Nessuna necessità di competenza informatica per la gestione di hardware, software e degli archivi.
- Nessun limite connesso alla necessità di dimensionamento del sistema: non occorre infatti stabilire a priori il dimensionamento dell'hardware, dato che, anche al crescere delle esigenze occorre esclusivamente aggiungere i posti di lavoro utente necessari.
- Nessun vincolo hardware e software.
- Totale eliminazione della responsabilità di archiviazione dei dati.
- Nessun vincolo contrattuale per l'eventuale cambio di fornitore.
- Estrema scalabilità.
- Aggiornamenti del software applicativo immediatamente disponibili.

6. Ottemperanza al Regolamento UE 2016 / 679 (GDPR) e relative misure di sicurezza (art. 32)

PA Digitale si impegna a rispettare sempre quanto previsto dal Regolamento UE 2016 / 679 (GDPR), e con particolare perizia quando è nominata Responsabile esterno del trattamento dati (oppure Sub responsabile esterno del trattamento dei dati). Nello specifico, adotta tutte le seguenti misure per ottemperare a quanto previsto dall'art. 32; dette misure (messe in esercizio da PA Digitale per garantire tanto l'Ottemperanza al GDPR quanto i più alti standard di sicurezza per le proprie soluzioni) sono illustrate nei capitoli seguenti.
Per i clienti che usufruiscono delle soluzioni Urbi Smart e WebTec - erogate in modalità Cloud - sono valide le misure descritte in ciascuno dei capitoli seguenti.
Per i clienti che usufruiscono della soluzione Urbi Smart erogata in modalità on premise (licenza d'uso) sono valide le misure descritte in ciascuno dei capitoli seguenti (fatta eccezione per l'intero capitolo 7 e per il paragrafo 9.2).
Infine, i clienti che usufruiscono della soluzione CDAN riterranno valide tutte le misure seguenti, eccetto che per alcuni paragrafi del capitolo 8 (8.1.b, 8.1.c, 8.1.d, 8.1.e - essendo CDAN una soluzione integrata con Urbi Smart e WebTec, ne eredita per queste parti le relative misure di sicurezza), per il paragrafo 9.2.

7. Sicurezza dei dati e continuità operativa

PA Digitale eroga i servizi Cloud - riportati ai capitoli 1, 2 e 3 - attraverso un Internet Data Center certificato in base al vigente standard internazionale ISO/IEC 27001 e alle Linee Guida ISO/IEC 27017 e ISO/IEC 27018, in cui le apparecchiature per la trasmissione dei dati e le architetture hardware/software preposte all'erogazione dei servizi sono poste in condizioni di massima **sicurezza applicativa e fisica** (sistemi antintrusione, sistemi antincendio, controllo accessi, telesorveglianza ai piani; ridondanza dei sistemi elettrici e di refrigerazione), **informatica e logica** (sistemi antintrusione).

Relativamente alla sicurezza fisica e infrastrutturale, l'Internet Data Center è dotato di protezione contro ogni minaccia, per garantire la massima sicurezza a dati e servizi. I sistemi di backup dei dati, il Disaster Recovery, la continuità dei servizi, offrono agli utenti i più elevati livelli di servizio, 24 ore su 24, 7 giorni su 7, 365 giorni all'anno. Tali garanzie sono fondamentali e indispensabili per gli Enti, sia per rispondere agli obblighi di legge in materia di **Business Continuity** (già citato art. 50, D. Lgs. 82/2005 - CAD), sia per poter garantire il corretto e regolare svolgimento della vita di cittadini e imprese nel caso di servizi in modalità online.

A tal fine, PA Digitale garantisce un servizio di **Disaster Recovery** completamente automatizzato in tutti i suoi processi e monitorato da personale tecnico specializzato 24 ore su 24, 7 giorni su 7, 365 giorni all'anno. Tutti i sistemi e apparati di rete/strutturali sono in configurazione fault-tolerance per evitare Single Point of Failure. La capacità di elaborazione del sistema di Disaster Recovery permette, in caso di disastro, il ripristino dell'erogazione dei servizi con prestazioni equivalenti al sito di normale operatività, in tempi conformi al Tier 3 e a quanto indicato al paragrafo sottostante *7.7 Servizi di backup e Disaster Recovery*. Attività di verifica e test di funzionamento dei sistemi sono svolte regolarmente per la massima sicurezza di dati e sistemi.

Il sito primario di erogazione servizi Cloud è presso il Data Center di Westpole S.p.A., in Via Francesco Sforza 13, Basiglio (MI). Il sito secondario di Disaster Recovery è presso il Data Center di Westpole S.p.A. in Via di Macchia Palocco 243, Acilia, Roma (RM).

Nel rispetto delle Circolari AgID n. 2 e 3 del 9 aprile 2018, l'IDC risulta qualificato come CSP - Tipo C ed è iscritto nel *Registro dei CSP Qualificati* consultabile al link https://catalogocloud.agid.gov.it/.

7.1 Internet Data Center

Le reti Metropolitane per i due Data Center (sito primario e sito secondario, citati al paragrafo precedente) si basano sulla cablatura in fibra la cui banda complessiva è di alcuni Gbps con possibilità di ampliamento immediato senza modifiche infrastrutturali. Il collegamento verso la rete pubblica internet viene garantito attraverso router di backbone con attestati i link di diversi operatori. Il protocollo di routing BGPV4, costantemente gestito sui router di backbone, decide le destinazioni selezionando il carrier con la miglior qualità di servizio da e verso specifiche aree geografiche. In caso di disservizio di uno dei carrier, il BGP provvede automaticamente a instradare tutto il traffico verso l'operatore funzionante e, se necessario, anche transitando per la connettività attestata sul sito secondario rispetto al Data Center che sta erogando il servizio.

I due Data Center sono connessi tra di loro da una dorsale in fibra, permettendone la gestione come fosse un "unico" Data Center distribuito. Il sistema di controllo degli accessi prevede una postazione di guardiania che identifica il personale che richiede accesso e fornisce badge che consente l'accesso alle sole aree di pertinenza.

7.2 Infrastruttura di sistema

L'**architettura del Data Center** è basata su componenti le cui principali caratteristiche sono:

- utilizzo di sole componenti di classe Enterprise;
- affidabilità delle singole componenti scelte;
- ridondanza fisica di tutti i componenti HW;
- ridondanza dei componenti SW di sistema e networking.

La disponibilità effettiva dell'infrastruttura presenta un uptime del 99.95%, garantita a diversi livelli sia grazie alle scelte architetturali che alle tecnologie utilizzate. Per garantire la massima disponibilità e fruibilità delle risorse atte all'erogazione dei servizi in modalità Cloud, PA Digitale monitora periodicamente le proprie risorse infrastrutturali predisponendo un Piano di Capacità/Capacity Plan con revisione minima annuale. Scopo di detto Piano è assicurare in ogni momento la capacità sufficiente per garantire il più alto livello di erogazione dei servizi in Cloud, in base alle attuali e future esigenze di business del mercato. Il Piano viene inoltre aggiornato in seguito a cambiamenti significativi del personale, dell'organizzazione o delle infrastrutture.

7.3 Sottosistema di virtualizzazione

I servizi sono erogati da un cluster di sistemi ad alta affidabilità VMware Enterprise in regime di Private Cloud, con risorse computazionali dedicate al fine di prevenire condivisione di risorse con altri ambienti. Alcune delle caratteristiche salienti:

- Vmotion: consente di migrare real time le VM tra host fisico a un altro cluster;
- Storage Vmotion: rilocazione di VM fra datastore senza interruzione del servizio;
- High Availability: in caso di failure di un host virtualizzatore o della VM.

7.4 Sottosistema storage

Per eliminare ogni rischio di interruzione del servizio dovuto a guasti HW, tutti i dischi delle VM e dei dati sono memorizzati esclusivamente su **SAN ad alte prestazioni dedicate al servizio**.
La configurazione della SAN garantisce assenza di Single Point of Failure, tutti i sistemi sono in costante monitoraggio che garantisce tempi di sostituzione componenti hardware senza completo fermo del sistema.
Le garanzie:

- **alta affidabilità dei componenti fisici**, tutti i componenti sono ridondati, cioè disco in RAID5 + hot-spare, SAN dual-fabric ecc.
- **scalabilità verticale e orizzontale dell'infrastruttura,** che è in grado di supportare richieste di workload e di spazio addizionale evitando situazioni di overbooking.

7.5 Sottosistemi firewall e componenti di sicurezza

L'architettura di sicurezza e firewall è implementata utilizzando **due firewall in cluster HA**, per la gestione dell'accesso internet e per la gestione della DMZ e LAN interna.
I server applicativi utilizzano **VLAN** per ottenere una separazione del livello database da quello applicativo, al fine di elevare la sicurezza di gestione dei documenti e di ridurre al minimo il rischio di compromissione dei sistemi in caso di attacco.
L'infrastruttura dispone di **sonde IPS** (Intrusion Prevention System) che garantiscono una protezione perimetrale da attacchi, per esempio di tipo DDOS (Distributed Denial of Service), di sonde antivirus per l'analisi di tutto il traffico web e per prevenire l'eventuale infezione causata da malware.
La sicurezza di accesso ai componenti del sistema è garantita attraverso l'uso di password a criptazione forte.
L'accesso all'IDC da parte di PA Digitale ai sistemi per scopi di amministrazione avviene attraverso connessioni **VPN** autenticate attraverso username/password e certificati digitali, oppure tramite VPN site 2 site IPSEC configurata direttamente fra i firewall di PAD e del sito primario. In quest'ultimo caso, è prevista un'ulteriore abilitazione specifica a livello di firewall.

7.6 Politiche di backup

Le politiche di backup adottate prevedono la gestione di tutti i dati relativi a Urbi Smart, WebTec e CDAN: database, documenti e componenti applicative. I backup hanno frequenza giornaliera e retention/storico di 30 giorni. I job di backup non impattano l'erogazione dei servizi; i backup dei database avvengono a caldo sul nodo del cluster "slave".

7.7 Servizi di backup e Disaster Recovery

La strategia di backup adottata per l'adozione delle Politiche descritte al punto precedente prevede l'implementazione e l'utilizzo di Veeam Backup and Replication e di NAS Platform Snapshots.
Le soluzioni adottate permettono il recupero dei dati, garantendone un corretto processo di ripristino e l'identificazione dei dati necessari recuperando il supporto di backup appropriato.
Sono pianificate delle prove di ripristino dei dati in maniera randomica, che consistono nel restore di un ambiente virtuale in un'area di test e le relative verifiche di buon funzionamento. La granularità dei backup relative ai database consente il recupero a livello del singolo record a una data specifica.
Il Disaster Recovery è gestito con tecnologia VMware Site Recovery Manager. Il sistema garantisce una procedura di disaster recovery con RPO di 4 ore ed RTO minimo di 4 ore e massimo di 48 ore.

