Ufficio PRA

PISTOIA

Manuale di Gestione Documentale

Sommario

1. Principi generali

Premessa

Questo manuale è redatto in conformità alle *Linee Guida sulla formazione, gestione e conservazione dei documenti informatici* dell'Agenzia per l'Italia Digitale.

Inoltre, è stato predisposto dal Responsabile della gestione documentale in conformità allo schema e alle linee guida elaborate dal Coordinatore della Gestione Documentale. Tutte le procedure, i flussi, le regole di classificazione, protocollazione, assegnazione e conservazione dei documenti sono adottati in coerenza con quanto previsto dallo schema di riferimento, garantendo uniformità e tracciabilità tra le diverse AOO.

Il Manuale:

- descrive il sistema di gestione dei documenti, dalla protocollazione della corrispondenza in entrata, in uscita e interna;
- fornisce le istruzioni per il corretto uso del protocollo informatico, la gestione dei flussi documentali e degli archivi.

Norme e testi di riferimento

- Linee Guida sulla formazione, gestione e conservazione dei documenti informatici di maggio 2021 e relativi allegati (Linee Guida): Queste Linee Guida costituiscono la normativa primaria di riferimento.
- DPR 445/2000 (TUDA) – Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa.
- D.lgs 82/2005 e ss.mm.ii. (CAD) – Codice dell'Amministrazione Digitale.
- D.lgs 196/2003 e ss.mm.ii. – Codice in materia di protezione dei dati personali.
- Circolare 18 aprile 2017, n. 2/2017 dell'Agenzia per l'Italia Digitale, recante le misure minime di sicurezza ICT per le pubbliche amministrazioni.

Coordinatore della Gestione documentale

Il Coordinatore della gestione documentale è nominato dall'Amministrazione con atto formale del legale rappresentante.

Riveste anche il ruolo di Responsabile della conservazione. Alla data di pubblicazione del presente Manuale coincide con il Responsabile dei Sistemi Informativi ACI.

Un Vicario è designato secondo quanto previsto dalle Linee Guida AgID 2021.

Il Coordinatore ha i seguenti compiti:

- predisporre lo schema del Manuale di gestione documentale, che disciplina la formazione, la gestione, la trasmissione, lo scambio e l'accesso ai documenti informatici, nel rispetto della normativa sulla protezione dei dati personali e in coerenza con il Manuale di conservazione;
- proporre misure organizzative e tempi per eliminare protocolli non conformi (di settore, di reparto, multipli, di telefax), in favore del solo protocollo informatico previsto dal CAD;
- validare, insieme al Responsabile della conservazione, al Responsabile dei sistemi informativi e al Responsabile della sicurezza dei dati, il piano di sicurezza informatica, relativo alla gestione e conservazione dei documenti informatici (alla data del presente documento tali responsabilità coincidono in un unico soggetto);
- verificare periodicamente l'adeguatezza del piano di classificazione rispetto ai procedimenti e agli affari in corso e aggiornarlo quando necessario;
- assicurare criteri uniformi nella gestione informatica dei documenti.

Responsabile della gestione documentale

Il Responsabile della gestione documentale (RGD) è nominato con atto formale del Direttore/Responsabile dell'AOO. Nel caso in cui il Direttore/Responsabile non proceda alla nomina del RGD, si assume che sia esso stesso RGD. Il Vicario del Responsabile deve essere nominato dal Direttore/Responsabile dell'AOO.

Al Responsabile della gestione documentale e al suo Vicario, nei casi previsti, spettano i seguenti compiti:

- predisporre il Manuale di gestione documentale relativo alla formazione, alla gestione, alla trasmissione, all'interscambio e all'accesso ai documenti informatici, nel rispetto della normativa in materia di trattamento dei dati personali e in coerenza con quanto previsto nel manuale di conservazione. Il RGD propone l'adozione di tale manuale per ogni AOO;
- assicurare che il Manuale di gestione documentale contenga, come parte integrante, il piano per la sicurezza informatica, per la quota parte di competenza, nel rispetto delle misure di sicurezza predisposte dall'AGID e dagli altri organismi preposti, delle disposizioni in materia di protezione dei dati personali e delle indicazioni di continuità operativa dei sistemi informatici;
- verificare l'avvenuta eliminazione dei protocolli di settore e di reparto, dei protocolli multipli e, più in generale, dei protocolli diversi dal protocollo informatico previsto

