

MANUALE DI GESTIONE DEI FLUSSI DOCUMENTALI E DEL PROTOCOLLO INFORMATICO DELL'ISTITUTO NAZIONALE DI RICERCA METROLOGICA

Questo manuale è stato redatto sulla base del modello elaborato nell'ambito del progetto Procedamus, (www.procedamus.it) adattato alle "Linee Guida sulla formazione, gestione e conservazione dei documenti informatici", emanate da AgID il 9 settembre 2020, ai sensi dell'art 71 del CAD (D. lgs. Del 7/03/2005 n. 82).

III. ABBREVIAZIONI

All'interno del presente Manuale saranno utilizzate una serie di sigle e/o abbreviazioni: di seguito viene riportato, in ordine alfabetico, il riepilogo di quelle maggiormente ricorrenti, alcune delle quali oggetto di ulteriori dettagli nel successivo paragrafo "definizioni".

AgID: Agenzia per l'Italia digitale

AOO: Area Organizzativa Omogenea;

CAD: Codice Amministrazione Digitale (D.lgs. 7 marzo 2005, n. 82, e successive integrazioni);

CGD – Coordinatore della Gestione Documentale

CIRC 27: Circolare AIPA del 16 febbraio 2001 n. 27;

CIRC 28: Circolare AIPA del 7 maggio 2001 n. 28;

CODPRI: Codice in materia di Protezione dei dati personali (D.lgs. 30 giugno 2003, n. 196);

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: "General Data Protection Regulation". Regolamento (UE) № 679/2016 del Parlamento Europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE.

IPA: Indice delle Pubbliche Amministrazioni;

PdA (AiP): Pacchetto di Archiviazione.

PdD (DiP): Pacchetto di Distribuzione.

PdV (SiP): Pacchetto di Versamento.

PEC: Posta Elettronica Certificata;

PEI: Posta Elettronica Istituzionale;

PI: Protocollo Informatico;

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

RPA: Responsabile del Procedimento Amministrativo; il dipendente che ha la responsabilità dell'esecuzione degli adempimenti amministrativi relativi ad un affare

SdP: Servizio per la tenuta del Protocollo informatico, della gestione, dei flussi documentali e degli archivi;

TUDA: Decreto del Presidente della Repubblica del 28 dicembre 2000 n.445- Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa;

UO: Unità Organizzativa.

UOP - Unità Organizzative di registrazione di Protocollo - rappresentano gli uffici che svolgono attività di registrazione di protocollo;

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

IV. DEFINIZIONI

Si riportano di seguito le sintetiche definizioni dei principali termini e concetti discendenti dall'applicazione della normativa inerente al protocollo informatico, che saranno oggetto di più approfondita trattazione all'interno del presente Manuale.

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.

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.

La AOO mette a disposizione delle Unità Organizzative dipendenti il servizio di protocollo dei documenti in entrata ed in uscita, utilizzando un'unica sequenza numerica propria della AOO stessa ed il servizio per la gestione documentale elettronica.

Archivio

Complesso dei documenti prodotti o acquisiti da un soggetto pubblico o privato durante lo svolgimento della propria attività; è la raccolta ordinata e sistematica degli atti e dei documenti, ricevuti, spediti, inviati o comunque formati dall'Amministrazione nell'esercizio delle funzioni attribuitegli dalla legge o da regolamenti, per il conseguimento dei propri fini istituzionali.

Pur considerando che l'archivio è unico per ogni AOO, per motivi tecnico-organizzativi e di responsabilità, viene convenzionalmente suddiviso in tre entità: corrente, di deposito e storica.

Archivio informatico

Archivio costituito da documenti informatici, organizzati in aggregazioni documentali informatiche.

Archiviazione elettronica

Processo di memorizzazione, su un qualsiasi idoneo supporto, di documenti informatici univocamente identificati mediante un codice di riferimento, antecedente all'eventuale processo di conservazione.

Assegnazione di un documento

Individuazione di un responsabile del procedimento amministrativo cui affidare un documento in gestione, ai sensi degli artt. 5 e 6 della L. 7 agosto 1990, n. 241.

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.

Casella di Posta Elettronica Istituzionale (PEI)

La PEI è la casella di posta elettronica "funzionale di Ente".

Casella di Posta Elettronica Certificata (PEC)

La PEC fornisce un servizio di messaggistica che sfrutta gli standard propri della posta elettronica assicurando al mittente l'attestazione di avvenuta ricezione del messaggio e al destinatario la garanzia dell'identità del mittente. La PEC istituzionale è strettamente connessa all'Indice delle Pubbliche Amministrazioni (IPA), ove sono pubblicati gli indirizzi di posta certificata associati alle AOO e alle funzioni organizzative previste dalle Pubbliche Amministrazioni.

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.

Dato anonimo

Dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile.

Dato personale

Qualunque informazione relativa a persona fisica, identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale.

Dato particolare

Qualunque dato personale, genetico o biometrico relativo allo stato di salute, o comunque idoneo a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché l'orientamento sessuale (art. 9 del GDPR).

Dati giudiziario

I dati personali idonei a rivelare provvedimenti di cui all'art. 10 del GDPR, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale.

Destinatario

Soggetto o sistema al quale il documento informatico è indirizzato.

Digest

Vedi Impronta crittografica.

Digitalizzazione

Trasposizione numerica delle immagini relative ad una pagina di un documento. È anche definita “scannerizzazione”, “scansione”, “acquisizione di immagini”.

Documenti da protocollare

Sono oggetto di registrazione obbligatoria i documenti ricevuti e spediti dall'amministrazione e tutti i documenti informatici. Ne sono esclusi le gazzette ufficiali, i bollettini ufficiali e i notiziari della pubblica amministrazione, le note di ricezione delle circolari e altre disposizioni, i materiali statistici, gli atti preparatori interni, i giornali, le riviste, i libri, i materiali pubblicitari, gli inviti a manifestazione e tutti i documenti già soggetti a registrazione particolare dell'amministrazione.

Documento amministrativo

Ogni rappresentazione, comunque formata, del contenuto di atti, anche interni o non relativi ad uno specifico procedimento, detenuti da una pubblica amministrazione e concernenti attività di pubblico interesse, indipendentemente dalla natura pubblicistica o privatistica della loro disciplina sostanziale (art. 22 L. 241/90).

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

Documenti a trattazione particolare

Rientrano in questa categoria i documenti che contengono dati personali, dati particolari e dati giudiziari.

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

Documento analogico

Rappresentazione non informatica di atti, fatti o dati giuridicamente rilevanti.

Duplicato informatico Vedi art. 1, comma 1, lett. i) quinquies del CAD.

eSeal

Vedi sigillo elettronico.

Esibizione

Operazione che consente di visualizzare un documento conservato

eSignature

Vedi firma elettronica.

Estratto di documento informatico

Parte del documento tratto dal documento originale

Estratto per riassunto di documento informatico

Documento nel quale si attestano in maniera sintetica fatti, stati o qualità desunti da documenti informatici.

Estrazione statica dei dati

Estrazione di informazioni utili da grandi quantità di dati (es. database, datawarehouse, ecc.), attraverso metodi automatici o semi-automatici

Evidenza informatica

Sequenza finita di bit che può essere elaborata da una procedura informatica.

Fascicolo

Il "fascicolo" è l'insieme ordinato di documenti, relativi ad uno stesso procedimento amministrativo/materia/tipologia, che si forma nel corso dell'attività amministrativa, allo scopo di riunire tutti i documenti utili per il procedimento stesso.

Fascicolo informatico

Aggregazione documentale informatica strutturata e univocamente identificata contenente atti, documenti o dati informatici prodotti e funzionali all'esercizio di una attività o allo svolgimento di uno specifico procedimento.

File

Insieme di informazioni, dati o comandi logicamente correlati, raccolti sotto un unico nome e registrati, per mezzo di un programma di elaborazione o di scrittura, nella memoria di un computer.

File container

Vedi Formato contenitore.

File wrapper

Vedi Formato contenitore.

File-manifesto

File che contiene metadati riferiti ad un file o ad un pacchetto di file.

Filesystem

Sistema di gestione dei file, strutturato mediante una o più gerarchie ad albero, che determina le modalità di assegnazione dei nomi, memorizzazione e organizzazione all'interno di uno storage.

Firma digitale

La firma digitale è un particolare tipo di firma elettronica qualificata basata su un sistema di chiavi asimmetriche a coppia, una pubblica e una privata, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici.

Firma elettronica

Dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati elettronici e utilizzati dal firmatario per firmare;

Firma elettronica avanzata

Una firma elettronica avanzata soddisfa i seguenti requisiti:

- a) è connessa unicamente al firmatario;
- b) è idonea a identificare il firmatario;
- c) è creata mediante dati per la creazione di una firma elettronica che il firmatario può, con un elevato livello di sicurezza, utilizzare sotto il proprio esclusivo controllo;

d) è collegata ai dati sottoscritti in modo da consentire l'identificazione di ogni successiva modifica di tali dati.

Firma elettronica qualificata

E' una firma elettronica avanzata, creata da un dispositivo per la creazione di una firma elettronica qualificata e basata su un certificato qualificato per firme elettroniche.

Flusso (binario)

Sequenza di bit prodotta in un intervallo temporale finito e continuativo che ha un'origine precisa ma di cui potrebbe non essere predeterminato il suo istante di interruzione.

Formato contenitore

Formato di file progettato per consentire l'inclusione ("imbustamento" o wrapping), in uno stesso file, di una o più evidenze informatiche soggette a differenti tipi di codifica e al quale possono essere associati specifici metadati.

Formato del documento informatico

Modalità di rappresentazione della sequenza di bit che costituiscono il documento informatico; comunemente è identificato attraverso l'estensione del file.

Formato "deprecato"

Formato in passato considerato ufficiale il cui uso è attualmente sconsigliato a favore di una versione più recente.

Funzioni aggiuntive del protocollo informatico

Nel sistema di protocollo informatico, componenti supplementari rispetto a quelle minime, necessarie alla gestione dei flussi documentali, alla conservazione dei documenti nonché alla accessibilità delle informazioni.

Funzioni minime del protocollo informatico

Componenti del sistema di protocollo informatico che rispettano i requisiti di operazioni ed informazioni minime di cui all'articolo 56 del D.P.R. 28 dicembre 2000, n. 445.

Funzione di hash crittografica

Funzione matematica che genera, a partire da una evidenza informatica, una impronta crittografica o digest (vedi) in modo tale che risulti computazionalmente difficile (di fatto impossibile), a partire da questa, ricostruire l'evidenza informatica originaria e generare impronte uguali a partire da evidenze informatiche differenti.

Gestione Documentale

Processo finalizzato al controllo efficiente e sistematico della produzione, ricezione, tenuta, uso, selezione e conservazione dei documenti.

Hash

Termine inglese usato, impropriamente, come sinonimo d'uso di "impronta crittografica" o "digest" (vedi).

Identificativo univoco

Sequenza di numeri o caratteri alfanumerici associata in modo univoco e persistente ad un'entità all'interno di uno specifico ambito di applicazione.

Impronta crittografica

Sequenza di bit di lunghezza predefinita, risultato dell'applicazione di una funzione di hash crittografica a un'evidenza informatica.

Integrità

Caratteristica di un documento informatico o di un'aggregazione documentale in virtù della quale risulta che essi non hanno subito nel tempo e nello spazio alcuna alterazione non autorizzata. La caratteristica dell'integrità, insieme a quella della completezza, concorre a determinare la caratteristica dell'autenticità.

Interoperabilità

Caratteristica di un sistema informativo, le cui interfacce sono pubbliche e aperte, e capaci di interagire in maniera automatica con altri sistemi informativi per lo scambio di informazioni e l'erogazione di servizi.

Leggibilità

Caratteristica di un documento informatico che garantisce la qualità di poter essere decodificato e interpretato da un'applicazione informatica.

Manuale di conservazione

Documento informatico che descrive il sistema di conservazione e illustra dettagliatamente l'organizzazione, i soggetti coinvolti e i ruoli svolti dagli stessi, il modello di funzionamento, la descrizione del processo, la descrizione delle architetture e delle infrastrutture.

Manuale di gestione

Documento informatico che descrive il sistema di gestione, anche ai fini della conservazione, dei documenti informatici e fornisce le istruzioni per il corretto funzionamento del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi.

Metadati

Dati associati a un o documento informatico, a un fascicolo informatico o a un'aggregazione documentale per identificarli, descrivendone il contesto, il contenuto e la struttura - così da permetterne la gestione del tempo - in conformità a quanto definito nella norma ISO 15489-1:2016 e più nello specifico dalla norma ISO 23081-1:2017.

Naming convention

Vedi Convenzioni di denominazione

Oggetto di conservazione

Oggetto digitale versato in un sistema di conservazione.

Oggetto digitale

Oggetto informativo digitale, che può assumere varie forme tra le quali quelle di documento informatico, fascicolo informatico, aggregazione documentale informatica o archivio informatico.

Pacchetto di archiviazione

Pacchetto informativo generato dalla trasformazione di uno o più pacchetti di versamento coerentemente con le modalità riportate nel manuale di conservazione.

Pacchetto di distribuzione

Pacchetto informativo inviato dal sistema di conservazione all'utente in risposta ad una sua richiesta di accesso a oggetti di conservazione.

Pacchetto di file (file package)

Insieme finito di più file (possibilmente organizzati in una struttura di sottoalbero all'interno di un filesystem) che costituiscono, collettivamente oltre che individualmente, un contenuto informativo unitario e auto-consistente.

Pacchetto di versamento

Pacchetto informativo inviato dal produttore al sistema di conservazione secondo il formato descritto nel manuale di conservazione.

Pacchetto informativo

Contenitore logico che racchiude uno o più oggetti di conservazione con i relativi metadati, oppure anche i soli metadati riferiti agli oggetti di conservazione.

Path

Percorso (vedi).

Pathname

Concatenazione ordinata del percorso di un file e del suo nome.

Percorso

Informazioni relative alla localizzazione virtuale del file all'interno del filesystem espressa come concatenazione ordinata del nome dei nodi del percorso.

Piano della sicurezza del sistema di conservazione

Documento che, nel contesto del piano generale di sicurezza, descrive e pianifica le attività volte a proteggere il sistema di conservazione dei documenti informatici da possibili rischi.

Piano della sicurezza del sistema di gestione Informatica dei documenti

Documento che, nel contesto del piano generale di sicurezza, descrive e pianifica le attività volte a proteggere il sistema di gestione informatica dei documenti da possibili rischi.

Piano di classificazione (Titolario)

Struttura logica che permette di organizzare documenti e oggetti digitali secondo uno schema desunto dalle funzioni e dalle attività dell'amministrazione interessata.

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.

Procedimento amministrativo

Modello di processo istituzionalmente eseguito da una amministrazione pubblica o da soggetti privati preposti all'esercizio di attività amministrative. Con il termine procedimento si intendono in senso allargato non solo i procedimenti ai sensi della L. 241/90, ma più in generale qualsiasi tipo di modello di processo amministrativo.

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.

Protocollo

Fase del processo di gestione documentale che certifica provenienza/destinazione e data certa di acquisizione/trasmissione del documento, mediante la sua identificazione univoca nell'ambito di una sequenza numerica collegata con l'indicazione temporale.

qSeal

Sigillo elettronico qualificato, come da art. 35 del Regolamento eIDAS.

qSignature

Firma elettronica qualificata, come da art. 25 del Regolamento eIDAS.

Rapporto di versamento (RdV)

Documento informatico che attesta l'avvenuta presa in carico da parte del sistema di conservazione dei pacchetti di versamento inviati dal produttore.

Registrazione di protocollo

La registrazione di protocollo per ogni documento ricevuto o spedito dalle pubbliche amministrazioni è effettuata mediante la memorizzazione delle seguenti informazioni:

- a) numero di protocollo del documento 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 per i documenti ricevuti o, in alternativa, il destinatario o i destinatari per i documenti spediti, registrati in forma non modificabile;
- d) oggetto del documento, registrato in forma non modificabile;
- e) data e protocollo del documento ricevuto, se disponibili;

f) l'impronta del documento informatico, se trasmesso per via telematica, costituita dalla sequenza di simboli binari in grado di identificarne univocamente il contenuto, registrata in forma non modificabile.

Registro di emergenza

Supporto alternativo su cui vengono riportate manualmente le registrazioni di protocollo nel caso di malfunzionamenti che rendano impossibile l'utilizzo della normale procedura automatica.

Registro di protocollo

Registro informatico ove sono memorizzate le informazioni prescritte dalla normativa per tutti i documenti ricevuti e spediti da un ente e per tutti i documenti informatici dell'ente stesso.

Registro particolare

Registro informatico individuato da una pubblica amministrazione per la memorizzazione delle informazioni relative a documenti soggetti a registrazione particolare.

Regolamento eIDAS (electronic IDentification Authentication and Signature)

Regolamento (UE) N° 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 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.

Responsabile del Procedimento Amministrativo (RPA)

È la persona cui è affidata la trattazione di un affare amministrativo, ivi compresa la gestione/creazione del relativo fascicolo dell'archivio corrente.

È la figura che ha la responsabilità del documento assegnatogli nella fase preparatoria se si tratta di un documento in partenza, ovvero che ne è responsabile della conservazione in caso di documento in arrivo.

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 del Servizio per la tenuta del protocollo informatico, dei flussi documentali e degli archivi (RdS) - (art. 61 DPR)

È la figura responsabile di tutte le operazioni di registrazione, di protocollo, di organizzazione e tenuta dei documenti all'interno della AOO stessa. Garantisce il corretto funzionamento, a norma di legge, del sistema di PI implementato nell'AOO anche nei confronti dei cittadini/ditte/altre PA.

Responsabile del servizio di conservazione

Soggetto che coordina il processo di conservazione all'interno del conservatore.

Responsabile della sicurezza dei sistemi di conservazione

Soggetto che assicura il rispetto dei requisiti di sicurezza all'interno del conservatore.

Responsabile dei sistemi informativi per la conservazione

Soggetto che coordina i sistemi informativi all'interno del conservatore.

Responsabile dello sviluppo e della manutenzione del sistema di conservazione

Soggetto che assicura lo sviluppo e la manutenzione del sistema all'interno del conservatore.

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 storicoculturale.

Segnatura di protocollo

L'apposizione o l'associazione all'originale del documento, in forma permanente e non modificabile degli elementi di identificazione riguardanti il documento stesso. Ciò per consentire di individuare in modo inequivocabile ciascun documento.

Serie

Raggruppamento di documenti con caratteristiche omogenee (vedi anche aggregazione documentale informatica).

Sidecar (file)

File-manifesto (vedi).

Sigillo elettronico

Dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati in forma elettronica, per garantire l'origine e l'integrità di questi ultimi.

Sistema di conservazione

Insieme di regole, procedure e tecnologie che assicurano la conservazione dei documenti informatici in attuazione a quanto previsto dall'art. 44, comma 1, del CAD

Sistema di gestione informatica dei documenti

L'insieme delle risorse di calcolo, degli apparati, delle reti di comunicazione e delle procedure informatiche utilizzati dalle amministrazioni per la gestione dei documenti

Segnatura di protocollo

L'apposizione o l'associazione, all'originale del documento, in forma permanente e non modificabile delle informazioni riguardanti il documento stesso.

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 della pubblica amministrazione è il sistema di cui all'articolo 52 del D.P.R. 28 dicembre 2000, n. 445

Timeline

Linea temporale virtuale su cui sono disposti degli eventi relativi ad un sistema informativo o a un documento informatico. Costituiscono esempi molto diversi di timeline un file di log di sistema, un flusso multimediale contenente essenze audio/video sincronizzate.

Titolare dell'oggetto di conservazione

Soggetto produttore degli oggetti di conservazione.

Trasferimento

Passaggio di custodia dei documenti da una persona o un ente ad un'altra persona o un altro ente.

Titolario di classificazione

Il titolare di classificazione si applica all'archivio corrente, ovvero all'insieme dei documenti usati per sbrigare gli affari in corso; è un quadro di classificazione articolato in categorie ed eventualmente in ulteriori sottopartizioni, in base al quale i documenti dell'archivio corrente vengono raggruppati secondo un ordine logico.

Unità Organizzativa (UO)

Per Unità Organizzativa si intende uno dei sottoinsiemi dell'Area Organizzativa Omogenea rappresentato da un complesso di risorse umane e strumentali cui sono affidate competenze omogenee nella trattazione di procedimenti amministrativi.

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

V. SOMMARIO

I. ATTO DI APPROVAZIONE.....	2
II. REGISTRAZIONE DELLE AGGIUNTE E VARIANTI.....	2
III. ABBREVIAZIONI	3
IV. DEFINIZIONI.....	5
V. SOMMARIO	16
CAPITOLO 1 - IL MANUALE DI GESTIONE	21
1.1. Scopo del Manuale di Gestione.....	21
1.2. Norme di riferimento inerenti il protocollo informatico.....	21
1.3. Modalità di redazione	23
1.4. Forme di pubblicità e di divulgazione	23
CAPITOLO 2 - QUADRO ORGANIZZATIVO ISTITUZIONALE	24
2.1. Area organizzativa omogenea e unità organizzativa responsabile	24
2.1.1. Elenco AOO - UOR	24
2.2. Servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi: compiti	25
2.3. Responsabile della gestione documentale	25
2.4. Profili di abilitazione alle informazioni del sistema di gestione documentale	27
2.5. Indirizzi di Posta Elettronica Istituzionale e di Posta Elettronica Certificata (PEC)	28
2.6. Responsabile della conservazione	28
CAPITOLO 3 - IL DOCUMENTO AMMINISTRATIVO.....	29
3.1. Documento informatico e analogico: definizione e disciplina giuridica	29
3.1.1. Valore probatorio del documento informatico sottoscritto	31
3.2. Redazione/formazione del documento amministrativo informatico	32
3.2.1. Validazione temporale	33
3.2.2. Formati.....	34
3.3. Redazione/formazione del documento amministrativo analogico	35
3.4. Il documento amministrativo informatico costituito dal corpo della PEC istituzionale	36
3.5. Il documento amministrativo informatico costituito dal corpo della e-mail istituzionale.....	36
3.7. Duplicato, copia ed estratto di documenti amministrativi informatici.....	38
3.7.1. Duplicato del documento amministrativo informatico	38
3.7.2. Copia o estratto di un documento amministrativo informatico.....	38
3.7.3. Duplicato di un documento amministrativo analogico o informatico.....	39
3.7.4. Copia informatica di un documento analogico	39
3.7.5. Estratto informatico di documento amministrativo informatico	40

3.7.6. Copia analogica di documento amministrativo informatico	41
3.8. Metadati associati ai documenti informatici e ai documenti amministrativi informatici.....	41
3.8.1. Metadati associati al documento informatico	41
3.8.2 Ulteriori metadati associati al registro delle fatture e degli altri documenti contabili equivalenti .	46
3.8.3 Metadati associati al documento amministrativo informatico	47
CAPITOLO 4 - IL FASCICOLO.....	52
4.1. Il fascicolo: tipologie	52
4.2. Il fascicolo analogico: formazione, implementazione, gestione e buone prassi.....	53
4.3. Raccoglitore	54
4.4. Il fascicolo informatico: formazione, implementazione, gestione e buone prassi.....	54
4.5. I fascicoli annuali ripetitivi	55
4.6. Il fascicolo ibrido.....	55
4.8. Il repertorio dei fascicoli informatici.....	56
4.9 Metadati associati ai fascicoli, alle serie dei fascicoli e alle altre aggregazioni documentali informatiche	56
CAPITOLO 5 - L'ARCHIVIO.....	60
5.1 L'archivio e la gestione documentale	60
CAPITOLO 6 - LA GESTIONE DELL'ARCHIVIO CORRENTE.....	61
6.1. Definizione	61
6.2. Gli strumenti della fase corrente	61
6.2.1. Registro di protocollo.....	61
6.2.2. Titolario (piano di classificazione).....	61
6.3. Registri e repertori informatici.....	62
6.3.1 Repertorio - Nozione	62
6.3.2. Repertori attivi	63
6.3.3. Repertorio dei fascicoli.....	64
6.4. Massimario di selezione	64
6.5. Spostamento di un archivio corrente analogico	65
CAPITOLO 7. – IL PROTOCOLLO INFORMATICO	66
7.1. La registrazione e la segnatura di protocollo.....	66
7.2 Registratura	67
7.3. Data e ora regolate sul UTC	67
7.4. Segnatura.....	67
7.4.1. Segnatura del documento informatico	67
7.4.2. Segnatura del documento analogico	68
7.5. Modalità di produzione e di conservazione delle registrazioni	68
7.6. La registrazione differita (o “protocollo differito”)	69

7.7. La ricevuta di avvenuta registrazione	69
7.7.1. La ricevuta di avvenuta registrazione del documento analogico	69
7.7.2. La ricevuta di avvenuta registrazione del documento informatico	70
7.8. Documenti esclusi dalla registrazione di protocollo.....	70
7.9. Il registro giornaliero di protocollo.....	71
7.10. Il registro di emergenza	72
7.11. Il Protocollo particolare	73
CAPITOLO 8 - FLUSSO DI LAVORAZIONE DEI DOCUMENTI	75
8.1. Distinzione dei documenti in base allo stato di trasmissione	75
8.2. Flusso del documento informatico in arrivo	76
8.2.1. Ricezione di documenti informatici nella casella di posta elettronica istituzionale.....	76
8.2.2. Ricezione dei documenti informatici tramite la casella di posta elettronica certificata (PEC) istituzionale.....	77
8.2.3. Ricezione di documenti informatici su supporti rimovibili	77
8.3 Flusso del documento analogico in arrivo	78
8.3.1. Ricezione di documenti cartacei a mezzo posta convenzionale (Poste italiane spa e di altri gestori autorizzati).....	78
8.3.2. Apertura delle buste	78
8.3.3. Conservazione ed eliminazione delle buste	79
8.3.4. Ricezione di documenti cartacei a mezzo fax	79
8.4. Priorità nella registrazione dei documenti informatici in arrivo	79
8.5. Casi di rigetto	80
8.6. Flusso del documento in partenza.....	80
8.6.1.Redazione, registrazione e spedizione di documenti analogici cartacei aventi per destinatario un soggetto terzo a mezzo posta convenzionale o telefax.....	80
8.6.2. Registrazione a protocollo di documenti analogici cartacei	80
8.6.3.Redazione, registrazione e spedizione di documenti analogici cartacei aventi per destinatario un ente o soggetto terzo a mezzo posta convenzionale o telefax	81
8.6.4. Redazione, registrazione e spedizione di documenti informatici	81
8.7. Flusso del documento informatico tra UOR della stessa AOO.....	82
8.8. Utilizzo delle firme elettroniche: firma elettronica semplice, firma elettronica avanzata, firma elettronica qualificata, firma digitale	83
8.9. Annullamento di una registrazione	83
8.10. Corresponsabilità di un documento e di un fascicolo.....	84
8.11. Comunicazione tra AOO di documenti amministrativi protocollati	85
CAPITOLO 9 - CASISTICA E COMPORTAMENTI.....	87
9.1. Gestione delle gare d'appalto	87
9.1.1. Gare e procedure negoziate gestite in modalità analogica. Presentazione delle offerte per gare ad evidenza pubblica	87

9.1.2. Gare e procedure negoziate gestite in modalità telematica.....	87
9.2. Gestione di concorsi e selezioni	87
9.3. Atti giudiziari	88
9.3.1. Notifiche.....	88
9.3.2. Comunicazioni.....	89
9.4. Documenti informatici con oggetto multiplo	89
9.5. Fatture elettroniche (Fattura PA)	89
9.6. DURC on-line	90
9.7. Denunce di infortuni	91
9.8. Certificati di malattia.....	91
9.9. Documenti del portale degli acquisti della pubblica amministrazione.....	91
9.9.1. Affidamenti diretti sulla piattaforma MePA. (Ordini diretti di acquisto OdA).....	92
9.9.2. Adesioni – Convenzioni MePA (Ordini diretti di acquisto OdA).....	93
9.9.3. Procedure negoziate MePA (Richiesta di offerta RdO)	93
9.10. Documenti pervenuti via PEC.....	94
9.10.1. Gestione di due documenti diversi trasmessi via PEC.....	94
9.10.2. Messaggio di PEC e allegati documenti di firmatari diversi	94
9.10.3. Gestione di soli allegati pervenuti via PEC e di documenti costituiti dal solo corpo della PEC.....	95
9.11. Documenti pervenuti a mezzo e- mail semplice (non certificata).....	95
9.12. Gestione del secondo esemplare	95
9.13. Documenti anonimi.....	96
9.14. Lettere prive di firma.....	96
9.15. Documenti informali scambiati tra UOR della stessa AOO	96
9.16. Lettere personali.....	96
9.17. Ricezione di documenti informatici su supporti rimovibili	97
CAPITOLO 10 - DALL'ARCHIVIO CORRENTE ALL'ARCHIVIO DI DEPOSITO	98
10.1. Archivio di deposito	98
10.2. Elenco di consistenza per l'archivio di deposito dei documenti analogici	100
10.3 Trasferimento dei fascicoli cartacei	100
10.4. Trasferimento dei fascicoli informatici.....	100
10.5. Trasferimento delle serie archivistiche	101
10.6. Ordinamento archivistico	101
10.7. Conservazione	102
CAPITOLO 11. IL SISTEMA INFORMATICO.....	106
11.1. Il modello organizzativo.....	106
11.2. Piano di sicurezza del sistema informatico	107
11.2.1. Il sistema di gestione documentale	107

11.2.2. Sicurezza fisica dei data center	107
11.2.3. La manutenzione e la continuità operativa degli impianti elettrici.....	108
11.2.4. Rete dati	108
11.2.5. Le postazioni di lavoro.....	108
11.2.6. La sicurezza delle postazioni di lavoro per lo smart working	109
11.3. Sicurezza dei documenti informatici	110
11.3.1. Accesso ai dati e ai documenti informatici	111
11.3.2. Le procedure comportamentali ai fini della protezione dei documenti	112

ALLEGATI

Allegato 1. RIFERIMENTI NORMATIVI UTILIZZATI PER LA REDAZIONE DEL PRESENTE MANUALE.

Allegato 2. TITOLARIO DI CLASSIFICAZIONE

Allegato 3. PIANO DI ORGANIZZAZIONE DELLE AGGREGAZIONI DOCUMENTALI

Allegato 4. MASSIMARIO DI SELEZIONE E SCARTO

Allegato 5. MANUALE DI CONSERVAZIONE

CAPITOLO 1 - IL MANUALE DI GESTIONE

1.1. Scopo del Manuale di Gestione

Il Manuale di gestione dei flussi documentali e del protocollo informatico serve a indicare le procedure e a fornire le istruzioni per la corretta formazione, gestione, tenuta e conservazione della documentazione analogica e digitale.

Esso descrive, altresì, le modalità di gestione dei flussi documentali e degli archivi, in modo tale da organizzare e governare la documentazione ricevuta, inviata o comunque prodotta dall'amministrazione secondo parametri di corretta registrazione di protocollo, smistamento, assegnazione, classificazione, fascicolatura, reperimento e conservazione dei documenti.