8. La gestione della sicurezza e sistemi di security management per le procedure applicative

La gestione della sicurezza costituisce una tra le componenti più delicate nell'ambito, più generale, della gestione dei dati dei Clienti. Sia l'infrastruttura che i servizi SaaS erogati in modalità Cloud da PA Digitale sono periodicamente sottoposti ad attività di Vulnerability Assessment e Penetration Test, effettuati da un ente terzo indipendente certificato da Accredia.

Dovendo implementare un IDC per l'erogazione dei servizi di amministrazione degli enti in modalità Cloud, PA Digitale ha da tempo sviluppato e attuato una metodologia per l'analisi dei rischi legati alla sicurezza e alla sua gestione attraverso opportuni meccanismi e strumenti di controllo e di intervento.

Le scelte adottate, in linea con quanto enunciato dall'Agenzia per l'Italia Digitale in materia di sicurezza, portano a:

- controllo e monitoraggio degli accessi in modo puntuale e nel tempo;
- identificazione di eventuali anomalie;
- intervento nel minor tempo possibile per ripristinare la situazione correttamente.

8.1 Principi applicabili al legittimo trattamento dei dati

Per soddisfare i requisiti di sicurezza, le soluzioni Urbi Smart, WebTec e CDAN osservano principi applicabili al legittimo trattamento dei dati (con particolare riguardo verso le Informazioni Personali Identificabili - PII), supportando una serie di servizi e di dispositivi atti a implementare funzioni di autenticazione, autorizzazione e crittografia. Tali servizi e dispositivi risultano adeguati alla nuova normativa UE 2016/679 in vigore dal 25.05.2018, così come disposto in Italia dal Decreto Legislativo 10 agosto 2018, n. 101 "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo 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)".

L'**autenticazione** prevede che gli utenti si debbano identificare con una serie nota di credenziali, ad esempio nome utente e password. Per i servizi on line di Urbi Smart è prevista a norma di legge l'autenticazione con le principali piattaforme ministeriali e regionali, che implementano SPID, CIE e CNS.

Per **autorizzazione**, invece, si intende l'assegnazione di determinati livelli di accesso al sistema, che si riflettono in ben identificate capacità operative sul sistema medesimo da parte del singolo utente correttamente identificato.

L'attribuzione dei privilegi degli utenti, intesi come regole sia di autenticazione che di autorizzazione, sono esclusivamente demandate all'Amministratore applicativo. Quest'ultimo può decidere se applicare su altri utenti i privilegi che regolano le policy di sicurezza, di accesso, visibilità e gestione dei dati.

La **sicurezza** dei dati è garantita:

- durante la fase di comunicazione client e server tramite utilizzo di protocollo https e crittografia di tipo TLS 1.2 o superiori
- nello storage all'interno del database
- durante la fase di comunicazione tra sottosistemi di infrastruttura (webserver, long run process server, dbms server, NAS) o applicativi (comunicazioni da/verso sistemi ministeriali e/o di terze parti mediante identificazione degli enti coinvolti nello scambio dei flussi informativi e degli utenti abilitati all'accesso ai servizi anche tramite l'utilizzo di certificati digitali).

I servizi sono sottoposti a controllo costante dell'erogazione e delle prestazioni del servizio mediante strumenti di supervisione, accessibili via web dal personale abilitato.

Di seguito le caratteristiche del gestionale espresse in forma sintetica che saranno dettagliate nei paragrafi successivi.

a. Erogazione servizio tramite protocollo https
b. Accessi al software protetti da "nome utente" e "password".
c. password di accesso "sicure".
d. Gradi di libertà predisposti in base alla profilazione ruoli degli utenti.
e. Protezione dei dati
f. Tracciabilità dei log di accesso per eventuali comunicazioni di Data Breach.
g. Tracciabilità delle variazioni ai dati del sistema

Infine, PA Digitale ha pubblicato la propria *Politica in Materia di Trattamento e Protezione dei Dati Personali* sul suo sito istituzionale, raggiungibile nella sua versione più aggiornata al link https://www.padigitale.it/privacy.

8.1.a Erogazione servizi mediante protocollo HTTPS

Sia i servizi di backoffice che i servizi on line di Urbi Smart, WebTec e CDAN possono essere erogati mediante protocollo HTTPS.

Il protocollo HTTPS consiste nel far transitare la comunicazione tramite il protocollo HTTP all'interno di una connessione criptata dal Transport Layer Security (TLS) 1.2 o superiori. Viene utilizzato per garantire trasferimenti riservati di dati nel web, in modo da impedire intercettazioni dei contenuti. Il principio che sta alla base di HTTPS è quello di avere:

- un'autenticazione del sito web visitato
- protezione della privacy
- integrità dei dati scambiati tra le parti comunicanti.

8.1.b Accessi al software protetti da nome utente e password

Urbi Smart, WebTec e CDAN utilizzano un sistema di **autenticazione basato su sessione**. Ogni programma all'interno delle tre soluzioni verifica la validità della sessione in corso (identificata da un token di sessione) prima di fornire la pagina richiesta. Allorché la sessione sia scaduta o non sia attiva, qualsiasi richiesta viene ridirezionata al sistema di autenticazione. Il sistema di autenticazione standard prevede autenticazione basata su **Login e Password.** L'utente è identificato all'interno di una base dati da un *nome utente* e da una *password*, secondo lo schema seguente:

- login: nomeutente@identificativodb
- password: Password_Utente

Nomeutente, identificativodb e password sono gli elementi essenziali e univoci per procedere alla validazione di un utente.

Su richiesta, sono disponibili integrazioni a strumenti di autenticazione standard (es. LDAP, Active Directory) attraverso cui ricondursi a utenti censiti in Urbi Smart e WebTec.

Come già anticipato, per i servizi on line di Urbi Smart è prevista a norma di legge l'autenticazione con le principali piattaforme ministeriali e regionali, che implementano SPID, CIE e CNS.

8.1.c Password di accesso sicure

Le password sono tutte crittografate; ad ogni utente, l'Amministratore applicativo può assegnare:

1. **Data Scadenza Utente**: questa data indica la data fino alla quale l'utente è valido. **Scaduta questa data l'utente viene disattivato**. Questa data serve per consentire di attivare un utente per un certo periodo di tempo: se si lascia il campo vuoto, oppure impostato a valore infinito 31-12-9999, l'utente è sempre attivo.
2. **Password d'Ufficio**: se non diversamente specificato, l'utente è costretto a modificare la password la prima volta che entra nella procedura.
3. **Data Attivazione Password:** questa data (impostata di default al giorno di creazione dell'utente) indica la data di attivazione della password per l'utente. In alcuni casi può essere utile attivare gli utenti in date posteriori alla creazione dell'utente stesso.
4. **Giorni Validità Password:** indica per quanti giorni la password di un utente è valida, a partire dalla data di attivazione. Questo campo è utile per definire un periodo di validità della password all'interno del range definito tra la data attivazione e la data scadenza. L'Amministratore applicativo può decidere la policy utente alla scadenza dei giorni di validità. Le due scelte possibili sono: a) Costringere l'utente a cambiare password b) disattivare l'utente.
5. **Max Giorni Non Loggato:** indica il numero massimo di giorni in cui un utente può restare attivo senza accedere a Urbi Smart e WebTec. Trascorso tale numero di giorni senza che l'utente acceda al sistema, la procedura lo disattiva in automatico.

All'atto della creazione di un nuovo utente, l'Amministratore gli attribuisce:

1. la **Password** (di default viene impostata come password d'ufficio)
2. la **Data di Scadenza Utente**
3. la **Data di Attivazione della Password** (impostata alla data del giorno) e il numero di **Giorni di Validità della Password**
4. il numero **Max Giorni Non Loggato** (se si vuole che venga disattivato l'utente che non accede a Urbi Smart e WebTec per più di un certo numero di giorni consecutivi).

La prima volta che il nuovo utente entra nella procedura deve utilizzare la password attribuita dall'amministratore. Se la password assegnatagli è una **password d'ufficio**, il sistema gli presenta in automatico la sezione per il cambio password obbligatorio: **l'utente deve inserire una nuova password compresa tra 8 e 30 caratteri (almeno 2 numeri e almeno 5 lettere dell'alfabeto ed almeno un carattere tra . ; $! - < >)**. Modificata la password può

ritornare a Urbi Smart e WebTec tramite link contenuto nella maschera. Se l'utente sbaglia le credenziali per tre volte consecutive viene disabilitato, e può essere riabilitato solo mediante l'intervento dell'Amministratore, che agirà sempre attraverso l'interfaccia di gestione utenti. Il numero minimo di tentativi disponibili per tentare l'accesso è settato a 3, ma l'Amministratore applicativo può decidere di aumentare questo valore, secondo le politiche interne al cliente.

Un utente viene inoltre disabilitato se:
1. è scaduto (**Data Scadenza Utente** scaduta)
2. è stato per **MaxGiorniNonLoggato** senza accedere a Urbi Smart e WebTec (se tale valore è stato settato).
3. la sua password è scaduta (**Giorni Validità Password**, settato) ed è stato definito che alla scadenza l'utente debba essere disattivato.

Anche in questi casi è necessario riabilitarlo tramite l'intervento dell'Amministratore, come sopra.
L'**annullamento** di un utente prevede di annullare logicamente l'utente medesimo, in modo da garantire che le credenziali di autenticazione non saranno mai più utilizzate per diversi utenti, neppure in tempi diversi. Un utente **ANNULLATO** viene ancora visualizzato nella lista degli utenti (in apposita sezione), ma non è più attivo e non è più possibile effettuare operazioni su di esso. In questo modo si garantisce che non sarà mai inserito un utente con lo stesso nome di un utente già utilizzato in precedenza (anche se annullato).

8.1.d Gradi di libertà predisposti in base alla profilazione ruoli degli utenti.