dal TUDA. Propone al Coordinatore della Gestione documentale idonee misure per la loro eliminazione, evitando di aprirne di nuovi;
- in caso di amministrazioni con più AOO, assicurare l'adozione di criteri uniformi per la gestione informatica dei documenti, sentiti i responsabili della gestione documentale;
- essere responsabile dell'archivio e della tenuta dei documenti, garantendo il buon funzionamento degli strumenti e dell'organizzazione delle attività di registrazione di protocollo, di gestione dei documenti e dei flussi documentali, incluse le funzionalità di accesso e le attività di gestione degli archivi di cui agli articoli 67, 68 e 69 del TUDA;
- sulla base del titolario, individuare i profili di abilitazione per l'accesso alle funzioni della procedura, distinguendo tra abilitazioni alla consultazione e abilitazioni all'inserimento e alla modifica delle informazioni registrate, in accordo con il Direttore/Responsabile dell'AOO;
- autorizzare lo svolgimento anche manuale delle operazioni di registrazione di protocollo su uno o più registri di emergenza, ogni qualvolta per cause tecniche non sia possibile utilizzare la normale procedura informatica, e curare l'apertura, l'uso e la chiusura di tale registro. Gestisce il registro di emergenza in accordo con quanto riportato nell'art. 63 del TUDA;
- autorizzare le operazioni di annullamento delle registrazioni di protocollo.
- vigilare sull'osservanza delle disposizioni del TUDA e delle norme vigenti da parte del personale autorizzato e degli incaricati.

Servizio per la gestione del Protocollo informatica (SGP)

Presso la AOO è istituito il Servizio per il protocollo informatico, la gestione dei flussi documentali e degli archivi, guidato dal Responsabile del servizio.

Il Servizio svolge i seguenti compiti:

a) definire i livelli di autorizzazione all'uso del sistema, distinguendo tra consultazione, inserimento e modifica dei dati;

b) garantire che le registrazioni e le segnature di protocollo siano effettuate nel rispetto del DPR 445/2000;

c) segnalare tempestivamente al fornitore eventuali guasti o anomalie del sistema, aprendo un ticket per il ripristino delle funzionalità;

d) conservare i documenti analogici in modo sicuro;

e) assicurare il corretto funzionamento degli strumenti e delle attività di registrazione, gestione dei documenti, flussi documentali, accesso e archiviazione;

f) autorizzare eventuali annullamenti di registrazioni di protocollo;

g) vigilare sul rispetto delle norme da parte del personale autorizzato e degli incaricati;

h) gestire l'apertura, l'uso e la chiusura del registro di emergenza con gli strumenti disponibili.

Conservazione del registro di protocollo

Il registro informatico di protocollo è generato automaticamente dal sistema e trasmesso al sistema di conservazione, che ne garantisce l'immodificabilità. Tale processo avviene in modo automatico, senza intervento da parte del SGP.

Firma digitale

Per lo svolgimento delle attività istituzionali del Responsabile di Protocollo, del suo Vicario e degli operatori autorizzati, su richiesta del Direttore o del Responsabile della Struttura di appartenenza, l'Ente fornisce la firma digitale o elettronica qualificata ai soggetti da essa delegati.

Tali soggetti sono in particolare autorizzati a firmare le attestazioni di conformità all'originale di cui all'art. 22, comma 2, del Codice dell'Amministrazione Digitale.

Caselle di posta elettronica

L'Area Organizzativa Omogenea (AOO) è dotata di una casella di posta elettronica certificata (PEC) istituzionale, in quanto questa costituisce il domicilio digitale dell'AOO, specificamente per le comunicazioni, istanze, dichiarazioni e notifiche che, sia in ingresso sia in uscita, sono soggette a registrazione di protocollo.

Divieto di registri di di protocollo diversi da quello informatico

Non è in nessun caso consentito l'utilizzo di registri di protocollo diversi da quello informatico, salvo il Registro di emergenza.

Tutela dei dati personali

L'Ente, in qualità di titolare dei dati di protocollo e dei dati personali contenuti nella documentazione amministrativa, garantisce il rispetto della normativa sulla protezione dei dati personali attraverso atti formali rivolti agli addetti autorizzati all'accesso e al trattamento.

Il Fornitore, incaricato dal Titolare o dal Responsabile della sicurezza delle informazioni, adotta misure organizzative per assicurare che i documenti trasmessi ad altre Amministrazioni riportino solo i dati strettamente necessari alle finalità previste dalla legge.

