



F N O P O

Manuale sulla formazione, gestione e conservazione dei documenti informatici

Sommario

PRINCIPI GENERALI E DEFINIZIONI	5
Introduzione.....	5
Scopo e Ambito di applicazione	5
Normativa di riferimento	8
Norme abrogate	9
Glossario dei termini e acronimi	9
1 ASPETTI ORGANIZZATIVI DELL'ENTE.....	22
Art. 1 Area Organizzativa omogenea e sua organizzazione	23
Art. 2 Sistema del protocollo informatico	23
Art. 3 Flusso organizzativo dei documenti inviati	23
Art. 4 Unità organizzative responsabili di protocollazione	23
Art. 5 Flusso organizzativo dei documenti ricevuti.....	24
Art. 6 Compiti del responsabile della gestione documentale	25
Art. 7 Posta elettronica certificata	25
Art. 8 Firma digitale	25
Art. 9 Titolario e classificazione dei documenti	25
Art. 10 Tutela dei dati personali	26
2. FORMAZIONE DEI DOCUMENTI INFORMATICI	26
Art. 11 Documento informatico	26
Art. 12 Copia di documento informatico	27
Art. 13 Obiettivo del piano di sicurezza	28
Art. 14 Gestione dei documenti informatici.....	28
Art. 15 Classificazione del documento	29
Art. 16 Documento ricevuto	29
Art. 17 Documento inviato	29
Art. 18 Documento interno formale	30
Art. 19 Documento interno informale	30
3. PROTOCOLLO INFORMATICO E REGISTRAZIONI PARTICOLARI.....	30
Art. 20 Registrazione di protocollo dei documenti ricevuti e spediti	30
Art. 21 Registrazione dei documenti interni.....	30
Art. 22 Segnatura di protocollo.....	30
Art. 23 Requisiti di sicurezza del sistema di protocollo informatico.....	31
Art. 24 Annullamento delle registrazioni di protocollo	31
Art. 25 Differimento dei termini di protocollazione	31

Art. 26 Registro giornaliero di protocollo	32
Art. 27 Registro di emergenza.....	32
Art. 28 Registri e repertori informatici	32
4. CASI PARTICOLARI DI REGISTRAZIONI DI PROTOCOLLO	32
Art. 29 Circolari e disposizioni generali	32
Art. 30 Documenti cartacei in partenza con più destinatari	33
Art. 31 Documenti cartacei ricevuti a mezzo telegramma.....	33
Art. 32 Documenti cartacei ricevuti a mezzo telefax	33
Art. 33 Domande di partecipazione a concorsi, avvisi, selezioni, corsi e borse di studio	33
Art. 34 Documenti non firmati	34
Art. 35 Documenti non soggetti a registrazione di protocollo	34
Art. 36 Protocollazione dei messaggi di posta elettronica convenzionale	34
Art. 37 Protocollazione di documenti digitali pervenuti erroneamente	34
Art. 38 Ricezione di documenti cartacei pervenuti erroneamente	34
Art. 39 Copie per conoscenza	35
Art. 40 Differimento delle registrazioni	35
Art. 41 Registrazioni con differimento dei termini di accesso.....	35
Art. 42 Corrispondenza personale o riservata	35
Art. 43 Documenti soggetti a scansione	36
Art. 44 Processo di scansione	36
5. PIANO DI CLASSIFICAZIONE DOCUMENTALE E SELEZIONE.....	37
Art. 45 Classificazione	37
Art. 46 Titolario o piano di classificazione	37
Art. 47 Modifica del Piano di classificazione	37
6. FORMAZIONE AGGREGAZIONI DOCUMENTALI.....	38
Art. 48 Aggregazioni documentali informatiche.....	38
Art. 49 Fascicolo informatico	38
Art. 50 Creazione del fascicolo informatico	38
Art. 51 Organizzazione dei documenti	38
Art. 52 Archivio informatico.....	39
7. FLUSSI DI LAVORAZIONE DOCUMENTALI INTERNI	40
Art. 53 Documenti in arrivo	40
Art. 54 Ricezione dei documenti su supporto cartaceo	40
Art. 55 Ricezione di documenti informatici sulla casella di posta istituzionale	40
Art. 56 Ricezione di documenti informatici sulla casella di posta elettronica non istituzionale.....	40
Art. 57 Ricezione di documenti informatici su supporti rimovibili	40

Art. 58 Attività di protocollazione dei documenti	40
Art. 59 Classificazione dei documenti	41
Art. 60 Assegnazione dei documenti ricevuti da vedere	41
Art. 61 Smistamento dei documenti protocollati	41
Art. 62 Documenti inviati dall'AOO	41
Art. 63 Modalità di invio dei documenti	41
Art. 64 Registrazione di protocollo e segnatura	41
Art. 65 Trasmissione di documenti informatici	41
Art. 66 Trasmissione di documenti cartacei a mezzo posta	42
Art. 67 Documenti in partenza per posta convenzionale con più destinatari	42
8. MISURE DI SICUREZZA E PROTEZIONE DEI DATI	43
Art. 68 Sicurezza	43
Art. 69 Obiettivi	43
Art. 70 Sicurezza nella formazione dei documenti	45
Art. 71 Trasmissione ed interscambio dei documenti informatici	45
Art. 72 Accesso ai documenti informatici	46
9. NORME TRANSITORIE E FINALI	46
Art. 73 Pubblicità del manuale	46
10. ALLEGATI	46
Allegato n. 1 Titolario piano di classificazione	46
Allegato n. 2 Manuale d'uso protocollo informatico	46

PRINCIPI GENERALI E DEFINIZIONI

Introduzione

Il “Manuale di formazione, gestione e conservazione dei documenti informatici” obbligatorio secondo le disposizioni delle linee Guida emanate dall’AGID, in vigore dal 01 gennaio 2022, è articolato in un file iniziale che costituisce il “Manuale di Gestione documentale” e da una serie di allegati tra i quali il “Manuale di conservazione”.

La struttura risponde ai seguenti obiettivi:

1. procedere, secondo quanto stabilito al paragrafo 1.11 delle linee guida AGID all’adozione del **manuale di gestione documentale** e del **manuale di conservazione** che rappresenta un preciso obbligo come specificato ai paragrafi 3.5 e 4.6, al quale, per la PA, fa seguito l’ulteriore obbligo della loro pubblicazione sul sito istituzionale dell’ente.
2. garantire un adattamento costante ai cambiamenti imposti dall’incessante rivoluzione digitale. Di qui la scelta di prevedere un testo “statico” che contenga la base normativa della materia e una serie di “allegati” i cui contenuti più “flessibili” potranno adeguarsi agevolmente all’evoluzione tecnologica.
3. dare maggiore autonomia di consultazione e, ove necessario, di approfondimento, di spedizione ai collaboratori interni ed esterni, nonché ai fornitori di servizi coinvolti nelle procedure di conservazione (Es. Conservatore esterno, ecc.).

La struttura finale risponderà ai seguenti titoli:

- MANUALE FORMAZIONE, GESTIONE E CONSERVAZIONE DOCUMENTI
INFORMATICI

Allegato 1 Titolario piano di classificazione

Allegato 2 Manuale d’uso del Protocollo Informatico Tinexta Visura

Scopo e Ambito di applicazione

Il presente documento costituisce il Manuale del sistema di formazione, gestione e conservazione dei documenti informatici del FNOPO

Denominazione:	FNOPO
Sede legale	Piazza Tarquinia 5/D - Roma (RM)
Legale rappresentante:	Vaccari Silvia
Codice Fiscale	80181890585
Partita IVA	80181890585
Telefono:	067000943
Sito web principale:	www.fnopo.it

In conformità con la normativa vigente dal 01 gennaio 2022, il presente “**Manuale di formazione, gestione e conservazione dei documenti informatici**”, di seguito anche solo “**Manuale**”,

costituisce il riferimento unico che raccoglie in un **manuale aggregato** la formazione e la gestione dei documenti, del protocollo informatico, dei flussi documentali, dell'archivio, della conservazione del FNOPO.

Il Manuale è uno strumento di lavoro rivolto agli operatori di protocollo e di conservazione, ai responsabili dei procedimenti amministrativi, ai prestatori di servizi esterni in quanto costituisce uno strumento che disciplina e rappresenta tutte le fasi della formazione, gestione, tenuta e conservazione del documento informatico, dal momento della sua acquisizione o formazione al completamento del suo iter procedurale fino alla sua selezione per lo scarto o la conservazione permanente.

Il Manuale, pertanto, fornisce tutte le indicazioni per il corretto funzionamento del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e dell'archivio. Nel presente manuale e nei suoi allegati saranno riportati tutti i soggetti attivabili nelle funzioni di formazione, gestione e conservazione dei documenti con le relative qualifiche.

Considerando la dimensione dell'ente, alcune mansioni e qualifiche saranno cumulate in un numero ristretto di soggetti, fermo restando l'assolvimento di tutti i compiti previsti dalla normativa vigente e la possibilità di procedere successivamente a ulteriori nomine.

Considerata la velocità dell'innovazione tecnologica in costante cambiamento, il Manuale mantiene una funzione statica e descrittiva dei procedimenti gestionali del documento informatico su base normativa della materia mentre gli allegati riportano contenuti *“flessibili che potranno adeguarsi all'evoluzione tecnologica”*. Tale processo di costante adeguamento degli <allegati> è realizzato in coerenza con il quadro normativo e attuativo in materia di digitalizzazione”.

In conformità con quanto previsto dal **paragrafo 3.5 delle Linee Guida emanate da AGID**, vengono di seguito riportati i seguenti principi generali da applicare.