Questo strumento ha lo scopo di analizzare i processi del workflow documentale e presentare i criteri e i metodi impiegati nel controllo dei processi del sistema di gestione documentale; pertanto sono qui descritte le attività di formazione, registrazione, classificazione, fascicolazione ed archiviazione dei documenti, oltre alla gestione dei flussi documentali ed archivistici in relazione ai procedimenti amministrativi dell'INRiM.

1.2. Norme di riferimento inerenti il protocollo informatico

La normativa inerente al protocollo informatico è piuttosto vasta: di seguito è riportato il riepilogo sintetico dei soli riferimenti di maggior rilevanza per la materia, indicati in ordine cronologico e con le relative abbreviazioni tra parentesi quadre; tali norme sono da intendersi comprensive delle aggiunte, varianti e correzioni intervenute nel tempo.

- Legge 7 agosto 1990, n. 241 – “Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi”. È la norma di riferimento che detta la disciplina del procedimento amministrativo e del diritto di accesso ai documenti amministrativi.
- Decreto del Presidente della Repubblica del 20 ottobre 1998, n. 428 [DPR 428/98] - “Regolamento recante norme per la gestione del protocollo informatico da parte delle pubbliche amministrazioni, pubblicato sulla Gazzetta Ufficiale n. 291 del 14 dicembre 1998”. È stato il primo atto ad introdurre la normativa inerente al protocollo informatico, dettando regole tecniche ed organizzative per la relativa implementazione. In tale decreto veniva fissato, per la prima volta, il termine del 1 gennaio 2004 per l'avvio di sistemi di protocollo informatico per le pubbliche amministrazioni. È stato abrogato dal DPR 445/2000 che ne ha recepito i contenuti.
- Decreto del Presidente del Consiglio dei Ministri del 31 ottobre 2000 [DPCM] - “Regole tecniche per il Protocollo Informatico di cui al DPR 428/98”. In attuazione di alcune disposizioni contenute nel DPR 428/98 (successivamente abrogato dal DPR 445/2000) è stato emanato il DPCM 31 ottobre 2000 che indica, nel dettaglio, le regole tecniche per l'attuazione della normativa. Il DPCM del 31 ottobre 2000 è stato abrogato nel 2020, salve le disposizioni presenti a:
 - 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.
- Decreto del Presidente della Repubblica del 28 dicembre 2000, n. 445 [DPR] - "Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa". Il DPR costituisce il documento di riferimento principale per il Protocollo Informatico. Con esso si effettua una razionalizzazione e semplificazione della normativa: con l'art. 77 viene abrogato, tra gli altri, il DPR 428/98, del quale il DPR recepisce pressoché integralmente le disposizioni normative; la normativa inerente al Protocollo Informatico viene semplificata e raggruppata negli articoli dal 50 al 70 del presente DPR.
 - Circolare AIPA del 16 febbraio 2001, n. AIPA/CR/27 [CIRC 27] - inerente "l'utilizzo della firma digitale nella Pubblica Amministrazione" (art. 17 del DPR del 10 novembre 1997, n. 513).
 - Circolare AIPA del 7 maggio 2001, n. AIPA/CR/28 [CIRC 28] - inerente "Regole tecniche per l'interoperabilità dei sistemi di protocollo informatico" (art. 18 comma 2 del DPCPM del 31 ottobre 2000).
 - Decreto Legislativo del 30 giugno 2003, n. 196 [CODPRI] - "Codice in materia di protezione dei dati personali".
 - Direttiva SMD-I-004 edizione 2004 [DIR] - Il protocollo informatico nella Difesa".
 - Decreto del Presidente della Repubblica del 11 febbraio 2005, n.68 - "Regolamento recante disposizioni per l'utilizzo della posta elettronica certificata a norma dell'articolo 27 della legge 16 gennaio 2003, n. 3."
 - Decreto Legislativo del 7 marzo 2005, n. 82 [CAD] - "Codice dell'Amministrazione digitale".
 - Direttiva SMA-ORD-040 edizione 2008 – "Norme di gestione dei codici di protocollo in ambito A.M."
 - Decreto del Presidente del Consiglio dei Ministri del 22 febbraio 2013 - "Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali".
 - Direttiva SMA-RGS-020 edizione 2010 - "Sicurezza per i sistemi di telecomunicazione e informatici non classificati dell'Aeronautica Militare (Direttiva di sicurezza per l'Information & Communication Technology)".
 - Decreto del Presidente del Consiglio dei Ministri del 3 dicembre 2013 – "Regole tecniche per il Protocollo Informatico ai sensi degli articoli 40-bis, 41, 47, 57-bis e 71, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005".
 - Direttiva CL-3-DV-014 edizione 2013 "Compiti attribuzione e responsabilità CERT e CIRT".
 - Regolamento UE n. 2016/679 [GDPR] – "Regolamento Generale sulla Protezione dei Dati (General Data Protection Regulation)", in vigore dal 25 maggio 2018.
 - Decreto Legislativo 10 agosto 2018, n. 101 – "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati

personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)”.

- AgID Linee Guida¹ sulla formazione, gestione e conservazione dei documenti informatici; applicabili dal 7 giugno 2021, tali linee guida aboliscono:
 - Circolare Agenzia Italia Digitale (AgID) n. 60 del 23 gennaio 2013 [CIRC] – “Regole tecniche per l’interoperabilità dei sistemi di protocollo informatico”;
 - DPCM del 3 dicembre 2013. Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, 23-ter, 44, 44 –bis, e 71 del Codice dell’amministrazione digitale di cui al decreto legislativo n. 82 del 2005”,
 - DPCM del 13 novembre 2014 – Regole tecniche in materia di formazione / trasmissione/ copia/ duplicazione/riproduzione e validazione temporale dei documenti informatici delle Pubbliche amministrazioni.
 - DPCM 3 dicembre 2013, contenente “Regole tecniche per il protocollo informatico”, fatte salve le disposizioni presenti a:
 - 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.

Nell’Allegato1 sono riportati tutti i riferimenti normativi utili per la redazione del seguente manuale.

1.3. Modalità di redazione

La redazione del manuale di gestione deve contemperare l’assolvimento dell’obbligo normativo e le esigenze concrete dell’Amministrazione. Per tale motivo è stato redatto previa verifica e analisi del modello organizzativo e delle procedure amministrative.

1.4. Forme di pubblicità e di divulgazione

Il manuale di gestione è reso pubblico mediante la diffusione sul sito istituzionale, come previsto dalle *Linee Guida sulla formazione, gestione e conservazione dei documenti informatici emanate dall’ AgID*.

Deve, inoltre, essere capillarmente divulgato alle unità organizzative responsabili (UOR) dell’Ente, al fine di consentire la corretta diffusione delle nozioni e delle procedure documentali.

¹ Come precisato dal Consiglio di Stato - nell’ambito del parere reso sullo schema di decreto legislativo del correttivo al CAD, n. 2122/2017 del 10.10.2017 - le Linee Guida adottate da AgID, ai sensi dell’art. 71 del CAD, hanno carattere vincolante e assumono valenza *erga omnes*.

CAPITOLO 2 - QUADRO ORGANIZZATIVO ISTITUZIONALE

L'articolo 50 c.4 del Decreto del Presidente della Repubblica del 28 dicembre 2000 n.445- Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa [TUDA] prescrive: "Ciascuna amministrazione individua, nell'ambito del proprio ordinamento, gli uffici da considerare ai fini della gestione unica o coordinata dei documenti per grandi aree organizzative omogenee, assicurando criteri uniformi di classificazione e archiviazione, nonché di comunicazione interna tra le aree stesse".

2.1. Area organizzativa omogenea e unità organizzative

L'area organizzativa omogenea (AOO) è l'insieme di funzioni e di strutture individuate dall'amministrazione cui sono assegnate funzioni omogenee. Essa, pertanto, presenta esigenze di gestione documentale in modo unitario e coordinato, ai sensi della normativa vigente.

L'unità organizzativa responsabile (UO) è, all'interno della AOO, un complesso organizzato di risorse umane e strumentali cui è stata affidata una competenza omogenea nell'ambito della quale i dipendenti assumono la responsabilità nella trattazione di affari, attività e procedimenti amministrativi.

2.1.1. Elenco AOO – ORGANIGRAMMA ED ELENCO UO

ELENCO AOO

L'INRiM è organizzato in una AOO unica.

ORGANIGRAMMA ED ELENCO UO dell'Amministrazione

Direzione generale

- **Direzione**
 - Acquisti Tecnici e Lavori
 - Approvvigionamenti
 - Comunicazione
 - Gare e Contratti
 - Pianificazione e Controllo
 - Risorse Economiche
 - Risorse Umane
 - Segreteria Generale
 - Servizio Prevenzione e Protezione
 - Trattamento Economico del Personale
- **Direzione Supporto alla Ricerca e Innovazione**
 - Knowledge Transfer
 - Servizi Metrologici
 - Supporto alla Ricerca
- **Direzione Tecnica**
 - Coordinamento tecnologico
 - Logistica e Manutenzione
 - Servizi Tecnici
 - Sistemi Informatici e Reti

A queste UO amministrative si aggiungono tre Divisioni scientifiche e una Segreteria Scientifica:

- Segreteria Direzione Scientifica
- AE Metrologia applicata e ingegneria
- ML Metrologia dei materiali innovativi e scienze della vita
- QN Metrologia quantistica e nanotecnologie

2.2. Servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi: compiti

La Segreteria Generale, sotto la supervisione del Responsabile della Gestione Documentale (cfr. par. 2.3) si occupa della gestione del ciclo di vita di tutta la documentazione amministrativa prodotta dagli Uffici dell'Ente.

La Segreteria Generale esercita le funzioni previste dagli art. 61 e 62 del TUDA, dall' art. 5 della Deliberazione CNIPA n. 11/2004, e dalle Linee Guida AgID; tali funzioni sono articolate nelle seguenti attività principali:

- ❖ Sviluppo e gestione del protocollo informatico e del sistema di gestione documentale, comprendenti:
 - predisporre lo schema del manuale di gestione del protocollo informatico con la descrizione dei criteri e delle modalità di revisione del medesimo;
 - provvedere alla pubblicazione del manuale sul sito istituzionale dell'amministrazione;
 - garantire il rispetto delle disposizioni normative durante le operazioni di registrazione e di segnatura di protocollo;
 - garantire la corretta conservazione della copia del registro giornaliero di protocollo;
 - sollecitare il ripristino del servizio in caso di indisponibilità del medesimo;
- ❖ Analisi e gestione dei flussi documentali;
- ❖ Conservazione a norma della documentazione amministrativa;
- ❖ Gestione degli archivi.

Ciascuna delle attività sopra elencate sarà descritta nei capitoli successivi del presente manuale.

2.3. Responsabile della gestione documentale

Il Responsabile della gestione documentale è preposto al servizio di cui all'articolo 61 del TUDA²; opera d'intesa con il Responsabile della Conservazione, il Responsabile dei sistemi informativi, il Responsabile dell'ufficio per la transizione al digitale e acquisisce il parere del Responsabile della protezione dei dati personali per l'espletamento dei propri compiti, quali:

² Art 61 c. 2 del D.P.R.445/2000 [TUDA] "Al servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi è preposto un dirigente ovvero un funzionario, comunque in possesso di idonei requisiti professionali o di professionalità tecnico archivistica acquisita a seguito di processi di formazione definiti secondo le procedure prescritte dalla disciplina vigente"

- ❖ predisporre e mantenere aggiornato il manuale di gestione documentale relativo alla formazione, alla gestione, alla trasmissione, all'interscambio, all'accesso ai documenti informatici nel rispetto della normativa in materia di trattamenti dei dati personali ed in coerenza con quanto previsto nel manuale di conservazione
- ❖ predisporre il piano per la sicurezza informatica relativo alla formazione, alla gestione, alla trasmissione, all'interscambio, all'accesso, alla conservazione dei documenti informatici;
- ❖ predisporre le misure di sicurezza prestabilite dall'AgID e dagli altri organismi preposti;
- ❖ predisporre delle disposizioni in materia di protezione dei dati personali in linea con l'analisi del rischio fatta;
- ❖ definire e assicurare criteri uniformi di trattamento dei documenti e di classificazione e archiviazione, nonché di comunicazione interna tra le AOO;
- ❖ produrre il pacchetto di versamento e assicurare il trasferimento del suo contenuto al sistema di conservazione, secondo le modalità operative definite nel manuale di conservazione.

Registro dei Responsabili della gestione documentale dell'INRiM:

Nominativo del Responsabile	Periodo nel ruolo	Deleghe	Periodo nel ruolo	Ambiti oggetto della delega
		Laura Degani	2020	- Redazione del Manuale di gestione e dei suoi allegati.
		Laura Degani	2021	- Studio e redazione del piano delle aggregazioni documentali

2.4. Profili di abilitazione alle informazioni del sistema di gestione documentale

Il sistema documentale Titulus del Consorzio Interuniversitario Cineca, adottato dall'INRiM, attraverso una *access control list* – ACL –permette, in base alle strutture interne di appartenenza, l'assegnazione di diritti di accesso, inserimento/modificazione e visibilità dei documenti; tali diritti sono attribuiti alle persone afferenti alle strutture interne delle UO, poste ad un livello gerarchico subordinato e figlio della UO di appartenenza.

Oltre ai diritti assegnati alle strutture, l'applicativo "Diritti" della ACL consente all'Amministratore di gestire i diritti da assegnare ad ogni utente; tali *diritti* sono associati a specifici profili, precedentemente creati dall'Amministratore e descritti nella seguente tabella:

PROFILI	ABILITAZIONE
Responsabile della Gestione Documentale	Funzioni decisionali e di delega
Amministratori di sistema	Funzioni gestionali a seguito della decisione del Responsabile della Gestione Documentale
Addetto all'Ufficio Protocollo	Funzioni operative Funzioni di visualizzazione dei propri documenti personali
Addetto Ufficio di diretta Collaborazione del Presidente e del Direttore generale	Funzioni operative limitatamente a documenti di competenza della propria UO Funzioni di visualizzazione dei propri documenti personali
Addetto ai Contratti	
Addetto alla Fattura Elettronica	
Personale amministrativo	
Personale tecnico	
Profilo UBUY	
Ricercatori	

Una sezione denominata "UO di responsabilità" presente nell'applicativo ACL permette di definire i diritti aggiuntivi relativi alla visione e alla modifica dei documenti prodotti da UO in cui una data persona riveste il compito di Responsabile.

Il profilo di ogni utente è generato mediante la personalizzazione di modelli predefiniti che permettono di limitare la visione di intere categorie di documenti restringendola ai soli documenti della propria UO (se l'utente è in possesso del diritto di visione di tutto il protocollo generale) oppure ai soli documenti personali (se l'utente è in possesso almeno del diritto di visione dei documenti della propria UO).

Le restrizioni alla visione dei documenti riservati o altamente confidenziali operano sui documenti visibili all'utente, come verrà descritto al § 7.11.

Le misure descritte permettono la protezione dei dati personali e dei dati sensibili, in adeguamento al Regolamento UE 2016/679;

2.5. Indirizzi di Posta Elettronica Istituzionale e di Posta Elettronica Certificata (PEC)

Gli Uffici di Direzione, e gli Uffici amministrativi sono dotati della casella di posta elettronica istituzionale per l'invio e la ricezione dei messaggi.

Tali indirizzi sono stati pubblicati sul sito IPA.

Tutti i dipendenti sono dotati di una casella di posta elettronica istituzionale.

La casella di posta elettronica certificata è stata attivata per il registro di protocollo della AOO e di tutti gli uffici (UO) che ad essa fanno riferimento.

Gli indirizzi di posta elettronica istituzionale e di posta elettronica certificata dell'INRiM sono dettagliati nella seguente tabella:

Direzione e uffici amministrativi	Indirizzi Email
Direzione Generale	direzione.generale@inrim.it inrim@pec.it
Direzione Scientifica	dirsci@inrim.it inrim@pec.it
Ufficio di diretta collaborazione al Presidente e al Direttore Generale	presidenza@inrim.it inrim@inrim.it inrim@pec.it
Segreteria Generale	inrim@inrim.it inrim@pec.it

2.6. Responsabile della conservazione

Il Responsabile della conservazione opera d'intesa con il Responsabile della gestione documentale, con il Responsabile del trattamento dei dati personali e con il Responsabile della sicurezza dei sistemi informativi.

Per quanto riguarda le funzioni e le attività connesse alla conservazione della documentazione amministrativa si rimanda al Manuale di Conservazione dell'INRiM (Allegato 5).

CAPITOLO 3 - IL DOCUMENTO AMMINISTRATIVO

L'Istituto Nazionale di Ricerca Metrologica ha adeguato i propri sistemi di gestione informatica dei documenti sulla base della normativa vigente.

In questo capitolo sono riportate le definizioni che la disciplina giuridica fornisce in merito ai documenti analogici ed informatici e quelle relative ai documenti amministrativi di entrambi i generi.

3.1. Documento informatico e analogico: definizione e disciplina giuridica

Per documento analogico si intende un documento amministrativo rappresentato su supporto cartaceo, leggibile direttamente e senza l'ausilio di strumenti o macchine.

Per documento informatico si intende la rappresentazione informatica di un documento amministrativo indipendentemente dal tipo di supporto digitale sul quale è affisso (CD Rom, file, DVD, etc.).

L'art. 1 lettera p del CAD definisce:

- ❖ documento analogico: la rappresentazione non informatica di atti, fatti o dati giuridicamente rilevanti
- ❖ documento informatico: il documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti;

L'Art. 20 c. 1-bis del CAD descrive la validità ed efficacia probatoria dei documenti informatici:

“Il documento informatico soddisfa il requisito della forma scritta e ha l'efficacia prevista dall'articolo 2702 del Codice civile quando vi è apposta una firma digitale o una firma elettronica avanzata o, comunque, è formato, previa identificazione informatica del suo autore, attraverso un processo avente i requisiti fissati dall'AgID ai sensi dell'articolo 71 del CAD, con modalità tali da garantire la sicurezza, integrità e immodificabilità del documento e, in maniera manifesta e inequivoca, la sua riconducibilità all'autore.

In tutti gli altri casi il documento informatico assume la caratteristica di immodificabilità se prodotto in modo che forma e contenuto non siano alterabili durante le fasi di tenuta e accesso e ne sia garantita la staticità nella fase di conservazione”

A differenza del documento analogico, che si caratterizza per la pluralità di forme (scrittura privata, atto pubblico, scrittura privata autenticata) che sostanziano il diverso valore giuridico-probatorio, il documento informatico si caratterizza per la pluralità di firme elettroniche (con il valore di sottoscrizione, firma, sigla o visto), che caratterizzano e diversificano l'efficacia giuridico-probatoria del documento.

Il CAD definisce la firma elettronica come un insieme di dati in forma elettronica utilizzati come metodo di identificazione informatica; la firma elettronica è, quindi, un meccanismo di associazione di dati per l'imputazione di effetti giuridici in capo a un determinato soggetto che ne appare l'autore.

- ❖ **La firma elettronica semplice: la cosiddetta “firma debole”** è intesa come l'insieme dei dati in forma elettronica, riconducibili all'autore (anche di tipo: log identificativo, indirizzo mail, ecc.), allegati o connessi ad atti o fatti giuridicamente rilevanti contenuti in un documento informatico, utilizzati come metodo di identificazione informatica.

- ❖ **La firma elettronica avanzata** è intesa come l'insieme di dati in forma elettronica allegati oppure connessi a un documento informatico che consentono l'identificazione del firmatario del documento e garantiscono la connessione univoca al firmatario.

Secondo il Regolamento UE n° 910/2014 eIDAS³ (electronic IDentification Authentication and Signature), la firma elettronica avanzata (FEA) è una firma elettronica che soddisfa i seguenti requisiti:

- è connessa unicamente al firmatario;
- è idonea a identificare il firmatario;
- è creata mediante dati per la creazione di una firma elettronica che il firmatario può, con un elevato livello di sicurezza, utilizzare sotto il proprio esclusivo controllo;
- è collegata ai dati sottoscritti in modo da consentire l'identificazione di ogni successiva modifica di tali dati.

- ❖ **La firma elettronica qualificata** (FEQ), è un tipo di firma elettronica avanzata.

Secondo il Regolamento eIDAS, la firma elettronica qualificata possiede queste caratteristiche:

- è creata su un dispositivo qualificato per la creazione di una firma elettronica
- è basata su un certificato elettronico qualificato
- ha effetto giuridico equivalente a quello di una firma autografa.

Ai sensi dell'art. 25, del Regolamento eIDAS **corrisponde alla firma digitale italiana**.

La firma digitale, infatti, è un particolare tipo di firma elettronica qualificata basata su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro; la firma digitale consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici.

Le *Linee Guida sulla formazione, gestione e conservazione dei documenti informatici*, emanate dall'AgID, specificano, inoltre, che l'immodificabilità e l'integrità di un documento digitale sono garantite anche dalla apposizione di un sigillo elettronico qualificato.

Il sigillo elettronico è descritto dal Regolamento eIDAS:

- ❖ **il sigillo elettronico** è caratterizzato da 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;
- ❖ **il sigillo elettronico avanzato** è un sigillo elettronico che soddisfa i seguenti requisiti:
 - a) è connesso unicamente al creatore del sigillo;
 - b) è idoneo a identificare il creatore del sigillo;

³ Regolamento (UE) n. 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

c) è creato mediante dati per la creazione di un sigillo elettronico che il creatore del sigillo elettronico può, con un elevato livello di sicurezza, usare sotto il proprio controllo per creare sigilli elettronici;

d) è collegato ai dati cui si riferisce in modo da consentire l'identificazione di ogni successiva modifica di detti dati.

- ❖ **Il sigillo elettronico qualificato** è un sigillo elettronico avanzato, creato da un dispositivo per la creazione di un sigillo elettronico qualificato e basato su un certificato qualificato per sigilli elettronici.

3.1.1. Valore probatorio del documento informatico sottoscritto

Gli atti per cui la legge prevede obbligatoriamente la forma scritta, soddisfano tale requisito se sottoscritti con firma elettronica avanzata, qualificata o digitale.

Il tipo di firma utilizzata differenzia il valore giuridico del documento, secondo le norme previste dalla legge.

- ❖ **Il documento informatico privo di sottoscrizione** è una copia informatica e forma piena prova dei fatti e delle cose rappresentate, se colui contro il quale sono prodotte non ne disconosce la conformità ai fatti o alle cose medesime (artt.2712 e 2713 del cc, art. 23 quater del CAD).
- ❖ **Il documento informatico sottoscritto con firma elettronica semplice** è liberamente valutabile dal giudice sia per quanto riguarda l'efficacia giuridica che per l'efficacia probatoria tenuto conto delle sue caratteristiche oggettive di qualità, sicurezza, integrità e immodificabilità.
- ❖ **Il documento informatico sottoscritto con firma avanzata**, se formato nel rispetto delle regole tecniche che garantiscano l'identificabilità dell'autore, l'integrità e l'immodificabilità, al pari di una scrittura privata, fa piena prova fino a querela di falso della provenienza della dichiarazione da chi l'ha sottoscritta, se colui contro il quale è prodotta ne riconosce la sottoscrizione ovvero se questa è legalmente considerata come riconosciuta.
- ❖ **Il documento informatico sottoscritto con firma qualificata**, se formato nel rispetto delle regole tecniche che garantiscano l'identificabilità dell'autore, fa piena prova fino a querela di falso della provenienza della dichiarazione da chi l'ha sottoscritta.
- ❖ **Il documento informatico sottoscritto con firma digitale**, se formato nel rispetto delle regole tecniche che garantiscano l'identificabilità dell'autore, fa piena prova fino a querela di falso della provenienza della dichiarazione da chi l'ha sottoscritta.

L'utilizzo del dispositivo si presume riconducibile al titolare, salvo che questi ne dia prova contraria.

L'associazione a un documento informatico di una firma digitale o di un altro tipo di firma elettronica qualificata basata su un certificato elettronico revocato, scaduto o sospeso equivale a mancata sottoscrizione; tuttavia le firme elettroniche qualificate e digitale, ancorché sia scaduto, revocato o sospeso il relativo certificato qualificato del sottoscrittore, sono valide se alle stesse è associabile un riferimento temporale opponibile ai terzi che collochi la generazione di dette firme rispettivamente in un momento precedente alla scadenza, revoca o sospensione del suddetto certificato.

La firma elettronica qualificata (che, come dettagliato al §3.1, corrisponde alla firma digitale italiana) è utilizzata per tutti i documenti per cui viene richiesto dalla normativa.

Si precisa che tutti i contratti stipulati dalla Pubblica Amministrazione, anche quando quest'ultima agisce *iure privatorum*, richiedono la forma scritta *ad substantiam*.

3.2. Redazione/formazione del documento amministrativo informatico

I documenti dell'amministrazione sono prodotti con sistemi informatici come previsto dalla vigente normativa e sono soggette, ove necessario, a registrazione di protocollo, segnatura, fascicolatura e repertoriazione

Il documento amministrativo informatico può essere formato mediante una delle seguenti modalità:

- ❖ **redazione tramite l'utilizzo di appositi strumenti software o servizi cloud qualificati che assicurino la produzione di documenti nei formati e nel rispetto delle regole di interoperabilità⁴:** in tal caso il documento informatico assume le caratteristiche di immodificabilità e di integrità con una o più delle seguenti modalità:
 - la sottoscrizione con firma digitale/firma elettronica qualificata, o di un sigillo elettronico qualificato o l'apposizione di una validazione temporale
 - il trasferimento a soggetti terzi con PEC con ricevuta completa
 - la memorizzazione su sistemi di gestione documentale che adottino idonee politiche di sicurezza o con il versamento ad un sistema di conservazione;
 - il versamento ad un sistema di conservazione

- ❖ **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:** in tal caso le caratteristiche di immutabilità e di integrità sono determinate dall'apposizione di una firma elettronica qualificata, di una firma digitale o di un sigillo elettronico qualificato o firma elettronica avanzata; sono altresì garantite dall'operazione di memorizzazione in un sistema di gestione documentale che garantisca l'inalterabilità del documento o in un sistema di conservazione;

Tra i documenti informatici acquisiti rientrano le istanze, le dichiarazioni e le comunicazioni di cui agli articoli 5 –bis, 40 –bis e 65 del CAD, ovvero:

 - le istanze, le dichiarazioni, i dati, le informazioni e i documenti scambiati, anche a fini statistici, tra le imprese e le amministrazioni pubbliche;
 - le comunicazioni provenienti od inviate a domicili digitali eletti dai gestori dei servizi pubblici.

- ❖ **registrazione informatica delle informazioni risultanti da transazioni o processi informatici o dalla presentazione telematica di dati attraverso moduli o formulari resi disponibili all'utente:** in tal caso le caratteristiche di immutabilità e di integrità sono determinate:

⁴ di cui all'allegato 2 delle Linee guida sulla formazione, gestione e conservazione dei documenti informatici emanate, dall'Agid.

- dall'apposizione di una firma elettronica qualificata, di una firma digitale o di un sigillo elettronico qualificato o firma elettronica avanzata;
 - ovvero dall'operazione di registrazione dell'esito della medesima operazione e dall'applicazione di misure per la protezione dell'integrità delle basi di dati e per la produzione e conservazione dei log di sistema;
 - ovvero con la produzione di una estrazione statica dei dati e il trasferimento della stessa nel sistema di conservazione.
- ❖ **generazione o raggruppamento anche in via automatica di un insieme di dati o registrazioni, provenienti da una o più basi dati, anche appartenenti a più soggetti interoperanti, secondo una struttura logica predeterminata e memorizzata in forma statica:** in tal caso le caratteristiche di immutabilità e di integrità sono determinate:
- dall'apposizione di una firma elettronica qualificata, di una firma digitale o di un sigillo elettronico qualificato o firma elettronica avanzata;
 - ovvero dall'operazione di registrazione dell'esito della medesima operazione e dall'applicazione di misure per la protezione dell'integrità delle basi di dati e per la produzione e conservazione dei log di sistema;
 - ovvero con la produzione di una estrazione statica dei dati e il trasferimento della stessa nel sistema di conservazione.

Gli atti formati dalle pubbliche amministrazioni con strumenti informatici, nonché i dati e i documenti informatici detenuti dalle stesse, costituiscono informazione primaria e originale da cui è possibile effettuare duplicazioni e copie.

3.2.1. Validazione temporale

La marca temporale è un servizio offerto da un Certificatore accreditato, che consente di associare data e ora, certe e legalmente valide, a un documento informatico, permettendo una validazione temporale del documento opponibile a terzi.

Il servizio di Marcatura Temporale può essere utilizzato anche su documenti non firmati digitalmente.

Il Regolamento eIDAS introduce due definizioni:

- ❖ validazione temporale elettronica, dati in forma elettronica che collegano altri dati in forma elettronica a una particolare ora e data, così da provare che questi ultimi esistevano in quel momento;
- ❖ validazione temporale elettronica qualificata, una validazione temporale elettronica che soddisfa i requisiti di cui all'articolo 42 del Regolamento eIDAS;

La validazione temporale elettronica dà luogo a una presunzione legale relativa alla certezza della data e dell'ora.

La marcatura temporale è normata dagli articoli 41 e 42 del Regolamento eIDAS.

Costituiscono validazione temporale:

- ❖ i riferimenti temporali realizzati dai certificatori accreditati mediante marche temporali;
- ❖ i riferimenti temporali apposti sul giornale di controllo da un certificatore accreditato secondo la scala di tempo UTC (IT) (INRiM) con una differenza non superiore ad un minuto primo;
- ❖ il riferimento temporale contenuto nella segnatura di protocollo;
- ❖ il riferimento temporale ottenuto attraverso la procedura di conservazione dei documenti in conformità alle norme vigenti, ad opera di un pubblico ufficiale o di una pubblica amministrazione;
- ❖ il riferimento temporale ottenuto attraverso l'utilizzo di posta elettronica certificata;
- ❖ il riferimento temporale ottenuto attraverso l'utilizzo della marcatura postale elettronica.

3.2.2. Formati

L'art. art. 40 c.1 del CAD prevede che le pubbliche amministrazioni formino gli originali dei propri documenti in formato elettronico.

La scelta dei formati per la formazione dei documenti amministrativi elettronici è stata effettuata considerando che essa, come da previsione normativa, deve garantire la leggibilità e la reperibilità del documento informatico nell'intero ciclo di vita dello stesso; pertanto nella scelta si è valutata l'apertura, la sicurezza, la portabilità, la funzionalità, l'interoperabilità, il supporto allo sviluppo e la diffusione dello stesso.

L'INRiM usa per la formazione e per la gestione dei documenti amministrativi informatici le seguenti tipologie di formato dettagliate in tabella:

Documento	Formato
Testo	OOML ; Ods; Pdf/a;
Calcolo	XML nel dialetto SpreadsheetML
Immagini	Jpg, Tiff;
Fatture	XML nel dialetto FatturaPA ⁵

Tali formati sono coerenti con le regole tecniche del documento informatico, del sistema di conservazione e del protocollo informatico ed ottemperano alle raccomandazioni di cui all'Allegato 2 "Formati di file e riversamento" delle LL.GG. AgID 2020.