Urbi Smart e WebTec permettono la definizione di tre tipologie di utenti in funzione della loro visibilità ed accessibilità alle varie procedure, e quindi in funzione del tipo di menù assegnato. In particolare:
1. **Utente Standard**: l'utente può entrare nell'area delle procedure abilitate e accedere di default a tutti i programmi raggiungibili in virtù del suo Profilo Primario (Visione, Gestione, Supervisore). È tuttavia possibile prevedere un ulteriore livello di autorizzazione, disabilitando l'accesso solo ad alcuni programmi.
2. **Utente Scrivania**: questo tipo di utente può accedere esclusivamente ai programmi che gli sono stati espressamente abilitati. L'utente Scrivania può accedere a Urbi Smart e WebTec solamente alle procedure che gli sono state assegnate, e la pagina di accesso proposta contiene soltanto i programmi che gli sono stati assegnati (non ha la navigazione completa dell'utente Standard).
3. **Utente Misto** (valido solo per Urbi Smart): è l'utente che è Standard per alcune procedure e Scrivania per altre. Ad esempio: un utente standard dell'anagrafe (che ha a disposizione tutte le scelte del menù anagrafico) al quale viene attivata la sola funzione di visualizzazione delle delibere o visualizzazione dei protocolli.

È possibile prevedere ulteriori autorizzazioni relative a specifiche applicazioni Urbi Smart e WebTec.
Tutti i programmi Urbi Smart e WebTec, al momento del rilascio, sono suddivisi per singole Procedure e ciascuno di essi viene rilasciato con un livello di accesso di default scelto fra tre tipologie di Programma: Programma di Visione, Programma di Gestione o Programma di Supervisore. Analogamente, eventuali Funzioni associate ai programmi stessi sono rilasciate con un valore di default fra Funzione Abilitata o Funzione Disabilitata.

Urbi Smart e WebTec prevedono la gestione delle abilitazioni organizzata a livelli:
- a livello di Procedura, relative a tutti i programmi della procedura;
- a livello di Programma, con accesso al programma, inserimento di dati, annullamento di dati, variazione di dati;
- abilitazioni all'interno del programma di particolari Funzioni.

Di conseguenza, sono previsti tre livelli di intervento per la definizione dei privilegi utente:
- associazione di uno dei Profili di Base previsti (a livello di procedura);
- abilitazione o meno dello specifico programma;
- abilitazione del programma con inibizione o meno di specifiche funzioni.

Nella tabella seguente sono evidenziate le abilitazioni di default sui programmi di una procedura in funzione dei Profili di Base di un utente:

Profilo Base	Abilitazione di default dei programmi della procedura
Visione	Solo programmi definiti come Visione

Gestione	Programmi definiti come Visione e Gestione
Supervisore	Programmi definiti come Visione, Gestione e Supervisore
Scrivania	Solo programmi esplicitamente assegnati

Controllo interventi sui soggetti

Il soggetto, sia esso una persona fisica o un soggetto giuridico, acquisisce in Urbi Smart e WebTec un'importanza elevata. Costituendo il punto centrale di indagini nell'ambito del sistema informativo ed essendo presente una sola volta come codice e relativo corredo anagrafico, necessita di una serie di controlli capillari sul trattamento delle sue informazioni. Due sono le sezioni previste per il controllo degli interventi sui soggetti: Variazione e Annullamento. Ogni variazione inerente a quello che è stato definito corredo anagrafico di un soggetto (fanno parte di questo gruppo per esempio cognome, nome, data nascita, codice fiscale) viene concessa esclusivamente se l'utente che vuole effettuare è autorizzato a compiere una Variazione e/o un Annullamento.

Gestione classi di utenti

La funzione è stata progettata per rendere più efficiente e ottimizzata la gestione delle profilazioni degli utenti. È possibile identificare una serie di utenti di riferimento (utenti di tipo classe) e permettere a tutti gli utenti collegati a una classe di ereditare le caratteristiche dell'utente capofila o di riferimento. Grazie a tale impostazione, è possibile effettuare estrazioni o applicare filtri esclusivamente a determinate classi di utenti.

Gestione stampe

La gestione dello spool delle stampe segue di pari passo la gestione degli utenti/classi utente. Ciascun utente può generare le stampe secondo le abilitazioni definite seguendo i criteri elencati nel presente paragrafo. Come per la gestione utenti, anche per la gestione delle stampe l'Amministratore applicativo ha la possibilità di sovrintendere l'intero sistema delle stampe, per mezzo di funzioni di ricerca mirata all'interno dello spool.

8.1.e Protezione dei dati

Anche per la protezione dell'accesso ai dati, il meccanismo si fonda su un sistema di permessi basato sui ruoli definiti in pianta organica e nella gestione utenti descritta al paragrafo precedente. L'accesso ai dati avviene solo attraverso l'applicazione; i server di database sono protetti **da un doppio sistema di firewall e da regole di routing** che non ne consentono la visibilità dall'esterno della rete.

La gestione della base dati unica relativa al singolo Ente è basata su database standard. Nel caso di utilizzo del sistema in modalità Cloud con collegamento al Data Center, il database adottato è Maria DB. In tutti i casi il sistema ne rispecchia le caratteristiche in termini tecnico-funzionali.

I database dei singoli Enti sono distinti e ad ognuno di essi è stato associato un utente/schema. Ad ogni schema non vengono concessi privilegi ulteriori che comportino l'accesso e/o la gestione di oggetti appartenenti ad altri schemi. Non esistono aree condivise tra i vari schemi.

La connessione dall'application server al database avviene attraverso un servizio di rete diverso per ogni Ente. Gli utenti di un ente, al momento dell'accesso, discriminano lo schema associato e l'autenticazione viene effettuata attraverso l'utente, lo schema e relativa password. Questi tre elementi sono indipendenti per ogni ente.

8.1.f Tracciabilità dei log di accesso (per eventuali comunicazioni di Data Breach)

Il sistema di autenticazione basato su sessione rende implicitamente disponibile una funzione di monitoraggio attività sul sistema. Attraverso apposita tabella, infatti, possono essere memorizzate le sessioni d'uso istanziate e chiuse, i tentativi di accesso non riusciti, i rinnovi di sessione, ecc. La richiesta al Session Manager, inoltrata ogni qualvolta un utente fa una richiesta a Urbi Smart, WebTec e/o a CDAN, consente di registrare informazioni sulle operazioni eseguite con tracciamento per ogni utente, programma, evento. La logica di base con cui sono sviluppati i programmi di Urbi Smart, WebTec e CDAN fa sì che ciascuna operazione svolta dagli utenti (visualizzazione di una maschera, inserimento, modifica o rimozione di dati) avvenga tramite il richiamo di un evento che viene tracciato. Vengono difatti tracciati:

- token di sessione
- utente loggato
- Remote IP da cui è pervenuta la chiamata
- TimeStamp dell'evento
- estremi della chiamata

La struttura è in grado di memorizzare anche situazioni del tipo:
- "Non si dispone delle credenziali per procedere." @ErroreLogin (dove ErroreLogin riporta l'esatta motivazione dell'errore)
- "Errore in fase di derivazione delle credenziali per la base dati. Chiudere e riaprire il browser, quindi riprovare"
- "Sessione non valida!"
- "Sessione scaduta!"
- "Sessione con IP reimpostato, rieffettuare la login!"
- "Non si dispone delle autorizzazioni per accedere, chiudere il browser e rieffettuare la login!"
- LOGIN utente
- LOGOUT utente.

8.1.g Tracciabilità delle variazioni ai dati del sistema

Urbi Smart e WebTec sono dotati di un sistema di monitoraggio delle variazioni alla base dati. Le variazioni applicative alla base dati vengono tracciate riportando, per ogni sessione di variazione:
- grandezza variata
- utente che ha effettuato la variazione
- istanza applicativa che ha provocato la variazione
- valore precedente alla variazione
- valore successivo alla variazione.

Funzioni applicative di interrogazione consentono l'analisi del monitoraggio.

9. Erogazione servizio di assistenza remota

PA Digitale fornisce il servizio di assistenza remota attraverso uno specifico settore di Help Desk e mediante due modalità differenti:
1. collegamento da remoto mediante software di accesso a desktop remoto, incluso nel contratto di assistenza;
2. accesso da remoto, tramite l'utente "PAD_SUPPORT" (per il solo Urbi Smart), adottato solo a seguito di sottoscrizione da parte del cliente di una specifica autorizzazione formale.

9.1. Collegamento da remoto

Viene utilizzata questa modalità nei casi in cui l'Operatore di Help Desk, per erogare il supporto al cliente richiedente, non abbia la necessità di operare sul sistema del cliente ma solamente di guidare l'Utente e visualizzare le operazioni che quest'ultimo effettua sull'applicativo.
Il collegamento viene effettuato mediante un software di accesso a desktop remoto, leader di mercato, che garantisce la sicurezza degli utenti e delle connessioni mediante infrastruttura certificata ISO/IEC 27001 e interamente conforme alle norme HIPAA e SOC2:
- Crittografia AES a 256 bit
- Autenticazione a due fattori
- Protezione da forza bruta
- Lista bianca per utenti e IP
- Elenco dei dispositivi fidati
- Reset della password forzato.

9.2. Accesso mediante utente "PAD_SUPPORT"

A seguito dell'autorizzazione del cliente, predisposta su carta intestata, debitamente sottoscritta e trasmessa via PEC, PA Digitale crea uno specifico utente e provvede alla configurazione dell'ambiente di lavoro.
Per mezzo di questa modalità, abilitata di volta in volta dal Cliente in ciascuna richiesta di assistenza, gli Operatori di Help Desk possono accedere in autonomia al database del cliente tramite uno specifico utente di sistema creato ad hoc (PAD_SUPPORT), al fine effettuare la corretta diagnostica delle problematiche segnalate. Gli Operatori di Help Desk potranno quindi effettuare le operazioni correttive direttamente "sulle" soluzioni applicative in uso dal Cliente - risolvendo dove possibile direttamente le necessità segnalate, senza la necessità che una persona che presidi l'intervento.
Attraverso questa modalità si incrementa l'efficienza dei servizi di Assistenza, velocizzando i tempi di risposta e

procedendo in maniera più rapida alla risoluzione delle problematiche evidenziate, nel rispetto della trasparenza così come della normativa sulla privacy, attraverso una puntuale tracciatura delle attività effettuate dagli Operatori di Help Desk. Tutte le operazioni sono infatti tracciate in uno specifico log che, al termine dell'intervento, viene firmato digitalmente, allegato al ticket di assistenza e messo a disposizione del Cliente nel caso in cui lo richieda.
Nell'eventualità che, per una specifica richiesta d'assistenza, il Cliente non voglia permettere l'utilizzo di tale funzionalità, il richiedente medesimo dovrà disabilitare il check "Assistenza tramite Backdoor in fase di inserimento del ticket", che di base è sempre valorizzato.