Nella progettazione dei sistemi e dei processi di gestione, archiviazione e conservazione dei documenti, sono applicati i principi di protezione dei dati personali, in accordo con il Responsabile della protezione dei dati (RPD), mediante adeguate misure tecniche e organizzative.

Il trattamento avviene in conformità all'art. 5 del GDPR, garantendo: liceità, correttezza, trasparenza, limitazione delle finalità, minimizzazione, esattezza, conservazione limitata, integrità e riservatezza.

In conformità alla normativa sulla protezione dei dati personali, gli addetti al protocollo tutelano i dati sensibili e giudiziari evitando di inserirli nel campo "oggetto" del registro di protocollo.

2. Modalità di utilizzo di strumenti informatici per la formazione dei documenti informatici e il loro scambio all'interno e all'esterno dell'AOO

Nell'ambito del processo di gestione documentale, il documento amministrativo, in termini operativi, è classificabile in:

- ricevuto;
- inviato.

Il documento amministrativo, in termini tecnologici, è classificabile in:

- informatico;
- analogico.

Documento ricevuto

La corrispondenza in ingresso può essere acquisita dalla AOO con modalità diverse, a seconda del mezzo utilizzato dal mittente.

Documenti informatici:

- invio tramite posta elettronica o PEC;
- su supporto rimovibile (ad esempio pen drive), consegnato direttamente al servizio di protocollo o inviato per corriere.

Documenti analogici:

- invio tramite posta convenzionale o corriere;
- posta raccomandata;
- consegna diretta da parte dell'interessato o tramite persona delegata alle UOR o agli Uffici aperti al pubblico.

Documento inviato

La corrispondenza in uscita può essere inviata con modalità simili a quelle previste per i documenti in ingresso, in base al destinatario:

- verso un'altra AOO interna ad ACI: tramite Posta Elettronica Organizzativa (PEO).
- verso un'AOO di un'altra pubblica amministrazione: tramite PEC con interoperabilità, allegando l'XML di segnatura, come previsto dall'allegato 6 delle Linee Guida AgID 2021.

- verso privati: preferibilmente tramite PEC (se disponibile) o PEO; solo se non si conoscono né l'indirizzo PEC né l'indirizzo PEO, è consentito l'invio mediante canale cartaceo.

Il documento informatico

Tutti i documenti digitali destinati all'invio tramite mail o PEC devono essere firmati digitalmente, protocollati ed inviati senza essere stampati.

In generale, un documento nativo digitale non deve mai essere trasformato in cartaceo per poi essere nuovamente digitalizzato.

Il documento analogico

Il documento amministrativo analogico che può essere prodotto:

- in modo tradizionale, ad esempio una lettera scritta a mano;
- con strumenti informatici, ad esempio una lettera creata con un text editor e poi stampata.

In quest'ultimo caso, si considera originale il documento analogico nella sua redazione definitiva, completa e autentica, comprendente tutti gli elementi di garanzia e informazione su mittente e destinatario, stampata su carta intestata e firmata a mano.

Un documento analogico può essere trasformato in documento informatico mediante procedure di conservazione a norma, descritte nel seguito del Manuale.

Formazione dei documenti – Aspetti operativi

I documenti dell'Amministrazione sono prodotti con sistemi informatici, secondo la normativa vigente.

Ogni documento formato per essere inviato internamente o esternamente:

- tratta un unico argomento, indicato sinteticamente ma in modo esaustivo;
- è riferito a un solo numero di protocollo;
- può far riferimento a più fascicoli;
- è identificato univocamente dal numero di protocollo assegnato.

Le firme (digitali per i documenti informatici, autografe per quelli analogici) necessarie alla validità giuridica devono essere apposte prima della protocollazione. Anche i documenti non firmati rispettano i requisiti di immodificabilità e integrità, garantiti dal software di gestione documentale, secondo le Linee Guida AgID 2021.

Ogni documento deve consentire l'identificazione dell'Ufficio mittente e riportare almeno: denominazione e logo dell'Amministrazione, AOO e UOR di origine, indirizzo e recapiti dell'UOR, luogo e data di redazione, numero di protocollo, numero di allegati, oggetto del documento e firma del responsabile.