1. gli aspetti organizzativi:

a) le modalità di utilizzo degli strumenti informatici per la formazione dei documenti informatici e per lo scambio degli stessi all'interno ed all'esterno dell'AOO, applicando le modalità di trasmissione indicate nell'allegato 6 “Comunicazione tra AOO di Documenti Amministrativi Protocollati”;

b) l'indicazione delle unità organizzative responsabili (UOR) delle attività di registrazione di protocollo, di archiviazione dei documenti all'interno dell'AOO;

c) l'indicazione delle regole di assegnazione dei documenti ricevuti con la specifica dei criteri per l'ulteriore eventuale inoltro dei documenti verso aree organizzative omogenee della stessa amministrazione o verso altre amministrazioni;

d) i criteri e le modalità per il rilascio delle abilitazioni di accesso, interno ed esterno all'Amministrazione, al sistema di gestione informatica dei documenti;

2. i formati dei documenti:

a) l'individuazione dei formati utilizzati per la formazione del documento informatico introdotti dalla Linee Guida tra quelli indicati nell'Allegato 2 “Formati di file e riversamento”;

b) la descrizione di eventuali ulteriori formati utilizzati per la formazione di documenti in relazione a specifici contesti operativi che non sono individuati nell'Allegato 2 “Formati di file e riversamento” delle Linee Guida;

c) le procedure per la valutazione periodica di interoperabilità dei formati e per le procedure di riversamento previste nell'Allegato 2 "Formati di file e riversamento" delle Linee Guida;

3. il protocollo informatico e le registrazioni particolari:

a) le modalità di registrazione delle informazioni annullate o modificate nell'ambito delle attività di registrazione;

b) la descrizione completa e puntuale delle modalità di utilizzo della componente «sistema di protocollo informatico» del sistema di gestione informatica dei documenti;

c) le modalità di utilizzo del registro di emergenza ai sensi dell'art. 63 del TUDA, inclusa la funzione di recupero dei dati protocollati manualmente;

d) l'elenco dei documenti esclusi dalla registrazione di protocollo, per cui è prevista registrazione particolare ai sensi dell'art. 53, comma 5, del TUDA;

e) determinazione dei metadati da associare ai documenti soggetti a registrazione particolare individuati, assicurando almeno quelli obbligatori previsti per il documento informatico dall'Allegato 5 "I Metadati" delle Linee Guida;

f) i registri particolari individuati per la gestione del trattamento delle registrazioni particolari informatiche anche associati ad aree organizzative omogenee definite dall'amministrazione sull'intera struttura organizzativa e gli albi, gli elenchi e ogni raccolta di dati concernente stati, qualità personali e fatti, riconosciuti da una norma;

4. le azioni di classificazione e selezione:

a) il piano di classificazione adottato dall'Amministrazione, con l'indicazione delle modalità di aggiornamento, integrato con le informazioni relative ai tempi, ai criteri e alle regole di selezione e conservazione, con riferimento alle procedure di scarto;

5. la formazione delle aggregazioni documentali

a) le modalità di formazione, gestione e archiviazione dei fascicoli informatici e delle aggregazioni documentali informatiche con l'insieme minimo dei metadati ad essi associati;

6. i flussi di lavorazione dei documenti in uso:

a) la descrizione dei flussi di lavorazione interni all'Amministrazione, anche mediante la rappresentazione formale dei processi attraverso l'uso dei linguaggi indicati da AgID, applicati per la gestione dei documenti ricevuti, inviati o ad uso interno;

7. le misure di sicurezza e protezione dei dati personali adottate:

a) le opportune misure tecniche e organizzative per garantire un livello di sicurezza adeguato al rischio anche in materia di protezione dei dati personali;

8. la conservazione:

a) il piano di conservazione per le Pubbliche Amministrazioni è allegato al manuale di gestione documentale, con l'indicazione dei tempi entro i quali le diverse tipologie di oggetti digitali devono essere trasferite in conservazione ed eventualmente scartate.

Normativa di riferimento

Ai fini del presente manuale si fa riferimento alle seguenti normative:

- Legge 241/1990, *Nuove norme sul procedimento amministrativo*;
- TUDA - DPR 445/2000, *Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa*;
- DPR 37/2001, *Regolamento di semplificazione dei procedimenti di costituzione e rinnovo delle Commissioni di sorveglianza sugli archivi e per lo scarto dei documenti degli uffici dello Stato*;
- D.lgs 196/2003 recante il *Codice in materia di protezione dei dati personali*;
- D.lgs 42/2004, *Codice dei beni culturali e del paesaggio, ai sensi dell'articolo 10 della legge 6 luglio 2002, n. 137*;
- Legge 9 gennaio 2004, n. 4 aggiornata dal decreto legislativo 10 agosto 2018, n. 106, *Disposizioni per favorire e semplificare l'accesso degli utenti e, in particolare, delle persone con disabilità agli strumenti informatici*;
- D.lgs 82/2005 e ss.mm.ii., *Codice dell'amministrazione digitale*;
- D.lgs. 33/2013, *Riordino della disciplina riguardante il diritto di accesso civico e gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni*;
- DPCM 22 febbraio 2013, *Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali, ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma 3, lettera b), 35, comma 2, 36, comma 2, e 71*;
- DPCM 21 marzo 2013, *Individuazione di particolari tipologie di documenti analogici originali unici per le quali, in ragione di esigenze di natura pubblicistica, permane l'obbligo della conservazione dell'originale analogico oppure, in caso di conservazione sostitutiva, la loro conformità all'originale deve essere autenticata da un notaio o da altro pubblico ufficiale a ciò autorizzato con dichiarazione da questi firmata digitalmente ed allegata al documento informatico, ai sensi dell'art. 22, comma 5, del Codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82 e successive modificazioni*;
 - Reg. UE 910/2014, *in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE - Regolamento eIDAS*;
 - Circolare 40 e 41 del 14 dicembre 2015 della Direzione generale degli archivi, *Autorizzazione alla distruzione di originali analogici riprodotti secondo le regole tecniche di cui al DPCM 13.11.2014 e conservati secondo le regole tecniche di cui al DPCM 13.12.2013*;
 - Reg. UE 679/2016 (GDPR), *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*;
 - Circolare 18 aprile 2017, n. 2/2017 dell'Agenzia per l'Italia Digitale, *recante le misure minime di sicurezza ICT per le pubbliche amministrazioni*;
 - Circolare n. 2 del 9 aprile 2018, *recante i criteri per la qualificazione dei Cloud Service Provider per la PA*;
 - Circolare n. 3 del 9 aprile 2018, *recante i criteri per la qualificazione di servizi SaaS per il Cloud della PA*;
 - Reg. UE 2018/1807, *relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea*;
 - DPCM 19 giugno 2019, n. 76, *Regolamento di organizzazione del Ministero per i beni e le attività culturali, degli uffici di diretta collaborazione del Ministro e dell'Organismo indipendente di valutazione della performance*.
- **LINEE GUIDA Sulla formazione, gestione e conservazione dei documenti informatici**, emanate da AGID il 10 settembre 2020 e successive modifiche e integrazioni.

Leggi abrogate dalla data di applicazione delle Linee Guida emanate da AGID:

- il DPCM 13 novembre 2014, contenente “Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici”;

- il DPCM 3 dicembre 2013, contenente “Regole tecniche in materia di sistema di conservazione”.
- Per quanto concerne il DPCM 3 dicembre 2013, contenente “Regole tecniche per il protocollo informatico”, a partire dalla data di applicazione delle Linee guida sono abrogate tutte le disposizioni fatte salve le seguenti:
 - art. 2 comma 1, *Oggetto e ambito di applicazione*;
 - art. 6, *Funzionalità*;
 - art. 9, *Formato della segnatura di protocollo*;
 - art. 18 commi 1 e 5, *Modalità di registrazione dei documenti informatici*;
 - art. 20, *Segnatura di protocollo dei documenti trasmessi*;
 - art. 21, *Informazioni da includere nella segnatura*.

Sempre a far data dalla data di applicazione delle Linee guida, la **circolare n. 60 del 23 gennaio 2013** dell’AgID in materia di “Formato e definizione dei tipi di informazioni minime ed accessorie associate ai messaggi scambiati tra le Pubbliche Amministrazioni” è abrogata e sostituita dall’allegato 6 “Comunicazione tra AOO di documenti amministrativi protocollati” delle Linee Guida.

Norme abrogate

A partire dalla data di applicazione delle Linee Guida Agid, sono abrogati:

- il DPCM 13 novembre 2014, contenente “Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici”;
- il DPCM 3 dicembre 2013, contenente “Regole tecniche in materia di sistema di conservazione”.

Per quanto concerne il DPCM 3 dicembre 2013, contenente “Regole tecniche per il protocollo informatico”, a partire dalla data di applicazione delle Linee guida sono abrogate tutte le disposizioni fatte salve le seguenti:

- art. 2 comma 1, *Oggetto e ambito di applicazione*;
- art. 6, *Funzionalità*; • art. 9, *Formato della segnatura di protocollo*;
- art. 18 commi 1 e 5, *Modalità di registrazione dei documenti informatici*;
- art. 20, *Segnatura di protocollo dei documenti trasmessi*;
- art. 21, *Informazioni da includere nella segnatura*.

Sempre a far data dalla data di applicazione delle Linee guida, la circolare n. 60 del 23 gennaio 2013 dell’AgID in materia di “Formato e definizione dei tipi di informazioni minime ed accessorie associate ai messaggi scambiati tra le Pubbliche Amministrazioni” è abrogata e sostituita dall’allegato 6 delle Linee Guida “Comunicazione tra AOO di documenti amministrativi protocollati”.

Glossario dei termini e acronimi

Ai fini del presente Manuale si intende:

- per Ente: FNOPO
- per AOO: Area Organizzativa Omogenea

Di seguito i termini e gli acronimi utilizzati nella guida.