10. Subappalto di servizi

Nei casi in cui PA Digitale abbia la necessità di subappaltare una componente e/o alcune attività previste dal servizio di utilizzo di Urbi Smart e/o WebTec, dopo aver verificato i requisiti di esperienza, di professionalità, di capacità e di affidabilità del fornitore, sottoscrive con quest'ultimo un contratto formale che contiene, oltre alle clausole contrattuali, il disciplinare tecnico che regolamenta la modalità di erogazione del servizio da prestare e le misure di sicurezza da adottare per garantire la sicurezza delle informazioni e di tutti i dati trattati (con particolare riguardo verso le Informazioni Personali Identificabili - PII).
Nel caso in cui il fornitore, per espletare il proprio servizio, non sia tenuto ad effettuare alcun trattamento di dati personali, tale divieto è espressamente indicato nel contratto di servizio. Nel caso in cui il fornitore debba effettuare un trattamento di dati personali, tale fornitore viene nominato Sub-Responsabile del trattamento dei dati in outsourcing, per ciascun servizio assegnato. Nella lettera di nomina sono riportate:

- le finalità del trattamento
- i dati da trattare
- la base giuridica
- la durata del trattamento
- le indicazioni nonché le specifiche istruzioni a cui attenersi affinché tutte le operazioni di trattamento informatico e manuale dei dati personali, nei limiti delle competenze e attribuzioni del fornitore, siano effettuate nel rispetto della normativa vigente e dei regolamenti aziendali in materia di tutela dei dati personali, prevedendo in particolare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo che il trattamento soddisfi i requisiti del Regolamento UE 2016/679 (art. 28 comma 4).

Non è previsto il subappalto di servizi per l'utilizzo di CDAN.

11. La restituzione dei dati a conclusione o revoca del contratto di Urbi Smart e WebTec

All'atto della conclusione e della revoca del contratto in essere, e a seguito del pagamento dell'eventuale debito in essere, PA Digitale in qualità di Responsabile esterno del trattamento:

- permetterà al Titolare del trattamento di prelevare dai sistemi elettronici di PA Digitale gli archivi informatici tramite apposita funzione;
- è tenuta a conservare nell'IDC (Internet Data Center) i dati del Cliente per un periodo non superiore a 90 (novanta) giorni dalla data di cessazione degli Ordinativi di fornitura, per qualsiasi causa essa intervenga. Decorso il suddetto termine, PA Digitale è autorizzata contrattualmente dal Cliente a cancellare fisicamente dall'IDC i dati e tutte le relative copie di salvataggio, con modalità di cancellazione sicura.

Tali misure si applicano ai Clienti che usufruiscano delle soluzioni Urbi Smart e WebTec in Cloud.

12. La restituzione dei dati a conclusione o revoca del contratto di Conservazione digitale dei documenti informatici

In caso di risoluzione del Contratto i documenti informatici originariamente versati dal Cliente nel sistema di Conservazione CDAN saranno a quest'ultimo restituiti nel loro formato originale, fatto salvo il caso che i suddetti documenti abbiano subito una conversione di formato per sopperire all'obsolescenza del formato originario; in quest'ultimo caso saranno restituiti nel formato convertito. Contestualmente, saranno restituiti anche i metadati associati ai documenti informatici originariamente forniti dal Cliente.
PA Digitale, in tutti i casi di risoluzione del Contratto, consentirà al Cliente di recuperare i propri documenti informatici, entro e non oltre 90 (novanta) giorni dalla cessazione del Contratto, dopo che questi avrà corrisposto a PA Digitale tutti gli importi contrattualmente dovuti. I documenti informatici dovranno essere prelevati dal Cliente secondo le modalità stabilite nel Manuale del sistema di Conservazione e dal Contratto - quindi non incombe su PA Digitale alcun obbligo di

provvedere alla materiale restituzione dei documenti informatici conservati. Decorso il suddetto termine, PA Digitale è autorizzata contrattualmente dal Cliente a cancellare dal proprio IDC i documenti informatici e gli annessi metadati di cui il Cliente è titolare (e tutte le relative copie di salvataggio), con modalità di cancellazione sicura.

Elenco delle trasmissioni telematiche

Documento n. 7

Per trasmissioni telematiche si intende: trasmissioni di documenti e dati effettuate con immissione diretta nel sistema dell'Ente destinatario, tramite accesso con autenticazione ad area riservata del sito web/portale dell'Ente.

Ente – soggetto - sistema	**Tipologia trasmissione**
Aran	Trasmissione contratto decentrato Trasmissione deleghe sindacali
AVPC - Autorità di vigilanza sui contratti pubblici di lavori servizi e forniture	Richiesta codice CIG (in forma ordinaria SIMOG e semplificata) Certificati di esecuzione lavori Sistema AVCPass
SICE	BILANCIO – ATTI
Corte dei Conti	Conto Consuntivo
Entratel	F24EP 770S e 770O Ricezione mod. 730/4 Comunicazione contratti non registrati non superiori ad € 10.000,00
Equitalia /	Provvedimenti scarico Ruoli
Guce / Simap	Pubblicazione atti, avvisi e concorsi
Inail	Denuncia annuale Denuncia Infortunio
Infocamere	Verifica autocertificazione imprese

Impresainungiorno.gov	Verifica documentazione impresa
Inps – Gestione ex Inpdap	Mutui – piccoli prestiti – cessioni stipendi Variazioni anagrafiche Cartolarizzazione crediti
INPS Inps – Gestione ex Inpdap	Assegni di maternità nucleo familiare Gestione Malattie UNIEMENS LISTA POSTA Assegno nucleo familiare e maternità
Istat	Statistiche demografiche
Me.Pa.	Acquisizione beni e servizi e verifica inadempienze
PERLAPA	GEDAP – Gestione distacchi e permessi sindacali e funzioni pubbliche elettive fruite dai dipendenti pubblici GEPAS – Gestione dichiarazioni di scioperi Rilevazione assenze retribuite del personale Permessi ex l.104/1992 Anagrafe delle prestazioni Monitoraggio lavoro flessibile
Ragioneria dello Stato	Monitoraggio trimestrale del personale Conto del personale e relazione allegata Rilevazione spesa sociale dei comuni Patto stabilità
SPORTELO UNICO PREVIDENZIALE	DURC
TESORERIA COMUNALE	Flussi stipendi Flussi mandati / reversali F24

Guida per l'attivazione del Registro di emergenza
art. 63 del DPR 445/2000

Documento n. 8

Per attivare il registro di protocollo di emergenza si devono verificare tre condizioni, non necessariamente dipendenti una dall'altra:

1) guasto al software di protocollazione informatica;
2) guasto al sistema informatico di gestione;
3) mancanza di energia elettrica.

Quando si verifica la condizione numero 1 si deve attivare un protocollo di emergenza su supporto informatico.
Quando si verificano le condizioni numeri 2 e 3 si deve attivare un protocollo di emergenza su supporto cartaceo.

Per l'attivazione del protocollo di emergenza si deve:

a) redigere il verbale di attivazione (documento n. 8.1)
b) compilare il registro di emergenza [su supporto informatico; manuale (documento n. 8.2)];
c) dare comunicazione alla struttura organizzativa dell'Amministrazione della attivazione dell'emergenza;
d) comunicare alla Soprintendenza archivistica l'attivazione del registro di emergenza.

Al termine dell'emergenza si deve:

a) revocare l'autorizzazione al protocollo di emergenza (documento n. 8.3)
b) inserire le registrazioni di emergenza nel protocollo informatico attivando l'apposita funzione, come previsto dal manuale operativo del sistema integrato all'applicativo
c) dare comunicazione alla struttura organizzativa dell'Amministrazione della revoca dell'emergenza;
d) conservare il registro di emergenza;
e) comunicare alla Soprintendenza archivistica il ripristino delle funzionalità del registro di protocollo informatico.

La numerazione del registro di emergenza è unica per l'intero anno. Ricomincia dal numero successivo all'ultimo generato per ogni attivazione.

Nel caso di attivazione del protocollo manuale (documento n. 8.2) si possono utilizzare fogli singoli con numerazione indicata nel margine destro, in modo che più operatori possano lavorare contemporaneamente. La numerazione indicata deve essere riportata per ogni documento registrato.

Autorizzazione allo svolgimento delle operazioni di registrazione di protocollo sul Registro di emergenza (art. 63 DPR 445/2000)

Documento 8.1

Ai sensi dell'art. 63 del DPR 28 dicembre 2000 n. 445 preso atto che, per le cause sotto riportate:

Data interruzione	
Ora interruzione	
Causa di interruzione	

non è possibile utilizzare la normale procedura informatica, si autorizza lo svolgimento delle operazioni di registrazione di protocollo sul Registro di emergenza.

Il Responsabile del Servizio archivistico per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi

Registro di protocollo di emergenza

Documento 8.2

Numero Registro emergenza	Data	Tipo	Mittente/Destinatrio	Oggetto	Classificazione	Fascicolo

Revoca autorizzazione allo svolgimento delle operazioni d registrazione di protocollo sul Registro di emergenza

Documento 8.3

Ai sensi dell'art. 63 del DPR. 28 dicembre 2000 n. 445, ricordato che, per le cause sotto riportate:

Data interruzione	
Ora interruzione	
Causa della interruzione	

non essendo possibile utilizzare la normale procedura informatica, è stato autorizzato lo svolgimento delle operazioni di registrazione di protocollo sul Registro di emergenza;

preso atto che, dalla data ed ora sotto riportate:

Data ripristino	
Ora ripristino	

è stato ripristinato il normale funzionamento della procedura informatica;

- si revoca l'autorizzazione allo svolgimento delle operazioni di registrazione di protocollo sul Registro di emergenza;
- si dispone il tempestivo inserimento delle informazioni relative ai documenti protocollati in emergenza nel sistema informatico, con automatica attribuzione della numerazione di protocollo ordinaria, mantenendo la correlazione con la numerazione utilizzata in emergenza.

Il Responsabile del Servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali
e degli archivi

Modelli per la riproduzione cartacea di documenti informatici

Documento n. 9

Nel caso della produzione di **copie cartacee conformi** di documenti informatici dovrà essere obbligatoriamente riportata l'indicazione:

Riproduzione cartacea del documento informatico sottoscritto digitalmente da <dati_firma> il <data_firma> ai sensi degli articoli 3 bis, 20, 21, e 23 del Dlgs.82/2005.