Sono utilizzati i formati supportati dalle applicazioni fornite dall'Amministrazione, conformi all'allegato 2 delle Linee Guida AgID 2021. Eventuali aggiornamenti o procedure di riversamento dei formati sono gestiti centralmente dal Coordinatore della Gestione Documentale.

Sottoscrizione dei documenti informatici

La sottoscrizione dei documenti informatici, quando richiesta, avviene mediante firma digitale conforme alla normativa vigente.

L'Amministrazione utilizza servizi forniti da un'Autorità di certificazione accreditata, iscritta nell'elenco pubblico tenuto da AgID.

I documenti informatici prodotti dall'Amministrazione, indipendentemente dal software usato, devono essere convertiti in uno dei formati standard previsti dalla normativa (ad esempio PDF) prima della firma digitale, per garantirne l'immodificabilità.

È preferibile utilizzare la firma PDF (PAdES). L'uso di firme in formato p7m (CAdES) è sconsigliato quando i documenti devono essere protocollati, poiché in questo caso la segnatura elettronica non risulta visibile sul documento. Pur essendo valido e correttamente protocollato, ciò può creare difficoltà operative.

I documenti firmati digitalmente non devono mai essere stampati, perché la stampa cancella le informazioni relative alla firma digitale. Chi riceve il documento deve poter verificare, tramite un visualizzatore PDF, la validità del certificato di firma, la scadenza e l'eventuale rispetto delle limitazioni indicate nel certificato.

Una volta stampato, un documento firmato digitalmente perde il valore della firma e ha la stessa validità di una semplice fotocopia.

Firma digitale

la firma digitale è lo strumento utilizzato per inviare e ricevere documenti da e per l'AOO e per sottoscrivere documenti, o qualsiasi altro "file" digitale con valenza giuridico-probatoria.

I messaggi ricevuti, sottoscritti con firma digitale, sono sottoposti a verifica di validità.

2.1 Posta elettronica certificata

L'uso della Posta Elettronica Certificata (PEC), di norma per comunicazioni verso l'esterno, consente di:

- garantire l'identità del mittente, con valore di firma elettronica semplice;
- conoscere in modo certo data e ora di trasmissione;
- confermare l'avvenuta consegna all'indirizzo PEC del destinatario;
- interoperare con altre AOO interne o di altre amministrazioni.

Gli automatismi del sistema di protocollo, aggiornati secondo l'allegato 6 delle Linee Guida AgID 2021, permettono la generazione automatica dei messaggi di conferma ricezione, riferiti a un solo documento protocollato per messaggio.

Un documento informatico trasmesso per via telematica si considera inviato e ricevuto se consegnato nella casella PEC del destinatario, come attestato dalla Ricevuta di Consegna.

Data e ora di formazione, trasmissione o ricezione di un documento informatico, redatto secondo la normativa vigente e le Linee Guida AgID 2021, sono opponibili a terzi.

La trasmissione telematica che assicura l'avvenuta consegna equivale alla notifica tramite posta raccomandata nei casi previsti dalla legge.

Per le comunicazioni verso Utenti esterni, l'invio digitale (firma digitale e mail/PEC) è obbligatorio. La stampa e l'invio cartaceo è ammesso solo se l'utente non dispone di alcun indirizzo email o PEC.

Per le altre pubbliche amministrazioni, l'invio deve sempre avvenire tramite PEC.

Le Imprese e i Professionisti sono obbligati a dotarsi di PEC; se non l'hanno fornita, il loro indirizzo può essere reperito nell'archivio INI-PEC (https://www.inipec.gov.it), registro ufficiale degli indirizzi PEC.

I cittadini privati non hanno ancora l'obbligo di possedere PEC: se non dispongono almeno di un indirizzo email, l'invio cartaceo diventa necessario.

3. Valutazione periodica di interoperabilità dei formati e procedure di riversamento

L'Amministrazione effettua una valutazione periodica dell'interoperabilità e dell'idoneità dei formati utilizzati per la produzione, gestione e conservazione dei documenti informatici, al fine di garantire nel tempo l'accessibilità, l'autenticità, l'integrità e la leggibilità degli stessi.

Cadenza della valutazione

La verifica viene svolta con cadenza annuale, e comunque ogniqualvolta si verifichino:

- modifiche normative o aggiornamenti delle Linee Guida AgID che incidano sui formati ammessi;
- aggiornamenti tecnologici che possano compromettere la leggibilità dei documenti;
- necessità di riversamento dovute a obsolescenza o dismissione di software/hardware.