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.
AgID	Agenzia per l'Italia Digitale
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 - AOO	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 <i>wrapper</i> (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.
<i>Digest</i>	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.
<i>eSeal</i>	Vedi sigillo elettronico.
Esibizione	operazione che consente di visualizzare un documento conservato
<i>eSignature</i>	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 <i>bit</i> 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.
<i>File container</i>	Vedi Formato contenitore.
<i>File wrapper</i>	Vedi Formato contenitore.
File-manifesto	File che contiene metadati riferiti ad un file o ad un pacchetto di file.
<i>Filesystem</i>	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 <i>wrapping</i>), 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 <i>hash</i> crittografica	Funzione matematica che genera, a partire da una evidenza informatica, una impronta crittografica o <i>digest</i> (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.
<i>hash</i>	Termine inglese usato, impropriamente, come sinonimo d'uso di "impronta crittografica" o " <i>digest</i> " (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 <i>hash</i> 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 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.
<i>Naming convention</i>	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 (<i>file package</i>)	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.
<i>Path</i>	Percorso (<i>vedi</i>).
<i>Pathname</i>	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.
<i>qSeal</i>	Sigillo elettronico qualificato, come da art. 35 del Regolamento eIDAS.
<i>qSignature</i>	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	<i>electronic IDentification Authentication and Signature</i> , 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.

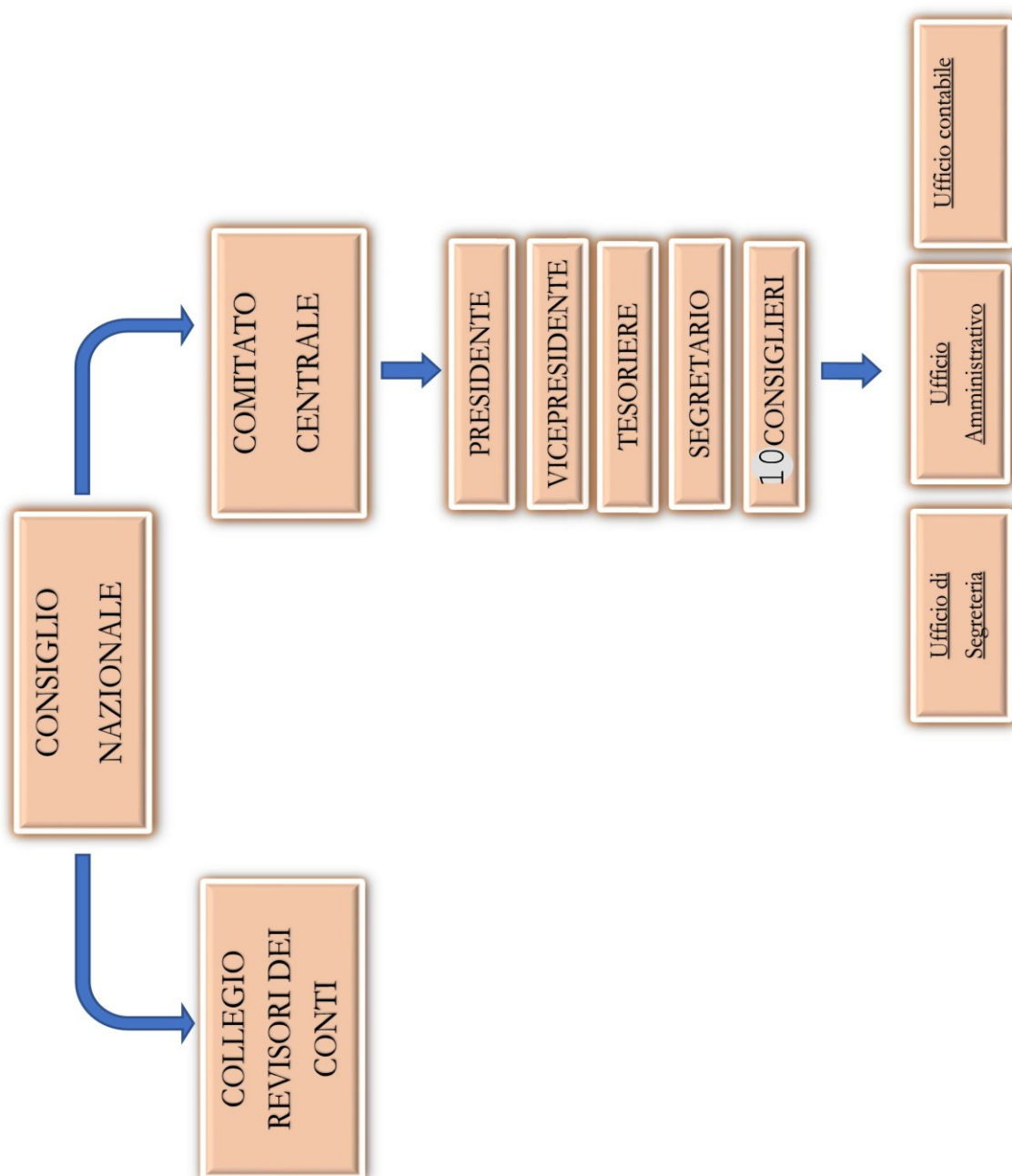
TERMINE	DEFINIZIONE
Responsabile della protezione dei dati	Persona con conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, in grado di assolvere i compiti di cui all'articolo 39 del Regolamento (UE) 2016/679.
Responsabile della sicurezza dei sistemi di conservazione	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 (<i>vedi</i>).
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
<i>Timeline</i>	Linea temporale virtuale su cui sono disposti degli eventi relativi ad un sistema informativo o a un documento informatico. Costituiscono esempi molto diversi di <i>timeline</i> 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.

Glossario degli Acronimi

ACRONIMO	DEFINIZIONE
AGID	Agenzia per l'Italia digitale
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 (<i>"General Data Protection Regulation"</i>), 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

1 ASPETTI ORGANIZZATIVI DELL'ENTE



Art. 1 Area Organizzativa omogenea e sua organizzazione

L'Amministrazione del FNOPO (Federazione Nazionale Ordini della Professione di Ostetrica) ha identificato l'Area Organizzativa Omogenea denominata:

- FNOPO Codice AOO: **A54908C**
- che è composta da n. 2 Unità Organizzative:
- **Ufficio per la transizione al digitale**
Codice Univoco: ADZJSP
- **Ufficio Fattura PA**
Codice Univoco: UF0B5V

All'interno dell'AOO il sistema di protocollazione è unico.

Il codice identificativo è il seguente: **A54908C**

così come viene indicato nell'Indice delle Pubbliche Amministrazioni (IPA)

il domicilio digitale è il seguente:

presidenza@pec.fnopo.it

Art. 2 Sistema del protocollo informatico

L'attività di protocollazione è quella fase del processo amministrativo che certifica provenienza e data di acquisizione del documento identificandolo in maniera univoca per mezzo dell'apposizione di informazioni numeriche e temporali. Il FNOPO gestisce con il sistema di protocollazione informatica, conforme alle Regole Tecniche degli artt. 40 bis, 41, 47, 57 bis e 71 del Codice dell'Amministrazione Digitale e del *TUDA*, tutti i documenti in partenza e in arrivo dell'Ente. Il registro di protocollo viene generato automaticamente dal sistema di protocollo che assegna a ciascun documento in entrata e in uscita il numero di protocollazione e la data. Il software applicativo del protocollo informatico utilizzato dall'Ente è descritto nell'apposito manuale d'uso.

Art. 3 Flusso organizzativo dei documenti inviati

Ad ogni documento spedito dall'AOO corrisponde un'unica operazione di registrazione di protocollo. I documenti informatici in uscita vengono redatti con mezzi informatici a norma di legge e sono convertiti prima della loro sottoscrizione con firma digitale in formati idonei che ne diano la garanzia di leggibilità per altri sistemi, la inalterabilità durante le fasi accesso e conservazione e l'immutabilità nel tempo. Il documento informatico principale così predisposto con eventuali allegati viene protocollato e inserito nel sistema documentale dell'Ente.