La presente copia, composta di n._____ pagine è conforme al documento originale informatico, memorizzato, conservato digitalmente e rintracciabile nel sistema informativo dell'Autorità di Bacino Distrettuale dell'Appennino Meridionale.

Il sottoscritto _____

Responsabile dell'Area _____

Data _____

Firma _____

Nel caso della produzione di **copie cartacee semplici** di documenti informatici dovrà essere obbligatoriamente riportata l'indicazione:

Riproduzione cartacea del documento informatico sottoscritto digitalmente da <dati_firma> il <data_firma> ai sensi degli articoli 3 bis, 20, 21, e 23 del Dlgs.82/2005, memorizzato, conservato digitalmente e rintracciabile nel sistema informativo dell'Autorità di Bacino Distrettuale dell'Appennino Meridionale.
F.to <dati_firma>
Firma autografa sostituita dall'indicazione del nome ai sensi dell'art. 3, c. 2, del Dlgs n.39/1993.

D. n. 18

Autorità di Bacino Distrettuale dell'Appennino Meridionale

Decreto del Segretario Generale n. 241 **del** 22 APR 2022

Oggetto: nomina del Responsabile della gestione documentale e del Responsabile della conservazione dei documenti informatici.

VISTO il D.lgs 82/2005 recante "*Codice dell'amministrazione digitale*" e ss.mm.ii;

VISTO il paragrafo 3.1.2 delle Linee Guida sulla formazione, gestione e conservazione dei documenti informatici adottate da AgID (Agenzia dell'Italia Digitale) con la determinazione n. 407/2020 e successivamente modificate con determinazione n. 371/2021 il quale prevede che *"Le Pubbliche Amministrazioni, nell'ambito del proprio ordinamento, provvedono a nominare, in ciascuna delle AOO, il responsabile della gestione documentale e un suo vicario, in possesso di idonee competenze giuridiche, informatiche ed archivistiche"*;

CONSIDERATO che questa Amministrazione individua una sola Area Organizzativa Omogenea (AOO) denominata Autorità di bacino distrettuale dell'Appennino Meridionale;

DATO ATTO che si rende necessario provvedere all'individuazione del Responsabile della GestioneDocumentale e del vicario;

DATO ATTO che il Responsabile della Gestione Documentale è preposto al Servizio per la gestioneinformatica dei documenti dei flussi documentali e degli archivi ed ha il compito di predisporre 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;

RITENUTO che il Responsabile della Gestione Documentale debba essere individuato all'interno dell'Ente a livello apicale;

VISTI, altresì, gli artt. 20, commi 3 e 5-bis, 23-ter, comma 4, 43, commi 1 e 3, 44, 44-bis e 71, comma 1, del D. Lgs. n. 82/2005 (Codice dell'Amministrazione Digitale) che disciplinano il sistema di conservazione dei documenti informatici;

ATTESO che l'art. 40, comma 1, capo III *"Formazione, gestione e conservazione dei documenti informatici"* del predetto Decreto così recita: *"Le Pubbliche Amministrazioni formano gli originali dei propri documenti con mezzi informatici secondo le disposizioni di cui al presente codice e le regole tecniche di cui all'articolo 71"*;

VISTO l'art. 44, comma 1-bis, del D. Lgs. n. 82/2005, secondo cui il sistema di conservazione dei documenti informatici è gestito da un Responsabile;

RICHIAMATO l'art. 43, comma 3, del medesimo Decreto;

DATO ATTO che si rende necessario provvedere ad individuare il Responsabile della conservazionedei documenti informatici;

RITENUTO che il Responsabile della conservazione dei documenti informatici debba essere individuato all'interno dell'Ente a livello apicale, potendo eventualmente avvalersi per quantoconcerne gli aspetti tecnico informatici, di un supporto esterno individuato tra i conservatori abilitati;

RITENUTO pertanto di nominare:

- quale responsabile della gestione documentale di questo Ente la dottoressa Antonietta Napolitano, dirigente del settore legislazione, contenzioso norme e direttive, alla quale è stato assegnato il Servizio per la tenuta del protocollo informatico e vicario il sig. Gennaro Carrino dipendente di questo ente, addetto al servizio di protocollo informatico;
- quale responsabile della conservazione dei documenti informatici di questo ente l'Ing. Filippo Pengue dirigente del settore compatibilità idrogeologica strutture ed infrastrutture e pianificazione sottordinata;

VISTI:

- il Codice dell'Amministrazione Digitale approvato con il D.v Lgs. n. 82/2005;
- le Linee Guida sulla formazione, gestione e conservazione dei documenti informatici adottateda AgID (Agenzia dell'Italia Digitale) con la determinazione n. 407/2020 e successivamentemodificate con determinazione n. 371/2021;
- il decreto del Segretario Generale n. 610 del 28 maggio 2021 con il quale è stato affidato a PA DIGITALE S.P.A. il servizio di transizione al digitale ivi compreso tra l'altro il servizio di conservazione digitale, la redazione del manuale di gestione, la redazione del manuale di conservazione etc;

DECRETA

1. **DI NOMINARE,** per le motivazioni espresse in premessa che qui si intendono richiamate:
   - Responsabile della Gestione Documentale di questa amministrazione la dottoressa Antonietta Napolitano, dirigente del settore legislazione, contenzioso norme e direttive, alla quale è stato assegnato il Servizio per la tenuta del protocollo informatico e di nominare Vicario il sig. Gennaro Carrino addetto al servizio per la tenuta del protocollo informatico;
   - Responsabile della conservazione dei documenti informatici l'Ing. Filippo Pengue dirigente del settore compatibilità idrogeologica strutture ed infrastrutture e pianificazione sottordinata;

2. **DI DARE ATTO** che è stato affidato a PA DIGITALE S.P.A. con decreto del S.G. n. 610 del 28.05.2021 l'incarico di conservazione digitale a norma.

3. Di pubblicare il presente decreto nella sezione Amministrazione Trasparente sottosezione *"provvedimenti"*.

Il Segretario Generale
Dott.ssa Geol. Vera Corbelli

Doc.11

Autorità di Bacino Distrettuale dell'Appennino Meridionale

Provincia di Caserta

Manuale di Conservazione

1 *Introduzione al documento*

1.1 Scopo e campo di applicazione del documento

Il presente documento è il Manuale di Conservazione come previsto dalle Linee Guida sulla formazione, gestione e conservazione dei documenti informatici di Agid in vigore dal 10 settembre 2020 (di seguito indicate come Linee Guida di Agid) e dal Codice dell'Amministrazione digitale DLgs 82/2005.

Come richiesto dalle Linee Guida di Agid, il presente documento "deve illustrare dettagliatamente l'Ente, i soggetti coinvolti e i ruoli svolti dagli stessi, il modello di funzionamento, la descrizione del processo, la descrizione delle architetture e delle infrastrutture utilizzate, le misure di sicurezza adottate e ogni altra informazione utile alla gestione e alla verifica del funzionamento, nel tempo, del sistema di conservazione".
In caso di ispezione da parte delle autorità di vigilanza preposte, il Manuale di Conservazione permette un agevole svolgimento di tutte le attività di controllo.
Il Manuale di Conservazione integra e dettaglia il Manuale del sistema di conservazione del conservatore esterno PA Digitale, documento di riferimento e disponibile nei siti:
https://www.padigitale.it/
https://www.agid.gov.it/it

Si rimanda al Manuale del sistema di conservazione di PA Digitale per indicazioni dettagliate circa:

- struttura organizzativa e ruoli di responsabilità del Conservatore
- formati e metadati associati agli oggetti conservati
- processo di conservazione e trattazione dei pacchetti di versamento, archiviazione e distribuzione
- dettaglio tecnico del sistema di conservazione
- monitoraggio e controlli effettuati dal Conservatore
- disposizioni in vigore nei luoghi dove sono conservati i documenti

Per quanto riguarda le tipologie degli oggetti sottoposti a conservazione, i rapporti con PA Digitale che realizza il processo di Conservazione, la sicurezza delle informazioni e il trattamento dei dati, il presente Manuale è integrato con i documenti:

- Specificità del Contratto, allegato tecnico parte integrante e sostanziale del contratto per l'affidamento del Servizio di Conservazione digitale di documenti informatici, che dettaglia le caratteristiche delle tipologie di documenti conservati
- Politica aziendale della sicurezza delle informazioni, che descrivere il Sistema di Gestione per la Sicurezza delle Informazioni (SGSI) di PA Digitale
- Politica in materia di trattamento e protezione dei dati personali
- Politica della qualità

I documenti sono disponibili sul sito:
https://www.padigitale.it/

1.2 Principi del Manuale

Il Manuale di Conservazione mira a:

- fornire una chiara presentazione del sistema di conservazione e dei processi erogati
- descrivere l'insieme delle fasi del processo
- includere le informazioni rilevanti, con un livello di dettaglio sufficiente ad agevolare le ispezioni, evitando informazioni tecniche articolate e non necessarie

Il Manuale di Conservazione è adottato dall'Ente con provvedimento formale ed è pubblicato sul sito istituzionale, nella Sezione Ente trasparente.

1.3 Normativa e standard di riferimento, terminologia

I principali riferimenti normativi relativi alla conservazione sono:

- Codice dell'Amministrazione digitale Dlgs 82/2005
- Linee Guida sulla formazione, gestione e conservazione dei documenti informatici di Agid, adottate con determinazione 407/2020 e in vigore dal 10 settembre 2020

Per ulteriori indicazioni e per quanto riguarda la terminologia (glossario e acronimi) e gli standard in uso si rimanda al Manuale del sistema di conservazione di PA Digitale.

2 *Modello organizzativo, ruoli e responsabilità*

2.1 Modello organizzativo

Il modello organizzativo adottato è in outsourcing: l'Ente affida il servizio di conservazione a conservatore esterno, ai sensi dall'art. 34, c. 1-bis del Codice dell'Ente digitale Dlgs 82/2005, fatte salve le competenze del Ministero della cultura, ai sensi del Codice dei beni culturali e del paesaggio DLgs 42/2004.

2.2 Ente, Titolare dell'oggetto della conservazione

L'Ente, Autorità di Bacino Distrettuale dell'Appennino Meridionale, è il Titolare dei documenti e dei fascicoli informatici posti in conservazione e, in relazione al modello organizzativo adottato, affida al Conservatore, PA Digitale, la gestione del servizio di conservazione secondo quanto previsto dalla normativa in materia e specificato nel contratto di servizio.