Attualmente non sono impiegati formati diversi da quelli elencati nelle suddette Linee Guida.

⁵ Fatture PA: normativa di riferimento

- La legge n. 244 del 24 dicembre 2007 (Finanziaria 2008) ha stabilito che la fatturazione nei confronti delle amministrazioni pubbliche debba avvenire esclusivamente in forma elettronica attraverso il Sistema di Interscambio.
- Il Decreto Ministeriale 3 aprile 2013, numero 55, disciplina le regole in materia di emissione, trasmissione e ricevimento della fattura elettronica e ne definisce il formato.

Per l'inserimento nel sistema di gestione documentale Titulus e, quindi, per il riversamento in conservazione, i formati OOML, Ods, XML, Jpg, Tiff vengono trasformati in Pdf/a.

3.3. Redazione/formazione del documento amministrativo analogico

Per documento analogico si intende un documento formato utilizzando una grandezza fisica (ad es., le tracce su carta, le immagini contenute nei film e le magnetizzazioni su nastro).

Nell'attività amministrativa, di norma il documento analogico è un documento formato su supporto analogico prodotto con strumenti analogici (ad es., documento scritto a mano) o con strumenti informatici (ad es., documento prodotto con un sistema di videoscrittura) e stampato su carta; l'originale analogico è il documento nella sua redazione definitiva, perfetta ed autentica negli elementi formali (sigillo, carta intestata, formulario amministrativo) e sostanziali, comprendente tutti gli elementi di garanzia e di informazione, del mittente e del destinatario e dotato di firma autografa.

I documenti analogici dotati di firma autografa aventi per destinatario un ente o un soggetto terzi sono di norma redatti in due esemplari, un originale per il destinatario e una minuta da conservare agli atti nel fascicolo corrispondente.

Per originale si intende il documento nella sua redazione definitiva, perfetta e autentica negli elementi sostanziali e formali (carta intestata, formulario amministrativo, sottoscrizione, etc.), da trasmettere al destinatario.

Si definisce minuta l'esemplare del documento corredato di sigle, firma e sottoscrizione autografe, conservato agli atti dell'Ente, cioè nel fascicolo relativo al procedimento amministrativo o all'affare trattato.

Il documento amministrativo analogico in uscita è redatto su carta intestata e deve, di norma, contenere:

- Data;
- Oggetto;
- Destinatario;
- Testo;
- Sottoscrizione;
- Sigla di eventuali istruttori;
- Elementi identificativi del responsabile del procedimento.
- Numero di allegati (indicare 0 zero se non presenti);
- Classificazione;
- Indicazioni atte a individuare il fascicolo di competenza;

Il documento è sottoscritto prima di essere protocollato; di norma la data di sottoscrizione e la data di protocollazione coincidono.

Pertanto, tutti i documenti su cui vengono apposti manualmente dati di registrazione a protocollo, sigle e firma autografa (che non sono sottoscritti con firma elettronica, semplice, avanzata o digitale), sono documenti amministrativi analogici.

Ai sensi del DPCM 21 marzo 2013, per particolari tipologie di documenti analogici originali unici, 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.

Per documenti originali unici si intendono tutti quei documenti il cui contenuto non può essere desunto da altre scritture o documenti di cui sia obbligatoria la tenuta (ad es., i verbali di una riunione o di un'assemblea).

3.4. Il documento amministrativo informatico costituito dal corpo della PEC istituzionale

La posta elettronica certificata costituisce un mezzo di trasmissione che consente lo scambio di comunicazioni e documenti la cui trasmissione e ricezione sono giuridicamente rilevanti. Tale modalità di trasmissione dei documenti viene utilizzata nei casi in cui è necessario avere prova opponibile dell'invio e della consegna del messaggio di posta.

Il documento trasmesso/ricevuto con PEC ha lo stesso valore legale della raccomandata con avviso di ricevimento.

In tal caso, l'avvenuta consegna del messaggio elettronico consente tra l'altro di ricorrere contro terzi.

La PEC, a differenza della posta elettronica semplice, ha le seguenti peculiarità:

- identificazione del mittente, se coincide con l'autore del documento;
- garanzia dell'integrità e della riservatezza dei messaggi;
- data certa di spedizione e consegna dei messaggi;
- ricevuta di avvenuta consegna o avviso di mancato recapito;
- tracciatura dei messaggi a cura del gestore.

Di norma, si dovrebbe usare la PEC per trasmettere e/o ricevere un documento informatico, ma può accadere che la comunicazione/istanza ricevuta sia costituita dal mero corpo della e-mail.

In questo caso si procede alla registrazione del messaggio in arrivo nel sistema di gestione documentale solo se il contenuto è rilevante al fine giuridico-probatorio.

3.5. Il documento amministrativo informatico costituito dal corpo della e-mail istituzionale

L'e-mail costituisce un documento informatico sottoscritto con firma elettronica semplice, in quanto il mittente viene identificato inserendo il proprio username e la propria password.

Le e-mail inviate da una casella istituzionale dell'INRiM sono considerate sottoscritte con firma elettronica semplice (cfr. §3.1) e sono soggette a protocollazione solo se il contenuto è rilevante al fine giuridico-probatorio.

In questo caso si procede alla conversione dell'e-mail in formato pdf/a prima di provvedere alla sua registrazione.

Trattandosi di un documento informatico nativo non si procederà alla stampa e apposizione tramite timbro della segnatura prima della registrazione a protocollo.

3.6. Distinzione dei documenti in base allo stato di trasmissione (arrivo, partenza, scambiati tra UO, fax, PEC, e-mail)

I documenti, siano essi analogici o informatici, in base allo stato di trasmissione si distinguono in:

- documenti in arrivo;
- documenti in partenza;
- documenti interni (scambiati tra UO);

Per **documenti in arrivo** si intendono tutti i documenti di rilevanza giuridico probatoria acquisiti dall'Amministrazione nell'esercizio delle proprie funzioni e provenienti da un diverso soggetto pubblico o privato.

Per **documenti in partenza** si intendono i documenti di rilevanza giuridico probatoria prodotti dall'Amministrazione pubblica nell'esercizio delle proprie funzioni e indirizzati ad un diverso soggetto pubblico o privato ed anche ai propri dipendenti come persone fisiche e non nell'esercizio delle loro funzioni.

Per **documenti interni** o tra uffici si intendono i documenti scambiati tra le diverse Unità Organizzative Responsabili (UO) afferenti alla stessa Area Organizzativa Omogenea (AOO) nelle realtà che hanno più di una AOO.

I documenti interni di preminente carattere giuridico-probatorio sono quelli redatti dal personale nell'esercizio delle proprie funzioni al fine di documentare fatti inerenti all'attività svolta e alla regolarità delle azioni amministrative o qualsiasi altro documento dal quale possano nascere diritti, doveri o legittime aspettative di terzi.

Sono, inoltre, da citare le **comunicazioni informali tra uffici**, ovvero lo scambio di informazioni, con o senza documenti allegati, delle quali è facoltativa la conservazione; questo genere di comunicazioni sono ricevute e trasmesse per posta elettronica interna e di norma non sono protocollate.

Di norma la ricezione dei documenti informatici è assicurata tramite la casella di posta elettronica certificata istituzionale – PEC – accessibile alla Segreteria Generale dell'INRiM, quale unica Unità Organizzativa responsabile della protocollazione in arrivo.

Il documento informatico trasmesso tramite casella di posta elettronica certificata – PEC si intende spedito dal mittente se inviato al proprio gestore e si intende consegnato al destinatario se reso disponibile all'indirizzo elettronico da questi dichiarato, nella casella di posta elettronica del destinatario messa a disposizione dal gestore.

3.7. Duplicato, copia ed estratto di documenti amministrativi informatici

3.7.1. Duplicato del documento amministrativo informatico

Il duplicato del documento informatico è un documento prodotto mediante idoneo processo o strumento che assicuri che il documento informatico, ottenuto sullo stesso sistema di memorizzazione o su un sistema diverso, contenga la stessa sequenza binaria del documento informatico di origine da cui è tratto.

I duplicati informatici, come definito al c.1bis dell'art.23 -ter del CAD, hanno il medesimo valore giuridico del documento informatico da cui sono tratti se prodotti in conformità delle regole tecniche descritte dalle *"Linee guida sulla formazione, gestione e conservazione dei documenti informatici"* emanate da AgID nel 2020; pertanto i duplicati informatici non necessitano di attestazione di conformità all'originale da parte di un notaio o di un pubblico ufficiale, stante la loro perfetta corrispondenza nel numero e nella sequenza dei valori binari e hanno il medesimo valore giuridico del documento informatico da cui sono tratti qualora prodotti mediante processi e strumenti che assicurino la predetta sequenza.

3.7.2. Copia o estratto di un documento amministrativo informatico

La copia o estratto di un documento informatico è un documento informatico che può mutare il formato del documento originario o che muta il supporto del documento originario informatico.

Le copie del documento informatico hanno la stessa efficacia probatoria dell'originale da cui sono tratte se la loro conformità non è espressamente disconosciuta, fermo l'obbligo di conservazione dell'originale informatico (c.2 bis art. 23 e art.71 del CAD).

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 processo⁶.

Il ricorso ad uno dei due metodi indicati 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 CAD⁷ nel caso in cui manchi l'attestazione di un pubblico ufficiale, la conformità della copia o dell'estratto informatico ad un documento informatico è

⁶ La certificazione di processo è prevista dal Decreto Legislativo 13 dicembre 2017, n. 217 (in G.U. 12/01/2018, n.9) al fine di permettere la dematerializzazione massiva dei documenti analogici garantendo la corrispondenza del contenuto e forma della copia informatica all'originale analogico senza ricorrere allo strumento del raffronto dei documenti in quanto oneroso e, in alcuni casi, impraticabile. I requisiti tecnici per la certificazione di processo sono individuati nell'Allegato 3 "Certificazione di Processo" delle LL.GG AgID "Linee Guida sulla formazione, gestione e conservazione dei documenti informatici".

⁷ L'art. 23bis comma 2 del CAD prevede che le copie e gli estratti informatici del documento informatico, se prodotti in conformità alle vigenti regole tecniche di cui all'articolo 71, 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.

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.

3.7.3. Duplicato di un documento amministrativo analogico o informatico

Il duplicato di un documento analogico è la riproduzione di un documento analogico originale distrutto o smarrito che lo sostituisce a tutti gli effetti legali: esempio rilascio del certificato di laurea, della carta di identità etc.

Il duplicato del documento informatico è un documento prodotto mediante idoneo processo o strumento che assicuri che il documento informatico, ottenuto sullo stesso sistema di memorizzazione o su un sistema diverso, contenga la stessa sequenza binaria del documento informatico di origine da cui è tratto.

I duplicati informatici hanno il medesimo valore giuridico del documento informatico da cui sono tratti se prodotti in conformità delle regole tecniche.

Il "duplicato informatico" è dunque un documento informatico ottenuto mediante la memorizzazione, sullo stesso dispositivo o su dispositivi diversi, della medesima sequenza di valori binari del documento originario. Pertanto, a differenza delle copie di documenti informatici, che si limitano a mantenere il contenuto dei documenti originari (ma non il loro formato), i duplicati informatici non necessitano di attestazione di conformità all'originale da parte di un notaio o di un pubblico ufficiale, stante la loro perfetta corrispondenza nel numero e nella sequenza dei valori binari e hanno il medesimo valore giuridico del documento informatico da cui sono tratti qualora prodotti mediante processi e strumenti che assicurino la predetta sequenza.

3.7.4. Copia informatica di un documento analogico

Per copia informatica di un documento analogico si intende:

- ❖ copia informatica del documento analogico data dal documento informatico avente contenuto identico a quello del documento analogico da cui è tratto ma diverso come forma;
- ❖ copia per immagine su supporto informatico di documento analogico avente contenuto e forma uguali all'originale.

Le copie informatiche di documenti analogici, spediti o rilasciati dai depositari pubblici autorizzati e dai pubblici ufficiali hanno la medesima efficacia probatoria degli originali se a esse è apposta o associata, da parte di colui che le spedisce o le rilascia, una firma elettronica avanzata o firma elettronica qualificata o altro tipo di firma ai sensi dell'art. 20 comma 1bis del CAD, ovvero del sigillo elettronico qualificato o avanzato da parte di chi effettua il raffronto e dichiarazione di conformità:

- ❖ per “rilascio” si intende la consegna di un supporto fisico idoneo a ricevere la memorizzazione della rappresentazione corrispondente al documento analogico e della dichiarazione di conformità munita della firma elettronica del pubblico ufficiale;
- ❖ per “spedizione” si intende l’inoltro telematico del/dei file corrispondenti per il tramite di un sistema di posta elettronica o di altro sistema di comunicazione informatica e della dichiarazione di conformità munita della firma elettronica del pubblico ufficiale.

Ai sensi dell’art. 23-ter c 1-bis del CAD, la copia su supporto informatico di documenti formati dalle pubbliche amministrazioni in origine su supporto analogico è prodotta mediante processi e strumenti che assicurano che il documento informatico abbia contenuto identico a quello del documento analogico da cui è tratto, previo raffronto dei documenti o attraverso certificazione di processo, già descritta al §3.7.2, nei casi in cui siano adottate tecniche in grado di garantire la corrispondenza del contenuto dell’originale e della copia.

La copia informatica ha il medesimo valore dell’originale analogico da cui è tratta se attestata conforme dal funzionario a ciò delegato nei modi stabiliti dalla legge.

L’attestazione di conformità della copia informatica di un documento amministrativo analogico, formato dalla Pubblica Amministrazione, ovvero da essa detenuto, può essere inserita nel documento informatico contenente la copia informatica o essere prodotta come documento informatico separato contenente un riferimento temporale e l’impronta di ogni copia per immagine.

In entrambi i casi l’attestazione dev’essere sottoscritta con firma digitale del notaio o con firma digitale o firma elettronica qualificata del pubblico ufficiale a ciò autorizzato; se prodotta come documento informatico separato, questo deve contenere un riferimento temporale e l’impronta di ogni copia o estratto informatico oggetto dell’attestazione.

3.7.5. Estratto informatico di documento amministrativo informatico

La copia che riproduce solo una parte del contenuto del documento viene definita “estratto”.

Gli estratti informatici devono essere prodotti in uno dei formati idonei definiti nel § 3.2.2.

L’estratto così formato, di uno o più documenti informatici, se sottoscritto con firma digitale o firma elettronica qualificata da chi effettua l’estratto hanno la stessa efficacia probatoria dell’originale, salvo che la conformità allo stesso non sia espressamente disconosciuta.

Laddove richiesta dalla natura dell’attività, l’attestazione di conformità può essere inserita nello stesso documento informatico contenente l’estratto, oppure prodotta come documento informatico separato; in entrambi i casi l’attestazione dev’essere sottoscritta con firma digitale del notaio o con firma digitale o firma elettronica qualificata del pubblico ufficiale a ciò autorizzato; se prodotta come documento informatico separato, questo deve contenere un riferimento temporale e l’impronta di ogni copia o estratto informatico oggetto dell’attestazione.

3.7.6. Copia analogica di documento amministrativo informatico

La copia analogica di documento amministrativo informatico è, di norma, la stampa cartacea.

La copia su supporto analogico di documento informatico, sottoscritto con firma elettronica avanzata, qualificata o digitale, per avere la stessa efficacia probatoria dell'originale da cui è tratta, deve essere certificata come conforme all'originale in tutte le sue componenti da un pubblico ufficiale autorizzato a eseguire tale attestazione nell'esercizio delle sue funzioni (copia "autentica"), salvo che la conformità allo stesso non sia espressamente disconosciuta. Resta fermo, ove previsto, l'obbligo di conservazione dell'originale informatico.

3.8. Metadati associati ai documenti informatici e ai documenti amministrativi informatici

In ambito informatico il metadato descrive il contenuto, la struttura e l'ambito in cui s'inquadra un documento informatico, per la sua gestione, conservazione e archiviazione.

Nel contesto degli oggetti digitali il termine metadati può essere associato a tre categorie funzionali:

- ❖ descrittiva: ha lo scopo di facilitare il recupero e l'identificazione dell'oggetto digitale;
- ❖ gestionale: ha lo scopo di supportare la gestione dell'oggetto digitale all'interno di una collezione;
- ❖ strutturale: ha lo scopo di collegare fra loro i componenti di oggetti informativi complessi.

3.8.1. Metadati associati al documento informatico

Al momento della formazione del documento informatico, devono essere generati e associati permanentemente ad esso i relativi metadati.

Al documento amministrativo informatico viene associato l'insieme dei metadati previsti per la registrazione di protocollo ai sensi dell'art 53 del TUDA,⁸ i metadati relativi alla classificazione ai sensi dell'articolo 56 del TUDA⁹ oltre all'insieme dei metadati descritti dall'Allegato 5 alle *"Linee guida sulla Formazione, gestione e conservazione dei documenti informatici"*, emanate da AgID nel 2020; in quest'ultimo documento i metadati prescritti dalla normativa e ulteriori metadati aggiuntivi obbligatoriamente associati ai documenti e alle aggregazioni documentali sono suddivisi in base alla loro funzione esplicativa (identificativi (idDoc), modalità di formazione, tipologia documentale, dati di registrazione, chiave descrittiva, soggetti coinvolti, allegati, classificazione etc.) atti a garantire indicizzazione, individuazione, ricerca dei documenti e il tracciamento di ogni passaggio dell'aggregazione per competenza o per conoscenza, al fine di garantire la massima

⁸ L'art. 53, comma 1, del TUDA prevede che "La registrazione di protocollo per ogni documento ricevuto o spedito dalle pubbliche amministrazioni è effettuata mediante la memorizzazione delle seguenti informazioni: a) numero di protocollo del documento 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 per i documenti ricevuti o, in alternativa, il destinatario o i destinatari per i documenti spediti, registrati in forma non modificabile; d) oggetto del documento, registrato in forma non modificabile; e) data e protocollo del documento ricevuto, se disponibili; f) l'impronta del documento informatico, se trasmesso per via telematica, costituita dalla sequenza di simboli binari in grado di identificarne univocamente il contenuto, registrata in forma non modificabile"

⁹ L'art. 56 del TUDA prevede che "Le operazioni di registrazione indicate all'articolo 53 e le operazioni di segnatura di protocollo di cui all'articolo 55 nonché le operazioni di classificazione costituiscono operazioni necessarie e sufficienti per la tenuta del sistema di gestione informatica dei documenti da parte delle pubbliche amministrazioni"

trasparenza nell'ambito di qualsiasi procedimento amministrativo della PA; sono contemplate, inoltre, le informazioni necessarie in vista della conservazione a lungo termine.

I metadati che devono essere associati al documento informatico, riportati dalle Linee Guida Agid, sono:

IdDoc¹⁰

E' identificato dai sottocampi:

1. **Impronta:** Rappresenta l'hash del documento (Binary Data)
2. **Algoritmo**¹¹ (Default = SHA-256)
3. **Identificativo:** Come da sistema di identificazione formalmente definito

MODALITÀ DI FORMAZIONE:¹²

Valori ammessi:

- Creazione tramite l'utilizzo di strumenti software che assicurino la produzione di documenti nei formati previsti nell'Allegato 2 delle Linee Guida AgID.
- 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.
- Memorizzazione su supporto informatico in formato digitale delle informazioni risultanti da transazioni o processi informatici, memorizzazione su supporto informatico in formato digitale delle informazioni risultanti da presentazione telematica di dati attraverso moduli o formulari resi disponibili all'utente;
- 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.

TIPOLOGIA DOCUMENTALE¹³:

Sono ammessi i valori:

¹⁰ Identificativo univoco e persistente associato in modo univoco e permanente al documento informatico in modo da consentirne l'identificazione. Inoltre, rappresenta le informazioni necessarie per verificare l'integrità del documento.

¹¹ Indica la tipologia dell'algoritmo applicato riportati nell'Allegato 6 delle Linee Guida AgID (tabella 1 del paragrafo 2.2 "Regole di processamento").

¹² Indica la modalità di generazione del documento informatico. Sono previste le seguenti modalità secondo quanto riportato nelle Linee guida:

- a) creazione tramite l'utilizzo di strumenti software che assicurino la produzione di documenti nei formati previsti nell'Allegato 2 delle Linee Guida AgID;
- 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

¹³ Metadato funzionale che indica la tipologia del documento tra quelle trattate per lo svolgimento delle attività.

- Fatture
- Determine
- Delibere
-

DATI DI REGISTRAZIONE¹⁴

E' costituito da cinque sottocampi con i relativi valori ammessi:

1. Tipologia di flusso:

- In uscita
- In entrata
- Interno (Documenti scambiati tra AOO)

2. Tipologia di registro:

- Nessuno,
- Protocollo Ordinario /Protocollo Emergenza
- Repertorio/Registro

3. Data registrazione

- Data di registrazione del documento (documento non protocollato)
- Data di registrazione di protocollo (documento protocollato)

4. Numero Documento

- Numero di protocollo del documento protocollato
- Numero di registrazione del documento non protocollato

5. IdRegistro: codice alfanumerico identificativo del registro in cui il documento viene registrato

CHIAVE DESCRITTIVA

E' costituito da due sottocampi:

1. Oggetto (testo libero)

2. Parola chiave (testo libero) da compilare facoltativamente attingendo da thesauri o da vocabolari controllati, per evitare ambiguità terminologiche e avere la possibilità di utilizzare il metadato come chiave di ricerca del documento. Il metadato è ricorsivo fino ad un massimo di 5 occorrenze

SOGGETTI¹⁵

E' costituito da cinque sottocampi con i relativi valori ammessi:

1. Ruolo

- Autore
- Mittente
- Destinatario

¹⁴ Metadato che comprende i dati di registrazione del documento sia nel caso di documento protocollato che non protocollato. Si intende per registrazione l'operazione che, in senso lato, associa ad un documento una data e un numero. In tale ottica quindi potrebbe non essere identificabile uno specifico registro, ma sono sempre identificabili una data di registrazione e un numero di registrazione del documento.

¹⁵ Indica il metadato che consente di individuare le informazioni relative a tutti i soggetti coinvolti e competenti sul documento a vario titolo e definiti dal campo Ruolo.

- Assegnatario
- Operatore
- Altro...

2. Tipo soggetto

- PF per Persona Fisica
- PG per Organizzazione
- PA per le Amministrazioni Pubbliche

3. Nominativo

- se Tipo soggetto = PF: cognome e nome;
- se Tipo soggetto = PG: denominazione
- se Tipo soggetto = PA: denominazione Amministrazione\denominazione AOO

4. Codice identificativo

- se Tipo soggetto = PF: codice fiscale
- se Tipo soggetto = PG: codice fiscale;
- se Tipo soggetto = PA: Codice IPA dell'Amministrazione \ Codice AOO

5. UO (alfanumerico) NON OBBLIGATORIO

Per una migliore e più facile visualizzazione i sottocampi 2, 3 e 4 sono riportati anche nella seguente tabella.

Tipo soggetto	Nominativo corrispondente al tipo di soggetto indicato	Codice identificativo corrispondente al tipo di soggetto indicato
PF (Persona fisica)	Cognome e nome	Codice fiscale
PG (Organizzazione)	Denominazione	Codice fiscale
PA (Pubblica Amministrazione)	Denominazione Amministrazione	Codice IPA dell'Amministrazione
	Denominazione AOO	Codice IPA dell'AOO

ALLEGATI:

Costituito da tra sottocampi:

1. **Numero di allegati** (Da 0 a N)
2. **Indice degli allegati** (se il numero degli allegati è > di 0)
 - IdDoc: Identificativo del documento relativo all'Allegato
 - Titolo dell'Allegato

CLASSIFICAZIONE (NON OBBLIGATORIO)

Costituito da tre sottocampi:

1. **Indice di classificazione** del documento secondo il Piano di classificazione utilizzato:
 - Titolo
 - Voce di Indice
 - Fascicolo

- Eventuale sottofascicolo
- 2. **Descrizione per esteso dell'Indice di classificazione indicato.**
- 3. **l'URI di pubblicazione del Piano di classificazione (se presente)**

VISIBILITÀ¹⁶

Costituito da un unico sottocampo

1. **Riservato** (Vero o Falso a seconda della riservatezza)

IDENTIFICATIVO DEL FORMATO¹⁷

Composto da due sottocampi:

1. **Tipo di formato**
2. **Prodotto software:**
 - Nome prodotto
 - Versione del prodotto
 - Produttore

VERIFICA: CHECK DI CONTROLLO PRESENZA DELLA FIRMA ELETTRONICA

- Firmato Digitalmente¹⁸ (vero o falso)
- Sigillato elettronicamente¹⁸ (vero o falso)
- Marcatura temporale¹⁸ (vero o falso)
- Conformità copie immagine nelle modalità di formazione del documento informatico previste nelle Linee Guida¹⁹

IDAGG: IDENTIFICATIVO UNIVOCO DELL'AGGREGAZIONE²⁰ (cfr metadati delle aggregazioni) non obbligatorio

IDENTIFICATIVO UNIVOCO E PERSISTENTE DEL DOCUMENTO PRINCIPALE (IDDOC)

VERSIONE DEL DOCUMENTO (valore numerico: 1, 2, 3...)

TRACCIATURE MODIFICHE DOCUMENTO²¹

Composto da quattro sottocampi:

¹⁶ Consente di gestire gli accessi al documento al solo personale autorizzato.

¹⁷ Indica il formato del documento e la versione del software utilizzato per la creazione del documento stesso.

¹⁸ Obbligatorio per:

- a) documenti informatici creati tramite l'utilizzo di strumenti software che assicurino la produzione di documenti nei formati previsti nell'Allegato 2 delle Linee Guida;
- b) documenti acquisiti 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.

¹⁹ Obbligatorio per documenti acquisiti 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.

²⁰ Identificativo univoco dell'Aggregazione come definito nel successivo paragrafo 4.9 -Metadati associati ai fascicoli, alle serie dei fascicoli e alle altre aggregazioni documentali informatiche-.

²¹ Tracciatura delle modifiche del documento (obbligatoria solo nel caso di più versioni o di annullamento del documento).

1. Tipo modifica:

Valori ammessi:

- Annullamento
- Rettifica
- Integrazione
- Annotazione

2. Codice fiscale dell'autore della modifica (Codice fiscale del soggetto definito con ruolo di Operatore nel metadato "Soggetti")**3. Data****4. Identificativo documento della versione precedente** (IdDoc versione precedente)**CONSERVAZIONE²²**

Valori ammessi:

- 9999 (illimitata)
- 5 anni
- 10 anni
-

NOTE (campo libero) NON OBBLIGATORIO**3.8.2 Ulteriori metadati associati al registro delle fatture e degli altri documenti contabili equivalenti**

Oltre ai metadati che vengono associati a tutti i documenti informatici, al registro delle fatture e degli altri documenti contabili equivalenti, ai sensi dell'art. del 42 del DL 24 aprile 2014, n. 66 (Legge 89/2014) sono resi obbligatori ulteriori metadati:

- Codice progressivo di registrazione;
- Numero di protocollo di entrata;
- Numero della fattura o del documento contabile equivalente;
- Data di emissione della fattura o del documento contabile equivalente;
- Nome del creditore e il relativo codice fiscale;
- Oggetto della fornitura;
- Importo totale, al lordo di IVA e di eventuali altri oneri e spese indicati;
- Scadenza della fattura;
- Gli estremi dell'impegno indicato nella fattura o nel documento contabile equivalente
- Rilevanza (o meno) della spesa ai fini IVA;
- Codice identificativo di gara (CIG), tranne i casi di esclusione dall'obbligo di tracciabilità di cui alla legge 13 agosto 2010, n. 136;

²² In generale il tempo di conservazione a livello di singolo documento deve essere indicato solo qualora esso presenti un tempo di conservazione distinto da quello assegnato all'aggregazione documentale

- Codice unico di Progetto (CUP), in caso di fatture relative a opere pubbliche, interventi di manutenzione straordinaria, interventi finanziati da contributi comunitari e ove previsto ai sensi dell'articolo 11 della legge 16 gennaio 2003, n. 3;
- Eventuali ulteriori informazioni

3.8.3 Metadati associati al documento amministrativo informatico

I metadati che devono essere associati al documento amministrativo informatico, riportati dalle Linee Guida Agid, sono:

IdDoc²³

Il metadato è costituito da tre sottocampi:

1. **Impronta crittografica del documento**
 - Impronta: Rappresenta l'hash del documento
 - Algoritmo: Rappresenta l'algoritmo applicato Default = SHA-256
2. **Segnatura**²⁴
3. **Identificativo**²⁵

MODALITÀ DI FORMAZIONE:

Valori ammessi:

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

TIPOLOGIA DOCUMENTALE:

Indicare:

- Fatture
- Determine
- Delibere
-

²³ Identificativo univoco e persistente associato in modo univoco e permanente al documento amministrativo informatico in modo da consentirne l'identificazione; rappresenta le informazioni necessarie per verificare l'integrità del documento

²⁴ Segnatura di protocollo, da indicare obbligatoriamente nel caso di documento amministrativo protocollato, a sua volta strutturato come da Allegato 6 delle Linee Guida AgID

²⁵ Come da sistema di identificazione formalmente definito

DATI DI REGISTRAZIONE

Costituito da sei sottocampi:

1. Tipologia di flusso

Valori ammessi:

- In uscita
- In entrata
- Interno (Documenti scambiati tra AOO)

2. Tipologia di registro

Valori ammessi:

- Protocollo Ordinario/Protocollo Emergenza
- Repertorio/Registro

3. Data registrazione

Valori ammessi:

- Data di registrazione del documento (per il documento non protocollato)
- Data di registrazione di protocollo (per il documento protocollato)

4. Numero Documento

Valori ammessi:

- Numero di protocollo del documento protocollato
- Numero di registrazione del documento non protocollato

5. IdRegistro²⁶**6. Amministrazione che effettua la registrazione:**

- Codice IPA Amministrazione
- Codice IPA AOO

CHIAVE DESCRITTIVA

Costituito da due sottocampi:

1. **Oggetto**
2. **Parole Chiave** (testo libero, facoltativo)

SOGGETTI

Costituito da sei sottocampi:

1. Ruolo

Valori ammessi:

- Autore
- Mittente
- Destinatario
- Assegnatario
- Operatore
- Altro

2. Tipo soggetto

²⁶ Codice identificativo del registro in cui il documento viene registrato il documento

A scelta tra:

- PF per Persona Fisica
- PG per Organizzazione
- PA per le Amministrazioni Pubbliche

3. Nominativo

- se Tipo soggetto = PF: cognome e nome
- se Tipo soggetto = PG: denominazione
- se Tipo soggetto = PA: denominazione Amministrazione \denominazione AOO

4. Codice identificativo

- se Tipo soggetto = PF: codice fiscale
- se Tipo soggetto = PG: codice fiscale
- se Tipo soggetto = PA: Codice IPA dell'Amministrazione \Codice AOO

5. UO

6. Indirizzi digitali di riferimento (PEC, domicilio digitale)

Per una migliore e più facile visualizzazione i sottocampi 2, 3 e 4 sono riportati anche nella seguente Tabella

Tipo soggetto	Nominativo corrispondente al tipo di soggetto indicato	Codice identificativo corrispondente al tipo di soggetto indicato
PF (Persona fisica)	Cognome e nome	Codice fiscale
PG (Organizzazione)	Denominazione	Codice fiscale
PA (Pubblica Amministrazione)	Denominazione Amministrazione	Codice IPA dell'Amministrazione
	Denominazione AOO	Codice IPA dell'AOO

ALLEGATI:

Costituito da due sottocampi:

1. **Numero di allegati** (Da 0 a N)
2. **Indice degli allegati** (se il numero degli allegati è > di 0)
 - IdDoc: Identificativo del documento relativo all'allegato
 - Titolo dell'Allegato

CLASSIFICAZIONE DEL DOCUMENTO SECONDO IL PIANO DI CLASSIFICAZIONE UTILIZZATO (sia nel caso di documento protocollato che di documento non protocollato)

Comprende tre sottocampi:

1. **Indice di classificazione** (Titolo, Voce di Indice, Fascicolo, eventuale sottofascicolo, etc)
2. **Descrizione per esteso dell'indice di classificazione**
3. **l'URI di pubblicazione del Piano di classificazione**

VISIBILITÀ:²⁷

1. **Riservato** (Vero o Falso)

IDENTIFICATIVO DEL FORMATO²⁸

Comprende due sottocampi:

1. **Tipo di formato**
2. **Prodotto software:**

Indicare:

- Nome prodotto
- Versione del prodotto
- Produttore

VERIFICA (check di controllo presenza Firma elettronica, Sigillo, Marcatura temporale e Conformità copie immagine)

Indicare:

- Firmato digitalmente,²⁹
- Sigillato elettronicamente
- Marcatura temporale
- Conformità copie immagine nelle modalità di formazione del documento informatico previste nelle Linee Guida.³⁰

IDAGG Identificativo univoco dell'Aggregazione (cfr. §4.9)

IDENTIFICATIVO UNIVOCO E PERSISTENTE DEL DOCUMENTO PRINCIPALE (IdDoc del documento principale)

VERSIONE DEL DOCUMENTO (valore numerico: 1, 2, 3, ...)