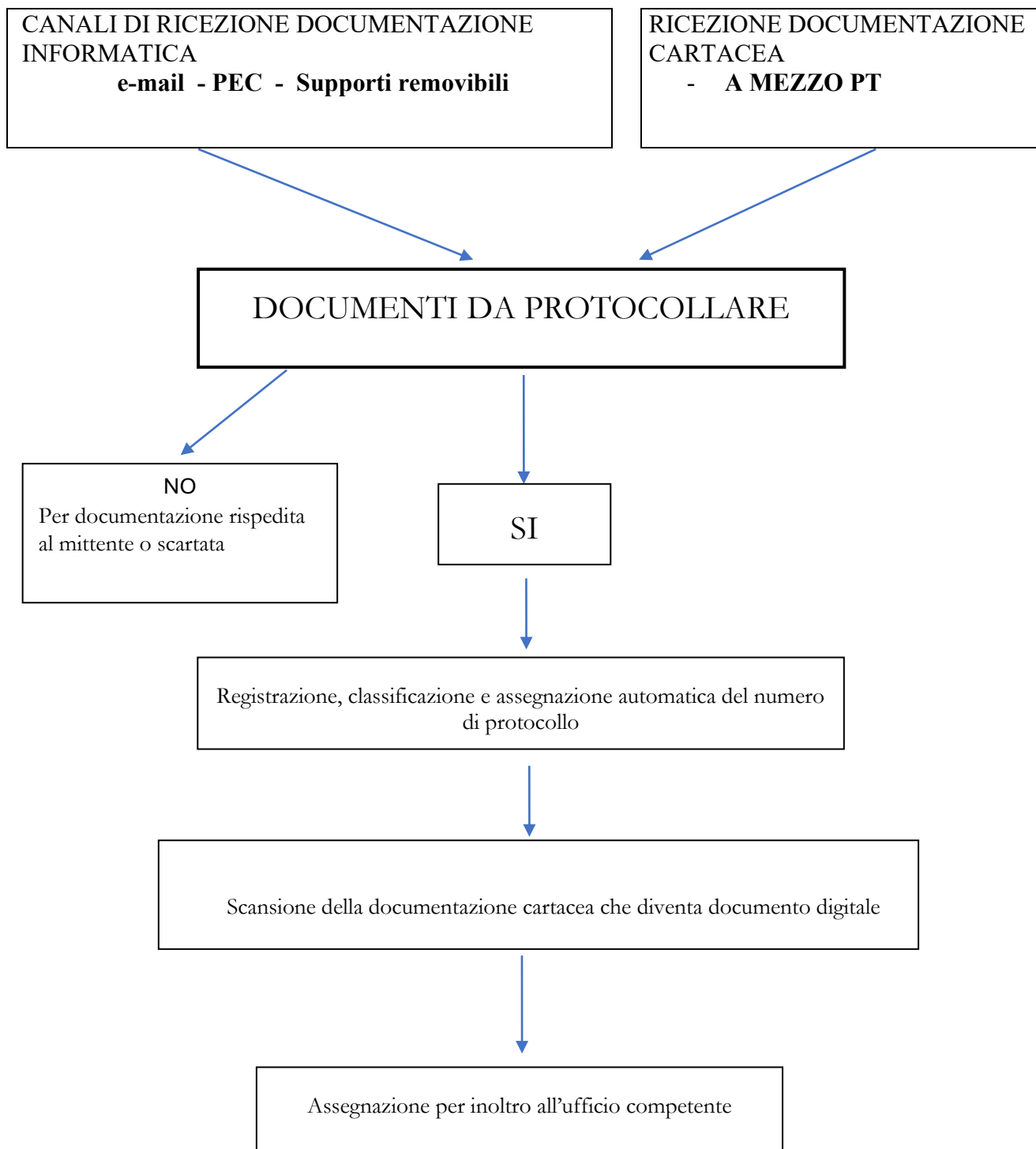
Art. 4 Unità organizzative responsabili di protocollazione

L'Ente non utilizza uffici UOP che svolgono attività di registrazione di protocollo.

Ai sensi della normativa vigente, con atto deliberativo l'Ente provvede alla nomina il responsabile del servizio di protocollo informatico, della gestione dei flussi documentali e degli archivi (RSP).

Art. 5 Flusso organizzativo dei documenti ricevuti

Viene schematizzato il flusso dei documenti ricevuti dalla AOO.



Art. 6 Compiti del responsabile della gestione documentale

È compito del responsabile del servizio protocollo:

- garantire il rispetto delle disposizioni normative durante le operazioni di registrazione e di segnatura di protocollo informatico;
- attribuire il livello di autorizzazione in riferimento alle procedure per l'accesso al sistema in riferimento alla consultazione oppure all'inserimento e alla modifica delle informazioni;
- garantire la corretta produzione e conservazione del registro giornaliero di protocollo;
- garantire la leggibilità nel tempo di tutti i documenti trasmessi o ricevuti dall'Area Organizzativa Omogenea - AOO, attraverso l'adozione dei formati standard previsti dalla normativa vigente;
- curare le funzionalità del sistema affinché, in caso di guasti o anomalie, siano ripristinate entro ventiquattro ore dal blocco delle attività e, comunque, nel più breve tempo possibile;
- autorizzare con appositi provvedimenti le operazioni di annullamento o di modifica della registrazione di protocollo;
- aprire e chiudere il registro di protocollazione di emergenza;
- vigilare sull'osservanza delle disposizioni del presente manuale da parte del personale autorizzato e degli incaricati;
- aggiornare il presente manuale in osservanza delle disposizioni.

Art. 7 Posta elettronica certificata

La casella di posta elettronica certificata presidenza@pec.fnopo.it è pubblicata sull'Indice delle Pubbliche Amministrazioni (IPA).

Art. 8 Firma digitale

L'Ente fornisce la firma digitale o elettronica qualificata ai soggetti da essa delegati a rappresentarla per l'espletamento delle attività istituzionali e per quelle connesse all'attuazione delle norme di gestione del protocollo informatico.

La firma digitale o elettronica qualificata viene acquistata da un'autorità iscritta nell'elenco dei certificatori accreditati tenuto dall'AGID.

Art. 9 Titolario e classificazione dei documenti

A norma dell'art. 56 del TUDA l'operazione di classificazione dei documenti costituisce una operazione necessaria e sufficiente per la tenuta del sistema di gestione informatica dei documenti e dell'archivio. Il piano di classificazione o titolario è lo strumento indispensabile che si utilizza per la corretta gestione dell'archivio in formazione. Il titolario di classificazione è strutturato su due livelli: titoli e classi; si tratta di un sistema logico astratto precostituito che organizza i documenti sulla base dell'organizzazione funzionale dell'Ente, consentendo di organizzare in maniera omogenea e coerente i documenti che si riferiscono ai medesimi affari o ai medesimi procedimenti amministrativi, strumento indispensabile per la interoperabilità dei sistemi.

Il titolario, allegato al presente manuale come Allegato n. 1, è articolato in titoli e classi, formulato in riferimento alle funzioni dell'Ente.

Art. 10 Tutela dei dati personali

L'ente in qualità di titolare del trattamento dei dati personali comuni, sensibili e/o giudiziari, contenuti nella documentazione trattata nell'ambito delle proprie funzioni istituzionali, si attiene alla normativa del regolamento europeo GDPR n. 2016/679 e alle disposizioni dell'autorità garante della protezione dei dati personali italiana ed europea.

2. FORMAZIONE DEI DOCUMENTI INFORMATICI

Art. 11 Documento informatico

Ai sensi delle Linee guida AGID sulla formazione, gestione e conservazione dei documenti informatici, il documento informatico è formato mediante una delle seguenti modalità:

- “a) creazione tramite l'utilizzo di strumenti software o servizi cloud qualificati che assicurino la produzione di documenti nei formati e nel rispetto delle regole di interoperabilità di cui all'allegato 2 - delle Linee guida;*
- b) acquisizione di un documento informatico per via telematica o su supporto informatico, acquisizione della copia per immagine su supporto informatico di un documento analogico, acquisizione della copia informatica di un documento analogico;*
- c) memorizzazione su supporto informatico in formato digitale delle informazioni risultanti da transazioni o processi informatici o dalla presentazione telematica di dati attraverso moduli o formulari resi disponibili all'utente;*
- d) generazione o raggruppamento anche in via automatica di un insieme di dati o registrazioni, provenienti da una o più banche dati, anche appartenenti a più soggetti interoperanti, secondo una struttura logica predeterminata e memorizzata in forma statica.*

Il documento informatico deve essere identificato in modo univoco e persistente. Nel caso della Pubblica Amministrazione, l'identificazione dei documenti oggetto di registrazione di protocollo è rappresentata dalla segnatura di protocollo univocamente associata al documento.

L'identificazione dei documenti non protocollati è affidata alle funzioni del sistema di gestione informatica dei documenti. In alternativa l'identificazione univoca può essere realizzata mediante associazione al documento di una sua impronta crittografica basata su funzioni di hash che siano ritenute crittograficamente sicure, e conformi alle tipologie di algoritmi previsti nell'allegato 6 delle linee guida nella tabella 1 del paragrafo 2.2 regole di processamento.

Il documento informatico è immutabile se la sua memorizzazione su supporto informatico in formato digitale non può essere alterata nel suo accesso, gestione e conservazione.

Nel caso di documento informatico formato secondo la sopracitata lettera a), l'immutabilità e l'integrità sono garantite da una o più delle seguenti operazioni:

- apposizione di una firma elettronica qualificata, di una firma digitale o di un sigillo elettronico qualificato o firma elettronica avanzata;*
- memorizzazione su sistemi di gestione documentale che adottino idonee misure di sicurezza in accordo con quanto riportato al § 3.9;*
- il trasferimento a soggetti terzi attraverso un servizio di posta elettronica certificata o un servizio elettronico di recapito certificato qualificato, come definito dal regolamento (UE) 23 luglio 2014 n. 910 del Parlamento europeo e del Consiglio in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno (regolamento eIDAS), valido ai fini delle comunicazioni elettroniche aventi valore legale;*
- versamento ad un sistema di conservazione.*

Nel caso di documento informatico formato secondo la sopracitata lettera b) l'immodificabilità ed integrità sono garantite da una o più delle seguenti operazioni mediante:

- *apposizione di una firma elettronica qualificata, di una firma digitale o di un sigillo elettronico qualificato o firma elettronica avanzata;*
- *memorizzazione su sistemi di gestione documentale che adottino idonee misure di sicurezza in accordo con quanto riportato al § 3.9 delle Linee guida;*
- *versamento ad un sistema di conservazione.*

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

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

La certezza dell'autore è la capacità di poter associare in maniera certa e permanente il soggetto che ha sottoscritto al documento stesso.

Al momento della formazione del documento informatico immodificabile, devono essere generati e associati permanentemente ad esso i relativi metadati. L'insieme dei metadati del documento informatico è definito nell'allegato 5 "Metadati" delle Linee guida. Potranno essere individuati ulteriori metadati da associare a particolari tipologie di documenti informatici. A tal proposito si ricorda che nel manuale di gestione devono essere riportati i metadati definiti per ogni tipologia di documento.