Metodologia di valutazione

L'Ufficio competente effettua un'analisi dei formati correntemente in uso, confrontandoli con:

- l'elenco dei formati aperti e raccomandati da AgID;
- le indicazioni provenienti dal sistema di conservazione adottato;
- le best practice nazionali e internazionali in tema di gestione documentale digitale.

Per ciascun formato, viene redatta una scheda di valutazione contenente:

- diffusione e supporto tecnico del formato;
- presenza di alternative aperte e interoperabili;
- rischi di obsolescenza tecnologica;
- eventuali azioni correttive (es. riversamento in altro formato).

Procedure di riversamento

Qualora dall'analisi emerga la necessità di sostituire un formato non più idoneo, l'Amministrazione avvia una procedura di riversamento che prevede:

- individuazione del formato di destinazione tra quelli aperti e raccomandati;
- definizione delle modalità tecniche di conversione (riversamento sostitutivo o migratorio);
- verifica di corrispondenza tra il documento originario e quello riversato in termini di contenuto, metadati e leggibilità;
- aggiornamento dei metadati di gestione e conservazione, registrando l'operazione di riversamento.

Tracciabilità e responsabilità

Tutte le attività di valutazione e riversamento vengono documentate in appositi verbali, archiviati a norma.

La responsabilità della valutazione periodica ricade sul Coordinatore della gestione documentale, che si avvale della collaborazione del Responsabile della conservazione e delle strutture tecniche competenti.

4. Documenti soggetti a registrazione particolare. Determine

Le determine dirigenziali costituiscono atti amministrativi formali adottati dai Direttori, dai Dirigenti e dai Responsabili di Ufficio PRA, nell'ambito delle rispettive competenze. Esse rappresentano una tipologia documentale peculiare della gestione documentale dell'Amministrazione.

In conformità all'art. 53 del DPR 445/2000, le determine sono soggette a registrazione particolare, distinta dal protocollo generale. Tale registrazione assicura la tracciabilità, la reperibilità e l'ordinamento cronologico all'interno della AOO.

Registrazione e numerazione

Le determine sono registrate mediante un'applicazione dedicata, che verifica la completezza formale (ad esempio, la presenza della sottoscrizione digitale o autografa).

Durante la registrazione, il sistema attribuisce un numero progressivo univoco per ciascuna AOO, che costituisce l'identificativo ufficiale della determina. La numerazione è annuale e riparte dal n. 1 ogni 1° gennaio.

Metadati

Il Registro delle Determine gestisce i seguenti metadati:

- Struttura Emittente
- Struttura Competente
- Redattore Determina
- Firmatario Determina
- Interim (si/no)
- Oggetto
- Progressivo
- Data Emissione
- Tipologia Documentale (Decisione di Contrarre / Determina di Affidamento / Altra determina)
- Anno
- CIG
- CPV

Gestione delle autorizzazioni

L'applicazione di registrazione delle determine gestisce le abilitazioni in coerenza con le regole amministrative interne.

L'applicazione di registrazione delle determine gestisce le abilitazioni in coerenza con le regole amministrative interne.

Per gli Uffici PRA, che fanno capo alla rispettiva Direzione Territoriale, la registrazione è riservata alle determine sottoscritte dal Responsabile di Ufficio PRA o dal Direttore Territoriale.

Il Direttore Territoriale, quale titolare della direzione e coordinamento degli Uffici PRA, può adottare determine relative a tali Uffici sia in vece del Responsabile di Ufficio PRA (nell'esercizio delle funzioni sostitutive), sia per le materie che rientrano nella propria competenza diretta.

5. Descrizione del flusso di lavorazione dei documenti

Il presente capitolo descrive il flusso di lavorazione dei documenti ricevuti, spediti o interni, incluse le regole di registrazione per i documenti pervenuti secondo particolari modalità di trasmissione.

Generalità

Per descrivere i flussi di lavorazione dei documenti all'interno dell'AOO, si fa riferimento ai diagrammi di flusso riportati nelle pagine seguenti.