TRACCIATURE MODIFICHE DOCUMENTO³¹

Composto da quattro sottocampi:

1. **Tipo modifica:**
 - Annullamento
 - Rettifica
 - Integrazione
 - Annotazione

²⁷ Consente di gestire gli accessi al documento al solo personale autorizzato; rappresenta il livello di sicurezza di accesso al documento

²⁸ Indica il formato del documento e la versione del software utilizzato per la creazione del documento stesso

²⁹ Obbligatorio per:

- a) documenti informatici creati tramite l'utilizzo di strumenti software che assicurino la produzione di documenti nei formati previsti nell'Allegato 2 delle Linee Guida;
- b) documenti acquisiti 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.

³⁰ Obbligatorio per documenti acquisiti 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.

³¹ Tracciatura delle modifiche del documento (obbligatoria solo nel caso di più versioni o di annullamento del documento).

2. **Codice fiscale dell'autore della** modifica (Codice fiscale del soggetto definito con ruolo di Operatore nel metadato "Soggetti")
3. **Data**
4. **Identificativo documento della versione precedente** (IdDoc versione precedente)

CONSERVAZIONE³²

Valori ammessi:

- 9999 (illimitata)
- 5 anni
- 10 anni
-

NOTE (campo libero non obbligatorio)

³² In generale il tempo di conservazione a livello di singolo documento deve essere indicato solo qualora esso presenti un tempo di conservazione distinto da quello assegnato all'aggregazione documentale

CAPITOLO 4 - IL FASCICOLO

Il fascicolo è l'unità di base dell'archivio corrente; si forma nel corso dell'attività amministrativa di ogni AOO allo scopo di riunire, a fini decisionali o informativi, i documenti utili allo svolgimento di tale attività.

All'interno di ciascun fascicolo i documenti sono inseriti secondo l'ordine cronologico di registrazione e la loro sedimentazione avviene in modo tale che si individui subito il documento più recente.

L'ordine cronologico di sedimentazione è rispettato anche all'interno dei sottofascicoli, se istruiti.

L'obbligo di fascicolatura dei documenti, imposto dall'art 64 c.4 del TUDA³³ e dall'art.41 c.2 del CAD³⁴, riguarda sia i documenti contraddistinti dalla segnatura di protocollo sia i documenti procedurali non registrati, indipendentemente dal supporto su cui sono creati.

La corretta tenuta del fascicolo garantisce sia la sedimentazione che l'esercizio del diritto di accesso.

4.1. Il fascicolo: tipologie

Si possono distinguere cinque tipologie di fascicolo:

- **Affare:** conserva i documenti relativi a una competenza non proceduralizzata né procedimentalizzata ma che nella consuetudine amministrativa la PA deve concretamente portare a buon fine. Per gli affari non esiste un termine per la conclusione previsto da norme; Il fascicolo per affare, comunque, ha una data di apertura e una durata circoscritta.
- **Attività:** conserva i documenti relativi a una competenza proceduralizzata, per la quale esistono documenti vincolati o attività di aggiornamento procedurale e per la quale non è comunque previsto l'adozione di un provvedimento finale; ha in genere durata annuale.
- **Procedimento amministrativo:** conserva una pluralità di documenti che rappresentano azioni amministrative omogenee e destinate a concludersi con un atto finale;
- **Persona fisica:** conserva i documenti relativi a diversi procedimenti amministrativi, distinti per affari o per attività, ma legati da un vincolo archivistico interno, relativo a una persona fisica determinata. La chiusura del fascicolo dipende dalla conclusione del rapporto giuridico con l'ente;
- **Persona giuridica:** conserva i documenti relativi a una persona giuridica con modalità simili a quelle del fascicolo di persona fisica.
Quasi sempre i fascicoli intestati alle persone giuridiche restano correnti per molti anni, costituendo serie aperte.

³³³³ L'art art. 64 c. 4 del TUDA prescrive che: «Le amministrazioni determinano autonomamente e in modo coordinato per le aree organizzative omogenee, le modalità di attribuzione dei documenti ai fascicoli che li contengono e ai relativi procedimenti, definendo adeguati piani di classificazione d'archivio per tutti i documenti, compresi quelli non soggetti a registrazione di protocollo»

³⁴ Art.41 c.2 del CAD «La pubblica amministrazione titolare del procedimento raccoglie in un fascicolo informatico gli atti, i documenti e i dati del procedimento medesimo da soggetti giuridici formati; all'atto della comunicazione dell'avvio del procedimento ai sensi dell'articolo 8 della legge 7 agosto 1990, n. 241, comunica agli interessati le modalità per esercitare in via telematica i diritti di cui all'articolo 10 della citata legge 7 agosto 1990, n. 241.»

Il fascicolo può essere ulteriormente suddiviso in sottofascicoli e inserti; queste suddivisioni sono identificate grazie a un'ulteriore sequenza numerica progressiva, gerarchicamente posta al di sotto del numero di fascicolo o del sottofascicolo.

Il sottofascicolo può essere chiuso prima del fascicolo, ma non viceversa, in quanto di norma trattasi di un endoprocedimento stesso.

4.2. Il fascicolo analogico: formazione, implementazione, gestione e buone prassi

Per ogni procedimento, affare e attività, l'Ente ha l'obbligo di conservare in un fascicolo cartaceo gli atti, i documenti e i dati da chiunque formati su supporto analogico; cioè un documento nativo su supporto cartaceo deve essere conservato in originale su tale supporto all'interno dell'apposito fascicolo.

Ovviamente un fascicolo analogico può contenere anche copie analogiche di documenti nativi digitalmente.

Inserire i documenti nell'apposito fascicolo permette la costituzione di un archivio organizzato essendo essi le unità logiche del sistema di gestione documentale e, di conseguenza, consente il facile e veloce reperimento dei documenti di un determinato procedimento permettendo il rispetto del principio di trasparenza e dell'istituto del diritto di accesso.

La fascicolazione deve essere effettuata in maniera sistematizzata da parte di tutte le UO costituenti l'Amministrazione.

Il responsabile del procedimento amministrativo è incaricato della corretta gestione dell'archivio corrente di sua pertinenza e ciò comporta in primo luogo la corretta creazione dei fascicoli e inserimento dei relativi documenti; in secondo luogo, il responsabile del procedimento è tenuto alla corretta gestione dei fascicoli stessi e tale incombenza varia a seconda del supporto con cui vengono creati.

I fascicoli analogici devono essere creati secondo le indicazioni qui fornite e successivamente conservati all'interno di appositi faldoni o cartelle nell'archivio corrente situato presso gli uffici di ciascuna UO.

Ogni fascicolo deve essere contraddistinto dai seguenti elementi, atti a determinarne l'identificazione all'interno del sistema documentale:

- anno di apertura (o di istruzione);
- numero di fascicolo, cioè un numero sequenziale all'interno dell'ultimo grado divisionale, da 1 a n con cadenza annuale;
- l'oggetto del fascicolo, cioè una stringa di testo per descrivere compiutamente un affare, una pratica, un dossier, una cartellina, una papèla, un procedimento amministrativo o più di questi insieme.

Per convenzione,

- il titolo va scritto in numeri romani, mentre gli altri gradi divisionali vanno scritti in cifre arabe.
- l'anno va separato dal titolo da un trattino (-);
- il titolo va separato dagli altri gradi divisionali da una barretta (/);
- gli altri gradi divisionali, invece, vanno separati dal numero del fascicolo da un punto (.);
- l'oggetto del fascicolo va scritto tra virgolette caporali (« »)

Esempio: 2016 - III/9.1 «Certificati di taratura».

Il fascicolo raccoglie i documenti, creati e ricevuti, fino al termine della pratica.

La chiusura della pratica comporta la chiusura del fascicolo.

Il faldone, per consentire l'agevole e immediato reperimento dei fascicoli deve riportare sul dorso le seguenti informazioni:

- l'ufficio produttore;
- l'oggetto;
- gli estremi cronologici;
- gli estremi identificativi dei fascicoli contenuti (indice di classificazione e numero progressivo di repertorio).

Laddove una pratica avesse dimensioni tali da occupare singolarmente più di un faldone, questi andranno contrassegnati con le medesime indicazioni esterne e con una numerazione progressiva, a partire dal numero 1, così da risultare immediata la comprensione del legame tra le unità di conservazione.

I fascicoli restano collocati presso ogni singola struttura (AOO/UO) per la parte di propria responsabilità e competenza nel trattamento dell'affare, fino al momento del loro trasferimento nell'archivio di deposito.

Un'attività secondaria, ma molto utile da un punto di vista di gestione corrente delle unità di archivio, è lo sfoltimento dei fascicoli; lo sfoltimento è l'operazione preliminare e propedeutica a una corretta conservazione

Non si forniscono limiti massimi di giacenza dei fascicoli chiusi presso l'archivio corrente poiché i tempi possono risultare diversi a seconda della natura della pratica e dell'attività d'ufficio.

I fascicoli di attività cessate non più consultati e che non hanno più alcuna utilità diretta presso gli uffici vengono postati nell'archivio di deposito, per evitare un eccessivo ingombro e una conseguente difficoltà nella gestione dei fascicoli aperti e attivi.

Il trasferimento dei fascicoli chiusi dall'archivio corrente all'archivio di deposito è effettuato a cura del Responsabile della gestione documentale o dal suo vicario ed avviene secondo le modalità presentate al § 10.2.

4.3. Raccoglitore

Il raccoglitore non è un fascicolo, ma un contenitore che raggruppa documenti analogici relativi a uno stesso argomento e afferenti a procedimenti diversi e quindi a fascicoli diversi, privi di una classificazione e una numerazione propria; si tratta di un dossier a uso e consumo del responsabile del procedimento amministrativo per propria memoria e auto-documentazione, di norma, non destinato alla conservazione.

4.4. Il fascicolo informatico: formazione, implementazione, gestione e buone prassi

Per ogni procedimento, affare e attività, l'Ente ha l'obbligo di conservare in un fascicolo informatico gli atti, i documenti e i dati, da chiunque formati, su supporto informatico; cioè un documento nativo su supporto informatico deve essere conservato in originale su tale supporto all'interno dell'apposito fascicolo.

Ovviamente un fascicolo informatico può contenere anche copie di qualunque tipo di documenti nativi cartacei, come descritto nel §3.7.4.

Il fascicolo informatico è creato dal RPA o da una persona incaricata, all'interno del sistema di gestione documentale Titulus ed è visualizzabile con possibilità di intervento da parte degli utenti abilitati a operare sui documenti della UO responsabile.

Istruendo i fascicoli, è necessario evitare:

- la frammentazione delle pratiche,
- l'accorpamento eccessivo di documenti all'interno della stessa unità,
- la tendenza a costituire fascicoli intestati ai destinatari invece che basati sull'analisi di processi e funzioni.

Se necessario, i fascicoli dell'archivio corrente possono essere rinominati.

Se il contenuto è costituito di documenti esclusivamente informatici questa attività è sufficiente; se è costituito da documenti informatici e documenti cartacei bisogna rinominare anche la camicia del fascicolo cartaceo.

Il fascicolo informatico in un sistema totalmente digitale garantisce la possibilità di essere direttamente consultato e alimentato dalle amministrazioni coinvolte nel procedimento.

Le regole per l'istruzione, l'identificazione e l'utilizzo del fascicolo sono conformi ai principi di una corretta gestione documentale e alla disciplina della formazione, gestione, trasmissione e conservazione del documento informatico.

4.5. I fascicoli annuali ripetitivi

È possibile prevedere la possibilità di aprire automaticamente fascicoli annuali ripetitivi.

L'indicazione della UO e del RPA concorrono all'identificazione del fascicolo e alla individuazione del responsabile.

La UO e il RPA devono essere gli stessi di ciascun documento, del fascicolo e degli eventuali sottofascicoli. Ogni qualvolta cambia il RPA il fascicolo informatico deve essere immediatamente trasferito per competenza al nuovo responsabile del procedimento.

I fascicoli informatici saranno trasferiti in conservazione, mediante pacchetto di versamento, a cura del Responsabile della gestione documentale o dal suo vicario dopo la loro chiusura, nelle modalità previste dal Manuale di conservazione

4.6. Il fascicolo ibrido

Il fascicolo, inteso come unità logica, può conservare documenti affissi su diverse tipologie di supporto.

Tale problematica, particolarmente sentita negli odierni sistemi di gestione documentale, produce il cosiddetto fascicolo ibrido; si tratta di un fascicolo composto da documenti formati su supporto cartaceo e su supporto informatico, e tale duplicità dà origine a due unità archivistiche fisiche di conservazione differenti.

L'unitarietà del fascicolo è comunque garantita dal sistema di classificazione mediante gli elementi identificativi del fascicolo (anno di istruzione, titolo/classe, numero del fascicolo, oggetto) e dal contenuto dei documenti.

Il risultato è che un fascicolo di tale natura occuperà due luoghi distinti (un faldone e un file system) e questa caratteristica permane per tutta la vita del fascicolo, dal momento della sua istruzione al momento del trasferimento nell'archivio di deposito e, infine, per il versamento all'archivio storico.

Tale peculiarità rende, ovviamente, più complessa la gestione del fascicolo e dei documenti che vi afferiscono: entrambi vanno gestiti correttamente rispettando le caratteristiche proprie del supporto su cui il documento è stato prodotto e deve essere conservato.

Qualora si ravvisi l'utilità di avere tutti i documenti presenti in un fascicolo in un determinato formato, è utile privilegiare il fascicolo informatico e creando le opportune copie per immagine dei documenti nativi analogici; è possibile inserire all'interno del fascicolo, qualora lo si ritenga necessario, anche documenti di carattere strumentale non soggetti a registrazione di protocollo, mediante la modalità denominata "non protocollato" prevista dal sistema di gestione informatica dei documenti Titulus.

Questa pratica non esenta dalla conservazione dell'originale cartaceo nel fascicolo di pertinenza.

4.8. Il repertorio dei fascicoli informatici

Il repertorio dei fascicoli informatici è costituito da un elenco ordinato e aggiornato dei fascicoli istruiti all'interno di ciascuna classe e di ciascun titolo del titolario di classificazione adottato, riportante metadati che ne garantiscono l'individuazione all'interno dell'archivio.

Il repertorio dei fascicoli informatici è unico per ogni AOO, ha cadenza annuale ed è generato e gestito in forma automatica dal sistema di gestione informatica dei documenti.

4.9 Metadati associati ai fascicoli, alle serie dei fascicoli e alle altre aggregazioni documentali informatiche

La Pubblica Amministrazione documenta la propria attività tramite funzioni del sistema di gestione informatica dei documenti finalizzate alla produzione, alla gestione e all'uso delle aggregazioni documentali informatiche, corredate da opportuni metadati che hanno l'obiettivo di:

- ❖ garantire l'identificazione permanente dei singoli oggetti informativi;
- ❖ identificativo univoco (numero di protocollo, data, autore, ecc.);
- ❖ garantire l'identificazione permanente delle relazioni tra gli oggetti informativi, ad es., indici di classificazione e fascicolatura;
- ❖ conservare le informazioni che supportano l'intelligibilità degli oggetti informativi, ad es., il procedimento amministrativo cui il documento è connesso.

Le aggregazioni documentali sono costituite da:

Fascicoli: il fascicolo è una 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.

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

Serie di fascicoli: le serie di fascicoli sono costituite da fascicoli accorpati per ragioni funzionali in base alla classe di riferimento o alla tipologia di fascicolo

Una descrizione più dettagliata delle aggregazioni documentali è riportata al §5.1 del *Manuale di Conservazione*, Allegato n. 5 a questo documento.

I metadati che, a norma delle Linee Guida AgID, devono essere associati ai fascicoli, alle serie dei fascicoli e alle altre aggregazioni documentali sono:

IdAgg³⁵

Comprende due sottocampi:

1. Tipo aggregazione:

- Serie Documentale
- Serie di fascicoli
- Fascicolo

2. IdAggregazione

TIPOLOGIA DEL FASCICOLO (solo nel caso del fascicolo):

Indicare a scelta tra:

- affare³⁶
- attività³⁷
- persona fisica³⁸
- persona giuridica³⁶
- procedimento amministrativo³⁹

TEMPO DI CONSERVAZIONE

Indicare a scelta tra:

- 9999 (illimitata)
- 5 anni
- 10 anni
-

³⁵ L'idAgg è una sequenza di caratteri alfanumerici associata in modo univoco all'aggregazione documentale informatica in modo da consentirne l'identificazione, indica se si tratta di un Fascicolo o di una Serie Documentale o di una serie fascicoli.

³⁶ Il fascicolo per affare conserva i documenti relativi a una competenza non proceduralizzata, ma che nella consuetudine amministrativa la PA deve concretamente portare a buon fine. Il fascicolo per affare ha una data di apertura e una durata circoscritta.

³⁷ Il fascicolo per attività comprende i documenti prodotti nello svolgimento di un'attività amministrativa semplice che implica risposte obbligate o meri adempimenti, per la quale quindi non è prevista l'adozione di un provvedimento finale. Ha in genere durata annuale.

³⁸ Fascicolo per persona fisica o giuridica: comprende tutti i documenti, anche con classifiche diverse, che si riferiscono a una persona (fisica o giuridica). Quasi sempre i fascicoli intestati alle persone restano correnti per molti anni, costituendo serie aperte.

³⁹ Il fascicolo per procedimento amministrativo conserva una pluralità di documenti che rappresentano azioni amministrative omogenee e destinate a concludersi con un provvedimento amministrativo.

SOGGETTO:

Contiene cinque sottocampi:

1. **Ruolo:**
 - Amministrazione titolare
 - Amministrazioni partecipanti
 - Soggetto intestatario persona fisico
 - Soggetto intestatario persona giuridica
 - RUP (solo nel caso del fascicolo)
2. **Tipo soggetto** (come descritto nella seguente tabella)
3. **Nominativo** (come descritto nella seguente tabella)
4. **Codice identificativo** (come descritto nella seguente tabella)

Tipo soggetto	Nominativo corrispondente al tipo di soggetto indicato	Codice identificativo corrispondente al tipo di soggetto indicato
PF (Persona fisica)	Cognome e nome	Codice fiscale
PG (Organizzazione)	Denominazione	Codice fiscale
PA (Pubblica Amministrazione)	Denominazione Amministrazione	Codice IPA dell'Amministrazione
	Denominazione AOO	Codice IPA dell'AOO

5. **UO** (Obbligatorio solo nel caso si stia indicando Ruolo = RUP)

ASSEGNAZIONE

Contiene sei sottocampi:

1. **Tipo assegnazione:**
 - Per competenza
 - Per conoscenza
2. **Data inizio assegnazione**
3. **Data fine assegnazione**
4. **Ruolo** (Definito come da Ruolo del metadato Soggetti.)
5. **Tipo soggetto** (Definito come da Tipo soggetto del metadato Soggetti)
6. **Codice** (Definito come da Codice del metadato Soggetti)

DATA APERTURA**CLASSIFICAZIONE**

Contiene tre sottocampi:

1. **Indice di classificazione** (codifica secondo il Piano di classificazione utilizzato)
2. **Descrizione per esteso dell'Indice di classificazione indicato**
3. **URI di pubblicazione del Piano di classificazione**

PROGRESSIVO (progressivo numerico calcolato nell'ambito della chiave della classificazione o in ordine cronologico nell'ambito dell'anno)

CHIAVE DESCRITTIVA

Comprende i due sottocampi:

1. **Oggetto**
2. **Parole Chiave** (campo facoltativo da compilare con l'ausilio di attingendo da thesauri o da vocabolari controllati, per evitare ambiguità terminologiche e avere la possibilità di utilizzare il metadato come chiave di ricerca. Il metadato è ricorsivo fino ad un massimo di 5 occorrenze.)⁴⁰

DATA CHIUSURA

INDICE DOCUMENTI (elenco degli identificativi dei documenti contenuti nell'aggregazione; metadato ricorsivo che va aggiornato).

PROCEDIMENTO AMMINISTRATIVO

Comprende quattro sottocampi:

1. **Materia/Argomento/Struttura** per la quale sono stati catalogati i procedimenti amministrativi
2. **Procedimento**
3. **Catalogo dei procedimenti (Uri di pubblicazione del catalogo)**
4. **Fasi**

Indicare il tipo di fase:

- Preparatoria
- Istruttoria
- Consultiva
- Decisoria o deliberativa
- Integrazione dell'efficacia

Indicare per ciascuna fase⁴¹

- **Data inizio fase** (da aggiornare per ogni fase)
- **Data fine fase** (alla chiusura di ogni fase)

INDICE DOCUMENTI

Indicare:

- **l'IdDoc di ogni documento:** elenco degli identificativi dei documenti contenuti nell'aggregazione

POSIZIONE FISICA DELL'AGGREGAZIONE DOCUMENTALE: testo libero, obbligatorio nel caso di fascicoli ibridi; in questo caso indica la posizione della componente cartacea del fascicolo.

IdAggPrincipale : Identificativo univoco e persistente del livello superiore di fascicolazione nel caso in cui si stia definendo un sottofascicolo o una sottoserie.

⁴⁰ Serve ad evitare ambiguità terminologiche e avere la possibilità di utilizzare il metadato come chiave di ricerca. Il metadato è ricorsivo fino ad un massimo di cinque occorrenze.

⁴¹ "Data inizio fase" e "Data fine fase" deve considerarsi dinamico, destinato ad essere aggiornato con lo stato di avanzamento dell'iter del procedimento/processo.

CAPITOLO 5 - L'ARCHIVIO

Per Archivio si intende il complesso dei documenti prodotti e acquisiti nello svolgimento della propria attività e l'esercizio delle proprie funzioni dall'INRiM.

I documenti che compongono l'archivio sono pertanto collegati tra loro da un nesso logico e necessario detto vincolo archivistico; in questa accezione si usa spesso la parola fondo come sinonimo di archivio.

L'Archivio, pur suddiviso in archivio corrente, archivio di deposito e archivio storico, è unico.

L'Archivio corrente è il complesso di documenti conservati presso gli uffici usati prevalentemente per finalità pratico-amministrative, per il disbrigo degli affari in corso.

L'Archivio di deposito è il complesso di documenti relativi ad affari esauriti, non più occorrenti alla trattazione degli affari in corso ma non ancora destinata istituzionalmente alla conservazione permanente e alla consultazione da parte del pubblico.

Archivio storico è il complesso di documenti relativi ad affari esauriti, destinati alla conservazione permanente e alla consultazione da parte del pubblico per finalità di studio o non di studio (privati, amministrativi o legali)

L'INRiM, in armonia con la normativa vigente, assicura il principio della trasparenza dell'azione amministrativa, il diritto di accesso ai documenti dell'archivio corrente e dell'archivio di deposito, previsto dall'Art.124 del Codice dei Beni Culturali e del Paesaggio, nonché il diritto alla consultazione dei documenti dell'archivio storico, nei limiti imposti dalle tutele e protezione dei dati sensibili in esso contenuti.

Le aggregazioni documentali in cui è articolato l'Archivio sono formate con lo schema gerarchico descritto nel Capitolo 5 del *Manuale di Conservazione* dell'Ente.

5.1 L'archivio e la gestione documentale

La gestione documentale è un processo che può essere suddiviso in tre fasi principali: formazione, gestione e conservazione, in ragione delle diverse modalità di organizzazione ed utilizzo dei documenti:

Nell'ambito di ognuna delle suddette fasi si svolgono una serie di attività che si distinguono per complessità, impatto, natura, finalità e/o effetto, anche giuridico, alle quali corrispondono approcci metodologici e prassi operative distinte.

Una corretta gestione dei documenti sin dalla loro fase di formazione rappresenta la migliore garanzia per il corretto adempimento degli obblighi di natura amministrativa, giuridica e archivistica tipici della gestione degli archivi pubblici; nella fase di formazione devono essere perseguiti obiettivi di qualità, efficienza, razionalità, sistematicità, accessibilità e coerenza alle regole tecniche che presidiano la formazione dei documenti informatici, tenendo in debito conto le esigenze e i bisogni pratici del lavoro quotidiano.

La gestione dei documenti informatici prosegue con il suo trasferimento in un sistema di conservazione dedicato a questa funzione, che può anche essere delegata a terzi, come descritto nel Capitolo 10 ; la tenuta del sistema di conservazione, i requisiti del processo di conservazione, le responsabilità e i compiti del Responsabile della conservazione e del Responsabile del servizio di conservazione, e le loro modalità di interazione sono dettagliate nell'Allegato n.5 *Manuale di Conservazione*.

CAPITOLO 6 - LA GESTIONE DELL'ARCHIVIO CORRENTE

6.1. Definizione

Come già descritto nel cap. 5, per archivio corrente si intende il complesso dei documenti relativi ad affari, ad attività e a procedimenti amministrativi in corso di istruttoria e di trattazione o, comunque, verso i quali sussista un interesse non ancora esaurito.

La fase corrente della gestione documentale assume un'importanza strategica per un corretto funzionamento dell'attività amministrativa e una garanzia per le esigenze di trasparenza e integrità.

L'organizzazione dell'archivio deve rispondere a criteri di efficienza ed efficacia al fine di garantire la certezza dell'attività giuridico amministrativa dell'Ente e la conservazione stabile della memoria nel tempo; l'archivio corrente è, quindi, il primo elemento gestionale per il corretto funzionamento del sistema documentale.

Il responsabile del procedimento amministrativo è tenuto alla corretta gestione, conservazione e custodia dei documenti e dei fascicoli, siano essi di natura analogica, digitale o ibrida, relativi ai procedimenti di propria competenza; a esso è quindi affidata l'attuazione delle disposizioni contenute in questo manuale in merito al corretto funzionamento dell'archivio corrente di propria pertinenza.

La UO che crea il fascicolo mantiene la responsabilità amministrativa dei documenti creati durante la fase corrente e la fase di deposito; quindi, per la fase corrente e di deposito, viene garantito il libero accesso, da parte delle sole UO che hanno la titolarità dei documenti, attraverso il sistema di gestione documentale.

6.2. Gli strumenti della fase corrente

Il trattamento dell'intero sistema documentale dell'ente comporta la predisposizione di strumenti di gestione dell'archivio corrente che permettano un'efficiente organizzazione e consultazione della documentazione, a prescindere dai supporti dei documenti.

6.2.1. Registro di protocollo

Il registro di protocollo è lo strumento finalizzato all'identificazione univoca e certa dei documenti ricevuti e spediti mediante la registrazione di determinati elementi che caratterizzano ogni singolo documento.

Il registro di protocollo svolge, quindi, una fondamentale funzione giuridico probatoria attestando l'esistenza di un determinato documento all'interno del sistema di gestione documentale e garantendone l'autenticità.

6.2.2. Titolario (piano di classificazione)

Il titolare è l'insieme delle voci logiche gerarchicamente strutturate e articolate in gradi divisionali (titolo/classe/eventuale sottoclasse) stabilite sulla base delle funzioni dell'ente.

Ciascun documento, registrato in modalità arrivo, partenza, interno, anche non protocollato, è classificato in ordine alla corrispondenza tra il suo contenuto e la relativa voce attribuibile, desunta dal titolare e successivamente fascicolato.

La classificazione, necessaria e fondamentale, è prodromica all'inserzione di un documento all'interno di un determinato fascicolo.

La relazione tra i documenti (vincolo archivistico) di un'unità archivistica è garantita dalla segnatura archivistica completa (anno di istruzione, classificazione, numero del fascicolo).

Il titolario può essere corredato da un'appendice denominata voci di indice; si tratta di un ulteriore strumento, strettamente correlato al titolario, che agevola le operazioni di classificazione. In esso sono presentate possibili varianti lessicali, trattate e riportate in modo analitico, che possono essere incontrate nel contenuto del documento.

Il titolario e, di conseguenza, il prontuario delle voci d'indice, sono inseriti nel sistema di gestione documentale.

Possono essere soggetti a revisione periodica, qualora ciò si renda necessario a seguito di modifiche di carattere normativo e/o statutario; in questo caso, essi sono adottati a partire dal 1° gennaio dell'anno successivo a quello di approvazione.

Il sistema di gestione documentale garantisce che le voci del titolario siano storicizzate, mantenendo stabili i legami dei fascicoli e dei documenti con la struttura del titolario vigente al momento della loro registrazione.

Il titolario adottato dall'INRiM è riportato, unitamente al prontuario delle diverse voci in esso contenute, nell'Allegato n. 2 di questo manuale

6.3. Registri e repertori informatici

6.3.1 Repertorio - Nozione

Questo termine definisce innanzitutto un peculiare tipo di aggregazione documentale che raccoglie documenti identici per forma e provenienza, ma difforni per contenuto, disposti in sequenza cronologica. Ciascun documento, in base a tale ordine, è identificato con un numero progressivo cui viene riconosciuta una valenza probatoria. Il repertorio può essere quindi considerato una maniera differente di organizzazione e ordinamento della documentazione e nello stesso tempo una forma differente di registrazione, parallela al registro di protocollo, prevista dall'art. 53, comma 5 del DPR n. 445/2000, che consente registrazioni particolari per determinate categorie di documenti.