La disponibilità e la riservatezza delle informazioni contenute nel documento informatico sono garantite attraverso l'adozione di specifiche politiche e procedure predeterminate dall'ente, in conformità con le disposizioni vigenti in materia di accesso e protezione dei dati personali. Nel caso della Pubblica Amministrazione, tali politiche e procedure sono contenute nel manuale di gestione documentale di cui al paragrafo 3.5. L'evidenza informatica corrispondente al documento informatico immodificabile è prodotta in uno dei formati contenuti nell'Allegato 2 "Formati di file e riversamento" alle linee guida ove sono specificate, anche, le caratteristiche e i criteri di scelta del formato stesso".

Art. 12 Copia di documento informatico

Un duplicato informatico ha lo stesso valore giuridico del documento informatico da cui è tratto se è ottenuto mediante la memorizzazione della medesima evidenza informatica, sullo stesso dispositivo o su dispositivi diversi; ad esempio, effettuando una copia da un PC ad una pen-drive di un documento nel medesimo formato.

La copia di un documento informatico è un documento il cui contenuto è il medesimo dell'originale ma con una diversa evidenza informatica rispetto al documento da cui è tratto, come quando si trasforma un documento con estensione ".doc" in un documento ".pdf". L'estratto di un documento informatico è una parte del documento con una diversa evidenza informatica rispetto al documento da cui è tratto. Tali documenti hanno lo stesso valore probatorio dell'originale da cui hanno origine

se la stessa conformità non viene espressamente disconosciuta. In particolare, la validità del documento informatico per le copie e/o estratti di documenti informatici è consentita mediante uno dei due metodi:

- raffronto dei documenti;
- certificazione di processo.

Il ricorso ad uno dei due metodi sopracitati assicura la conformità del contenuto della copia o dell'estratto informatico alle informazioni del documento informatico di origine.

Fatto salvo quanto previsto dall'art. 23bis comma 2 del CAD10 nel caso in cui non vi è l'attestazione di un pubblico ufficiale, la conformità della copia o dell'estratto informatico ad un documento informatico è garantita mediante l'apposizione della firma digitale o firma elettronica qualificata o firma elettronica avanzata, nonché del sigillo elettronico qualificato e avanzato da parte di chi effettua il raffronto.

Laddove richiesta dalla natura dell'attività, l'attestazione di conformità delle copie o estratti informatici di documenti informatici può essere inserita nel documento informatico contenente la copia o l'estratto. L'attestazione di conformità delle copie o dell'estratto informatico di uno o più documenti informatici può essere altresì prodotta come documento informatico separato contenente un riferimento temporale e l'impronta di ogni copia o estratto informatico. Il documento informatico contenente l'attestazione è sottoscritto con firma digitale o con firma elettronica qualificata o avanzata del notaio o del pubblico ufficiale a ciò autorizzato.

Le copie e gli estratti informatici del documento informatico, se prodotti in conformità alle vigenti regole tecniche di cui all'articolo 71 del CAD, hanno la stessa efficacia probatoria dell'originale da cui sono tratte se la loro conformità all'originale, in tutti le sue componenti, è attestata da un pubblico ufficiale a ciò autorizzato o se la conformità non è espressamente disconosciuta. Resta fermo, ove previsto, l'obbligo di conservazione dell'originale informatico.

Art. 13 Obiettivo del piano di sicurezza

Il piano di sicurezza garantisce che:

- * i documenti e le informazioni trattati dall'amministrazione/AOO siano resi disponibili, integri e riservati;
- * i dati personali comuni, sensibili e/o giudiziari vengano custoditi in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta, in relazione alle conoscenze acquisite in base al progresso tecnico, alla loro natura e alle specifiche caratteristiche del trattamento.

Art. 14 Gestione dei documenti informatici

Il sistema operativo delle risorse elaborative del Sistema Informativo utilizzate per erogare il servizio di protocollo informatico con il PdP all'amministrazione/AOO, deve essere conforme alle specifiche previste dalla classe ITSEC F-C2/E2 o a quella C2 delle norme TCSEC e loro successive evoluzioni (scritture di sicurezza e controllo accessi).

Il sistema operativo del server che ospita i file utilizzati come deposito dei documenti è configurato in modo tale da consentire:

- * l'accesso esclusivamente al server del protocollo informatico in modo che qualsiasi altro utente non autorizzato non possa mai accedere ai documenti al di fuori del sistema di gestione documentale,

* la registrazione delle attività rilevanti ai fini della sicurezza svolte da ciascun utente, in modo tale da garantire l'identificabilità dell'utente stesso. Tali registrazioni sono protette da modifiche non autorizzate.

Il sistema di gestione informatica dei documenti:

- * garantisce la disponibilità, la riservatezza e l'integrità dei documenti e del registro di protocollo;
- * garantisce la corretta e la puntuale registrazione di protocollo dei documenti in entrata ed in uscita;
- * fornisce informazioni sul collegamento esistente tra ciascun documento ricevuto dall'amministrazione e gli atti dalla stessa formati al fine dell'adozione del provvedimento finale;
- * consente il reperimento delle informazioni riguardanti i documenti registrati;
- * consente, in condizioni di sicurezza, l'accesso alle informazioni del sistema da parte dei soggetti interessati, nel rispetto delle disposizioni in materia di "privacy" con particolare riferimento al trattamento dei dati sensibili e giudiziari;
- * garantisce la corretta organizzazione dei documenti nell'ambito del sistema di classificazione d'archivio adottato.

Art. 15 Classificazione del documento

Il documento amministrativo come oggetto di scambio, in termini funzionali è classificabile in:

- * ricevuto,
- * inviato,
- * interno formale,
- * interno informale.

Il documento amministrativo come oggetto di scambio, in termini tecnologici è classificabile in

- * informatico,
- * analogico.

Secondo quanto stabilito dalla corrente normativa il documento amministrativo è solo di tipo informatico. Solo durante la fase transitoria di migrazione verso l'adozione integrale delle tecnologie digitali da parte dell'amministrazione, il documento amministrativo, in via del tutto eccezionale, è disponibile anche nella forma analogica (di solito carta).

Art. 16 Documento ricevuto

Per documento ricevuto si intende qualsiasi tipo di corrispondenza (in formato digitale o analogico) inviato da un soggetto fisico o giuridico; i mezzi di recapito sono il servizio postale pubblico o privato, la posta elettronica certificata o convenzionale, fax, telegramma.

Art. 17 Documento inviato

I documenti informatici, compresi di eventuali allegati, anch'essi digitali informatici, sono inviati, di norma, per mezzo della posta elettronica certificata o convenzionale se la dimensione del documento non supera la dimensione massima dei messaggi stabilita dal sistema di posta utilizzata dall'AOO.

In caso contrario il documento informatico viene riversato, a norma di legge, su supporto digitale rimovibile non modificabile e trasmesso con altri mezzi di trasposto al destinatario.

Art. 18 Documento interno formale

I documenti interni di rilevanza amministrativa giuridico-probatoria sono formati con tecnologie informatiche dal personale interno all'amministrazione (AOO) nell'esercizio delle proprie funzioni. Lo scambio di norma avviene per mezzo della posta elettronica convenzionale o di quella certificata.

Art. 19 Documento interno informale

I documenti interni informali sono di norma memorie informali, appunti, brevi comunicazioni di rilevanza meramente informativa scambiate tra uffici, questo genere di documenti non deve essere protocollato.

3. PROTOCOLLO INFORMATICO E REGISTRAZIONI PARTICOLARI

Art. 20 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:

- a) numero di protocollo, generato automaticamente dal sistema e registrato in forma non modificabile;
- b) data di registrazione di protocollo, assegnata automaticamente dal sistema e registrata in forma non modificabile;
- c) mittente o destinatario dei documenti ricevuti o spediti;
- d) oggetto del documento;
- e) l'indicazione del numero di codice fiscale o di Partita IVA, ovvero, nei casi di indisponibilità degli stessi, il nome ed il cognome dell'eventuale soggetto cui si riferisce l'atto;
- f) data e numero di protocollo dei documenti ricevuti, se disponibili;
- g) impronta del documento informatico, se trasmesso per via telematica;
- h) classificazione: Titolo, classe;
- i) assegnazione.

La procedura di registrazione di protocollo del software gestionale è indicata in allegato 2.

Art. 21 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.

Art. 22 Segnatura di protocollo

La segnatura di protocollo apposta, o associata, al documento è effettuata contemporaneamente alla registrazione di protocollo.

Ai fini dell'inserimento devono essere compilati i seguenti campi:

“Numero riferimento” e “Data di riferimento”: sono i riferimenti del documento oggetto del protocollo;

“Mittente” o “Destinatario”, scegliendo fra le categorie disponibili; selezionando una ‘Lista’ la procedura registra l’associazione del protocollo con tutti i componenti della lista.

“Oggetto”: ossia l’oggetto del documento;

“Classificazione”: intesa come macrocategoria da assegnare al protocollo ed ha come finalità quella di facilitare la ricerca del protocollo inserito.

“Allegati”: cliccando su nuovo si può allegare il documento informatico nei formati prestabiliti (eml, pdf, doc, ecc.); è possibile inserire un documento tramite l’opzione di ‘copia e incolla’ del file.

Art. 23 Requisiti di sicurezza del sistema di protocollo informatico

Il sistema di protocollo informatico, eventualmente integrato in un sistema di gestione informatica dei documenti, assicura il rispetto delle disposizioni in materia di sicurezza predisposte dall’AgID ottemperando alle misure minime di sicurezza ICT emanate dall’AGID con circolare del 18 aprile 2017, n. 2/2017 e dagli altri organismi preposti e delle disposizioni in materia di protezione dei dati personali.