Ente: Autorità di Bacino Distrettuale dell'Appennino Meridionale
Sede: Viale Lincoln Ex Area Saint Gobain - CAP 81100 Caserta (CE)
Sito web: https://www.distrettoappenninomeridionale.it/
Codice Fiscale: 93109350616

2.3 Responsabile della conservazione

Il Responsabile della conservazione opera secondo quanto previsto dall'art. 44, c. 1-quater, del Codice dell'Amministrazione digitale Dlgs 82/2005.
Il Responsabile della conservazione:

- è un ruolo previsto dall'organigramma del Titolare dell'oggetto di conservazione
- è un dirigente o un funzionario interno formalmente designato e in possesso di idonee competenze giuridiche, informatiche e archivistiche

Il Responsabile della conservazione dell'Ente definisce e attua le politiche complessive del sistema di conservazione e ne governa la gestione con piena responsabilità e autonomia, in relazione al modello organizzativo adottato.
Il Responsabile della conservazione è persona fisica inserita stabilmente nell'organico dell'Ente titolare dell'oggetto della conservazione; la normativa gli attribuisce compiti riguardanti le funzioni, gli adempimenti, le attività e le responsabilità del processo di conservazione. L'obiettivo principale del Responsabile della conservazione è definire e impostare le modalità di trattamento della documentazione soggetta a conservazione.
Le Linee guida di Agid enfatizzano il ruolo del Responsabile della conservazione che diviene fondamentale all'interno del processo di conservazione, insieme ai suoi delegati o ai terzi affidatari.
Quando il servizio di conservazione è affidato a un Conservatore, le attività in capo al Responsabile della conservazione sono demandate, tutte o in parte, al responsabile del servizio di conservazione del Conservatore, rimanendo in ogni caso inteso che la responsabilità giuridica generale sui processi di conservazione, non essendo delegabile, rimane in capo al Responsabile della conservazione dell'Ente.
Il Responsabile della conservazione provvede a predisporre il manuale di conservazione e ne cura l'aggiornamento periodico in presenza di cambiamenti normativi, organizzativi, procedurali o tecnologici rilevanti.

Le attività attribuite dalle Linee guida di Agid al Responsabile della conservazione ed eventualmente affidate al Conservatore sono:

- definire le politiche di conservazione e i requisiti funzionali del sistema di conservazione, in conformità alla normativa vigente e tenuto conto degli standard internazionali, in ragione delle specificità degli oggetti digitali da conservare (documenti informatici e aggregazioni informatiche), della natura delle attività che il Titolare dell'oggetto di conservazione svolge e delle caratteristiche del sistema di gestione informatica dei documenti adottato
- gestire il processo di conservazione e garantire nel tempo la conformità alla normativa vigente
- generare e sottoscrivere il rapporto di versamento
- generare e sottoscrivere il pacchetto di distribuzione con firma digitale o firma elettronica qualificata
- effettuare il monitoraggio della corretta funzionalità del sistema di conservazione
- effettuare la verifica periodica, con cadenza non superiore ai cinque anni, dell'integrità e della leggibilità dei documenti informatici e delle aggregazioni documentarie degli archivi
- al fine di garantire la conservazione e l'accesso ai documenti informatici, adottare misure per rilevare tempestivamente l'eventuale degrado dei sistemi di memorizzazione e delle registrazioni e, ove necessario, per ripristinare la corretta funzionalità, adottare analoghe misure con riguardo all'obsolescenza dei formati

- provvedere alla duplicazione o copia dei documenti informatici in relazione all'evolversi del contesto tecnologico
- predisporre le misure necessarie per la sicurezza fisica e logica del sistema di conservazione
- assicurare la presenza di un pubblico ufficiale, nei casi in cui sia richiesto il suo intervento, garantendo allo stesso l'assistenza e le risorse necessarie per l'espletamento delle attività al medesimo attribuite
- assicurare agli organismi competenti previsti dalle norme vigenti l'assistenza e le risorse necessarie per l'espletamento delle attività di verifica e di vigilanza.

Responsabile della conservazione: Filippo Pengue
Ente: Autorità di Bacino Distrettuale dell'Appennino Meridionale
Decreto di nomina S.G. n. 249 del 22.04.2022

Il Responsabile della conservazione, sotto la propria responsabilità, può delegare lo svolgimento delle proprie attività o parte di esse a uno o più soggetti, all'interno dell'Ente.

2.4 Conservatore

Autorità di Bacino Distrettuale dell'Appennino Meridionale, avvalendosi di quanto previsto dal Codice dell'Amministrazione digitale DLgs 82/2005 e dalle Linee guida di Agid, ha affidato lo svolgimento delle attività di conservazione a PA Digitale che svolge tali attività tramite l'erogazione del servizio denominato CDAN Conservazione digitale a norma.

Denominazione sociale PA Digitale SpA
Sede legale Pieve Fissiraga (LO), via Leonardo da Vinci 13
Sedi operative Arezzo (AR), via Piero Gobetti 21/A; Roma (RM), via Filippo Caruso 23; Napoli (NA), via Giovanni Porzio 4 - Centro Direzionale Isola E3
Sito web https://www.padigitale.it/
E-mail amministrazione@padigitale.it
Pec protocollo.pec.padigitalespa@legalmail.it
Telefono 0371-5935460, 0371-5935780
Codice Fiscale / Partita IVA 06628860964
Numero REA 1464686

Gli obiettivi di PA Digitale tramite il servizio CDAN sono:

- garantire conservazione, archiviazione e gestione dei documenti informatici e dei fascicoli informatici
- erogare servizi di accesso basati sui contenuti digitali conservati
- fornire supporto, formazione e consulenza al Titolare dell'oggetto di conservazione per i processi di dematerializzazione

PA Digitale assume l'incarico di svolgere le attività affidate dal Responsabile della conservazione dell'Ente in accordo con quanto previsto dal contratto, dagli allegati tecnici contrattuali e dalle disposizioni delle Linee guida di Agid.
PA Digitale provvede ad attribuire lo svolgimento delle attività al responsabile del servizio della conservazione e a più persone, che per competenza ed esperienza, garantiscano la corretta esecuzione dei processi di conservazione definiti dalle norme, dal contratto e dal Manuale del sistema di conservazione. Per il dettaglio delle figure di responsabilità interne al Conservatore si rimanda al Manuale del sistema di conservazione di PA Digitale.
Gli estremi identificativi del responsabile del servizio di conservazione CDAN di PA Digitale (cognome, nome, codice fiscale) sono riportati anche nelle informazioni associate ai documenti conservati.
L'affidamento dello svolgimento delle attività del Responsabile della conservazione è stato conferito da Autorità di Bacino Distrettuale dell'Appennino Meridionale a PA Digitale alla sottoscrizione del contratto di adesione al servizio CDAN. La conservazione è svolta affidando a PA Digitale il ruolo e i compiti fissati nel documento di nomina a Responsabile del servizio di conservazione.

2.5 Produttore dei pacchetti di versamento

Il responsabile della gestione documentale svolge il ruolo di Produttore dei pacchetti di versamento e provvede a trasmettere i pacchetti al sistema di conservazione del Conservatore PA Digitale.
Per pacchetto di versamento si intende: insieme finito di più file (possibilmente organizzati in una struttura di sottoalbero all'interno di un filesystem) che costituiscono collettivamente oltre che individualmente un contenuto informativo unitario e auto-consistente e che viene inviato dal Produttore al sistema di conservazione.
Autorità di Bacino Distrettuale dell'Appennino Meridionale provvede a:

- generare e trasmettere al sistema di conservazione i pacchetti di versamento nelle modalità e con i formati concordati con il Conservatore e descritti nel Manuale del sistema di conservazione di PA Digitale
- verificare il buon esito della operazione di trasferimento al sistema di conservazione tramite la presa visione del rapporto di versamento prodotto dal sistema di conservazione stesso.

2.6 Utente

L'utente è il soggetto che può richiedere al sistema di conservazione l'accesso per acquisire le informazioni di interesse nei limiti previsti dalla legge. Tali informazioni vengono fornite dal sistema di conservazione secondo le modalità definite nel Manuale del sistema di conservazione di PA Digitale.
Il sistema di conservazione permette ai soggetti autorizzati l'accesso diretto, anche da remoto, ai documenti informatici conservati e consente la produzione di un pacchetto di distribuzione direttamente acquisibile dai soggetti autorizzati.
Per pacchetto di distribuzione si intende: insieme finito di più file (possibilmente organizzati in una struttura di sottoalbero all'interno di un filesystem) che costituiscono collettivamente oltre che individualmente un contenuto informativo unitario e auto-consistente e che è inviato dal sistema di conservazione all'Utente in risposta a una sua richiesta di accesso a oggetti di conservazione.
Il Responsabile della conservazione è identificato come Utente del Sistema di conservazione. L'Ente può definire nel ruolo di Utente ulteriori operatori a tal fine abilitati.
L'abilitazione e l'autenticazione degli utenti avviene in base alle procedure di gestione utenze indicate nel Piano della sicurezza del sistema di conservazione, e nel rispetto delle misure di sicurezza previste dal Codice in materia di protezione dei dati personali DLgs 196/2003 agg. 2018.

3 Formazione e gestione dei documenti e dei fascicoli informatici

3.1 Formazione e gestione dei documenti e dei fascicoli informatici da conservare

Autorità di Bacino Distrettuale dell'Appennino Meridionale forma e gestisce i documenti e i fascicoli informatici seguendo le disposizioni del Codice dell'Amministrazione digitale DLgs 82/2005 e delle Linee guida di Agid, utilizzando gli strumenti informatici a disposizione, inclusi gli applicativi URBI di PA Digitale direttamente interfacciati con il sistema di conservazione CDAN.

3.2 Controlli

Autorità di Bacino Distrettuale dell'Appennino Meridionale assicura che i documenti inviati in conservazione siano statici e non modificabili, in modo tale che il contenuto non possa essere alterabile durante le fasi di conservazione e accesso e sia quindi immutabile nel tempo.

3.3 Gestione delle anomalie

Il sistema di conservazione CDAN è configurato per accettare documenti in formati prestabiliti e con metadati definiti. Al venir meno di una di queste condizioni, sopraggiungendo l'impossibilità di accettare il documento, CDAN lascia in attesa il documento in entrata senza immetterlo nel sistema di conservazione e contestualmente segnala l'anomalia all'Ente.
Il trattamento delle anomalie avviene mediante l'utilizzo di un'interfaccia web disponibile e accessibile alle risorse preposte al monitoraggio degli invii in conservazione.