In altre parole: gli atti per i quali è prevista una registrazione particolare sono annotati in registri (un tempo cartacei ora informatici), detti appunto repertori, analoghi a quelli di protocollo che rivestono una valenza probatoria ad essi assimilabile. Si possono formare quindi repertori dei decreti, delle deliberazioni, dei contratti, delle sentenze, etc.

I documenti sono comunque inseriti nel fascicolo archivistico di loro pertinenza per la loro minuta e in originale (o in copia conforme) nel repertorio.

Il complesso dei documenti registrati a repertorio per forma omogenea costituisce una serie.

La numerazione di repertorio si rinnova ogni anno solare: inizia il 1° gennaio e termina il 31 dicembre di ogni anno.

6.3.2. Repertori attivi

Elenco dei repertori attivi	
Albo ufficiale in arrivo	Registri Iva acquisti istituzionali intraUe
Comunicazione	Registri Iva acquisti istituzionali extraUe
Contratti	Registri Iva acquisti istituzionali San Marino
Delibere Consiglio di Amministrazione interno	Registri Iva acquisti promiscui
Proposte	Registri Iva acquisti commerciali
Protocollo particolare in Arrivo	Registri Riepilogativi Acquisti Promiscui
Protocollo particolare in Partenza	Registri Riepilogativi Acquisti Istituzionali Non Residenti
Verbale consiglio di Amministrazione	Registri Riepilogativi Vendite
DURC	Registri Riepilogativi Acquisti Commerciali
Rapporto di versamento	Libri Giornale
Registro informatico giornaliero di protocollo	Libri Inventari
Registri Iva acquisti	Libri Cespiti
Registri Iva vendite	Liquidazioni IVA
Decreto del Direttore Generale	Elenchi Intrastat
Decreto del Presidente	Registri Dichiarazioni di Intento
Contratti in forma pubblica amministrativa	Registri Iva Acquisti Istituzionali Residenti
Determine	Registri Riepilogativi Acquisti Istituzionali Residenti
Registri Iva Corrispettivi	Registri delle Tirature
Circolari del Direttore Generale	Verbali di gara
Autorizzazioni missioni e rimborsi	

6.3.3. Repertorio dei fascicoli

I fascicoli istruiti durante lo svolgimento dell'attività amministrativa, sono annotati nel repertorio dei fascicoli che viene costantemente aggiornato.

Il repertorio dei fascicoli, ripartito per ciascun titolo del titolario, è lo strumento di gestione e di reperimento dei fascicoli; la struttura del repertorio rispecchia quella del titolario di classificazione e, di conseguenza, varia in concomitanza con l'aggiornamento di quest'ultimo.

Mentre il titolario rappresenta, in astratto, le funzioni e le competenze che l'ente può esercitare in base alla propria missione istituzionale, il repertorio dei fascicoli rappresenta, in concreto, le attività svolte e i documenti prodotti in relazione a tali attività.

6.4. Massimario di selezione

Il massimario di selezione è uno strumento da utilizzare durante la fase di deposito dell'Archivio, come previsto dall'art. 68 del TUDA⁴².

Il massimario di selezione (Allegato 4 a questo documento) è lo strumento con cui l'Ente individua le disposizioni di massima e definisce i criteri e le procedure attraverso i quali i documenti, non rivestendo interesse storico ai fini della conservazione permanente e avendo esaurito un interesse pratico e corrente, possono essere eliminati legalmente, previa autorizzazione della Soprintendenza Archivistica territoriale, ai sensi del D.lgs. 22 gennaio 2004, n. 42.

Il massimario individua le tipologie documentali in rapporto ai procedimenti che le costituiscono e, a partire da tali tipologie, rende possibile applicare i criteri e le disposizioni atti ad individuare i termini di conservazione: il massimario è, quindi, uno strumento indirizzato sia alla conservazione che all'eliminazione dei documenti (scarto).

Del massimario è parte integrante il prontuario di selezione nel quale sono menzionati i tempi di conservazione in relazione alle tipologie documentarie.

Le operazioni di selezione, necessarie a garantire la corretta gestione e la conservazione del complesso documentale dell'Ente, avvengono nella fase di deposito, in modo tale da sedimentare solo la documentazione ritenuta rilevante ai fini della conservazione a lungo termine.

La proposta di scarto formulata su apposito modulo (*elenco di scarto*) corredata da disposizione dirigenziale, in cui sono indicate le tipologie documentarie, gli estremi cronologici, le motivazioni dell'eliminazione e, solo per i documenti analogici, il volume (espresso in metri lineari o in chilogrammi,) è inviata alla Soprintendenza Archivistica del Piemonte e della Valle d'Aosta nelle modalità concordate; come già sopra esposto, infatti, l'attività è soggetta ad autorizzazione della Soprintendenza archivistica ai sensi del D.lgs. 42/2004 art. 21.

A seguito dell'autorizzazione, l'Ente avvia il procedimento per individuare il soggetto legittimato al ritiro del materiale e alla eliminazione fisica dei documenti; la ditta affidataria individuata effettua le operazioni di ritiro e macero della documentazione cartacea con rilascio di relativo verbale di esecuzione.

⁴² L'art 68 c. 1 del TUDA prevede venga elaborato il piano di conservazione degli archivi (Massimario di selezione e scarto dei documenti amministrativi) per la definizione dei criteri di organizzazione dell'archivio, di selezione periodica e di conservazione permanente dei documenti, e che tale piano debba essere integrato con il sistema di classificazione.

Per i fascicoli informatici la proposta di scarto segue lo stesso iter per quanto riguarda l'autorizzazione della Soprintendenza e il responsabile della gestione documentale invierà un documento informatico firmato digitalmente.

Il fascicolo inerente al procedimento di scarto è a conservazione illimitata.

6.5. Spostamento di un archivio corrente analogico

Qualora una UO dovesse spostare la documentazione corrente dovrà darne informazione tempestiva al Responsabile della gestione documentale, producendo un apposito elenco dei fascicoli soggetto di spostamento.

Lo spostamento dell'archivio corrente non necessita di alcuna autorizzazione preventiva da parte della Soprintendenza archivistica pertinente per territorio.⁴³

⁴³ D.lgs 42/2004, art. 21, c. 3: «Lo spostamento degli archivi correnti dello Stato e degli enti ed istituti pubblici non è soggetto ad autorizzazione».

CAPITOLO 7. – IL PROTOCOLLO INFORMATICO

La protocollazione rappresenta una delle fasi determinanti nella gestione documentale; il protocollo è uno strumento tecnico necessario per gestire la documentazione organizzando la fase corrente e quelle successive.

Il registro di protocollo è un atto pubblico di fede privilegiata; come tale, fa fede fino a querela di falso e, in particolare, circa la data e l'effettivo ricevimento o spedizione di un documento determinato, di qualsiasi forma e contenuto. Esso, dunque, è idoneo a produrre effetti giuridici tra le parti.

Il registro di protocollo ha cadenza annuale: inizia il 1° gennaio e termina il 31 dicembre di ogni anno ed è unico per ciascuna delle AOO.

7.1. La registrazione e la segnatura di protocollo

La registrazione di protocollo è l'insieme dei metadati che il registro di protocollo deve memorizzare, per tutti i documenti ricevuti o spediti dalla Pubblica Amministrazione, al fine di garantirne l'identificazione univoca e certa.

Sono oggetto di registrazione obbligatoria i documenti ricevuti e spediti dall'Ente, ossia i cui destinatari sono esterni all'ente o scambiati tra AOO dello stesso ente, e tutti i documenti informatici, ad eccezione dei documenti informatici già soggetti a registrazione particolare e di quelli espressamente esclusi dalla normativa vigente dall'art. 53, comma 5 del TUDA⁴⁴.

Per registrazione di protocollo si intende l'apposizione o l'associazione al documento, in forma permanente e non modificabile, delle informazioni riguardanti il documento stesso.

Il registro di protocollo memorizza l'insieme dei metadati di tutti i documenti ricevuti o spediti dalla Pubblica Amministrazione, al fine di garantirne l'identificazione univoca e certa, così come disposto dall'articolo 53, comma 1, del TUDA, che indica le informazioni che caratterizzano il registro di protocollo a cui si aggiungono le informazioni inerenti l'assegnazione interna all'amministrazione e la classificazione.

La registrazione si effettua di norma entro la giornata di arrivo o comunque entro 24 ore lavorative dal ricevimento o, se intercorrono dei giorni festivi o di chiusura programmata degli Uffici, nel primo giorno lavorativo utile.

Ogni numero di protocollo individua un unico documento e gli eventuali allegati allo stesso e, di conseguenza, ogni documento con i relativi allegati reca un solo numero di protocollo immutabile.

La registrazione di protocollo per ogni documento è effettuata mediante la memorizzazione di:

- elementi obbligatori immutabili,
- elementi obbligatori modificabili
- elementi non obbligatori e modificabili.

⁴⁴ L'art. 53, comma 5 del TUDA prevede che: "Sono oggetto di registrazione obbligatoria i documenti ricevuti e spediti dall'amministrazione e tutti i documenti informatici. Ne sono esclusi le gazzette ufficiali, i bollettini ufficiali e i notiziari della pubblica amministrazione, le note di ricezione delle circolari e altre disposizioni, i materiali statistici, gli atti preparatori interni, i giornali, le riviste, i libri, i materiali pubblicitari, gli inviti a manifestazioni e tutti i documenti già soggetti a registrazione particolare dell'amministrazione".

Ai sensi dell'art 54 del TUDA, la registrazione degli elementi obbligatori immodificabili del protocollo informatico non può essere modificata, integrata, cancellata ma soltanto annullata mediante un'apposita procedura in capo al Responsabile della gestione documentale e a persone espressamente delegate.

L'inalterabilità e l'Immodificabilità della registrazione di protocollo devono essere garantite dal sistema di gestione documentale.

7.2 Registratura

Gli elementi obbligatori immodificabili servono ad attribuire al documento data e provenienza certa attraverso la registrazione di determinate informazioni rilevanti sul piano giuridico-probatorio.

Essi sono:

- ❖ numero di protocollo progressivo e costituito da almeno sette cifre numeriche;
- ❖ data di registrazione;
- ❖ corrispondente, ovvero:
 - mittente per il documento in arrivo,
 - destinatario per il documento in partenza;
- ❖ oggetto;
- ❖ impronta del documento informatico;
- ❖ numero degli allegati;
- ❖ descrizione degli allegati.

L'insieme di tali elementi è denominato registratura.

7.3. Data e ora regolate sul UTC

Il server del protocollo informatico è regolato sul tempo universale coordinato (UTC) e, in particolare, sulla scala di tempo nazionale italiana UTC (IT).

7.4. Segnatura

La segnatura di protocollo, così come descritta dall'art. 55 del TUDA, consiste nell'apposizione o nell'associazione al documento in originale, in forma non modificabile e permanente, delle informazioni memorizzate nel registro di protocollo.

Essa consente di individuare ciascun documento in modo univoco.

7.4.1. Segnatura del documento informatico

Le informazioni minime da associare al documento informatico sono:

- ❖ codice identificativo dell'amministrazione;
- ❖ codice identificativo dell'AOO;

- ❖ codice identificativo del registro;
- ❖ numero di protocollo,
- ❖ data di protocollo;
- ❖ anno solare di riferimento del registro di protocollo.

Oltre alle informazioni minime la segnatura prevede:

- ❖ classificazione in base al titolario di classificazione adottato e vigente al momento della registrazione del documento;
- ❖ codice identificativo dell'ufficio a cui il documento è assegnato;
- ❖ ogni altra informazione utile o necessaria, già disponibile al momento della registrazione.

Quando il documento è indirizzato ad altre amministrazioni ed è sottoscritto con firma digitale e trasmesso con strumenti informatici, la segnatura di protocollo può includere le informazioni di registrazione del documento purché siano adottate idonee modalità di formazione dello stesso in formato pdf/a mentre la sua sottoscrizione viene effettuata mediante la busta crittografica PAdES.

7.4.2. Segnatura del documento analogico

Le informazioni da associare al documento analogico, tramite timbro o altro sistema di identificazione del documento come stampa della segnatura, desunte dal sistema di protocollo e gestione documentale, sono:

- ❖ l'identificazione in forma sintetica o estesa dell'amministrazione e dell'AOO individuata ai fini della registrazione e della gestione del documento;
- ❖ il numero progressivo di protocollo;
- ❖ la data di protocollo nel formato GGMMAAAA;
- ❖ la classificazione in base al titolario di classificazione adottato e vigente al momento della registrazione del documento;
- ❖ la sigla della UO/RPA o delle UO/RPA a cui il documento è assegnato per competenza e responsabilità;
- ❖ le eventuali sigle della UO/RPA o delle UO/RPA in copia conoscenza.

Gli elementi della segnatura devono essere presenti sia nei documenti prodotti da registrare in partenza, sia nei documenti scambiati tra le UO della medesima AOO (protocollo tra uffici).

7.5. Modalità di produzione e di conservazione delle registrazioni

Ogni registrazione di protocollo informatico produce un record nel sistema di gestione documentale che viene accodato in una base dati accessibile esclusivamente all'amministratore del sistema.

Ogni operazione di inserimento e modifica viene registrata inoltre su un file di log corredato da codici di controllo in grado di evidenziare eventuali tentativi di manipolazione.

Da esso l'amministratore del sistema è in grado di ottenere l'elenco delle modifiche effettuate su una data registrazione, permettendo quindi una completa ricostruzione cronologica di ogni registrazione e successiva lavorazione (smistamento, invio per conoscenza, restituzione, fascicolatura ecc.), ottenendo in dettaglio:

- ❖ nome dell'utente;
- ❖ data e ora;
- ❖ postazione di lavoro;
- ❖ tipo di operazione (inserimento/modifica/visualizzazione/cancellazione);
- ❖ valore dei campi soggetti a modifica.

Al fine di garantire l'immodificabilità delle registrazioni, il registro informatico di protocollo giornaliero viene trasmesso in conservazione entro la giornata lavorativa successiva.

7.6. La registrazione differita (o "protocollo differito")

Per "protocollo differito" si intende la registrazione di documenti in arrivo, autorizzata con provvedimento motivato del Responsabile della gestione documentale o da persona espressamente delegata, in cui sono indicati nello specifico la data alla quale si differisce la registrazione del documento stesso e la causa che ne ha determinato il differimento.

È possibile effettuare la registrazione differita di protocollo nel caso di temporaneo, eccezionale e imprevisto carico di lavoro e qualora dalla mancata registrazione di un documento nell'ambito del sistema nel medesimo giorno lavorativo di ricezione, possa venire meno un diritto di terzi. La registrazione differita di protocollo informatico è possibile esclusivamente per i documenti in arrivo.

La registrazione differita non si applica per i documenti informatici pervenuti via PEC, in quanto la PEC ha lo stesso valore giuridico della raccomandata AR e quindi fa fede la data di invio della PEC allo stesso modo del timbro postale di invio della raccomandata AR.

7.7. La ricevuta di avvenuta registrazione

La ricevuta di avvenuta protocollazione prodotta dal sistema di protocollo deve riportare i seguenti dati:

- ❖ il numero e la data di protocollo;
- ❖ l'indicazione dell'AOO che ha acquisito il documento;
- ❖ il mittente;
- ❖ l'oggetto;
- ❖ numero e descrizione degli allegati se presenti;
- ❖ l'operatore di protocollo che ha effettuato la registrazione.

7.7.1. La ricevuta di avvenuta registrazione del documento analogico

Qualora il documento analogico sia consegnato direttamente dal mittente o da altra persona a ciò delegata e sia richiesto il rilascio di una ricevuta attestante l'avvenuta consegna del documento, è cura di chi effettua

la protocollazione rilasciare la ricevuta di avvenuta protocollazione prodotta direttamente dal sistema di gestione documentale.

La ricevuta può essere altresì ritirata dall'interessato o da persona espressamente delegata nei giorni successivi.

7.7.2. La ricevuta di avvenuta registrazione del documento informatico

Qualora il documento informatico sia pervenuto tramite PEC, la ricevuta di protocollazione è rilasciata direttamente dal sistema di gestione documentale.

Se il documento informatico è pervenuto tramite e-mail, la ricevuta, se richiesta, sarà generata in formato pdf o pdf/a e inviata via e-mail al mittente.

7.8. Documenti esclusi dalla registrazione di protocollo

Sono esclusi per legge dalla registrazione di protocollo, come previsto dall'art. 53 - comma 5 del DPR n. 445 del 28/12/2000:

- ❖ le gazzette ufficiali;
- ❖ i bollettini ufficiali P.A.;
- ❖ i notiziari P.A.;
- ❖ le note di ricezione delle circolari;
- ❖ le note di ricezione di altre disposizioni;
- ❖ i materiali statistici;
- ❖ gli atti preparatori interni;
- ❖ i giornali;
- ❖ le riviste;
- ❖ i libri;
- ❖ i materiali pubblicitari;
- ❖ gli inviti a manifestazioni

Sono parimenti esclusi dalla registrazione di protocollo:

- ❖ i certificati medici dei dipendenti. Se pervenuti via PEC, essi sono registrati ma non protocollati.
- ❖ i documenti già soggetti a registrazione mediante registri particolari dell'Amministrazione e descritti al §6.3.2.
- ❖ i documenti già soggetti ad altro tipo di registrazione particolare presso l'Amministrazione;
- ❖ buste paga;
- ❖ certificazione unica;

- ❖ buoni d'ordine;
- ❖ disposizioni di pagamento;
- ❖ distinte di liquidazione;
- ❖ mandati;
- ❖ reversali;
- ❖ fatture;
- ❖ verbali di violazione del codice della strada;
- ❖ verbali di violazioni amministrative.
- ❖ allegati, se non accompagnati da lettera di trasmissione, compresi gli elaborati tecnici;
- ❖ documenti di interesse effimero (biglietti d'occasione, condoglianze, auguri, congratulazioni, ecc.);
- ❖ richieste di ferie ed altri permessi;
- ❖ comunicazioni informali tra uffici;
- ❖ corsi di aggiornamento;
- ❖ documenti di trasporto, bolle di accompagnamento e lettere di vettura corrieri;
- ❖ estratti conto bancari e postali;
- ❖ richieste di rimborso spese e missioni;
- ❖ ricevute di ritorno delle raccomandate a/r.
- ❖ le comunicazioni di bandi di concorso da parte di enti diversi

Sono esclusi dalla registrazione di protocollo atti, documenti e certificazioni scaricati da portali e già tracciati su apposite piattaforme che ne curano la registrazione, attribuendo loro un codice univoco e la persistenza nel tempo.

7.9. Il registro giornaliero di protocollo

Il Registro giornaliero di protocollo è costituito dall'elenco delle informazioni inserite con l'operazione di registrazione di protocollo nell'arco di uno stesso giorno.

Il registro giornaliero di protocollo è prodotto in maniera automatica dal software di gestione documentale entro il giorno lavorativo seguente, mediante la generazione o il raggruppamento delle informazioni registrate secondo una struttura logica predeterminata e memorizzato in forma statica, immodificabile e integra.

Attualmente, in base allo stato dell'arte delle tecnologie e dei formati, è utilizzato il formato XML, a mente dell'Allegato 2 alle Linee Guida AgID

Le succitate Linee guida AgID, al paragrafo 3.1.6, stabiliscono che il registro giornaliero di protocollo deve essere trasmesso al Sistema di Conservazione entro la giornata lavorativa successiva, all'interno della

struttura organizzativa del soggetto produttore; nel caso dell'INRiM, il registro giornaliero di protocollo viene trasmesso dal sistema di gestione Titulus al sistema di conservazione CONSERVA di Cineca.

7.10. Il registro di emergenza

Nei casi di emergenza, in cui non sia possibile utilizzare il sistema di protocollo informatico, è necessario registrare i documenti su un supporto alternativo, denominato Registro di emergenza.

L'utilizzo del Registro di emergenza è previsto solo in casi di estrema gravità, dove l'emergenza colpisca l'intero campus o colpisca il Conservatore CINECA e il sistema di protocollo informatico non possa essere utilizzato per tempi superiori alle ventiquattro ore.

Qualora l'impossibilità di utilizzare la procedura informatica si prolunghi oltre le 24 ore, per cause di eccezionale gravità, il Responsabile della gestione documentale contatta il Conservatore CINECA ed autorizza l'uso del registro di emergenza per periodi successivi di non più di una settimana.

Le procedure per avvalersi del Registro di emergenza predisposte da CINECA sono le seguenti:

SCENARIO 1: blocco del sistema da parte di INRiM

Vengono predisposti da CINECA un ambiente e una utenza dedicata su una macchina pubblica del CINECA, su cui sarà possibile registrare i documenti.

Si specifica che:

- l'utente è abilitato a registrare solo protocolli in arrivo o in partenza;
- ai documenti non si possono associare file (i file verranno inseriti a posteriori dall'Amministratore di Titulus, quando tornerà in linea);
- i protocolli saranno temporanei e riportati a regime in un apposito campo dedicato al registro di emergenza.

SCENARIO 2: stato di blocco del sistema da parte di CINECA

Verranno predisposti uno o più file excel (uno per ogni registro di protocollo) in cui verranno segnati gli eventuali protocollo urgenti in arrivo o partenza.

I campi che è necessario valorizzare sono:

- AOO
- Causa e data/ora inizio del blocco
- Data/ora fine del blocco
- Oggetto
- mittente/destinatario
- Nome repertorio
- numero protocollo/repertorio temporaneo

Al ripristino si provvederà ad inserire manualmente i documenti registrati temporaneamente sul registro di emergenza, completandoli di tutti i dati obbligatori.

Sulla registrazione, nel campo delle annotazioni si riporteranno gli estremi del provvedimento di autorizzazione, la causa, la data e l'ora di inizio dell'interruzione nonché la data e l'ora del ripristino della funzionalità del sistema.

7.11. Il Protocollo riservato

Sono previste particolari forme di riservatezza e di accesso controllato al protocollo unico per:

- ❖ documenti di carattere politico e di indirizzo di competenza del Direttore Generale che, se resi di pubblico dominio, potrebbero ostacolare il raggiungimento degli obiettivi prefissati;
- ❖ documenti dalla cui conoscenza, anche da parte del personale dell'ente, possa derivare pregiudizio a terzi o al buon andamento dell'attività amministrativa;
- ❖ tipologie di documenti individuati dalla normativa vigente relativamente a dati sensibili i cd. sensibilissimi;
- ❖ documenti legati a vicende di persone o a fatti privati anche prive di dati sensibili;
- ❖ documenti relativi a procedimenti disciplinari del personale dipendente;
- ❖ documenti legati a vicende di persone o a fatti privati contenenti sensibili e dati giudiziari.

Le tipologie di documenti soggetti a forme di riservatezza e rientranti tra le categorie documentali sopra descritte saranno individuate dal Responsabile della gestione documentale d'intesa con i Responsabili delle UO.

Per questi documenti i diritti di accesso e di visione degli utenti di Titulus vengono gestiti e attivati attraverso la *Access Control List (ACL)* che permette di regolamentare l'accesso ai documenti registrati nel sistema documentale e di escludere in modo selettivo la visione dei documenti riservati, garantendone, di conseguenza, la riservatezza (cfr. § 2.4).

Una volta versata all'Archivio di deposito la documentazione riservata sarà conservata nel rispetto della normativa sulla tutela dei dati personali.

Per ragioni informative e di tenuta complessiva dell'archivio particolare, presso la UO competente viene conservato l'originale dei documenti analogici registrati; per i documenti informatici non viene fatta alcuna stampa.

Agli altri eventuali destinatari in copia conoscenza viene inoltrata una copia del documento analogico sempre in busta chiusa, sigillata e firmata sui lembi di chiusura.

I soggetti destinatari di documentazione riservata sono responsabili della corretta tenuta della documentazione stessa anche nel rispetto della normativa sulla tutela dei dati personali.

La posta in arrivo su cui il mittente esplicita direttamente e chiaramente la volontà di riservatezza ("Riservata", "SPM", "Personale" o simili) non deve essere aperta ma consegnata direttamente al destinatario che deciderà se è il caso di richiedere un protocollo riservato.

7.11.1 Tutela dei dati personali

Le procedure e il sistema di protocollo informatico sono sviluppati nel rispetto delle norme sul diritto di accesso e sulla protezione dei dati personali; l'accesso al sistema di protocollo informatico e la trattazione dei dati di protocollo è consentito solo al personale autorizzato.

In particolare i dipendenti dell'ufficio del protocollo (UO Segreteria Generale) sono tenuti a non divulgare notizie di natura particolare o riservata, a non trarre profitto personale o a procurare danno a terzi e all'amministrazione dalla conoscenza di fatti e documenti riservati.

L'amministrazione titolare dei dati di protocollo e dei dati personali contenuti nella documentazione di propria pertinenza dà attuazione al dettato del Regolamento (UE) 2016/679 del Parlamento europeo e del D.lgs. 196/2003.

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

CAPITOLO 8 - FLUSSO DI LAVORAZIONE DEI DOCUMENTI

Il presente capitolo descrive il flusso di lavorazione dei documenti ricevuti, spediti o interni, secondo le definizioni riportate nel § 8.1.

Nel presente capitolo, inoltre, sono riportate le regole di registrazione per i documenti pervenuti secondo particolari modalità di trasmissione.

I flussi di lavorazione dei documenti all'interno della AOO sono stati predisposti prendendo in esame i documenti che possono avere rilevanza giuridico probatoria.

Essi si riferiscono ai documenti:

- ❖ ricevuti dalla AOO dall'esterno;
- ❖ inviati dalla AOO all'esterno.

La comunicazione informale tra uffici, intesa come lo scambio di informazioni, con o senza documenti allegati, ricevuto e trasmesso per posta elettronica interna non interessa il sistema di protocollo.

8.1. Distinzione dei documenti in base allo stato di trasmissione

I documenti, siano essi analogici o informatici, in base allo stato di trasmissione si distinguono in:

- ❖ documenti in arrivo;
- ❖ documenti in partenza;
- ❖ documenti interni (scambiati tra UO);
- ❖ documenti interni di preminente carattere giuridico-probatorio
- ❖ comunicazioni informali tra uffici
- ❖ comunicazioni tra AOO

Per documenti in arrivo si intendono tutti i documenti di rilevanza giuridico probatoria acquisiti dall'Amministrazione nell'esercizio delle proprie funzioni e provenienti da un diverso soggetto pubblico o privato.

Per documenti in partenza si intendono i documenti di rilevanza giuridico probatoria prodotti dall'Amministrazione pubblica nell'esercizio delle proprie funzioni e indirizzati ad un diverso soggetto pubblico o privato ed anche ai propri dipendenti come persone fisiche e non nell'esercizio delle loro funzioni.

Per documenti interni o tra uffici si intendono i documenti scambiati tra le diverse Unità Organizzative Responsabili (UO).

I documenti interni di preminente carattere giuridico-probatorio sono quelli redatti dal personale nell'esercizio delle proprie funzioni al fine di documentare fatti inerenti all'attività svolta e alla regolarità delle azioni amministrative o qualsiasi altro documento dal quale possano nascere diritti, doveri o legittime aspettative di terzi.

Per comunicazioni informali tra uffici si intende lo scambio di informazioni, con o senza documenti allegati, delle quali è facoltativa la conservazione.

Questo genere di comunicazioni è ricevuto e trasmesso per posta elettronica interna e, di norma, non è protocollato.

Per comunicazione tra AOO di documenti amministrativi protocollati si intende lo scambio di documenti amministrativi protocollati scambiati tra AOO appartenenti allo stesso ente o ad enti differenti. Questo tipo di comunicazione segue le prescrizioni contenute nell' Allegato 6 alle Linee Guida AgID.

8.2. Flusso del documento informatico in arrivo

La documentazione in arrivo perviene all'Ufficio del Protocollo e viene classificata, registrata nel sistema di gestione documentale e smistata alla UO competente o al RPA competente, secondo l'assegnazione dei procedimenti già compiuta dal Responsabile della UO.

L'informativa della registrazione è resa immediatamente disponibile in due modalità:

- ❖ attraverso un messaggio e-mail che il sistema di gestione documentale invia automaticamente alla casella di posta elettronica indicata dal Responsabile della UO;
- ❖ attraverso l'accumulo nella vaschetta del menu principale del sistema di gestione documentale.

I documenti amministrativi informatici in arrivo possono pervenire con diverse modalità:

- ❖ tramite posta elettronica convenzionale (e-mail);
- ❖ tramite posta elettronica certificata (PEC);
- ❖ su supporto rimovibile (Cd ROM, DVD, ecc.) con consegna diretta o trasmesso a mezzo servizio postale o corriere;
- ❖ da altre banche dati.

I documenti che transitano attraverso il servizio postale (pubblico o privato), indirizzati a tutta l'amministrazione, sono consegnati quotidianamente alla Segreteria Generale, che si fa carico di selezionare e smistare la corrispondenza.

8.2.1. Ricezione di documenti informatici nella casella di posta elettronica istituzionale

L'e-mail è un mezzo di trasmissione che può anche costituire documento informatico se il messaggio è contenuto nel corpo della mail stessa.

Si possono avere i seguenti casi:

- ❖ documento che arriva alla casella di posta elettronica istituzionale dell'INRiM;
- ❖ documento allegato alla e-mail istituzionale: con PDF creator si crea il PDF/a e lo si associa al sistema di gestione documentale procedendo alla registrazione in arrivo con le consuete modalità;
- ❖ documento costituito dal corpo della mail: con PDF Creator si crea il pdf/a e lo si associa al sistema di gestione documentale procedendo alla registrazione in arrivo con le consuete modalità.
I documenti informatici così pervenuti saranno protocollati, di norma, entro le 24 ore lavorative dal giorno di arrivo;
- ❖ il documento via e-mail può non essere firmato e allora lo si dichiara nel campo immodificabile.

Se è firmato digitalmente non serve alcuna descrizione.

8.2.2. Ricezione dei documenti informatici tramite la casella di posta elettronica certificata (PEC) istituzionale

La posta elettronica certificata - PEC- è un vettore attraverso il quale è spedito/ricevuto un documento informatico che può essere allegato o incorporato nel corpo stesso.

Il documento informatico trasmesso tramite casella di posta elettronica certificata si intende spedito dal mittente se inviato al proprio gestore e si intende consegnato al destinatario se reso disponibile all'indirizzo elettronico da questi dichiarato, nella casella di posta elettronica del destinatario messa a disposizione dal gestore.

Una registrazione (sia in arrivo che in partenza via PEC), non permette di modificare i file informatici associati ad essa.

Il sistema di gestione documentale genera tutte le ricevute previste dalla normativa in materia di posta elettronica certificata.

La ricezione dei documenti informatici è assicurata tramite la casella di istituzionale PEC, accessibile alla Segreteria Generale dell'INRIM quale unica Unità Organizzativa responsabile della protocollazione in arrivo. La PEC utilizzata dall'Ente è di tipo "chiuso" e incorporata nel sistema di gestione documentale.