In particolare, il sistema di protocollo informatico deve garantire:

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

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

Art. 24 Annullamento delle registrazioni di protocollo

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

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

Art. 25 Differimento dei termini di protocollazione

La registrazione della documentazione pervenuta deve avvenire nell’arco di 24/48 ore. Il responsabile del servizio, 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; il sistema informatico mantiene traccia del ricevimento dei documenti.

Art. 26 Registro giornaliero di protocollo

Il responsabile del servizio di protocollo - RSP - provvede alla produzione del registro giornaliero di protocollo, costituito dall'elenco delle informazioni inserite con l'operazione di registrazione di protocollo nell'arco di uno stesso giorno.

Al fine di garantire la non modificabilità delle operazioni di registrazione, il contenuto del registro giornaliero informatico di protocollo è riversato, entro il giorno successivo, ai sensi dell'art. 6 comma 5 del DPCM 3/12/2013 e viene trasmesso entro lo stesso termine al sistema di conservazione garantendone l'immodificabilità del contenuto secondo le modalità di conservazione.

Art. 27 Registro di emergenza

Il Responsabile del Servizio per la tenuta del protocollo informatico autorizza lo svolgimento delle operazioni di protocollo su un registro di emergenza a norma dell'articolo 63 del *TUDA* e provvede successivamente a impartire le disposizioni per il riversamento dei dati nel protocollo informatico. Il RSP prima di autorizzare l'avvio della protocollazione sul registro di emergenza, il RSP imposta e verifica la correttezza della data e dell'ora sui rispettivi registri di emergenza.

Sul registro di emergenza sono riportate:

- * una numerazione progressiva nel formato AAAAMMGGNNNN;
- * la causa;
- * la data;
- * l'ora di inizio dell'interruzione.

Ogni registro di emergenza si rinnova ogni anno solare e, pertanto, inizia il primo gennaio e termina il 31 dicembre di ogni anno.

Qualora nel corso di un anno non venga utilizzato il registro di emergenza, il RSP annota su questo il mancato uso.

Art. 28 Registri e repertori informatici

Come previsto dal paragrafo 3.3.3 delle Linee Guida AGID, il registro di protocollo e i registri dei documenti soggetti a registrazione particolare, i repertori, gli albi, gli elenchi e ogni raccolta di dati concernente stati, qualità personali e fatti realizzati dalle amministrazioni su supporto informatico in luogo dei registri cartacei sono formati attraverso la generazione o il raggruppamento anche in via automatica di un insieme di dati o registrazioni, provenienti da una o più banche dati, anche appartenenti a più soggetti che operano fra loro, secondo una struttura logica predeterminata e memorizzata in forma statica.

4. CASI PARTICOLARI DI REGISTRAZIONI DI PROTOCOLLO

Art. 29 Circolari e disposizioni generali

Le circolari, le disposizioni generali e tutte le altre comunicazioni che abbiano più destinatari si registrano con un solo numero di protocollo generale.

I destinatari sono descritti in appositi elenchi da associare alla minuta del documento e alla registrazione di protocollo secondo le modalità previste dalla gestione anagrafiche del sistema.

Art. 30 Documenti cartacei in partenza con più destinatari

Qualora i destinatari siano in numero maggiore di uno, la registrazione di protocollo è unica e la registrazione viene riportata sui documenti degli altri destinatari, predisponendo un elenco dei destinatari che viene allegato alla minuta dell'originale.

Art. 31 Documenti cartacei ricevuti a mezzo telegramma

I telegrammi vanno trattati come documenti senza firma, specificando tale modalità di trasmissione nel sistema di protocollo informatico.

Art. 32 Documenti cartacei ricevuti a mezzo telefax

Il documento ricevuto a mezzo telefax è un documento analogico a tutti gli effetti qualora ne venga accertata la fonte di provenienza, soddisfa il requisito della forma scritta e la sua trasmissione non deve essere seguita dalla trasmissione dell'originale.

Nel caso che al telefax faccia seguito l'originale, poiché ogni documento viene individuato da un solo numero di protocollo, indipendentemente dal supporto e dal mezzo di trasmissione, l'addetto alla registrazione a protocollo, dopo aver registrato il telefax, deve attribuire all'originale la stessa segnatura del documento pervenuto via telefax ed apporre la seguente dicitura: "già pervenuto via fax il giorno.....".

Il fax ricevuto con un terminale telefax dedicato (diverso da un PC) è fotocopiato dal ricevente qualora il supporto cartaceo non fornisca garanzie per una corretta e duratura conservazione. Su di esso o sulla sua fotoriproduzione va apposta, a cura del ricevente, la dicitura "Documento ricevuto via Telefax".

Il fax ricevuto direttamente su una postazione di lavoro (esempio un PC con l'applicativo per invio e ricezione di fax) è la rappresentazione informatica di un documento che può essere, sia stampato e trattato come un fax convenzionale come descritto nei commi precedenti, sia visualizzato e trattato interamente con tecniche informatiche.

In questo secondo caso il "file" rappresentativo del fax, viene inviato al protocollo generale, per essere sottoposto alle azioni di protocollazione e segnatura secondo gli standard XML correnti e poi, trattato secondo le regole precedentemente dichiarate per la gestione dei documenti informatici. L'articolo 14 della legge n. 98/2013, di conversione del Decreto Legge n. 69/2013, prevede che le comunicazioni tra Pubbliche Amministrazioni dovranno avvenire esclusivamente per via telematica. E' fatto assoluto divieto l'utilizzo del telefax.

Art. 33 Domande di partecipazione a concorsi, avvisi, selezioni, corsi e borse di studio

La corrispondenza ricevuta con rimessa diretta dell'interessato o persona delegata, viene protocollata al momento della presentazione, dando ricevuta di avvenuta consegna con gli estremi della segnatura di protocollo.

Analoga sorte è riservata alla corrispondenza ricevuta in formato digitale o per posta certificata, modalità di presentazione telematica che deve, comunque, essere prevista nel bando.

Art. 34 Documenti non firmati

L'addetto al servizio di protocollo, sulla base delle regole stabilite dal RSP attestanti la certezza giuridica di data, forma e provenienza, per ogni documento deve attestare che un determinato documento così come si registra è pervenuto.

Le lettere anonime, pertanto, vanno protocollate e identificate come tali, con la dicitura “mittente sconosciuto o anonimo” e “documento non sottoscritto”.

Per le stesse ragioni le lettere con mittente, prive di firma, vanno protocollate e vengono identificate come tali.

Il RSP valuta di caso in caso se trattasi di documento soggetto a registrazione di protocollo particolare.

Art. 35 Documenti non soggetti a registrazione di protocollo

Sono esclusi dalla registrazione di protocollo: gazzette ufficiali, bollettini ufficiali, 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.

Art. 36 Protocollazione dei messaggi di posta elettronica convenzionale

Il sistema di posta elettronica ordinaria, non consente con certezza una completa e sicura individuazione del mittente pertanto, questa corrispondenza viene normalmente trattata come segue:

- * nel caso di invio di documento firmato in modalità autografa e scannerizzato esso viene trattato come un documento inviato via fax previa verifica della provenienza dell'indirizzo e-mail del mittente da parte del Responsabile del Procedimento Amministrativo;

- * nel caso in cui non vi sia provenienza certa né documento digitalizzato firmato in maniera autografa, il Responsabile del Procedimento Amministrativo valuta caso per caso l'opportunità di trattare l'e-mail;

- * nel caso in cui il documento pervenga firmato digitalmente esso è equiparabile al documento elettronico pervenuto in altre maniere. Va da sé, in tal caso, che il mittente non ha la certezza che il messaggio sia stato ricevuto correttamente;

- * nel caso pervenga una e-mail con contenuto non sottoscritto esso verrà trattato come un documento anonimo.

Art. 37 Protocollazione di documenti digitali pervenuti erroneamente

Nel caso in cui venga erroneamente protocollato un documento digitale non indirizzato all'amministrazione l'addetto protocollatore provvede o all'annullamento del protocollo o alla protocollazione in uscita indicando come oggetto “**protocollato per errore**” e rispedisce il messaggio al mittente.

Art. 38 Ricezione di documenti cartacei pervenuti erroneamente

Nel caso in cui venga erroneamente protocollato un documento non indirizzato all'amministrazione, l'addetto al protocollo provvede o all'annullamento del protocollo o alla protocollazione in uscita indicando come oggetto “**protocollato per errore, inviato a ..**”.

Il documento oggetto della rettifica viene inviato al destinatario con la dicitura “protocollato per errore”.

Art. 39 Copie per conoscenza

Nel caso di copie per conoscenza chi effettua la registrazione e lo smistamento dell'originale e delle copie, registra sul registro di protocollo a chi sono state inviate le copie per conoscenza. Tale informazione viene riportata anche sulla segnatura di protocollo.

Art. 40 Differimento delle registrazioni

Le registrazioni di protocollo dei documenti ricevuti sono effettuate in giornata, salvo provvedimento motivato del RSP.

In caso di impedimento alla registrazione di protocollo di tutti gli atti, nello stesso giorno di presentazione, viene data priorità a quelli per i quali riveste particolare importanza la puntuale protocollazione.

Nel caso di un temporaneo ed eccezionale carico di lavoro che non permette di evadere la corrispondenza ricevuta nella medesima giornata lavorativa e qualora dalla mancata registrazione di protocollo del documento nella medesima giornata lavorativa di ricezione possa venire meno un diritto di terzi, con motivato provvedimento del RSP, l'addetto al protocollo è autorizzato all'uso del protocollo differito.

Il protocollo differito consiste nel differimento dei termini di registrazione, cioè nel provvedimento del RSP con il quale vengono individuati dal RSP i documenti da ammettere alla registrazione differita, le cause e il termine entro il quale la registrazione di protocollo deve comunque essere effettuata.