3.4 Formato dei documenti informatici

Autorità di Bacino Distrettuale dell'Appennino Meridionale utilizza per formare i documenti destinati alla conservazione i formati idonei per la conservazione a lungo termine (DPCM 3/12/2013 Regole tecniche per il protocollo informatico, Allegato 2 Formati sino al 1° gennaio 2022 e successivamente Linee guida di Agid, Allegato 2 Formati di file e riversamento) e definiti nel Manuale del sistema di conservazione di PA Digitale.

3.5 Metadati dei documenti informatici

Autorità di Bacino Distrettuale dell'Appennino Meridionale associa ai documenti i metadati previsti per il Documento amministrativo informatico (DPCM 3/12/2013 Regole tecniche per il protocollo informatico, Allegato 5 Metadati sino al 1° gennaio 2022 e successivamente Linee guida di Agid, Allegato 5 I metadati) e descritti nel Manuale del sistema di conservazione di PA Digitale.
Eventuali ulteriori metadati aggiuntivi, sono individuati e specificati nel documento Specificità del Contratto, allegato tecnico parte integrante e sostanziale del contratto per l'affidamento del Servizio di Conservazione digitale di documenti informatici, che dettaglia le caratteristiche delle tipologie di documenti conservati dall'Ente.

3.6 Metadati dei fascicoli informatici

Autorità di Bacino Distrettuale dell'Appennino Meridionale associa ai fascicoli i metadati previsti per le Aggregazioni documentali informatiche (DPCM 3/12/2013 Regole tecniche per il protocollo informatico, Allegato 5 Metadati sino al 1° gennaio 2022 e successivamente Linee guida di Agid, Allegato 5 I metadati) e descritti nel Manuale del sistema di conservazione di PA Digitale.

4 Sistema di conservazione

4.1 Descrizione generale del servizio di conservazione CDAN

Il servizio di conservazione CDAN permette di mantenere e garantire nel tempo le caratteristiche di autenticità, integrità, affidabilità, leggibilità, reperibilità e la validità legale dei documenti informatici, nel rispetto della normativa vigente.
Il servizio è erogato in modalità SaaS (Software as a Service) tramite interfaccia web disponibile e accessibile alle risorse preposte individuate dall'Ente.
CDAN integra i sistemi e gli strumenti di produzione e gestione documentale in uso presso l'Ente, intervenendo solamente nella fase di conservazione per i documenti e i fascicoli che l'Ente sceglie di conservare.
Gli applicativi URBI di PA Digitale per la produzione e gestione dei documenti e dei fascicoli informatici sono interfacciati con CDAN.
Il versamento in conservazione dei documenti e dei fascicoli informatici è effettuato unicamente dagli operatori abilitati dall'Ente, utilizzando la modalità messe a disposizioni da PA Digitale anche tramite gli applicativi URBI.

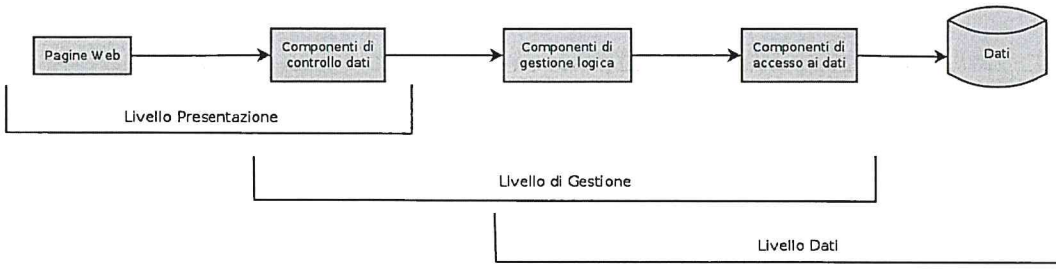
Il processo di conservazione si articola nelle seguenti fasi:

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 nel Manuale del sistema di conservazione, con i formati di conservazione e con le eventuali personalizzazioni specifiche realizzate per l'Ente
3. Preparazione del rapporto di conferma
4. Eventuale rifiuto del pacchetto di versamento, nel caso in cui le verifiche di cui alla fase 2 abbiano evidenziato anomalie e/o non conformità
5. Ricezione degli oggetti da conservare
6. Verifica degli oggetti da conservare
7. Generazione automatica del rapporto di versamento relativo a ciascun pacchetto di versamento, univocamente identificato dal sistema di conservazione e contenente un riferimento temporale, specificato con riferimento al Tempo Universale Coordinato (UTC), e una o più impronte, calcolate sull'intero contenuto del pacchetto di versamento
8. Sottoscrizione del rapporto di versamento con firma digitale apposta da PA Digitale
9. Preparazione e gestione del pacchetto di archiviazione
10. Sottoscrizione del pacchetto di archiviazione con firma digitale apposta da PA Digitale e apposizione di una validazione temporale con marca temporale alla relativa impronta (Chiusura del pacchetto di archiviazione)
11. Quando richiesto, preparazione e sottoscrizione con firma digitale di PA Digitale del pacchetto di distribuzione ai fini dell'esibizione richiesta dall'Utente
12. Quando richiesto, produzione di duplicati informatici effettuati su richiesta dell'Ente, in conformità a quanto previsto dalla normativa vigente
13. Quando richiesto, eventuale scarto del pacchetto di archiviazione dal sistema di conservazione

Per la descrizione dettagliata del servizio di conservazione CDAN si rimanda al Manuale del sistema di conservazione di PA Digitale.

4.2 Sistema di conservazione

La strutturazione logica dell'applicativo di conservazione realizzata e gestita da PA Digitale prevede la presenza di una architettura a tre livelli:



- il Livello di Presentazione costituisce l'interfaccia tramite la quale l'operatore dell'Ente o gli applicativi

URBI di PA Digitale sono in grado di interagire con il sistema di conservazione
- il Livello di Gestione si occupa di definire e gestire tutte le logiche di funzionamento del sistema
- il Livello Dati è invece responsabile dell'accesso fisico ai dati del sistema

Le componenti tecnologiche, ossia gli strumenti informatici a supporto delle funzionalità del sistema di conservazione, che implementano il sistema di conservazione, sono:
- client dell'operatore che utilizza il servizio di conservazione; è il componente primario ed essenziale per interagire con il sistema di conservazione e può essere rappresentato dal browser o dagli applicativi URBI di PA Digitale che si interfacciano per l'esecuzione delle operazioni automatizzate
- server web, server che si occupa della gestione degli accessi, del controllo del traffico, del filtraggio di eventuali richieste anomale, del controllo delle prestazioni, ecc.
- applicazione di conservazione e database, programma di conservazione digitale che viene eseguito su un apposito server applicativo
- database, server deputato alla memorizzazione di dati e informazioni
- fornitore di servizi di firma digitale, ente certificato con cui è stata effettuata l'integrazione al fine di ottenere la possibilità di apporre automaticamente le firme digitali
- fornitore di servizi di marca temporale, ente certificato con cui è stata effettuata l'integrazione al fine di ottenere la possibilità di apporre automaticamente le marche temporali
- gestore backup, sistema automatico di salvataggio periodico dei dati del sistema di conservazione al fine di garantire la salvaguardia delle informazioni
- gestore disaster recovery, sistema automatico di salvataggio periodico dei dati del sistema di conservazione in un sito differente da quello primario; questo permette di avere garanzie di integrità dei dati anche in caso di eventi catastrofici che investano il sito primario
- rete internet, rete che permette l'accesso al sistema di conservazione e che consente l'interconnessione tra loro delle diverse componenti.

Per la descrizione delle componenti fisiche e delle procedure di monitoraggio, controllo ed evoluzione del sistema di conservazione si rimanda al Manuale del sistema di conservazione di PA Digitale.

4.3 Procedure di ricerca ed esibizione dei documenti conservati

Le funzionalità messe a disposizione degli Utenti individuati dall'Ente consentono di richiedere in autonomia i pacchetti di distribuzione e di accedere ad apposite aree dell'applicazione web al fine di scaricare sulla propria postazione di lavoro i pacchetti messi a disposizione dal sistema.
Per pacchetto di distribuzione si intende: insieme finito di più file (possibilmente organizzati in una struttura di sottoalbero all'interno di un filesystem) che costituiscono collettivamente oltre che individualmente un contenuto informativo unitario e auto-consistente e che viene inviato dal sistema di conservazione all'utente in risposta ad una sua richiesta di accesso a oggetti di conservazione.
L'esibizione può avvenire mediante apposite funzionalità presenti all'interno degli applicativi software di PA Digitale:
- esibizione dal sistema di conservazione
- esibizione da URBI
- La produzione di duplicati informatici dei documenti conservati può avvenire a seguito di una richiesta proveniente dall'ambiente URBI oppure da una richiesta effettuata direttamente all'interno del sistema di conservazione.

Per la descrizione dettagliata delle modalità di esibizione ed esportazione di pacchetti di distribuzione si rimanda al Manuale del sistema di conservazione di PA Digitale.

4.4 Strategie adottate a garanzia della conservazione

Il Conservatore, PA Digitale, effettua il controllo di leggibilità, eseguito secondo le seguenti modalità:
- controllo di leggibilità, che consiste nel verificare che i singoli bit degli oggetti siano tutti correttamente leggibili, garanzia del buono stato del supporto di memorizzazione
- controllo di integrità, che consiste nel ricalcolare l'hash di ciascun oggetto e verificare che corrisponda all'hash memorizzato nel sistema, ragionevole certezza dell'integrità degli oggetti dato che la funzione di hash restituisce un valore differente anche a seguito della modifica di un solo bit dell'oggetto.

Per la descrizione dettagliata delle modalità di controllo di leggibilità si rimanda al Manuale del sistema di conservazione di PA Digitale.

5 Documenti conservati

5.1 Tipologie di documenti conservati

Autorità di Bacino Distrettuale dell'Appennino Meridionale concorda con PA Digitale le tipologie di documenti (classi documentali) da conservare.
Sono inclusi anche i fascicoli informatici, conservati come file in formato xml.
Le tipologie di documenti gestite dal sistema CDAN sono dettagliatamente descritte nel documento Specificità del Contratto, allegato tecnico parte integrante e sostanziale del contratto per l'affidamento del Servizio di Conservazione digitale di documenti informatici.
L'allegato tecnico per ciascuna tipologia di documento conservato definisce formati, metadati, sottoscrizione digitale, frequenza di versamento e software/altre informazioni per la visualizzazione dei documenti.