I principi di gestione della casella di PEC rispondono ad alcuni obblighi imprescindibili:

- ❖ Il documento informatico che perviene nella casella di PEC va gestito, di norma, entro le 24 ore lavorative successive alla ricezione.
- ❖ il mittente, che non sempre coincide con il proprietario della PEC, deve essere sempre identificato.
- ❖ qualora il documento ricevuto in allegato alla PEC non sia pdf o pdf/a (con o senza firma digitale) viene comunque registrato al protocollo.
- ❖ se il documento informatico è privo di firma, questo va evidenziato in un campo immutabile con la dicitura: *firma mancante*.
- ❖ la verifica della validità della firma digitale è a cura del RPA del documento.
- ❖ spetta al Responsabile della gestione documentale valutare se accettare il documento informatico non sottoscritto o non conforme agli standard.

Per altri esempi di buone norme si veda il Capitolo 9 - Casistica e comportamenti-

I documenti informatici così pervenuti sono protocollati, di norma, entro le 24 ore lavorative successive dal giorno di arrivo.

8.2.3. Ricezione di documenti informatici su supporti rimovibili

I documenti digitali possono pervenire anche in modalità diverse dalla posta elettronica o dalla posta elettronica certificata e quindi su supporti diversi, quali, ad esempio, Hard-Disk, CD, DVD; l'Ufficio Protocollo verifica la leggibilità dei dati contenuti nel supporto informatico e provvede alla registrazione solo in caso di esito positivo.

È cura della UO responsabile verificarne le caratteristiche e la provenienza certa.

I documenti informatici così pervenuti sono protocollati, di norma, entro le 24 ore lavorative successive dal giorno di arrivo.

8.3 Flusso del documento analogico in arrivo

La corrispondenza analogica in arrivo perviene alla AOO secondo le seguenti modalità:

- ❖ posta pervenuta per il tramite di Poste italiane spa e di altri gestori autorizzati;
- ❖ posta recapitata personalmente, *brevi manu*;
- ❖ posta ricevuta via telefax.

Di norma si procede all'apertura e alla registrazione di protocollo nella stessa giornata di consegna e comunque, di norma, entro le 24 ore lavorative successive alla ricezione.

Nel caso in cui non sia possibile l'immediata protocollazione di un documento consegnato a mano (ad es., per momentanea indisponibilità del sistema informatico), viene concordato l'invio telematico della ricevuta di protocollo all'indirizzo mail fornito da chi consegna il documento.

In casi eccezionali, si rilascia la fotocopia del frontespizio del documento col timbro del protocollo.

8.3.1. Ricezione di documenti cartacei a mezzo posta convenzionale (Poste italiane spa e di altri gestori autorizzati)

La corrispondenza in ingresso, di norma, va aperta e protocollata nel medesimo giorno lavorativo di ricezione.

Le operazioni di registrazione a protocollo e di segnatura di tutti i documenti in arrivo alla AOO, nonché la classificazione dei documenti medesimi sono centralizzate e svolte dagli addetti del Servizio di protocollo informatico.

Il Servizio provvede, nell'operazione di smistamento dei documenti pervenuti, all'assegnazione di ciascun documento alla UO competente per la trattazione del relativo procedimento e/o affare.

L'operazione di assegnazione dei documenti comprende l'inoltro informatico, nell'ambito del sistema di protocollo, dell'immagine del documento scansionato; l'originale analogico viene posto a disposizione del RPA inserendo la busta nell'apposito casellario.

Il responsabile della UO assegnataria viene avvisato tramite e-mail inoltrato dal sistema di protocollo dell'avvenuta assegnazione del documento; egli può qualora ritenga che il documento non sia di sua competenza, restituirlo, lo stesso giorno del ricevimento, al servizio protocollo il quale provvederà ad una nuova assegnazione.

La UO assegnataria è incaricata delle successive operazioni di fascicolazione, vale a dire della corretta creazione e gestione del fascicolo relativo all'affare o al procedimento cui il documento si riferisce.

8.3.2. Apertura delle buste

Tutte le buste sono aperte a cura dell'Ufficio del protocollo, afferente alla Segreteria Generale.

Fanno eccezione e pertanto non vanno aperte, le buste relative a gare d'appalto o concorsi che verranno inviate alla UO competente.

8.3.3. Conservazione ed eliminazione delle buste

Le buste pervenute tramite posta raccomandata, corriere o altra modalità per la quale si renda rilevante evidenziare il mezzo di trasmissione e il timbro postale (ad es., una fattura passiva proveniente da un fornitore estero arrivata in prossimità del termine di scadenza per il pagamento), sono spillate assieme al documento e trasmesse alla UO.

Le altre buste sono conservate a parte in plichi quotidiani per 30 giorni. Trascorso tale termine sono eliminate senza formalità.

8.3.4. Ricezione di documenti cartacei a mezzo fax

I documenti ricevuti via fax da enti e soggetti esterni terzi vanno protocollati e scansionati contestualmente alla registrazione a protocollo.

Nel caso che il fax sia seguito dall'arrivo del corrispondente documento in originale e quest'ultimo sia identico, deve essere attribuita all'originale la stessa segnatura del documento pervenuto via fax. Il fax va allegato all'originale.

Se l'originale successivamente pervenuto differisce dal fax pervenuto in precedenza, l'originale va considerato un documento diverso e pertanto va protocollato con un nuovo numero.

8.4. Priorità nella registrazione dei documenti informatici in arrivo

Indipendente dal mezzo telematico di arrivo, è data priorità nella registrazione a protocollo a:

- ❖ atti giudiziari notificati;
- ❖ documenti del Ministero;
- ❖ documenti di rilevanza finanziario-contabile (MEF – Corte dei Conti, etc.);
- ❖ documenti ricevuti direttamente dal Direttore Generale;
- ❖ documenti ricevuti direttamente dall' Ufficio di Diretta Collaborazione al Presidente e al Direttore Generale
- ❖ documenti ricevuti direttamente dalla segreteria del Direttore Scientifico
- ❖ documenti ricevuti direttamente dall'Ufficio Legale:
- ❖ fatture passive pervenute al di fuori del Sistema di interscambio (es. le fatture in formato elettronico provenienti da fornitori esteri).

È data inoltre priorità ai documenti pervenuti con PEC in considerazione del fatto che il sistema rilascia automaticamente al mittente la ricevuta di avvenuta consegna del documento.

Tale casistica è soltanto indicativa ed è suscettibile di variazione in concomitanza con altre priorità che si dovessero presentare (scadenze bandi di concorso, gare, etc.).

8.5. Casi di rigetto

Per rigetto si intende la segnalazione di un ufficio della erronea assegnazione di competenza su un determinato documento ricevuto in smistamento.

Pertanto il rigetto avviene solo per i documenti in arrivo.

Prima del rigetto l'ufficio deve riportare nella registrazione una annotazione motivando e indicando l'ufficio competente.

Il documento informatico ritorna così in carico al protocollo che potrà immediatamente inoltrarlo alla ufficio competente.

Nessun documento deve rimanere in carico al protocollo, soprattutto se pervenuto con PEC.

8.6. Flusso del documento in partenza

8.6.1. Redazione, registrazione e spedizione di documenti analogici cartacei aventi per destinatario un soggetto terzo a mezzo posta convenzionale o telefax

I documenti analogici cartacei dotati di firma autografa, aventi per destinatario un soggetto terzo, vanno di norma redatti in due esemplari, un originale per il destinatario e una minuta in originale da conservare nel fascicolo relativo al procedimento o all'affare della UO mittente.

Successivamente alla registrazione a protocollo, i documenti da spedire su supporto cartaceo sono trasmessi all'ufficio addetto allo smistamento della corrispondenza ovvero spediti direttamente dalla UO mittente di norma lo stesso giorno lavorativo della protocollazione.

Le ricevute dell'avvenuta trasmissione sono trattenute dalla UO RPA e conservate all'interno del fascicolo di pertinenza del documento.

8.6.2. Registrazione a protocollo di documenti analogici cartacei

La registrazione a protocollo dei documenti analogici cartacei in partenza è effettuata dal personale dell'AOO o della UO interessata, abilitato ad accedere al sistema informatico Titulus e incaricato di tale tipo di operazione.

Le operazioni comprendono la classificazione e l'obbligo dell'acquisizione in formato immagine del documento tramite il processo di scansione e conseguente memorizzazione nel sistema informativo Titulus.

Sono esclusi dalla digitalizzazione solo quei documenti o allegati per i quali la procedura di scansione sia impossibile o difficoltosa in ragione del formato (documento rilegato e voluminoso, foglio di carta eccedente il formato A4, ecc.) o per il tipo di supporto (CD, DVD, ecc.) e, in ogni caso, i documenti e gli allegati in formato cartaceo che superino n. 20 fogli in formato A4.

Nei casi in cui, per le ragioni suesposte, non sia possibile digitalizzare integralmente i documenti e gli allegati, va inserita nel campo *Note della registrazione del protocollo* la dicitura "si trasmette per via postale il documento cartaceo composto da n _ fogli"; "l'allegato composto da n _ fogli"; gli allegati composti da n. _ fogli", ecc.

Successivamente alla registrazione, il responsabile del procedimento assicura la fascicolazione del documento analogico cartaceo redatto secondo l'impostazione grafica di un modello istituzionale prescelto dalla AOO, sia nel sistema informativo Titulus che nel corrispondente fascicolo cartaceo.

8.6.3. Redazione, registrazione e spedizione di documenti analogici cartacei aventi per destinatario un ente o soggetto terzo a mezzo posta convenzionale o telefax

I documenti analogici cartacei dotati di firma autografa prodotti da una AOO o da una UO dell'Ente, aventi per destinatario un ente o soggetto terzo, vanno di norma redatti in due esemplari, un originale per il destinatario e una minuta in originale da conservare nel fascicolo relativo al procedimento o all'affare dell'AOO o della UO mittente.

Successivamente alla registrazione a protocollo i documenti da spedire su supporto cartaceo sono trasmessi all'ufficio addetto allo smistamento della corrispondenza (per l'AOO Amministrazione centrale) ovvero spediti direttamente dalla UO mittente di norma lo stesso giorno lavorativo della protocollazione.

Qualora i documenti, successivamente alla registrazione a protocollo, vengano trasmessi via fax va apposta sull'originale del documento la seguente dicitura: "la trasmissione via fax del presente documento non prevede l'invio del documento originale"

Solo su richiesta del destinatario verrà trasmesso anche l'originale.

Le ricevute dell'avvenuta trasmissione sono trattenute dalla UO che ha effettuato la trasmissione e conservate all'interno del fascicolo di pertinenza del documento.

8.6.4. Redazione, registrazione e spedizione di documenti informatici

Il documento informatico in partenza, sottoscritto con firma digitale e marcatura temporale a cura dello stesso soggetto legittimato ad apporre sul corrispondente cartaceo la firma autografa, deve essere registrato a protocollo dell'AOO.

Il file firmato digitalmente deve essere associato nel contesto dell'operazione di registrazione con memorizzazione nel sistema Titulus.

Se il documento informatico sottoscritto con firma digitale è destinato a enti o soggetti terzi esterni all'Ente, esso dev'essere trasmesso, a cura dell'AOO o della UO mittente, per posta elettronica alla casella di PEC del destinatario indicando gli estremi della registrazione di protocollo, oppure attivando la funzione di interoperabilità del sistema di protocollo fra enti laddove già attiva.

Per la spedizione di documenti informatici l'AOO si avvale di un servizio di posta elettronica certificata conforme al DPR 11/2/2005 n. 68 in grado di garantire la sicurezza del canale di comunicazione e la certezza della data di spedizione e consegna dei documenti.

Il documento informatico prodotto deve essere redatto preferibilmente nel formato Pdf/a o per casi particolari (cfr. Capitolo 9), secondo gli altri formati stabiliti in precedenza (cfr. § 3.2.2) e, in base alla tipologia di documento informatico, deve avere i seguenti requisiti minimi di forma e contenuto per poter essere registrato al protocollo:

a) documento informatico formato attraverso l'acquisizione della copia per immagine su supporto informatico di un documento analogico:

- ❖ sigillo;
- ❖ data completa (luogo, giorno, mese, anno) scritta per esteso;
- ❖ indicazione dell'indirizzo PEC o e-mail del destinatario;
- ❖ il nominativo del RPA;
- ❖ numero di protocollo;
- ❖ numero degli allegati;
- ❖ sottoscrizione autografa (nei casi previsti dalla normativa deve essere corredato da dichiarazione di conformità sottoscritta con firma digitale)

b) documento informatico redatto tramite l'utilizzo di appositi strumenti software:

- ❖ sigillo;
- ❖ data completa (luogo, giorno, mese, anno) scritta per esteso;
- ❖ indicazione dell'indirizzo PEC o e-mail del destinatario;
- ❖ il nominativo del RPA;
- ❖ numero degli allegati;
- ❖ firma digitale.
- ❖ Il numero di protocollo può essere inserito solo nel caso si adottino particolari accorgimenti nella formazione del documento e si utilizzi il formato PAdES per la sottoscrizione digitale.

Può essere predisposto un flusso all'interno del sistema gestionale per i visti eventualmente richiesti all'interno dell'amministrazione, prima della protocollazione del documento firmato digitalmente.

8.7. Flusso del documento informatico tra UO della stessa AOO

Il documento tra uffici (o interno) è quello che una UO invia ad un'altra UO della stessa AOO.

Trattandosi di documenti endoprocedimentali, possono essere prodotti in pdf/a, registrati in Titulus e protocollati, avendo cura di individuare i nominativi delle copie per conoscenza a cui il sistema informatico invierà il link al documento per email. La registrazione a protocollo permette di ufficializzare il documento; si ricorda, infatti, che un documento protocollato è un documento di fede privilegiata con valore probatorio contrastabile solo con querela di falso (Cfr. § 8.8).

I documenti destinati ad una altra UO che necessitano di essere firmati, in mancanza di una firma elettronica personale (cfr. § 8.8), andranno stampati e firmati con firma autografa; in questo caso il documento dovrà contenere di tutti gli elementi di garanzia e di informazione del mittente e del destinatario.

Onde evitare la proliferazione di documenti cartacei, il documento così preparato verrà digitalizzato mediante la scansione, registrato nel sistema informativo Titulus e protocollato. La UO ricevente provvederà alla classificazione e fascicolazione del documento ricevuto per il quale varrà la registrazione di protocollo già effettuata dalla UO mittente.

Sono esclusi dalla digitalizzazione solo quei documenti o allegati per i quali la procedura di scansione sia impossibile o difficoltosa in ragione del formato (documento rilegato e voluminoso, foglio di carta eccedente il formato A4, ecc.) o per il tipo di supporto (CD, DVD, ecc.) e, in ogni caso, i documenti e gli allegati in formato cartaceo che superino n. 10 fogli in formato A4.

Nei casi in cui, per le ragioni suesposte, non sia possibile digitalizzare integralmente i documenti e gli allegati, va inserita nel campo *Note* della registrazione del protocollo la dicitura: “si trasmette per via postale (oppure *brevi manu*) il documento cartaceo composto da n _ fogli”; “l’allegato composto da n _ fogli”; gli allegati.

8.8. Utilizzo delle firme elettroniche: firma elettronica semplice, firma elettronica avanzata, firma elettronica qualificata, firma digitale

La firma elettronica semplice, descritta al Cap. 3.1, può essere utilizzata per i documenti interni.

Le annotazioni sulle registrazioni del sistema di gestione documentale sono considerate firma elettronica avanzata e vengono utilizzate per l’attestazione di regolare esecuzione del servizio/fornitura e l’autorizzazione al pagamento delle fatture elettroniche.

I libri contabili previsti dalla normativa per cui l’Ente ha dematerializzato il processo di produzione e conservazione, sono firmati con firma digitale in formato CADES.

Le fatture elettroniche in formato PA (XML) destinate a pubbliche amministrazioni italiane, i contratti stipulati in forma pubblica amministrativa, i contratti stipulati mediante scrittura privata, i contratti stipulati (scambio di lettera commerciale) sulla piattaforma Consip per il mercato elettronico della pubblica amministrazione (MePA), gli accordi tra pubbliche amministrazioni sono firmati con firma digitale in formato CADES.

Nei casi in cui sia richiesto per norma di legge o opportuno inserire annotazioni successivamente alla sottoscrizione digitale è necessario utilizzare una firma digitale in formato PAdES).

8.9. Annullamento di una registrazione

È consentito l’annullamento di una registrazione di protocollo per motivate e verificate ragioni.

Solo il Responsabile della gestione documentale e le persone espressamente delegate sono autorizzate ad annullare la registrazione.

L’annullamento anche di una sola delle informazioni generate o assegnate automaticamente dal sistema e registrate in forma immodificabile determina l’automatico e contestuale annullamento dell’intera registrazione di protocollo.

I motivi per i quali è richiesto l’annullamento possono essere:

- ❖ errore di inserimento delle informazioni registrate in forma immodificabile nel caso che dette informazioni non siano generate o assegnate automaticamente dal sistema;
- ❖ il documento registrato deve essere sostituito per rettifica del destinatario o dell’oggetto;
- ❖ la motivazione per cui il documento è stato prodotto è venuta meno purché il documento non sia già stato diffuso.

Nel caso in cui il documento da annullare sia sostituito da una nuova registrazione, negli estremi del provvedimento di autorizzazione all'annullamento si indica che il documento è stato correttamente registrato con protocollo n. ___ del ___.

La registrazione annullata resta visibile all'interno del sistema di gestione documentale e della sequenza numerica con la dicitura "Annullato".

Il documento analogico annullato riporta gli estremi dell'annullamento e viene conservato dall'Archivio dei documenti cartacei dell'Ente.

Se il documento analogico o informatico annullato costituisce una tipologia documentale soggetta a registrazione particolare (ad es., un contratto) per la quale è prevista la conservazione perenne, lo stesso sarà conservato nel proprio repertorio con la dicitura "annullato" assieme alla richiesta di annullamento.

In tema di annullamento dei provvedimenti occorre far riferimento alle disposizioni di cui alla L. 241/1990 in merito agli strumenti di autotutela.

Nel software di gestione del protocollo informatico *Titulus*, adottato dall'Ente, i documenti annullati sono inseriti nei rispettivi fascicoli o, nel caso di documento non inerenti a specifici procedimenti, in un fascicolo annuale.

Nella registrazione di protocollo appaiono in forma ben visibile, oltre agli elementi già indicati, anche la data, il cognome e nome dell'operatore che ha effettuato l'annullamento.

Le informazioni relative al protocollo rimangono comunque memorizzate nel registro informatico per essere sottoposte alle elaborazioni previste dalla procedura, comprese le visualizzazioni e le stampe, nonché la data, l'ora, l'autore dell'annullamento e gli estremi dell'autorizzazione all'annullamento del protocollo.

Si può procedere all'annullamento di un documento ricevuto con PEC sebbene il mittente abbia già la ricevuta di avvenuta consegna. In questo caso il mittente riceverà una notifica di annullamento del suo documento con la relativa motivazione.

Non si annulla mai un documento informatico trasmesso con PEC in quanto il destinatario è già in possesso del documento stesso; in questo caso si può procedere con la redazione di un nuovo documento che annulla e sostituisce il precedente (in questo caso è necessario citare il riferimento del protocollo); tale nuovo documento dovrà essere protocollato e inviato via PEC.

8.10. Corresponsabilità di un documento e di un fascicolo

La corresponsabilità di un documento e/o di un fascicolo è la partecipazione al procedimento amministrativo di:

- ❖ più UO della stessa AOO (corresponsabilità di servizi interna);
- ❖ più AOO di enti diversi (corresponsabilità di servizi esterna)

Nella corresponsabilità di servizi interna, pur essendo la responsabilità amministrativa tra più UOR e di conseguenza tra più RPA, la responsabilità della tenuta dei documenti in originale (per quelli analogici), come di quella del fascicolo, spetta esclusivamente alla UO che ha la competenza prevalente sul procedimento amministrativo e riportata per prima nella registrazione di protocollo.

Spetta pertanto alla prima UO indicata aprire il fascicolo e poi renderlo disponibile alle altre UO coinvolte nella corresponsabilità di servizi.

8.11. Comunicazione tra AOO di documenti amministrativi protocollati

In attuazione di quanto disposto dell'art. 47 del D.lgs. 82/2005 relativamente alle comunicazioni tra amministrazioni di documenti amministrativi informatici protocollati, l'Allegato 6 al documento "Linee Guida sulla formazione, gestione e conservazione dei documenti informatici" emanato dall'AgID nel 2020, individua le modalità tecniche per assicurare la trasmissione di documenti amministrativi informatici tra AOO della pubblica amministrazione.

Tali modalità saranno implementate e/o modificate in relazione all'evoluzione tecnologica e alle eventuali future esigenze manifestate dalle amministrazioni.

Per dare seguito alla comunicazione tra AOO mittente e AOO destinataria, le stesse possono adottare una delle modalità previste dalla norma:

- posta elettronica, in cui il messaggio di protocollo (documento, allegati e segnatura di protocollo) è trasportato come allegato della stessa e il contenuto del messaggio di posta elettronica non deve intendersi come parte del messaggio di protocollo;
- cooperazione applicativa, utilizzando il Simple Object Access Protocol (SOAP), assicurando l'implementazione delle interfacce di servizio SOAP⁴⁵.

Per assicurare la comunicazione tra AOO le Amministrazioni devono registrare e mantenere aggiornato, per ogni AOO individuata nella propria organizzazione, l'Indice dei domicili digitali delle pubbliche amministrazioni e dei gestori di pubblici servizi (IPA) (di seguito IPA) con:

- indirizzo di posta elettronica certificata;
- endpoint di esposizione dei servizi indicati SOAP (Simple Object Access Protocol)

Le AOO mittente e AOO destinataria, per dare seguito alla comunicazione di messaggi protocollati utilizzando il Simple Object Access Protocol, implementano le interfacce di servizio descritte nei Web Services Description Language (WSDL)⁴⁶.

Nello specifico:

- la AOO mittente DEVE implementare protocollo-*mittente.wSDL*;
- la AOO destinataria DEVE implementare protocollo-*destinatario.wSDL*.

La segnatura informatica DEVE essere associata in forma permanente al documento primario e agli allegati che con esso formano il messaggio di protocollo.

⁴⁵ Il Simple Object Access Protocol (SOAP) è un protocollo leggero basato su XML per lo scambio di informazioni in un ambiente decentralizzato e distribuito; SOAP descrive la struttura e i tipi di dati dei *payload* dei messaggi utilizzando l'emergente standard *W3C XML Schema* emesso dal World Wide Web Consortium (W3C)

⁴⁶ WSDL è un formato XML per descrivere i servizi di rete come un insieme di endpoint che operano su messaggi contenenti informazioni orientate ai documenti o alle procedure. Le operazioni e i messaggi vengono descritti in modo astratto e quindi associati a un protocollo di rete concreto e al formato del messaggio per definire un endpoint. Gli endpoint concreti correlati vengono combinati in endpoint astratti (servizi).

A tal fine l'AOO mittente:

- deve riportare nella segnatura informatica l'impronta (digest) del documento primario e, se presenti, degli allegati;
- deve assicurare l'autenticità, integrità e il non ripudio della segnatura informatica attuando le regole tecniche in materia di firma elettronica dei documenti informatici emanate dall'AgID⁴⁷.

La AOO mittente deve assicurare il controllo della validità amministrativa del documento primario, degli eventuali allegati e dei dati riportati nella segnatura informatica prima della composizione del messaggio di protocollo.

Le informazioni contenute nella segnatura informatica devono essere memorizzate nel sistema di gestione dei documenti della AOO mittente e in quello delle AOO destinatarie.

Le comunicazioni tra le AOO di documenti amministrativi protocollati sono valide ai fini del procedimento amministrativo una volta che ne sia verificata la provenienza, ovvero se:

- sono sottoscritte con firma digitale o altro tipo di firma elettronica qualificata;
- sono dotate di segnatura di protocollo di cui all'articolo 55 del TUDA;

L'AOO mittente assicura che siano rispettate **le regole di processamento** e **i flussi di comunicazione** previste dall'Allegato 6 alle Linee Guida AgID.

⁴⁷ AgID. *Linee guida contenenti le Regole Tecniche e Raccomandazioni afferenti la generazione di certificati elettronici qualificati, firme e sigilli elettronici qualificati e validazioni temporali elettroniche qualificate.*

CAPITOLO 9 - CASISTICA E COMPORTAMENTI

Si forniscono, di seguito, le indicazioni comportamentali relative ad alcune casistiche particolari.

9.1. Gestione delle gare d'appalto

9.1.1. Gare e procedure negoziate gestite in modalità analogica. Presentazione delle offerte per gare ad evidenza pubblica

Gli uffici che indicano le procedure possono dare disposizione di apporre sulla busta una dicitura, ad es., "Non aprire: offerta per la procedura negoziata per la realizzazione di... - CIG: ... - CUP: ...".

Le buste sigillate, dalla cui confezione si evinca la partecipazione ad una gara d'appalto o -a una procedura negoziata, non vanno aperte e si registrano a protocollo per garantire la data certa di acquisizione.

La segnatura va apposta sulla busta.

Inoltre, per le offerte consegnate nel giorno di scadenza, l'ufficio deputato alla ricezione apporrà sulla busta anche l'ora di consegna.

Se la registrazione avviene dopo l'ora fissata per la consegna o se la consegna avviene dopo la scadenza fissata dal bando di gara, a protocollo viene inserita anche una annotazione immodificabile del tipo: "documento pervenuto/consegnato alle ore hh.mm del giorno gg/mm/aaaa come risulta dall'indicazione riportata sulla busta che si digitalizza".

Nell'oggetto si riporta la descrizione della gara/offerta così come è riportata sulla busta.

9.1.2. Gare e procedure negoziate gestite in modalità telematica

I documenti inerenti alle gare svolte mediante portale telematico o pervenuti in modalità elettronica possono essere soggetti a registrazione di protocollo e comunque sono inseriti nel sistema di gestione documentale.

La UO provvede a inserire i file di gara nelle rispettive registrazioni di protocollo o, in base alla natura del documento, come documenti non protocollati.

9.2. Gestione di concorsi e selezioni

Relativamente alle domande spedite per posta fa fede, ai fini del termine di scadenza, il timbro postale di spedizione ovvero il tagliando della raccomandata, sempreché la normativa di riferimento non preveda riferimenti temporali diversi.

Il competente ufficio dell'amministrazione centrale, cui i plichi vanno direttamente e tempestivamente recapitati a cura dell'Ufficio postale, appone sulle domande e sugli allegati il giorno e l'ora di arrivo.

Per i plichi recapitati a mano tale compito sarà eseguito dall'Ufficio di portineria.

La verifica del rispetto del termine di scadenza (giorno ed ora) relativi alla presentazione della domanda spetta all'ufficio competente dell'amministrazione centrale.

Il responsabile del procedimento trasmette quotidianamente al servizio di protocollo una nota con cui attesta l'elenco delle domande pervenute con indicazione della rispettiva data, raggruppate per tipologia di concorso.

Il servizio di protocollo attribuisce alla nota un unico numero di protocollo e la restituisce al responsabile del procedimento.

A ciascuna domanda elencata nella nota va allegata una copia della nota protocollata.

Nella registrazione di protocollo si riporta:

- come numero di allegati l'effettiva quantità pervenuta e indicata sul documento dalla UO ricevente;
- nel campo allegati la dicitura "N. ... allegati trattenuti dal Servizio/Ufficio ...".

La documentazione per la partecipazione a concorsi, selezioni, etc., per cui non sia stato possibile procedere alla registrazione a protocollo nella giornata di ricezione, deve essere protocollata con provvedimento di differimento della registrazione alla data di ricezione.

Se le istanze di partecipazione a concorsi e procedure di selezione sono inviate in modalità telematica, a mezzo PEC, gli allegati saranno automaticamente associati alla registrazione.

Verificato il termine di scadenza, l'ufficio competente provvede ai sensi dei precedenti commi.

Il rilascio della ricevuta di consegna della domanda all'interessato o a persona incaricata dallo stesso va effettuato a cura dell'ufficio competente.

9.3. Atti giudiziari

Ai fini dell'identificazione del corrispondente di atti e/o note inerenti a contenzioso, occorre tener presente la differenza tra la notifica (effettuata direttamente all'Amministrazione) e altri tipi di comunicazione.

9.3.1. Notifiche

La notifica avviene con la consegna dell'atto eseguita dall'ufficiale giudiziario, nelle mani proprie del destinatario o a soggetto rappresentante dell'amministrazione autorizzato a ricevere l'atto, o da altro soggetto abilitato tramite servizio postale, a mezzo PEC o nelle altre modalità stabilite dalla legge.

Se l'atto è notificato a mano si considera come data di notifica quella indicata nella referta di notifica del documento; se è notificato con raccomandata si considera il giorno in cui si ritira la raccomandata.

Ai sensi dell'art. 149-bis c.p.c., la copia estratta dal documento originale deve essere firmata digitalmente dall'ufficiale giudiziario e, se non è fatto espresso divieto dalla legge, la notificazione può eseguirsi a mezzo posta elettronica certificata, anche previa estrazione di copia informatica del documento analogico; in questo caso, l'ufficiale giudiziario trasmette copia informatica dell'atto sottoscritta con firma digitale all'indirizzo di posta elettronica certificata del destinatario risultante da pubblici elenchi o comunque accessibili alle pubbliche amministrazioni.

La notifica si intende perfezionata nel momento in cui il gestore rende disponibile il documento informatico nella casella di posta elettronica certificata del destinatario.

Per mittente si intende la parte istante, cioè il legale/avvocato delegato mediante procura alle liti che agisce in nome e per conto del soggetto interessato e che ha richiesto la notifica dell'atto.

Anche un sindacato o un'associazione non riconosciuta, può essere mittente, nel caso in cui agisca in nome e per conto di un lavoratore in una controversia sindacale.

Il mittente del documento non è l'organo giudiziario indicato generalmente sul frontespizio dell'atto (ad es., Tribunale, Corte di Appello), ma colui che ha richiesto la notificazione, generalmente il legale a cui il ricorrente/attore ha conferito il mandato di procura alle liti (quindi il corrispondente apposto di norma sulla prima pagina dell'atto in alto a destra).

9.3.2. Comunicazioni

Quando l'atto è notificato presso l'**Avvocatura Distrettuale o Generale dello Stato**, in quanto soggetto che assicura la difesa in giudizio dell'Amministrazione, l'Avvocatura stessa generalmente procede alla trasmissione dell'atto all'INRiM, dandone informativa; in tal caso si tratta di una comunicazione, non di una notifica, il cui mittente da indicare nella registrazione di protocollo è appunto l'Avvocatura, come per tutte le comunicazioni dalla stessa provenienti.

Diverse sono poi le comunicazioni (quali quelle consistenti in avvisi di deposito di note o di fissazione di udienza) che provengono direttamente dalla **cancelleria dell'autorità giudiziaria** (Tribunale, Corte di appello, ecc.) innanzi a cui pende il giudizio.

In questi casi il mittente è sicuramente l'autorità giudiziaria medesima.