Il protocollo differito si applica solo ai documenti in arrivo e per tipologie omogenee che il RSP descrive nel provvedimento.

Art. 41 Registrazioni con differimento dei termini di accesso

Per i procedimenti amministrativi o gli affari per i quali si renda necessaria la riservatezza temporanea delle informazioni, cioè il differimento dei termini di accesso (ad esempio, gare e appalti, verbali di concorso, etc.), è prevista una forma di accesso riservato al protocollo unico.

Il Responsabile dell'immissione dei dati indica, contestualmente alla registrazione di protocollo, anche l'anno, il mese e il giorno, nel quale le informazioni temporaneamente riservate divengono soggette all'accesso nelle forme ordinariamente previste.

Art. 42 Corrispondenza personale o riservata

La corrispondenza nominativamente intestata è regolarmente aperta dagli uffici incaricati della registrazione di protocollo dei documenti in arrivo, a meno che sulla busta non sia riportata la dicitura "riservata" o "personale".

La corrispondenza con la dicitura "riservata" o "personale" non è aperta e viene consegnata in busta chiusa al destinatario il quale, dopo averne preso visione, se valuta che i documenti ricevuti non sono personali, è tenuto a trasmetterli al più vicino ufficio abilitato alla registrazione di protocollo dei documenti in arrivo.

Art. 43 Documenti soggetti a scansione

I documenti ricevuti su supporto cartaceo, dopo le operazioni di registrazione, classificazione e segnatura, sono acquisiti in formato immagine non modificabile con l'ausilio di scanner e collegati al prodotto di registrazione di protocollo.

Art. 44 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 abilitato alla conservazione;
- * 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.

5. PIANO DI CLASSIFICAZIONE DOCUMENTALE E SELEZIONE

Art. 45 Classificazione

La classificazione dei documenti è di importanza primaria in quanto consente di organizzare in maniera logica tutti i documenti che entrano a far parte del sistema documentario dell'Ente, a prescindere dalle modalità di acquisizione o produzione.

Attraverso la classificazione si stabilisce la posizione che ogni documento assume nell'archivio in formazione, consentendo una sedimentazione che rispecchi lo sviluppo dell'attività svolta dall'Ente. La classificazione si realizza con l'utilizzo del Titolario o Piano di classificazione (allegato n. 1).

Art. 46 Titolario o piano di classificazione

Il titolare o piano di classificazione è lo schema logico utilizzato per organizzare i documenti d'archivio in base alle funzioni e alle materie di competenza dell'Ente.

Il piano di classificazione si suddivide, in titoli e classi.

Il titolo (o la voce di I livello) individua per lo più funzioni primarie e di organizzazione dell'ente (macrofunzioni); la successiva partizione in classi corrisponde a specifiche competenze che rientrano concettualmente nella macrofunzione descritta dal titolo.

Tutti i documenti ricevuti e prodotti, indipendentemente dal supporto sul quale vengono formati, sono classificati in base al citato titolare.

Art. 47 Modifica del Piano di classificazione

1. Il Titolare di classificazione è uno strumento tendenzialmente stabile nel tempo, ma non statico. Esso può essere modificato o integrato a seguito di assegnazioni di nuove funzioni, ovvero di sviluppo o modifica di funzioni istituzionali già possedute.

6. FORMAZIONE AGGREGAZIONI DOCUMENTALI

Art. 48 Aggregazioni documentali informatiche

L'attività svolta dall'Ente è *documentata tramite funzioni del sistema di gestione informatica dei documenti, finalizzata alla produzione, alla gestione e all'uso delle aggregazioni documentali informatiche, corredate da opportuni metadati, così come definiti nell'allegato 5 "Metadati" delle Linee guida.*

Art. 49 Fascicolo informatico

Ai sensi dell'art. 41 del CAD la pubblica amministrazione titolare del procedimento raccoglie in un fascicolo informatico gli atti, i documenti e i dati del procedimento medesimo da chiunque formati. La gestione dei flussi documentali si realizza mediante fascicoli informatici predisposti secondo il piano di classificazione e relativo piano di organizzazione delle aggregazioni documentali ai sensi dell'art. 64 del TUDA, anche con riferimento a fascicoli non afferenti a procedimenti. Ogni documento informatico ricevuto, interno, spedito, deve essere sempre classificato e inserito in una aggregazione archivistica (fascicolo o serie documentale).

Art. 50 Creazione del fascicolo informatico

La creazione di un nuovo fascicolo informatico avviene attraverso la piattaforma informatica dall'utente operatore del protocollo come descritto al punto **4.2 Gestione Fascicoli** del manuale d'uso (allegato n. 2).

Art. 51 Organizzazione dei documenti

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

Art. 52 Archivio informatico

L'archivio informatico – formato ai sensi del capo IV “Sistema di gestione informatica dei documenti” del TUDA – è progettato in modo da assicurare certezza e trasparenza all'attività giuridico amministrativa dell'Ente produttore.

Fino a quando non si avrà in maniera esclusiva un archivio digitale, l'ente dovrà provvedere all'archiviazione dei documenti digitali e analogici.

Per i documenti informatici si fa riferimento al Manuale di Conservazione (allegato n. 8). Per i documenti analogici, anche se trasformati attraverso lo scanner in documenti digitali e divenuti parte integrante di un fascicolo digitale, l'utente del protocollo previa segnatura archivistica, provvede all'archiviazione e conservazione secondo i termini di legge.

7. FLUSSI DI LAVORAZIONE DOCUMENTALI INTERNI

Le procedure relative ai flussi sono adeguate alle dimensioni dell'Ente.

Art. 53 Documenti in arrivo

Si intendono documenti in arrivo, i documenti pervenuti dall'AOO nell'esercizio delle proprie funzioni.

Art. 54 Ricezione dei documenti su supporto cartaceo

I documenti di tipo cartaceo possono pervenire all'AOO attraverso:

- * servizio postale;
- * consegna diretta all'ufficio protocollo oppure agli uffici/sportelli URP abilitati presso l'amministrazione al ricevimento della documentazione,

Tutti i documenti devono pervenire all'ufficio protocollo per la registrazione esclusi quelli non soggetti a registrazioni.

Art. 55 Ricezione di documenti informatici sulla casella di posta istituzionale

La ricezione dei documenti informatici è assicurata tramite:

- * caselle di posta elettronica certificata (istituzionale e non);
- * caselle di posta elettronica dei singoli uffici;

L'utente protocollatore controlla quotidianamente i messaggi pervenuti nelle casella di posta istituzionale e verifica se sono da protocollare.

Art. 56 Ricezione di documenti informatici sulla casella di posta elettronica non istituzionale

Nel caso in cui il messaggio venga ricevuto su un'altra casella di posta elettronica non istituzionale o comunque non adibita al servizio di protocollazione, il messaggio viene inviato alla casella istituzionale con richiesta di protocollazione.

Art. 57 Ricezione di documenti informatici su supporti rimovibili

I documenti digitali possono essere recapitati anche per vie diverse dalla posta elettronica.

I documenti informatici ricevuti su supporto rimovibile che si riescono a decodificare e interpretare con le tecnologie a disposizione dell'ente vengono inseriti nel flusso di lavorazione e sottoposti a tutti i controlli e gli adempimenti del caso.

Art. 58 Attività di protocollazione dei documenti

Superati tutti i controlli precedenti i documenti, digitali o analogici, vengono protocollati e "segnati" nel registro di protocollo generale informatico.

Art. 59 Classificazione dei documenti

Il documento ricevuto, indipendentemente dal supporto sul quale è formato, viene classificato in base al titolare di classificazione dall'addetto alla registrazione di protocollo.

Art. 60 Assegnazione dei documenti ricevuti da vedere

Il Responsabile del Procedimento Amministrativo è il responsabile del servizio per la tenuta del protocollo informatico (articolo 12 del decreto del Presidente della Repubblica 428/1998) il quale decide l'ufficio dell'amministrazione incaricato della gestione del procedimento relativo al documento da protocollare.

Art. 61 Smistamento dei documenti protocollati

La consegna dei documenti protocollati all'ufficio individuato viene effettuata almeno una volta al giorno, salvo la consegna immediata per i documenti indicati come urgenti.

Art. 62 Documenti inviati dall'AOO

Per documenti in partenza si intendono i documenti amministrativi, redatti dal personale degli uffici dell'AOO nell'esercizio delle proprie funzioni, aventi rilevanza giuridico-probatoria ed inviati ad altre Amministrazioni, a privati.

Art. 63 Modalità di invio dei documenti

I mezzi di spedizione della corrispondenza di norma avvengono con l'utilizzo della Posta Elettronica Certificata.

Art. 64 Registrazione di protocollo e segnatura

La protocollazione e la segnatura della corrispondenza in partenza è effettuata dall'Ufficio protocollo.

Art. 65 Trasmissione di documenti informatici

Le modalità di composizione e di scambio dei messaggi, il formato della codifica e le misure di sicurezza sono conformi al decreto legislativo n. 82 del 2005 e successive modificazioni e integrazioni.

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

I documenti informatici vengono inviati dall'indirizzo di Posta Elettronica Certificata.

Art. 66 Trasmissione di documenti cartacei a mezzo posta

L'ufficio di protocollo provvede direttamente a tutte le operazioni di spedizione della corrispondenza provvedendo anche all'affrancatura e all'eventuale pesatura, alla ricezione e alla verifica delle distinte di raccomandate compilate dagli uffici. Al fine di consentire il regolare svolgimento di tali operazioni, la corrispondenza in partenza deve essere consegnata all'ufficio di protocollo entro le ore 12,00 di ogni giorno lavorativo. Nell'eventualità l'ufficio utente dovesse inviare grossi quantitativi di corrispondenza è tenuto ad avvertire preventivamente l'ufficio protocollo. La consegna al servizio postale avviene, di norma, entro il giorno lavorativo successivo alla trasmissione della busta, plico o simili al Servizio protocollo per la spedizione.