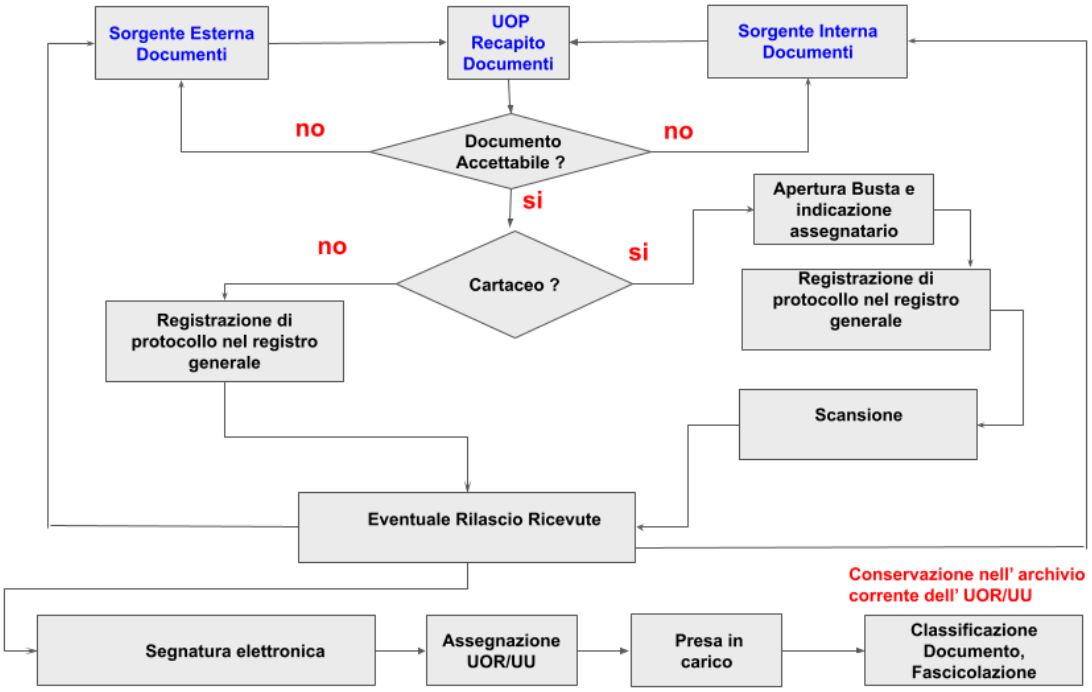
I diagrammi riguardano i documenti:

- ricevuti dalla AOO, sia dall'esterno sia dall'interno, quando devono essere ritrasmessi in modo formale all'interno dell'AOO;
- inviati dalla AOO, sia verso l'esterno sia verso altre strutture interne, in modo formale.

I flussi relativi alla gestione documentale all'interno dell'AOO sono rappresentati graficamente nel paragrafo seguente, con particolare attenzione ai casi di rilevanza giuridico-probatoria.

Per comunicazioni informali tra uffici si intende lo scambio di informazioni, con o senza documenti allegati, la cui conservazione è facoltativa. Tali comunicazioni avvengono tramite posta elettronica interna e non interessano il sistema di protocollo.

Flusso dei documenti ricevuti dall'AOO



Provenienza esterna dei documenti

I documenti trasmessi da soggetti esterni all'Amministrazione comprendono, oltre a quelli già descritti, i documenti informatici su supporto rimovibile.

I documenti che arrivano tramite servizio postale sono ritirati secondo le regole stabilite dal Responsabile dell'AOO.

Provenienza di documenti interni formali

Per sorgente interna si intende qualsiasi UOR (Unità Organizzativa Responsabile) della AOO che invia formalmente documenti tramite il responsabile del procedimento, per poi trasmetterli, nelle modalità appropriate, ad un altro UOR della stessa AOO, ad altra AOO dell'Ente o ad altra Amministrazione.

I documenti informatici devono rispettare gli standard descritti nei capitoli precedenti e vengono recapitati tramite posta elettronica, preferibilmente certificata.

Se gli allegati superano la capacità della casella di posta elettronica, è possibile trasferirli su supporto rimovibile o, preferibilmente, tramite condivisione informatica (es. GDrive).

Ricezione di documenti informatici sulla casella di posta istituzionale

Di norma, i documenti informatici vengono ricevuti tramite la casella di posta elettronica certificata (PEC) istituzionale.

La AOO, previa verifica della validità della firma digitale e della leggibilità del documento, procede alla registrazione di protocollo.