Le comunicazioni che provengono dalla cancelleria dell'autorità giudiziaria arrivano tramite l'applicativo del processo civile telematico – PTC, sono conservate nella casella PEC, rilasciata dall'ordine professionale a cui è iscritto l'avvocato che ha in carico la pratica.

Si noti che nei procedimenti giuslavoristici, contestualmente al ricorso introduttivo del giudizio si trova il decreto di fissazione di udienza, in calce al ricorso stesso; in tal caso si è in presenza, contestuale, sia di un atto di parte che di un atto prodotto dall'organo giurisdizionale.

9.4. Documenti informatici con oggetto multiplo

Nel caso di documenti in arrivo che trattano più argomenti di competenza di UO diverse tra loro, concretando il caso del cosiddetto "oggetto multiplo", il documento viene registrato redigendo l'oggetto in maniera esaustiva con tutte le informazioni necessarie a comprendere i vari argomenti.

La classificazione del documento riguarderà l'argomento prevalente o comunque individuato come tale e smistato alla UO competente sullo stesso.

Compatibilmente con la funzionalità del sistema di gestione documentale, ciascuna UO corresponsabile potrà (dovrà) creare la propria copia informatica al fine di proseguire con la gestione e la fascicolatura.

Nel caso di documento in partenza è compito della UO responsabile verificare che il documento prodotto tratti un solo argomento, chiaramente espresso nel campo "oggetto".

9.5. Fatture elettroniche (Fattura PA)

La fattura elettronica destinata alla pubblica amministrazione rispetta i requisiti di formato e contenuto prescritti dal Decreto Ministeriale 3 aprile 2013, n. 55 (e successive modifiche), e viene trasmessa e ricevuta attraverso il Sistema di Interscambio (SdI).

È obbligatorio emettere fatture elettroniche nei confronti di tutte le amministrazioni pubbliche italiane (ciclo attivo e passivo).

Non si accettano più fatture cartacee emesse in data pari o successiva al 31 marzo 2015, salvo per i soggetti non tenuti a rispettare l'obbligo di fatturazione elettronica (es. fornitori esteri, persone fisiche o giuridiche senza partita IVA).

Le fatture cartacee che avrebbero dovuto essere emesse in formato elettronico vanno restituite al mittente utilizzando lo stesso canale di comunicazione, in piena simmetria delle forme.

Le fatture cartacee pervenute a mezzo PEC, emesse a far data dal 31 marzo 2015 in poi, devono essere annullate con la seguente motivazione: "Ai sensi della Legge 24 dicembre 2007, art. 1 commi 209-214, le fatture emesse nei confronti dell'ente in data pari o successiva al 31 marzo 2015 devono essere trasmesse in forma elettronica secondo il formato di cui all'allegato A "Formato della fattura elettronica" del Decreto Ministeriale 3 aprile 2013, n. 55".

Il mittente riceverà la notifica di annullamento, comprensiva di motivazione, a mezzo PEC.

La fattura elettronica PA non è prevista per i fornitori non residenti in Italia che dovranno attendere l'emanazione di uno specifico decreto.

In tal caso la fattura andrà gestita come qualsiasi documento analogico: protocollata, assegnata e fascicolata.

La fattura elettronica perviene in formato XML via PEC, agli indirizzi dichiarati dall'ente e registrati sull'indice IPA nel corrispondente servizio di fatturazione.

La fattura così pervenuta è automaticamente protocollata, assegnata alla UO competente - che provvede alla classificazione e alla fascicolatura - e trasmessa al sistema di contabilità dove dovrà essere presa in carico per la verifica di correttezza e conformità.

Sul sistema contabile si provvede alla registrazione della stessa sul registro delle fatture, entro 10 giorni dal ricevimento (DL 66/2014 art. 42).

La data di protocollo fa fede quale termine iniziale dei 15 giorni entro cui la fattura va accettata o rifiutata con motivazione (la mancata notifica di rifiuto entro 15 giorni equivale ad accettazione), nonché dei 30 giorni previsti dalla legge decorsi i quali, in assenza di pagamento, iniziano automaticamente a decorrere gli interessi moratori (D.lgs. 192/2012, art. 1, comma 1, lett. d).

Per inoltrare e ricevere le fatture elettroniche è stato integrato il sistema documentale con il sistema di contabilità.

Le fatture elettroniche trasmesse dai fornitori alle PA (ciclo passivo), così come quelle emesse dall'ente (ciclo attivo), sono obbligatoriamente conservate in modalità elettronica, secondo quanto espressamente disposto D.M. 17 giugno 2014.

9.6. DURC on-line

Ai sensi dell'art. 4 della Legge 78/2014, la verifica della regolarità contributiva avviene con modalità esclusivamente telematiche.

In caso di Documento unico di regolarità contributiva (DURC) già disponibile, questi avrà durata pari a quanto indicato nel documento stesso, in caso di non disponibilità del documento il sistema ne comunicherà la data di disponibilità.

Il documento così ottenuto avrà validità di 120 giorni dalla data di emissione.

Per le verifiche immediatamente disponibili on-line, si procede acquisendo l'immagine come documento non protocollato all'interno del sistema di gestione documentale.

Per i DURC richiesti, ma non immediatamente disponibili, occorre attendere la ricezione dell'avviso di disponibilità del documento che perviene a mezzo PEC. Anche questo avviso è acquisito come documento non protocollato. A questo punto è possibile consultare il sistema del DURC on-line e procedere come per i DURC immediatamente disponibili.

9.7. Denunce di infortuni

Il datore di lavoro è tenuto a denunciare all'INAIL gli infortuni da cui siano colpiti i dipendenti prestatori d'opera, indipendentemente da ogni valutazione circa la ricorrenza degli estremi di legge per l'indennizzo.

Le denunce di infortunio sono inviate esclusivamente in modalità telematica accedendo al portale dell'INAIL con apposite credenziali rilasciate ai dipendenti incaricati.

L'invio delle denunce tramite PEC è consentito solo in caso di malfunzionamento del sistema.

Considerato che il sistema per l'invio telematico della denuncia prevede l'inserimento obbligatorio di dati ulteriori rispetto a quelli presenti sul certificato del pronto soccorso, è onere del lavoratore consegnare la dichiarazione di infortunio sul lavoro compilata in ogni sua parte.

Il delegato alle denunce che ricevesse tale modulo compilato in modo incompleto dovrà chiederne tempestivamente l'integrazione all'infortunato.

Il funzionario attesta la data certa e la piena conoscenza dell'infortunio sottoscrivendo e datando il documento.

Questa procedura sostituisce il protocollo in arrivo del documento, quindi le denunce di infortunio sono una tipologia di documenti esclusa dalla registrazione di protocollo.

9.8. Certificati di malattia

I certificati di malattia sono acquisiti consultando la banca dati dell'INPS con apposite credenziali rilasciate ai dipendenti incaricati.

Dopo averli visualizzati sono stampati o salvati come file e inseriti nel fascicolo personale. I certificati di malattia sono una tipologia di documenti esclusa dalla registrazione di protocollo.

9.9. Documenti del portale degli acquisti della pubblica amministrazione

Gli strumenti messi a disposizione sulla piattaforma di e-Procurement gestito da Consip S.p.A. per conto del Ministero Dell'Economia e delle Finanze sono:

- ❖ Il Mercato Elettronico della P.A. (MePA), ai sensi dell'art. 11 del D.P.R. 101/2002, mediante il quale le Pubbliche Amministrazioni possono acquistare beni e servizi offerti dai fornitori abilitati presenti sui diversi cataloghi del sistema, il cui importo deve essere inferiore alla soglia comunitaria.
- ❖ Le Convenzioni contratti quadro stipulati da Consip ai sensi dell'art. 26 della Legge 488/99) nell'ambito dei quali i fornitori aggiudicatari di gare - esperite in modalità tradizionale o smaterializzata a seguito della pubblicazione di bandi - si impegnano ad accettare ordinativi di fornitura emessi dalle singole Amministrazioni che hanno effettuato l'abilitazione al sistema Acquisti in rete.
- ❖ Gli Accordi quadro, aggiudicati da Consip a più fornitori a seguito della pubblicazione di specifici Bandi, definiscono le clausole generali che, in un determinato periodo temporale, regolano i contratti da stipulare. Nell'ambito dell'Accordo quadro, le Amministrazioni che hanno effettuato l'abilitazione al sistema Acquisti in Rete, attraverso la contrattazione di "Appalti Specifici", provvedono poi a negoziare i singoli contratti, personalizzati sulla base delle proprie esigenze.

Si descrivono le procedure di acquisto d'uso più frequente:

- ❖ Affidamenti diretti sulla piattaforma MePA (Mercato Elettronico Pubblica Amministrazione)
- ❖ Adesioni
- ❖ Convenzioni
- ❖ Negoziazioni sulla piattaforma MePA (Mercato Elettronico Pubblica Amministrazione).

9.9.1. Affidamenti diretti sulla piattaforma MePA. (Ordini diretti di acquisto Oda)

Nei casi previsti dalla normativa e dai regolamenti vigenti, si fa ricorso ad un ordine diretto, che consiste nel selezionare l'articolo di proprio interesse fra quelli presenti nel catalogo dei fornitori e di effettuare l'ordine di acquisto al fornitore che è in grado di fornire l'articolo al prezzo più conveniente per l'amministrazione.

Il processo può essere così brevemente schematizzato:

1. il punto istruttore effettua una bozza dell'ordine attraverso la piattaforma e la invia al punto ordinante.
2. Il punto ordinante, cioè la persona che dispone di potere di spesa e del dispositivo di firma digitale, controlla la bozza, genera attraverso la piattaforma il file pdf/a che costituisce il documento d'ordine, lo scarica localmente, lo firma digitalmente, lo registra nel sistema di protocollo e lo ricarica a sistema.

La piattaforma MePA chiede il numero di protocollo come campo obbligatorio per procedere nella registrazione.

Nel sistema di contabilità si provvede alla registrazione delle opportune scritture contabili per l'emissione del corrispondente documento gestionale.

Nel caso sia un documento di tipo "ordine", questo può essere trasmesso al sistema di gestione documentale dove si genera una bozza per la registrazione a protocollo e la fascicolatura.

Nel caso invece sia un documento di tipo “contratto” dal sistema contabile può essere richiamato il numero di protocollo assegnato all’ordine emesso sulla piattaforma MePA.

9.9.2. Adesioni – Convenzioni MePA (Ordini diretti di acquisto OdA)

Quando l’articolo che si intende acquistare è presente in una delle convenzioni Consip attive, l’Amministrazione aderisce a tale convenzione ed effettua un ordine al fornitore che è vincitore della gara precedentemente espletata da Consip Spa.

Il processo può essere così brevemente schematizzato:

1. Il punto istruttore seleziona la convenzione, effettua una bozza dell’ordine attraverso la piattaforma e la invia al punto ordinante.
2. Il punto ordinante controlla la bozza, genera attraverso la piattaforma il file pdf/a che costituisce il documento d’ordine (Ordine di Acquisto OdA), lo scarica localmente, lo firma digitalmente, lo registra nel sistema di protocollo e lo ricarica a sistema.

La piattaforma MePA chiede il numero di protocollo per procedere nella registrazione.

Nel sistema di contabilità si provvede alla registrazione delle opportune scritture contabili per l’emissione del corrispondente documento gestionale.

Nel caso sia un documento di tipo “ordine”, questo può essere trasmesso al sistema di gestione documentale dove è generata una bozza per la registrazione a protocollo e la fascicolatura.

Nel caso invece sia un documento di tipo “contratto” dal sistema contabile può essere richiamato il numero di protocollo assegnato all’ordine emesso sulla piattaforma MePA.

9.9.3. Procedure negoziate MePA (Richiesta di offerta RdO)

Nei casi previsti dalla normativa e dai regolamenti vigenti, si ricorre ad un Richiesta di offerta (RdO), che consiste nell’espletamento di una gara telematica con gli strumenti offerti dalla piattaforma MePA.

Si può ricorrere alla Richiesta di offerta (RdO) anche per effettuare indagini di mercato, finalizzate a una procedura di affidamento diretto.

Nell’esecuzione dell’iter che conduce alla creazione della RdO, è possibile allegare dei documenti prodotti dall’amministrazione, sia di carattere amministrativo che tecnico-economico, al fine di supportare i fornitori nella predisposizione dell’offerta; esempi di tali documenti sono il disciplinare di gara, il capitolato tecnico, ecc.

Le buste arrivate sulla piattaforma MePA possono essere aperte solo alla scadenza della gara telematica con una seduta pubblica web.

Nel caso lo strumento dell’RdO sia utilizzato per una procedura negoziata, i documenti di gara saranno salvati localmente dall’Ufficio ordinante e registrati sul sistema di gestione documentale come documenti non protocollati.

Al momento della stipula del contratto con il fornitore aggiudicatario, il file pdf/a che costituisce il documento di stipula viene generato tramite la piattaforma.

L'Ufficio ordinante, in possesso della firma digitale e autorizzato ad espletare le attività transazionali attraverso gli strumenti di acquisto disponibili sul sistema di e-procurement per i quali risulta abilitato, salva il documento di stipula, lo firma digitalmente e lo registra nel sistema di protocollo e re-inviato alla piattaforma tramite il Portale

Nel Mercato Elettronico della P.A, infatti, il contratto di fornitura s'intende perfezionato nel momento in cui l'ordine, conforme ai requisiti previsti dal Bando e dall'offerta pubblicata a catalogo dal fornitore, è sottoscritto e inviato dall'Amministrazione tramite il Portale

Nel caso lo strumento dell'RdO sia utilizzato per effettuare un'indagine di mercato ai fini di una procedura di affidamento diretto, l'Ufficio ordinante salverà localmente solo i documenti relativi all'aggiudicatario.

9.10. Documenti pervenuti via PEC

La ricezione via PEC di un documento comprova il fatto che lo stesso ha raggiunto il destinatario.

Sono soggetti a registrazione di protocollo:

- il messaggio;
- i file allegati.

Per quanto riguarda la corretta identificazione del mittente, bisogna tener presente che la PEC è solo un vettore; il mittente è colui che sottoscrive il documento allegato o, nel caso di testo nel corpo del messaggio senza allegato, colui che lo trasmette.

In caso ci sia la necessità di rispondere al messaggio PEC, magari per richiedere il perfezionamento dei documenti inviati o per altra causa, la regola generale da seguire, in base al principio di simmetria delle forme, prevede che a un documento pervenuto con PEC si risponda con un documento trasmesso con PEC, utilizzando lo stesso canale di comunicazione.

9.10.1. Gestione di due documenti diversi trasmessi via PEC

Se con un unico messaggio pervengono due o più documenti, si provvede alla registrazione dei singoli documenti e non del messaggio; saranno eseguite, quindi tante registrazioni quanti sono i documenti pervenuti e si provvederà ad inserire opportune annotazioni di richiamo tra le diverse registrazioni.

9.10.2. Messaggio di PEC e allegati documenti di firmatari diversi

Nel caso in cui con uno stesso messaggio PEC pervengano documenti di firmatari diversi, senza alcun documento con funzione di lettera di trasmissione, si può agire in diversi modi:

- a. è prodotta una registrazione distinta per ciascun documento, corredata di annotazioni esplicative, come descritto al §9.10.1.
- b. in alternativa è lasciato l'indirizzo così come pervenuto e nell'oggetto è scritto: "Trasmissione di documenti con firmatari diversi".
- c. oppure, se si evince che l'indirizzo PEC è riconducibile in modo certo a uno dei firmatari dei documenti trasmessi, si indica nell'oggetto: "Cognome Nome trasmette per sé e per ...".

9.10.3. Gestione di soli allegati pervenuti via PEC e di documenti costituiti dal solo corpo della PEC

Qualora pervengano a mezzo PEC documenti identificabili come allegati e il documento principale si limita all'oggetto del messaggio, presentato dal protocollo informatico come oggetto nell'apposito campo in fase di registrazione, l'oggetto proposto rimane inalterato e si redige la seguente annotazione:

«Considerato che nessuna [istanza /lettera di accompagnamento /altro] è pervenuta tramite questa PEC e che il documento allegato è (descrizione allegato/i), si deduce che la richiesta sia rappresentata da quanto descritto nel campo oggetto dal mittente. Si è pertanto proceduto con la protocollazione».

Il messaggio contenuto nel corpo della PEC deve considerarsi come documento sottoscritto e valido a tutti gli effetti di legge e, pertanto, va protocollato.

9.11. Documenti pervenuti a mezzo e- mail semplice (non certificata)

Si descrivono di seguito diverse casistiche:

- ❖ se richiesto dal responsabile del procedimento, o da suo delegato, si registrano a protocollo anche le e-mail semplici, limitatamente ai casi in cui il loro contenuto sia rilevante nell'ambito di un procedimento, valutando caso per caso.

Per richiesta si intende l'inoltro della e-mail alla casella di posta elettronica istituzionale associata all'Ufficio del Protocollo; infatti, l'art. 65 comma 1 lettera c) del CAD fornisce la possibilità di sostituire la firma autografa su un modulo analogico con l'invio del modulo compilato da un indirizzo di posta elettronica istituzionale fornito dall'ente.

- ❖ le richieste di informazioni su orari di apertura e sul funzionamento di procedure (anche provenienti dall'estero) non sono soggette a registrazione di protocollo e ad esse si può rispondere a mezzo e-mail non protocollata.

Invece lamentele, doglianze, comunicazioni di disservizi devono essere valutate caso per caso. Nei casi di particolare gravità e rilevanza si procede alla registrazione a protocollo.

- ❖ l'e-mail contenente dati o informazioni prodromiche alla formazione di un provvedimento amministrativo non sono soggette a registrazione di protocollo; sono, altresì, esclusi dalla registrazione a protocollo gli atti preparatori (bozze, proposte non ufficiali, etc.).
- ❖ per i documenti registrati a protocollo dal mittente e trasmessi a mezzo e-mail si dovrà valutare caso per caso.

9.12. Gestione del secondo esemplare

Per essere certi che il secondo esemplare di un documento già protocollato sia effettivamente un secondo originale è necessario verificare l'esatta corrispondenza tra i due esemplari, inclusi gli allegati, in tutte le loro parti (firme, date, segnature di protocollo, ecc.).

Per i documenti sottoscritti con firma elettronica è necessario verificare anche che la data e l'ora di firma coincidano.

Una volta appurata la perfetta identità tra i due documenti, si agirà diversamente nel trattamento a seconda della modalità di ricezione del secondo esemplare:

- ❖ se il secondo esemplare perviene in formato analogico, si appone su di esso la segnatura di protocollo e l'indicazione "Secondo esemplare".

Nella registrazione di protocollo si inserisce l'annotazione: "Pervenuto secondo esemplare mediante raccomandata a/r"; questo permette in futuro di recuperare tutti gli esemplari pervenuti.

- ❖ nel caso di arrivo mediante PEC o altro sistema informatico (e-mail semplice, ecc.) si effettua una registrazione come "Documento non protocollato", riportandovi tutti i dati già inseriti nella registrazione di protocollo del primo esemplare (oggetto, mittente, RPA, classificazione, fascicolo, etc.).

Si inserisce, inoltre, l'annotazione "Il documento non è stato protocollato in quanto trattasi di secondo esemplare del documento già pervenuto e registrato col prot. n. _ del gg/mm/aaaa".

Nella registrazione di protocollo del primo esemplare andrà invece inserita l'annotazione "Pervenuto secondo esemplare via PEC (o altro mezzo) – vedi id. n. _).

9.13. Documenti anonimi

La ratio che deve governare il comportamento di un operatore durante la fase di registrazione di un documento in arrivo deve essere improntata all'avalutatività; in altre parole, l'operatore di protocollo deve attestare che un determinato documento, così come si è registrato, è pervenuto.

Si tratta di una delicata competenza di tipo certificativo, attestante la certezza giuridica di data, forma e provenienza per ogni documento.

Le lettere anonime, pertanto, sono soggette a registrazione di protocollo.

Se il documento anonimo è pervenuto a mezzo PEC si lascia come mittente l'indirizzo PEC.

9.14. Lettere prive di firma

Le lettere prive di firma vanno protocollate; spetta al responsabile dell'Ufficio competente valutare, successivamente, la loro validità ed efficacia ai fini del procedimento e/o processo.

9.15. Documenti informali scambiati tra UO della stessa AOO

I documenti informatici prodotti a seguito della protocollazione e scansione di documenti originali cartacei trasmessi tra le UO della stessa AOO sono inoltrati in formato digitale tramite il sistema di protocollo informatico senza procedere all'inoltro dell'originale analogico, che resta nella disponibilità della UO mittente, che procederà alla sua gestione e fascicolatura.

Le comunicazioni informali tra uffici non sono soggette a registrazione di protocollo in base al principio di non aggravio del procedimento, ma a cura delle UO interessate possono essere acquisite nel sistema di protocollo come documento non protocollato.

9.16. Lettere personali

Tutte le buste vanno aperte e conseguentemente protocollate fatta eccezione per quelle riportanti diciture come "riservato", "personale", "confidenziale" o simili da cui si evinca il carattere di corrispondenza privata.

Tali missive vanno inoltrate ancora chiuse al destinatario.

9.17. Ricezione di documenti informatici su supporti rimovibili

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

Considerata l'assenza di standard tecnologici e formali in materia di registrazione di file digitali, la AOO si riserva la facoltà acquisire e trattare tutti i documenti informatici ricevuti su supporto rimovibile che riesce a decodificare e interpretare con le tecnologie a sua disposizione.

Superata questa fase il documento viene inserito nel flusso di lavorazione e sottoposto a tutti i controlli e gli adempimenti del caso.

CAPITOLO 10 - DALL'ARCHIVIO CORRENTE ALL'ARCHIVIO DI DEPOSITO

10.1. Archivio di deposito

L'archivio di deposito è la fase intermedia del processo di tenuta dei documenti prodotti dall'Ente nel corso della propria attività e si colloca temporalmente tra l'archivio corrente e l'archivio storico.

L'archivio di deposito è il momento di decantazione dei documenti e delle informazioni relative, organizzati in fascicoli inerenti ad affari, ad attività e a procedimenti conclusi, per i quali non risulta più necessaria la trattazione corrente o verso i quali sussista solo un interesse sporadico.

Le attività che connotano questa fase d'archivio sono definite dal DPR 445/2000, artt. 67, 68 e 69, e riguardano l'obbligo della periodicità dei trasferimenti di documenti dall'archivio corrente, la conservazione ordinata delle unità archivistiche e la disponibilità dei mezzi di corredo per assicurare le funzioni di controllo e di ricerca del materiale (registri di protocollo, piani di classificazione repertori dei fascicoli, etc.).

I documenti sono conservati con le modalità indicate dal Responsabile della gestione documentale, rispettando l'organizzazione che essi avevano nell'archivio corrente.

La produzione e gestione informatica di dati e di documenti comporta una diversificazione delle procedure di gestione durante la fase di deposito determinata dalla peculiarità del supporto; ciononostante non cambia il ruolo e la funzione concettuale svolta dall'archivio di deposito nella tenuta del sistema documentale.

Si tratta, in ogni caso, di una fase di sedimentazione della documentazione, ossia di un periodo in cui i documenti esauriscono nel tempo le proprie funzioni rivelando la propria natura temporanea o permanente, a seconda del valore delle informazioni in essi contenute.

I documenti nativi digitali sono caratterizzati dalla predeterminazione dei termini di conservazione; ciò significa che la durata della vita di un documento è determinata nel momento stesso in cui il documento viene creato; si tratta di una forma di impostazione della selezione a priori dei documenti, attività che avviene anche per i documenti analogici, ma che è messa in atto solo in un secondo momento, durante la fase di deposito.

L'archivio di deposito dei documenti analogici è gestito e conservato a cura della Segreteria Generale, che si occupa di organizzare i seguenti servizi e attività:

- ❖ Attività preliminari finalizzate alla creazione di locali d'archivio a norma:
 - Individuare, attrezzare adeguatamente e gestire i locali da destinare a deposito d'archivio (accesso limitato al solo personale qualificato, pulizia periodica etc.);
 - Individuare il responsabile del servizio.
- ❖ Attività ordinarie caratterizzanti la gestione dell'archivio di deposito:
 - Trasferimenti periodici dei documenti dagli uffici e acquisizione delle unità da parte dell'archivio di deposito: preparare annualmente il trasferimento dei fascicoli relativi ad affari conclusi con la predisposizione di appositi elenchi di consistenza;
 - Concentrazione ordinata dei documenti, mantenendo le aggregazioni (serie e fascicoli) create nella fase di formazione e procedere alla revisione degli elenchi di trasferimento:

effettuare una schedatura sommaria delle unità trasferite in archivio attribuendo una numerazione univoca, continua e progressiva che determina la posizione logica e fisica delle unità nell'elenco di consistenza e nel locale d'archivio;

- Selezione della documentazione sulla base dei Massimari di selezione adottati dall'INRiM;
 - Campionatura di determinate tipologie documentali da non destinare integralmente alla conservazione a lungo termine;
 - Scarto della documentazione;
 - Riordinamento e ricostituzione delle serie originarie (rispetto del vincolo archivistico, del Piano di organizzazione delle aggregazioni documentali, del Titolare di classificazione, della successione cronologica annuale delle serie);
 - Conservazione adeguata dei documenti: mantenimento delle condizioni ambientali ottimali secondo le linee guida predisposte dalla Soprintendenza Archivistica del Piemonte e della Valle d'Aosta⁴⁸ (Cfr. § 11.1);
 - Versamento della documentazione all'archivio storico: predisposizione degli elenchi di versamento e aggiornamento dell'elenco di consistenza;
 - Servizio di ricerca documentale (recupero dei documenti/unità richieste – consultazione - creazione di copie semplici o conformi);
 - Predisposizione di statistiche sia per le attività di trasferimento e versamento che di consultazione: consente un'adeguata programmazione degli spazi e ottimizzazione dei servizi;
 - Elaborazione e aggiornamento del piano di conservazione degli archivi.
- ❖ Attività straordinaria - in caso di necessari interventi di recupero del pregresso:
- Ricognizione, censimento o mappatura della documentazione presente nel locale adibito a deposito e della documentazione impropriamente conservata presso gli uffici produttori;
 - Messa in sicurezza del locale di deposito e spostamento di tutto ciò che non è documento;
 - Schedatura delle unità documentarie;
- ❖ Selezione della documentazione e redazione di:
- Elenco di scarto, contenente la descrizione della documentazione da distruggere;
 - Elenco di versamento all'archivio storico, contenente la descrizione della documentazione da conservare senza limiti di tempo;
 - Elenco di consistenza dell'archivio di deposito, contenente la descrizione della documentazione rimasta dopo lo scarto ed il versamento in archivio storico, da conservare in archivio di deposito in attesa del suo versamento in archivio storico;

⁴⁸ <http://www.sato-archivi.it/Sito/index.php/home/aree-di-intervento/spostamento-e-allestimento-sedi.html>

– Procedura di scarto.

10.2. Elenco di consistenza per l'archivio di deposito dei documenti analogici

E' buona prassi che le UO producano una schedatura sommaria delle unità trasferite dall'archivio corrente all'archivio di deposito.

Alle unità trasferite è attribuita una numerazione univoca, continua e progressiva che determina la posizione logica e fisica delle unità nell'elenco di consistenza e nel locale d'archivio.

I fascicoli e le serie archivistiche vengono disposti nei locali di deposito rispettando l'ordinamento archivistico loro proprio, provvedendo a integrare e aggiornare l'elenco di consistenza con i trasferimenti effettuati dagli uffici.

10.3 Trasferimento dei fascicoli cartacei

Periodicamente, e comunque almeno una volta all'anno, il RPA trasferisce, per la conservazione nell'archivio di deposito al Responsabile della gestione documentale, i fascicoli relativi ad affari, attività e a procedimenti amministrativi conclusi e non più necessari a una trattazione corrente.

Per il trasferimento viene predisposto a cura del RPA l'elenco dei fascicoli trasferiti indicando, nell'intestazione, l'ufficio di provenienza della documentazione, e per ogni unità trasferita la classificazione, il numero progressivo di repertorio del fascicolo, l'oggetto e gli estremi cronologici.

I fascicoli sono trasferiti rispettando l'ordine dei documenti all'interno dei fascicoli che viene mantenuta anche dopo l'eliminazione di appunti, stampe, fotocopie, buste, normativa, documenti non protocollati e quelli che contengono informazioni riportate anche in altri documenti destinati alla conservazione permanente (scarto in itinere o sfrondata del fascicolo); di grande importanza per la corretta conservazione del materiale cartaceo è l'eliminazione di graffe metalliche, buste in plastica e materiali diversi dalla carta.

Qualora i Responsabili delle UO si trovassero nelle condizioni di dovere trasferire fascicoli o documenti prodotti e chiusi da molto tempo, oppure i cui RPA non siano più in servizio, essi dovranno essere trasferiti nelle condizioni in cui si trovano, senza operare interventi sull'ordinamento degli stessi e redigendo l'elenco di consistenza.

Nei casi in cui ciò non sia possibile, i responsabili delle UO concorderanno le modalità opportune di trasferimento, caso per caso, con il Responsabile della gestione documentale.

Prima del trasferimento i RPA provvedono anche a verificare che i fascicoli risultino chiusi anche nel sistema informatico di gestione documentale.

Alla ricezione dei fascicoli il Responsabile della gestione documentale verifica la corrispondenza dell'elenco di consistenza con il verbale di trasferimento, sottoscritto insieme all'elenco anche dal RPA al momento della consegna dei fascicoli.

10.4. Trasferimento dei fascicoli informatici

Il Responsabile della gestione documentale provvede, almeno una volta all'anno, a generare e a trasmettere i pacchetti di versamento al sistema di conservazione avvalendosi del processo di automazione disponibile nel sistema di gestione documentale, così come descritto nell'Allegato 5 - *Manuale di Conservazione*.

Prima del versamento il RDP provvederà allo sfoltimento dei fascicoli di propria competenza (scarto in itinere) eliminando i documenti non destinati alla conservazione, presenti nel fascicolo.

10.5. Trasferimento delle serie archivistiche

Le serie archivistiche (contratti, decreti, verbali, ecc.) sono trasferite all'archivio di deposito nella loro unitarietà, secondo un termine che può variare da serie a serie.

Le modalità di trasferimento sono le medesime previste per i fascicoli cartacei e informatici.

Se la serie archivistica è ibrida, cioè composta sia da documenti analogici che da documenti digitali, si procederà nel seguente modo:

- ❖ il fascicolo digitale nel sistema di gestione documentale conterrà tutti i documenti informatici in formato nativo e la copia per immagine dei documenti analogici associata alla registratura;
- ❖ il fascicolo analogico sarà composto dagli originali analogici dei documenti e dall'elenco dei documenti digitali comprensivo dei rispettivi numeri di protocollo;

10.6. Ordinamento archivistico

L'ordinamento delle unità archivistiche nell'archivio di deposito avviene nel rispetto del principio di provenienza e dell'ordine originario; in particolare per i fascicoli, l'ordine è quello stabilito dal repertorio dei fascicoli.

Il titolario di classificazione è parte integrante del presente Manuale (Allegato 2) ed è applicabile solo ai documenti prodotti/ricevuti dopo la sua adozione; il piano di classificazione, infatti, non ha mai efficacia retroattiva.