Art. 67 Documenti in partenza per posta convenzionale con più destinatari

Qualora i destinatari siano più di uno, e comunque in numero maggiore di tre, può essere autorizzata la spedizione di copie dell'originale. L'elenco dei destinatari, in formato cartaceo, è allegato alla minuta.

8. MISURE DI SICUREZZA E PROTEZIONE DEI DATI

Art. 68 Sicurezza

Il piano di sicurezza informatica del sistema informativo dell'amministrazione è definito dall'organizzazione dell'Ente che gestisce il sistema informatico generale. Il responsabile della conservazione, di concerto con il responsabile per la transizione digitale, con il responsabile della gestione documentale e acquisito il parere del responsabile della protezione dei dati personali, predispone il piano della sicurezza del sistema di gestione informatica dei documenti, prevedendo opportune misure tecniche e organizzative per garantire un livello di sicurezza adeguato al rischio in materia di protezione dei dati personali, ai sensi dell'art. 32 del Regolamento UE 2016/679, anche in funzione delle tipologie di dati trattati, quali quelli riferibili alle categorie particolari di cui agli artt. 9-10 del Regolamento stesso.

Art. 69 Obiettivi

La politica in merito alla sicurezza dell'Ente è finalizzata a assicurare che:

- i documenti e le informazioni trattati dall'amministrazione/AOO siano resi disponibili, integri e riservati;
- i dati personali comuni, sensibili e/o giudiziari vengano custoditi in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta, in relazione alle conoscenze acquisite in base al progresso tecnico, alla loro natura e alle specifiche caratteristiche del trattamento.

A tale fine l'Ente definisce:

- le politiche generali e particolari di sicurezza da adottare all'interno della AOO;
- le modalità di accesso al servizio di gestione documentale, di protocollo, ed archivistico;
- gli interventi operativi adottati sotto il profilo organizzativo, procedurale e tecnico, con particolare riferimento alle misure minime di sicurezza, di cui all'Articolo 32 GDPR, in caso di trattamento di dati personali;
- i piani specifici di formazione degli addetti;
- le modalità con le quali deve essere effettuato il monitoraggio periodico dell'efficacia e dell'efficienza delle misure di sicurezza.

Il Responsabile della gestione documentale adotta le misure tecniche e organizzative di seguito specificate, al fine di assicurare la sicurezza dell'impianto tecnologico dell'A OO, la riservatezza delle informazioni registrate nelle banche dati, l'univoca identificazione degli utenti interni ed esterni:

- protezione periferica della Intranet dell'amministrazione/AOO;
- protezione dei sistemi di accesso e conservazione delle informazioni;
- assegnazione ad ogni utente del sistema di gestione dei documenti e del protocollo di una credenziale di identificazione pubblica (user ID), di una credenziale riservata di autenticazione (password) e di un profilo di autorizzazione;
- cambio delle password con frequenza prestabilita durante la fase di esercizio;
- piano di continuità del servizio con particolare riferimento, sia alla esecuzione e alla gestione delle copie di riserva dei dati e dei documenti da effettuarsi con frequenza giornaliera, sia alla capacità di ripristino del sistema informativo in caso di disastro;
- conservazione delle copie di riserva dei dati e dei documenti, in locali diversi e se possibile lontani da quelli in cui è installato il sistema di elaborazione di esercizio che

ospita il PdP;

- gestione delle situazioni di emergenza informatica attraverso la costituzione di un gruppo di risorse interne qualificate (o ricorrendo a strutture esterne qualificate);
- impiego e manutenzione di un adeguato sistema antivirus e di gestione dei “moduli” (patch e service pack) correttivi dei sistemi operativi;
- cifratura o uso di codici identificativi (o altre soluzioni ad es. separazione della parte anagrafica da quella “sensibile”) dei dati sensibili e giudiziari contenuti in elenchi, registri o banche di dati, tenuti con l’ausilio di strumenti elettronici, allo scopo di renderli temporaneamente inintelligibili anche a chi è autorizzato ad accedervi e permettendo di identificare gli interessati solo in caso di necessità;
- impiego delle misure precedenti anche nel caso di supporti cartacei di banche dati idonee a rilevare lo stato di salute e la vita sessuale;
- archiviazione giornaliera, in modo non modificabile, delle copie del registro di protocollo, dei file di log di sistema, di rete e applicativo contenenti le informazioni sulle operazioni effettuate da ciascun utente durante l’arco della giornata, comprese le operazioni di backup e manutenzione del sistema. I dati personali registrati nel log del sistema operativo, del sistema di controllo degli accessi e delle operazioni svolte con il sistema di protocollazione e gestione dei documenti utilizzato saranno consultati solo in caso di necessità dal RSP e dal titolare dei dati e, ove previsto dalle forze dell’ordine.

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

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

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

Ad ogni utente è assegnata:

- una credenziale di accesso, costituita da una componente pubblica che permette l’identificazione dell’utente da parte del sistema (userID), e da una componente privata o riservata di autenticazione (password);
- una autorizzazione di accesso (profilo) che limita le operazioni di protocollo, gestione documentale e workflow effettuabili alle sole funzioni necessarie.

La visibilità normalmente attribuita ad un utente si limita alla documentazione relativa ai servizi di competenza. La visibilità su altri documenti può essere attribuita dal responsabile della pratica o del procedimento.

L’accesso diretto alla banca dati, l’inserimento di nuovi utenti, la modifica dei diritti e le impostazioni sui documenti sono consentiti esclusivamente agli amministratori del sistema.

I diversi livelli di autorizzazione sono assegnati agli utenti dal RSP, in base alle indicazioni fornite dai Responsabili dei servizi di appartenenza.

Gli accessi esterni a documenti, dati e informazioni non divulgabili sono subordinati alla registrazione sul sistema e al possesso di apposite credenziali, rilasciate previa identificazione diretta da parte di un dipendente abilitato.

Gli accessi esterni a documenti, dati e informazioni divulgabili sono consentiti anche senza autenticazione all’accesso, garantendo comunque il diritto alla riservatezza e all’oblio, e la tutela dei dati personali in conformità alle disposizioni vigenti.

Gli accessi esterni vengono di norma gestiti attraverso il sito web dell’Ente. I dati in libera consultazione vengono esposti in formato aperto (con dovute eccezioni, indotte anche da considerazioni di carattere tecnico, organizzativo o gestionale) che ne consentano il riutilizzo.

Art. 70 Sicurezza nella formazione dei documenti

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

- l'identificabilità del soggetto che ha formato il documento e l'amministrazione/AOO di riferimento;
- la sottoscrizione dei documenti informatici, quando prescritta, con firma digitale ai sensi delle vigenti norme tecniche;
- l'idoneità dei documenti ad essere gestiti mediante strumenti informatici e ad essere registrati mediante il protocollo informatico;
- l'accesso ai documenti informatici tramite sistemi informativi automatizzati;
- la leggibilità dei documenti nel tempo;
- l'interscambiabilità dei documenti all'interno della stessa AOO e con AOO diverse.

I documenti sono prodotti con prodotti di office automation o, a regime, con l'ausilio dell'applicativo che possiede i requisiti di leggibilità, interscambiabilità, non alterabilità, immutabilità nel tempo del contenuto e della struttura. Si adottano preferibilmente i formati PDF/A, XML, TIFF.

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

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

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

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

Art. 71 Trasmissione ed interscambio dei documenti informatici

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

Al fine di tutelare la riservatezza dei dati personali, i dati, i certificati ed i documenti trasmessi all'interno della AOO o ad altre pubbliche amministrazioni, contengono soltanto le informazioni relative a stati, fatti e qualità personali di cui è consentita la diffusione e che sono strettamente necessarie per il perseguimento delle finalità per le quali vengono trasmesse.

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

- accesso all'indice dei gestori di posta elettronica certificata allo scopo di verificare l'integrità del messaggio e del suo contenuto;
- tracciamento delle attività nel file di log della posta;
- gestione automatica delle ricevute di ritorno.

Lo scambio per via telematica di messaggi protocollati tra AOO di amministrazioni diverse presenta, in generale, esigenze specifiche in termini di sicurezza, quali quelle connesse con la protezione di categorie particolari di dati (dati sensibili) e/o giudiziari come previsto dal Reg. UE 2016/679 (GDPR) e dal D.Lgs. 196/03 come novellato dal D.Lgs. 101/18.

Per garantire alla AOO ricevente la possibilità di verificare l'autenticità della provenienza, l'integrità del messaggio e la riservatezza del medesimo, viene utilizzata la tecnologia di firma digitale a disposizione delle amministrazioni coinvolte nello scambio dei messaggi.

Art. 72 Accesso ai documenti informatici

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

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

Ciascun utente del PdP può accedere solamente ai documenti che sono stati assegnati al suo UOR, o agli Uffici Utente (UU) ad esso subordinati.

Il sistema consente altresì di associare un livello differente di riservatezza per ogni tipo di documento trattato dall'amministrazione.

9. NORME TRANSITORIE E FINALI

Art. 73 Pubblicità del manuale

Il Manuale, è reso disponibile a tutto il personale dell'AOO tramite il sistema di gestione documentale; viene pubblicato sul sito istituzionale del FNOPO nella sezione "Amministrazione trasparente".

10. ALLEGATI

Il testo degli allegati è riportato nei file in formato pdf contraddistinti dal seguente titolo.

Allegato n. 1 Titolario piano di classificazione

Allegato n. 2 Manuale d'uso protocollo informatico