Autorità di Bacino Distrettuale dell'Appennino Meridionale conserva tramite il servizio CDAN le seguenti tipologie di documenti:

Tipo di documento	Data di attivazione	Formati ammessi
[DIGITALE]Conservazione per PEC	19-05-2022	PEC: .EML e .XML
[DIGITALE]Documento generico di protocollo	19-05-2022	Qualsiasi
[DIGITALE]Fattura elettronica attiva	19-05-2022	.XML (FE PA)
[DIGITALE]Fattura elettronica attiva B2B	19-05-2022	.XML (FE B2B)
[DIGITALE]Fattura elettronica passiva	19-05-2022	.XML (FE PA)
[DIGITALE]Fattura elettronica passiva B2B	19-05-2022	.XML (FE B2B)
[DIGITALE]Notifica SDI	19-05-2022	.XML (FE PA)
[DIGITALE]Notifica SDI B2B	19-05-2022	.XML (FE B2B)
[DIGITALE]PEC FAE	19-05-2022	PEC: .EML e .XML
[DIGITALE]PEC FAE B2B	19-05-2022	.EML e .XML
[DIGITALE]Registro giornaliero modifiche di protocollo	19-05-2022	.PDF (PDF/A)
[DIGITALE]Registro giornaliero protocollo	19-05-2022	.PDF (PDF/A)

Per la descrizione e le caratteristiche delle tipologie di documenti conservati nel sistema CDAN si rimanda al documento Specificità del Contratto e al Manuale del sistema di conservazione di PA Digitale.

6 Responsabilità del processo di conservazione

6.1 Modello di funzionamento

Il sistema di conservazione opera secondo i modelli organizzativi esplicitamente concordati dall'Ente con PA Digitale.

La conservazione non viene svolta all'interno della struttura organizzativa dell'Ente, titolare dei documenti e dei fascicoli informatici da conservare, ma è affidata a PA Digitale, che svolge le attività per le quali ha ricevuto formale affidamento, nei limiti delle stesse e per le quali opera in modo autonomo e ne è responsabile.

La sequenza di attività che vanno dalla fase propedeutica alla formazione dei documenti e dei fascicoli informatici alla fase di conservazione degli stessi è di seguito schematicamente rappresentata:

Fase	Descrizione e MACRO FASI del processo di conservazione	Attività a carico dell'Ente	Attività a carico di PA Digitale
Sistema di gestione documentale dell'Ente			
1	Produzione/formazione/emissione dei documenti e dei fascicoli informatici e contestuale generazione e associazione dei relativi metadati	X	
2	Produzione del pacchetto di versamento	X	
3	Deposito in conservazione del pacchetto di versamento e dei relativi documenti e fascicoli informatici completi dei relativi metadati L'Ente mantiene copia dei documenti inviati in conservazione almeno fino alla messa a disposizione da parte del sistema di conservazione del rapporto di versamento.	X	
Sistema di conservazione digitale dei documenti informatici			
4	Acquisizione da parte del sistema di conservazione del pacchetto di versamento prodotto dall'Ente per la sua presa in carico		X
5	Verifica che il pacchetto di versamento egli oggetti in esso descritti siano coerenti e conformi alle prescrizioni di cui al Manuale del sistema di conservazione e a eventuali personalizzazioni		X
6	Eventuale rifiuto del pacchetto di versamento, nel caso in cui le verifiche di cui alla fase 5 abbiano evidenziato delle anomalie		X
7	Generazione, anche in modo automatico, del rapporto di versamento relativo a ciascun pacchetto di versamento		X
8	Firma del rapporto di versamento e messa a disposizione dell'Ente		X
9	Recupero del rapporto di versamento firmato digitalmente	X	
10	Preparazione e gestione del pacchetto di archiviazione		X
11	"Chiusura" del pacchetto di archiviazione mediante sottoscrizione con firma digitale di PA Digitale e apposizione di marca temporale		X
12	Richieste di esibizione dei documenti informatici conservati	X	
13	Preparazione del pacchetto di distribuzione ai fini dell'esibizione richiesta dall'utente con tutti gli elementi necessari a garantire l'integrità e l'autenticità degli stessi		X
14	Richiesta dell'Ente di duplicati informatici	X	

Fase	Descrizione e MACRO FASI del processo di conservazione	Attività a carico dell'Ente	Attività a carico di PA Digitale
15	Produzione di duplicati informatici su richiesta dell'Ente		X
16	Eventuale chiusura del servizio di conservazione	X	X

Autorità di Bacino Distrettuale dell'Appennino Meridionale definisce con PA Digitale la configurazione del servizio CDAN in base alle specifiche esigenze, concordando le modalità di gestione e fruizione oltre alla quantità e tipologia di documenti da conservare.
Per la descrizione dettagliata del modello di funzionamento del servizio di conservazione CDAN e delle tipologie di compiti previsti si rimanda al Manuale del sistema di conservazione di PA Digitale.

7 Misure di sicurezza

7.1 Misure di sicurezza dell'Ente

Autorità di Bacino Distrettuale dell'Appennino Meridionale provvede alle misure di sicurezza nelle fasi di trattamento, formazione e gestione dei documenti e dei fascicoli informatici definiti come da conservare.
All'interfaccia web per la gestione dei documenti inviati in conservazione (dedicata alle operazioni di verifica stato dei documenti, esibizione, ecc.) accedono solo gli utenti individuati dall'Ente e che possiedono i privilegi di accesso.
L'Ente si assicura preventivamente all'invio in conservazione che i documenti siano privi di qualsiasi agente di alterazione, pertanto i documenti da conservare non devono contenere virus, macroistruzioni corrispondenti in comandi interni che, al verificarsi di determinati eventi, possono generare automaticamente modifiche o variazione dei dati contenuti nel documento, né codici eseguibili corrispondenti in istruzioni, non sempre visibili all'operatore, che consentono all'elaboratore di modificare il contenuto del documento informatico.
Il Conservatore declina ogni responsabilità nel caso non sia rispettata la reciproca salvaguardia.

7.2 Misure di sicurezza del sistema di conservazione

Il sistema CDAN è conforme ai requisiti di sicurezza prescritti dalla normativa.
Come previsto dalle norme vigenti in materia, PA Digitale adotta idonee e preventive misure di sicurezza al fine di ridurre al minimo i rischi di:

- distruzione o perdita, anche accidentale, dei documenti informatici
- danneggiamento delle risorse hardware su cui i documenti informatici sono registrati e dei locali ove i medesimi vengono custoditi
- accesso non autorizzato
- trattamenti non consentiti dalla legge o dai regolamenti aziendali

Le misure di sicurezza adottate assicurano:

- l'integrità dei documenti informatici, da intendersi come salvaguardia dell'esattezza dei dati, difesa da manomissioni o modifiche da parte di soggetti non autorizzati
- la disponibilità dei dati e dei documenti informatici da intendersi come la certezza che l'accesso sia sempre possibile quando necessario; indica quindi la garanzia di fruibilità dei documenti informatici, evitando la perdita o la riduzione dei dati anche accidentale utilizzando un sistema di backup
- la riservatezza dei documenti informatici da intendersi come garanzia che le informazioni siano accessibili solo da persone autorizzate e come protezione delle trasmissioni e controllo degli accessi stessi

Per la descrizione delle misure di sicurezza e delle infrastrutture si rimanda al Manuale del sistema di conservazione di PA Digitale e al documento Politica aziendale della sicurezza delle informazioni.

8 Trattamento dei dati personali

8.1 Misure per la protezione e il trattamento dei dati personali

Nelle fasi di creazione, digitalizzazione, trattamento e invio in conservazione dei documenti informatici, l'Ente pone massima cura nel rispetto delle disposizioni previste dal Codice in materia di protezione dei dati personali DLgs 196/2003 agg. 2018.

In materia di trattamento dei dati personali PA Digitale garantisce la tutela degli interessati in ottemperanza a quanto disposto dal Regolamento UE 2016/679, disciplinato in Italia dal DLgs 101/2018. In particolare, agli interessati sono fornite le informative di cui agli artt. 13 e 14 del richiamato provvedimento. Nella suddetta informativa l'Ente è informata sui diritti di accesso ai dati personali e altri diritti (art. 15 del Regolamento UE 2016/679).
La titolarità del trattamento di dati personali contenuti nei documenti oggetto di conservazione è in capo all'Ente, in quanto produttore e titolare dei documenti oggetto di conservazione.
PA Digitale è nominata quale "responsabile esterno" del trattamento dei dati personali necessari allo svolgimento del processo di conservazione. Pertanto PA Digitale si impegna, nel trattamento dei suddetti dati, ad attenersi alle istruzioni e a svolgere i compiti indicati dall'Ente.
Il Responsabile del trattamento dei dati personali all'interno di PA Digitale assume la responsabilità sulla garanzia del rispetto delle vigenti disposizioni in materia di trattamento dei dati personali e sulla garanzia che il trattamento dei dati affidati dall'Ente avvenga nel rispetto delle istruzioni impartite dal titolare del trattamento dei dati personali, con garanzia di sicurezza e di riservatezza.

PA Digitale nel ruolo di Conservatore tratta i dati personali con strumenti automatizzati per il tempo strettamente necessario a conseguire gli scopi per cui sono stati raccolti. Specifiche misure di sicurezza, come descritte nel Manuale del sistema di conservazione di PA Digitale, sono osservate per prevenire la perdita dei dati, usi illeciti o non corretti e accessi non autorizzati.
Le finalità del trattamento sono:

- Erogazione del servizio di conservazione digitale dei documenti informatici
  I dati raccolti sono utilizzati per l'attivazione del Servizio di conservazione CDAN. PA Digitale utilizza i dati raccolti per lo svolgimento dell'attività connessa e/o derivante dal Servizio di conservazione dei documenti informatici dell'Ente.
- Scopi di natura commerciale
  PA Digitale potrà utilizzare le coordinate di posta elettronica fornite dall'Ente per inviare comunicazioni relative a prodotti e/o servizi analoghi a quelli acquistati dall'Ente salva in ogni caso la possibilità dell'interessato di opporsi a tale trattamento.
- Altre forme di utilizzo dei dati
  Per motivi d'ordine pubblico, nel rispetto delle disposizioni di legge per la sicurezza e la difesa dello Stato, per la prevenzione, accertamento e/o repressione dei reati, i documenti informatici e i dati forniti a PA Digitale potranno essere comunicati a soggetti pubblici, quali forze dell'ordine, autorità pubbliche e autorità giudiziaria per lo svolgimento delle attività di loro competenza.

Per l'illustrazione dettagliata del trattamento dei dati personali effettuato da PA digitale si rimanda al documento Politica in materia di trattamento e protezione dei dati personali e al Manuale del sistema di conservazione di PA Digitale.