I fascicoli prodotti in precedenza, quindi, vengono archiviati sulla base dei titolari/piani di classificazioni in vigore al momento della produzione dei documenti afferenti, specificatamente nell'anno di chiusura del fascicolo.

L'ordinamento, infatti, comporta la ricostruzione delle serie originarie chiuse per anno; la data di riferimento è quella di chiusura della pratica.

Pertanto, il dato cronologico è fondamentale perché per ogni anno si ricostruiscono le serie di fascicoli sulla base della classificazione attribuita ai fascicoli e desumibile dal repertorio dei fascicoli.

Se il fascicolo è pluriennale e il suo periodo di attività cade a cavallo di una modifica del titolario verrà inserito, in base alla sua classificazione, nella serie dell'ultimo anno di vita della pratica, annotando la doppia classificazione di parte della documentazione causata dalla modificazione o aggiornamento del piano di classificazione.

Fascicoli e documenti analogici, prodotti senza l'applicazione di un titolario o piano di classificazione, sono ordinati dopo un'adeguata analisi degli stessi, al fine di un ordinamento secondo criteri condivisi e orientati a essere perduranti nel tempo.

Gli interventi su questa documentazione vanno comunque valutati insieme alla Soprintendenza Archivistica del Piemonte e della valle d'Aosta.

10.7. Conservazione

Il Responsabile della gestione documentale attua tutte le iniziative finalizzate alla corretta conservazione della documentazione, sia in ambito analogico che digitale.

Per la conservazione della documentazione analogica, il Responsabile della gestione documentale verifica che nei depositi d'archivio siano rispettati i criteri che garantiscano la sicurezza della documentazione (ordinamento, sicurezza dei locali con sistemi antincendio e antintrusione, analisi del rischio di allagamento, ed intrusione, il controllo di temperatura e umidità relativa per la corretta conservazione del materiale cartaceo e la prevenzione da infestazioni biologiche, ordinaria manutenzione e pulizia, prevenzione da danno foto-ossidativo, spolveratura periodica), in collaborazione con i servizi preposti alle attività tecniche e ai servizi generali.

Il Responsabile della gestione documentale provvede anche ad attuare interventi di restauro, nei casi in cui si rendessero necessari, nelle modalità previste dal D.lgs. 42/2004 commi 4, 6 e 7 (Cfr. Capitolo 11).

Il processo completo di conservazione dei documenti, adottato dall'INRiM, è descritto dettagliatamente, secondo le indicazioni fornite dalle LL.GG. AgID, nell'Allegato 5 - *Manuale di Conservazione*.

CAPITOLO 11. L'ARCHIVIO STORICO

L'Archivio storico, o sezione separata dell'Archivio, è costituito dai documenti relativi agli affari esauriti da oltre quarant'anni, ai sensi dell'art. 30 c. 4 del D.lgs. 42/2004 – Codice dei Beni Culturali e del Paesaggio, di seguito Codice) che devono essere conservati in modo permanente, (Cfr. Allegato n. 4 - *Massimario di selezione e scarto*).

Attualmente tali documenti coincidono con l'archivio dell'Istituto Elettrotecnico Nazionale Galileo Ferraris, sul quale l'INRiM ha diretta responsabilità di conservazione.

I documenti analogici selezionati per la conservazione permanente devono essere ordinati (art. 30 c. 4 D.lgs. 42/2004), rispettando i criteri delineati nelle fasi corrente e di deposito ma tenendo conto che, dopo tutti i successivi scarti, tale parte dell'archivio deve ormai assumere uno stato definitivo; pertanto i documenti devono essere trasferiti, contestualmente agli strumenti che ne garantiscono l'accesso (protocolli, repertori, rubriche, schedari, elenchi, ecc.), nell'apposita separata sezione di archivio (art. 60 DPR 445/2000).

L'archivio storico, oltre ad essere conservato in ordine, deve inoltre essere inventariato (art. 30, c. 4 D.lgs. 42/2004), cioè dotato di uno strumento di descrizione complessiva che, affiancando gli strumenti originari di gestione (protocolli, repertori, ecc.), ne faciliti l'accesso ai fini giuridico-amministrativi (mai del tutto esauriti) e di ricerca scientifica, e ne consenta la tutela anche patrimoniale.

Il riordino e la inventariazione deve essere affidata a personale, eventualmente anche esterno all'Ente, dotato di adeguata professionalità specifica (archivisti qualificati); in via preliminare dovrà essere richiesto, con congruo anticipo, un parere preventivo di opportunità alla Soprintendenza Archivistica, e quindi a richiedere l'autorizzazione prescritta per l'esecuzione dell'intervento, previa la presentazione di un progetto di intervento, completo di tutti i dati ed elaborati tecnico-scientifici necessari (art. 21, c. 5 D.lgs. 42/2004).

Al termine delle operazioni, una copia degli inventari sarà consegnata alla Soprintendenza Archivistica competente sul territorio;

Il Responsabile della gestione documentale, come responsabile generale di tutto il sistema archivistico dell'Ente, è comunque tenuto a supervisionare e garantire anche la gestione dell'archivio storico (art. 61 c. 3 lett. f DPR 445/2000).

È dovere del Responsabile della gestione documentale provvedere all'eventuale ricondizionamento e restauro delle unità archivistiche selezionate per la conservazione permanente ogni volta che se ne presenti la necessità e provvedere ad eventuali operazioni di digitalizzazione preventiva.

Anche per quanto riguarda il restauro si dovrà fare ricorso alle professionalità individuate dall'art 29 del D.lgs. 42/2004, e dovrà essere richiesta l'autorizzazione prescritta alla Soprintendenza, previa presentazione di un progetto redatto dai professionisti a cui verrà affidato il lavoro.

11.1. Locali e condizioni di conservazione

Il D.lgs. 42/2004, Codice dei Beni Culturali e del Paesaggio, stabilisce che gli archivi e i singoli documenti degli enti pubblici sono considerati beni culturali e sono soggetti, pertanto, a particolare tutela; come per la documentazione conservata nell'Archivio di deposito cartaceo, l'Ente è tenuto alla corretta conservazione della documentazione.

La conservazione, così come descritta dall'art. 29 c.1 del Codice, è assicurata «mediante una coerente, coordinata e programmata attività di studio, prevenzione, manutenzione e restauro».

Il Codice definisce:

- l'attività di prevenzione come: *“il complesso delle attività idonee a limitare le situazioni di rischio connesse al bene culturale nel suo contesto”* (art. 29 c.2);
- la manutenzione come: *“il complesso delle attività e degli interventi destinati al controllo delle condizioni del bene culturale e al mantenimento dell'integrità, dell'efficienza funzionale e dell'identità del bene e delle sue parti”* (art. 29 c.3).

È dovere dell'Ente provvedere al rispetto delle specifiche condizioni di conservazione, elencate nel documento *“Sedi d'archivio: caratteristiche e requisiti”*, redatto dalla Soprintendenza Archivistica per il Piemonte e la Valle d'Aosta⁴⁹.

È obbligatorio in particolare:

- mantenere i locali adibiti a deposito della documentazione sani ed areati, con temperatura e umidità il più possibile stabili. I valori indicativi, ottimali per la conservazione di materiale cartaceo, sono di circa 15-18 gradi centigradi di temperatura e 50-60% di umidità relativa. idonee ad evitare l'insorgenza di polvere, muffe e batteri.

I parametri ambientali di umidità e temperatura andranno dunque sempre monitorati, per mezzo di termo-igrometri stabilmente posizionati nei locali, e, se necessario, tenuti sotto controllo tramite condizionatori e deumidificatori;

- dotare i locali di appositi impianti per la deumidificazione, il condizionamento ed il filtraggio dell'aria, così da assicurare una appropriata ed illimitata conservazione dei materiali e dei supporti documentari;

⁴⁹ *“Sedi d'archivio: caratteristiche e requisiti”* a cura della Soprintendenza Archivistica per il Piemonte e la Valle d'Aosta http://www.sato-archivi.it/Sito/images/stories/modelli_scaricabili/requisiti_strutturali_archivio.pdf

- provvedere a un sistema di illuminazione dei depositi che protegga i materiali dalla foto ossidazione dovuta all'esposizione diretta ai raggi del sole, schermando, quindi, le fonti di luce naturale.

Per la corretta conservazione del materiale cartaceo vengono adottati comportamenti abituali per il buon mantenimento delle condizioni dei locali, quali:

- tutti i locali dell'Archivio e gli arredi interni devono essere regolarmente puliti e periodicamente disinfestati e derattizzati.
- tutti gli impianti e le attrezzature adibite al controllo dell'illuminazione, climatico e di prevenzione incendi vanno sottoposti a verifiche di manutenzione regolari e periodiche, al fine di garantirne la costante efficienza.

L'accesso ai locali destinati alla conservazione o alla movimentazione del materiale archivistico è consentito solo al personale della Segreteria Generale ed è controllato tramite sistemi di sicurezza e di anti-intrusione adeguati; è consentito l'accesso ad estranei solo se autorizzati (ad es. per attività di manutenzione e logistica) e sotto la supervisione della Segreteria Generale.

Per le strutture da adibire a deposito archivistico è opportuno, e fortemente consigliato dalla Soprintendenza competente sul territorio, ottenere (o aggiornare) il certificato di prevenzione incendi (CPI) da parte del competente comando dei Vigili del Fuoco⁵⁰.

Per diminuire il rischio di innesco e propagazione di un incendio, è vietato:

- Adibire i locali di conservazione archivistica ad altri usi potenzialmente pericolosi. In particolare, è vietato conservare insieme ai documenti sostanze chimiche o materiali infiammabili (carburanti, detersivi, cancelleria, materie plastiche...)
- Tenere e usare nei depositi di archivio elettrodomestici, apparati pericolosi o fiamme libere (fotocopiatrici, stufe elettriche o a fiamma, fornelli...)
- È inoltre necessario che i depositi d'archivio siano dotati dei seguenti sistemi di protezione:
 - Dispositivi di separazione e compartimentazione (pareti, porte, infissi), in grado di evitare la propagazione dell'incendio per un periodo di tempo sufficiente all'estinzione (comunque non inferiore a REI 120).
 - Dispositivi di rilevazione incendi (fumo e calore), collegati a centrali di controllo presidiate (forze dell'ordine, vigilanza privata, alloggio dei custodi...) in grado di garantire una reazione entro pochi minuti dall'allarme.
 - Dispositivi di estinzione manuale (estintori a parete o carrellati), in quantità commisurata al carico d'incendio esistente. Benché di minor efficacia, sono da preferire gli estintori a polvere, poiché gli estinguenti a schiuma o CO2 possono provocare gravi danni al materiale cartaceo. Ugualmente pericolosi possono rivelarsi i normali idranti ad acqua.

⁵⁰ L'attuale normativa (D.P.R. n. 151 del 01/08/2011) prevede che il CPI sia obbligatorio per i depositi che conservano quantità di carta superiore ai 5000 kg. (pari a circa 83 m.l. di documenti), nonché per tutti gli immobili sottoposti a tutela ai sensi del D.lgs. 42/2004 e destinati a contenere biblioteche o archivi; tuttavia, in particolari situazioni di rischio, la Soprintendenza può richiedere il CPI anche per quantità inferiori di materiale archivistico.

11.2. Manutenzione e cura del materiale archivistico

Per assicurare la corretta custodia e la buona tenuta dell'archivio la Segreteria Generale deve provvedere a predisporre le operazioni periodiche di pulizia e spolveratura del materiale conservato e a attivare gli interventi previsti dalla normativa vigente in caso di danneggiamenti e sottrazioni di documenti.

Il materiale archivistico può essere sottoposto, in caso di necessità, a restauro secondo quanto previsto dalla normativa in materia e con l'autorizzazione della Soprintendenza Archivistica del Piemonte e della Valle d'Aosta (d.lgs. 42/2004, articolo 21 comma 4 e 5).

Le operazioni di restauro e di spolveratura dei materiali sono affidate a personale specializzato, anche ricorrendo a ditte esterne specializzate nel settore.

CAPITOLO 12. IL SISTEMA INFORMATICO

Il sistema informatico è l'insieme delle risorse di calcolo, degli apparati, delle reti di comunicazione e delle procedure informatiche utilizzati dalle amministrazioni per la gestione dei documenti. (DPR 445/2000, art.1, lettera r).

La gestione dei flussi documentali è un insieme di funzionalità che consentono di trattare e di organizzare la documentazione prodotta (in arrivo, in partenza e interna) dalle amministrazioni.

Nell'attuazione delle Linee Guida AgID, le Pubbliche Amministrazioni sono tenute ad ottemperare alle misure minime di sicurezza ICT emanate dall'AgID con circolare del 18 aprile 2017, n. 2/2017.

In tale ottica, il Responsabile della gestione documentale ovvero, ove nominato, il Coordinatore della gestione documentale, in accordo con il Responsabile della conservazione, con il Responsabile per la transizione digitale e acquisito il parere del Responsabile della protezione dei dati personali, predispone il piano della sicurezza del sistema di gestione informatica dei documenti prevedendo opportune misure tecniche e organizzative per garantire un livello di sicurezza adeguato al rischio in materia di protezione dei dati personali, ai sensi dell'art. 32 del Regolamento UE 679/2016 (GDPR)⁵¹, anche in funzione delle tipologie di dati trattati, quali quelli riferibili alle categorie particolari di cui agli artt. 9-10 del Regolamento stesso.

12.1. Il modello organizzativo

I servizi di *information and communication technology* per il supporto all'attività amministrativa e per le esigenze della ricerca dell'Ente sono curati dall'UO Sistemi Informatici e Reti.

Nell'ambito della gestione documentale, l'Ente ha acquisito dal Consorzio Cineca l'applicativo Titulus con una soluzione di tipo *Software as a Service* (SaaS): le funzionalità del programma sono rese disponibili attraverso interfaccia web, il cui accesso è subordinato a un processo di autenticazione informatica effettuato mediante il sistema centralizzato dell'Ente.

⁵¹ L'art. 32 del Regolamento (UE) 2016/679 prevede che:

“1. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:

- a) la pseudonimizzazione e la cifratura dei dati personali;
- b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
- c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
- d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

2. Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.

3. L'adesione a un codice di condotta approvato di cui all'articolo 40 o a un meccanismo di certificazione approvato di cui all'articolo 42 può essere utilizzata come elemento per dimostrare la conformità ai requisiti di cui al paragrafo 1 del presente articolo.

4. Il titolare del trattamento e il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri”

La conduzione operativa del sistema è curata direttamente dal Consorzio Cineca, a cui, in virtù di un'apposita convenzione, sono demandati gli oneri di installazione, manutenzione, gestione, aggiornamento, monitoraggio di tutte le componenti fisiche e logiche infrastrutturali, di verifica della correttezza delle funzioni applicative e dell'integrità delle basi di dati in conformità a quanto previsto dalla normativa vigente in materia di sicurezza e di protezione dei dati e di continuità operativa.

Nel presente capitolo, il termine "conservazione" è utilizzato in luogo di "registrazione" dei dati su dispositivi di memorizzazione on-linee near-line o su supporti per il salvataggio dei dati in modalità off-line.

12.2. Piano di sicurezza del sistema informatico

La sicurezza dei dati, delle informazioni e dei documenti informatici memorizzati (poi archiviati) nel sistema di gestione documentale è garantita dall'applicazione informatica adottata dall'Ente.

Il Centro Sistemi Informativi e Reti dell'INRiM provvede all'acquisizione di beni e di servizi tecnologici di interesse generale dell'Ente e all'acquisizione di dispositivi tecnologici e applicativi per le esigenze della Amministrazione Centrale; sovrintende al rispetto delle norme e degli standard per la sicurezza nell'uso delle tecnologie e cura l'interoperabilità dei sistemi informativi.

Il Centro Sistemi Informativi e Reti provvede inoltre a definire linee guida per l'uso delle tecnologie in conformità con quanto prescritto dalla normativa vigente.

Il Consorzio Interuniversitario Cineca, in qualità di Conservatore, predispone e aggiorna annualmente il piano della sicurezza informatica relativo a formazione, gestione, trasmissione, interscambio, accesso, memorizzazione dei documenti informatici, ivi compresa la gestione delle copie di sicurezza nel rispetto delle misure minime di sicurezza previste nel disciplinare tecnico descritto nell'Allegato B del D.lgs. 30 giugno 2003 e successive modificazioni e in conformità anche al Regolamento UE 679/2016.

12.2.1. Il sistema di gestione documentale

Il sistema di gestione documentale è costituito dall'insieme delle tecnologie presenti presso il data center del Consorzio Interuniversitario Cineca e da tutti i dispositivi e i programmi presenti presso le sedi dell'Ente che permettono l'utilizzo del sistema.

In particolare, sono parte integrante dell'infrastruttura i cablaggi e gli apparati di rete presenti presso le sedi dell'Ente e necessari per la connettività verso il Consorzio Cineca per mezzo della rete GARR, i sistemi informatici e le componenti software sottese al sistema di autenticazione adottato da INRiM e tutte le postazioni di lavoro utilizzate dagli utenti del sistema di gestione documentale.

Le misure di sicurezza fisica e logica specifiche e le procedure comportamentali adottate per la protezione dell'infrastruttura del sistema di gestione documentale, delle informazioni e dei dati sono riportate nei paragrafi seguenti.

In essi è data evidenza di quali ambiti siano gestiti e curati dal Consorzio Cineca, quali siano curati dal Centro Sistemi Informativi e Reti dell'INRiM e quali rimangono in carico all'AOO.

12.2.2. Sicurezza fisica dei data center

Le misure adottate per garantire un adeguato livello di sicurezza fisica del data center del Consorzio Cineca sono riportate nel Manuale di Conservazione Del Consorzio Interuniversitario CINECA; esso illustra le misure

per la protezione fisica dei locali tecnici finalizzate a garantire l'integrità e la disponibilità degli apparati di rete, dei server e delle applicazioni, nonché le misure adottate per la protezione dei dati e le caratteristiche del servizio di Disaster Recovery per il quale è dichiarato un punto di ripristino (Restore Point Objective- RPO) pari a 24H; tali misure sono state anche integralmente riportate al capitolo 7 del Manuale di Conservazione dell'INRiM, allegato n.5 a questo documento.

12.2.3. La manutenzione e la continuità operativa degli impianti elettrici

Gli impianti elettrici dell'INRiM sono monitorati da sistemi automatici di allarme in grado di allertare i tecnici di manutenzione degli impianti elettrici in caso di anomalie e permetterne l'intervento entro il tempo di protezione garantito dai sistemi UPS.

12.2.4. Rete dati

I sistemi server dell'INRiM non sono coinvolti nella gestione documentale; per quanto riguarda la sicurezza delle reti e delle postazioni di lavoro, di seguito descritte, sono, di fatto, fatte salve le prescrizioni del d.lgs.196/2003"Codice in materia di protezione dei dati personali" e della CIRCOLARE AgID n. 2/2017 in materia di "Misure Minime Di Sicurezza ICT Per Le Pubbliche Amministrazioni"

Il Centro Sistemi Informativi e Reti, in qualità di amministratore della rete dell'Ente, assicura in modo esclusivo e tempestivo la gestione, il monitoraggio, l'aggiornamento e l'ampliamento della rete dati di INRiM (cablaggio e parte attiva), sia sotto l'aspetto fisico che logico, fino alla presa utente compresa.

L'amministratore della rete di INRiM registra – in appositi file di log– i dati relativi all'accesso alla rete all'accesso ad internet o al traffico telematico in generale (escluso il contenuto della trasmissione dati).

I dati registrati nei file di log sono raccolti, memorizzati e conservati in conformità alla normativa vigente. Le informazioni contenute nei file di log possono essere messe a disposizione dell'autorità giudiziaria, la quale può richiedere la non cancellazione e la conservazione per un periodo più lungo di quanto disposto dalla legge.

12.2.5. Le postazioni di lavoro

Le postazioni di lavoro degli utenti dell'Amministrazione Centrale sono competenza del Centro Sistemi Informativi e Reti.

La AOO verifica il coerente utilizzo delle postazioni di lavoro per l'utilizzo del sistema di gestione documentale, da tavolo o portatili, o gli strumenti comunque funzionalmente assimilabili e preordina la necessaria dotazione di dispositivi (hardware) e programmi (software) tali da consentire il corretto funzionamento e il mantenimento in condizioni di sicurezza ai fini del regolare svolgimento dell'attività lavorativa.

Le postazioni di lavoro soddisfano i seguenti criteri di sicurezza:

- ❖ il sistema operativo è aggiornato e aggiornabile;
- ❖ gli applicativi installati e i loro componenti software aggiuntivi (ad es., plug-in) sono aggiornati e aggiornabili;

- ❖ sono dotate di un programma antivirus con funzionalità automatica di aggiornamento periodico;
- ❖ l'accesso al sistema operativo della postazione di lavoro è protetto da password di adeguata complessità, cambiata con cadenza regolare;
- ❖ sono dotate di firewall locale impostato per consentire solo le connessioni instaurate dal client stesso e per i servizi legittimi (client mode);
- ❖ salvo motivate e documentate eccezioni, sulle postazioni di lavoro non è permessa la connessione remota dall'esterno della Rete Dati di INRiM (RDP, SSH, VNC, ecc.);
- ❖ la connessione da remoto alle postazioni di lavoro dall'interno della Rete Dati dell'INRiM, ove attivata, viene effettuata esclusivamente mediante protocolli di comunicazione sicuri ed è consentita solo previo consenso dell'utente che in quel momento sta utilizzando l'elaboratore.

12.2.6. La sicurezza delle postazioni di lavoro per lo smart working

In data 17 marzo 2020 sono state pubblicate dall'AgID alcune raccomandazioni allo scopo di supportare le Pubbliche Amministrazioni e i lavoratori pubblici in smart working e sostenerli nel contrastare eventuali attacchi informatici con comportamenti responsabili; tali raccomandazioni sono state elaborate sulla base delle misure minime di sicurezza informatica per le pubbliche amministrazioni fissate dalla circolare AgID n. 1/2017.

Il personale dell'INRiM che lavora in smart working adotta i comportamenti corrispondenti alle raccomandazioni elaborate dall'AgID:

- ❖ Seguire prioritariamente le policy e le raccomandazioni dettate dalla propria Amministrazione
- ❖ Utilizzare i sistemi operativi per i quali attualmente è garantito il supporto
- ❖ Effettuare costantemente gli aggiornamenti di sicurezza del tuo sistema operativo
- ❖ Assicursi che i software di protezione del sistema operativo (Firewall, Antivirus, ecc.) siano abilitati e costantemente aggiornati
- ❖ Assicursi che gli accessi al sistema operativo siano protetti da una password sicura e comunque conforme alle password policy emanate dalla tua Amministrazione
- ❖ Non installare software proveniente da fonti/repository non ufficiali
- ❖ Bloccare l'accesso al sistema e/o configura la modalità di blocco automatico quando ci si allontana dalla postazione di lavoro
- ❖ Non cliccare su link o allegati contenuti in email sospette
- ❖ Utilizzare l'accesso a connessioni Wi-Fi adeguatamente protette
- ❖ Collegarsi a dispositivi mobili (pen-drive, hdd-esterno, etc) di cui si conosce la provenienza (nuovi, già utilizzati, forniti dalla tua Amministrazione)
- ❖ Effettuare sempre il log-out dai servizi/portali utilizzati dopo aver concluso la sessione lavorativa.

12.3. Sicurezza dei documenti informatici

L'accesso al sistema di gestione documentale del personale INRiM è gestito centralmente ed è subordinato all'abilitazione a cura del Responsabile della gestione documentale o, ove nominato, a cura del Coordinatore della gestione documentale.

Le identità digitali utilizzate per l'accesso al sistema di gestione documentale sono costituite da nome utente e password. L'identificazione informatica dell'utente, cioè la validazione dell'identità digitale, è operata attraverso una infrastruttura di autenticazione centralizzata basata su Lightweight Directory Access Protocol (LDAP).

L'accesso al sistema di gestione documentale da parte di soggetti esterni all'Ente non è consentito.

Il sistema di gestione documentale rispetta le misure di sicurezza previste dagli artt. 31-36 e dal disciplinare tecnico di cui all'Allegato B del D.lgs. 30 giugno 2003, n. 196.

I dati sono resi disponibili e accessibili a chiunque ne abbia diritto:

Si individuano i soggetti preposti al trattamento dei dati:

- ❖ **Titolare del trattamento** – È il destinatario delle norme, ossia la persona fisica e/o giuridica, l'amministrazione pubblica o altro ente a cui compete decidere finalità, modalità del trattamento dei dati personali e gli strumenti utilizzati, compresa la sicurezza;
- ❖ **Responsabile del trattamento** – La persona fisica, giuridica, l'amministrazione pubblica o altro ente designato, facoltativamente, dal titolare a trattare i dati compreso il profilo relativo alla sicurezza: o i Direttori dei Dipartimenti, Centri servizi, Centri speciali, Scuole; o il Direttore Generale per gli Uffici di staff; o i Dirigenti per le Aree dirigenziali dell'Amministrazione Centrale o i Responsabili della gestione documentale di ogni AOO.
- ❖ **Responsabile esterno del trattamento** – In coerenza con il modello organizzativo adottato dall'INRiM per la conduzione del Sistema di gestione documentale, al Consorzio Cineca è conferito il ruolo di Responsabile esterno del trattamento; in virtù di tale ruolo è il Consorzio che, per le attività di conduzione del sistema, gestione applicativa e assistenza, provvede alla nomina dell'amministratore di sistema, ne assolve i compiti e conseguenti adempimenti.
- ❖ **Incaricato del trattamento** – La persona fisica autorizzata a compiere operazioni di trattamento dati dal Titolare o dal Responsabile.

I Responsabili del trattamento designano, con provvedimento espresso, gli Incaricati del trattamento dei dati operanti all'interno della struttura di competenza.

Nello svolgimento dei compiti è fatto divieto agli Incaricati di comunicare e/o di divulgare qualsivoglia dato sensibile e/o personale.

Tale obbligo di riservatezza è esteso anche al periodo successivo alla scadenza dell'incarico, fino a quando le suddette informazioni non vengano divulgate a opera del Titolare, oppure divengano di dominio pubblico.

12.3.1. Accesso ai dati e ai documenti informatici

Il sistema di gestione documentale Titulus, adottato dall'INRiM garantisce:

- ❖ la protezione delle informazioni relative a ciascun utente nei confronti degli altri;
- ❖ la garanzia di accesso ai documenti, alle informazioni e ai dati esclusivamente agli utenti abilitati;
- ❖ il controllo differenziato dell'accesso alle risorse del sistema per ciascun utente o gruppo di utenti;
- ❖ la registrazione delle attività svolte da ciascun utente anche rilevanti ai fini della sicurezza, in modo tale da garantirne l'identificazione;
- ❖ l'immodificabilità dei contenuti e, comunque, la loro tracciabilità.

Il controllo degli accessi è assicurato dall'utilizzo di credenziali di autenticazione con differenti profili di autorizzazione in relazione ai diversi ruoli di ciascun utente.

I trattamenti associabili a ciascun profilo, preventivamente individuati dal Responsabile della gestione documentale di concerto con il Responsabili del trattamento dei dati, sono in sintesi:

- ❖ inserimento dei dati per effettuare una registrazione;
- ❖ modifica dei dati di una registrazione;
- ❖ annullamento di una registrazione;
- ❖ ricerca di informazioni registrate ai fini della visualizzazione o consultazione;
- ❖ visualizzazione e consultazione;
- ❖ download dei documenti associati alla registrazione.

Periodicamente, e comunque almeno annualmente, è verificata a cura del Responsabile della gestione documentale di concerto con i responsabili delle strutture, la sussistenza delle condizioni per il mantenimento dei profili di autorizzazione per tutte le UO.

Quando l'accesso ai dati e agli strumenti informatici è consentito esclusivamente mediante uso della componente riservata della credenziale per l'autenticazione, sono impartite idonee e preventive disposizioni volte a individuare chiaramente le modalità con le quali il Titolare può assicurare la disponibilità di dati o di strumenti informatici in caso di prolungata assenza o di impedimento dell'incaricato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema.

In tal caso, la custodia delle copie delle credenziali è organizzata garantendo la relativa segretezza e individuando preventivamente per iscritto i soggetti incaricati della loro custodia, i quali devono informare tempestivamente l'Incaricato dell'intervento effettuato.

Le stesse credenziali non possono essere assegnate a persone diverse, neppure in tempi diversi, quindi le credenziali sono strettamente personali.

Ciascun utente ha la possibilità di cambiare la propria password in qualsiasi momento ed è auspicabile che ciò avvenga nel caso in cui si presume che essa abbia perso il requisito della segretezza.

12.3.2. Le procedure comportamentali ai fini della protezione dei documenti

Le postazioni di lavoro, da tavolo e portatili, o gli strumenti comunque funzionalmente assimilabili, di proprietà di INRiM e, a vario titolo, messi a disposizione del personale, sono uno strumento di lavoro e il loro utilizzo è finalizzato allo svolgimento delle attività professionali e istituzionali dell'Ente.

Ogni utente adotta comportamenti corretti, tali da preservare il buon funzionamento degli strumenti e da ridurre i rischi per la sicurezza dei sistemi informativi.

In ogni caso, l'utilizzo delle risorse informatiche non deve pregiudicare il corretto adempimento della prestazione lavorativa, ostacolare le attività dell'INRiM o essere destinato al perseguimento di interessi privati in contrasto con quelli pubblici.

Si sottolineano le seguenti responsabilità:

- ❖ il dipendente è tenuto a segnalare immediatamente ai referenti informatici ogni sospetto di effrazione, incidente, abuso o violazione della sicurezza;
- ❖ in caso di cessazione del rapporto di lavoro, il dipendente deve restituire all'INRiM qualsiasi risorsa informatica assegnata e mettere a disposizione ogni informazione di interesse istituzionale;

L'utente è tenuto a bloccare o a spegnere il personal computer in caso di sospensione o di termine dell'attività lavorativa, assicurandosi di evitarne l'utilizzo improprio da parte di terzi, mediante inserimento di apposite credenziali di accesso.

Le stazioni di lavoro, da tavolo e portatili, o gli strumenti comunque funzionalmente assimilabili, messe a disposizione del personale, non devono essere lasciati incustoditi. Al termine dell'orario di servizio, i computer devono essere spenti prima di lasciare gli uffici.

In caso di allontanamento temporaneo, l'utente deve attivare il salvaschermo con sblocco tramite password.

In linea generale è fortemente raccomandato di evitare la memorizzazione di dati sensibili o giudiziari su dispositivi mobili (palmari, notebook, smart phone, penne USB, dischi rigidi esterni, memory card, ecc.). Quando, per giustificati motivi, ciò si rendesse necessario, è fatto obbligo di adottare le misure idonee prescritte dal già citato Allegato B al D.lgs. 30 giugno 2003, n. 196.

Le credenziali di accesso (generalmente, nome utente e password) sono strettamente personali e ogni attività non regolare effettuata e riconducibile alle stesse è imputata al titolare delle credenziali medesime.