Se i messaggi non rispettano gli standard tecnici o non sono firmati digitalmente, ma devono essere conservati come documenti di riferimento, vengono inseriti nel sistema di gestione documentale nel formato originale, classificati come “posta elettronica”, e successivamente protocollati, smistati, assegnati e gestiti. In questo caso, il loro valore giuridico è assimilabile a quello di una missiva non sottoscritta: la rilevanza probatoria viene valutata dal Responsabile del Procedimento Amministrativo (RPA) nell’ambito del procedimento.

Gli addetti al protocollo controllano quotidianamente i messaggi ricevuti nelle caselle di posta istituzionale.

Anche se le PEC vengono scaricate automaticamente nel Protocollo Informatico, è necessario che gli addetti controllino manualmente la webmail almeno una volta al giorno, per garantire che eventuali messaggi non scaricati automaticamente siano comunque individuati e protocollati tempestivamente.

Ricezione di documenti informatici sulla casella di posta elettronica non istituzionale

Se un messaggio è ricevuto su una casella di posta non istituzionale o non destinata al servizio di protocollazione e se il messaggio è di interesse per l’Amministrazione, può essere:

- inoltrato alla casella di posta istituzionale (PEO o PEC, a seconda del tipo di casella di origine), oppure
- salvato in formato PDF e protocollato direttamente.

In ogni caso, sul messaggio vengono effettuati i controlli di validità, leggibilità e integrità già previsti per la ricezione ordinaria dei documenti.

Ricezione di documenti informatici su supporti rimovibili

I documenti informatici possono essere ricevuti anche per vie diverse dalla posta elettronica, ma l'uso di supporti rimovibili è consentito solo in casi assolutamente eccezionali, ad esempio su richiesta delle Forze dell'Ordine o quando non sia possibile utilizzare altri canali (mail, PEC o condivisione tramite Drive).

I supporti rimovibili devono essere verificati con scansione antivirus prima dell'acquisizione.

A causa della mancanza di standard tecnologici e formali, la AOO acquisisce e tratta solo i documenti che riesce a decodificare e interpretare con le tecnologie disponibili.

Una volta acquisito, il documento viene inserito nel flusso di lavorazione e sottoposto a tutti i controlli e adempimenti previsti.

Ricezione di documenti analogici a mezzo posta convenzionale

I documenti analogici ricevuti per posta o ritirati dal personale dagli uffici postali sono consegnati al Servizio Protocollo.

Le buste o i contenitori vengono inizialmente controllati per verificare indirizzo e destinatario.

Il documento cartaceo in entrata viene scansionato e protocollato con segnatura elettronica. L'originale cartaceo è conservato insieme alla stampa della prima pagina scansionata, con la segnatura elettronica riportata.

Documenti relativi a gare

La corrispondenza con indicazioni come "Gara d'appalto", "Offerta" e simili o comunque riconducibile a gare non viene aperta dal Servizio Protocollo.

Si appone la segnatura di protocollo su una fotocopia della busta, che viene ritagliata, incollata sulla busta stessa e consegnata a mano alla AOO competente, con acquisizione della firma per ricevuta.

Corrispondenza personale

Non deve essere aperta né protocollata.

Va consegnata al destinatario, che valuta se inoltrarla al Servizio Protocollo per la registrazione, solo se di interesse per l'Amministrazione.

Altri documenti

La corrispondenza non rientrante nelle categorie sopra indicate viene aperta e sottoposta ai controlli preliminari prima della registrazione.

Di norma, le buste vengono aperte il giorno lavorativo di arrivo e i documenti contestualmente protocollati. La busta viene allegata al documento per conservare i timbri postali.

Errata ricezione di documenti informatici

Se sulla casella di posta istituzionale dell'AOO (certificata o no) arrivano messaggi chiaramente destinati ad un'altra AOO, l'operatore di protocollo:

- protocolla in entrata il messaggio ricevuto.
- successivamente, protocolla in uscita il messaggio per:
    - inviarlo alla AOO competente, se identificabile;
    - oppure, se non è possibile, restituirlo al mittente con la dicitura: "Messaggio pervenuto per errore - non di competenza di questa AOO".

Errata ricezione di documenti analogici

Se al Servizio Protocollo arrivano documenti destinati ad altri soggetti, si applicano le seguenti procedure:

1. Busta indirizzata ad un'altra AOO dell'Ente:

- Se possibile, inviare direttamente alla AOO corretta.
- Se la busta viene aperta per errore:
    - il documento viene protocollato in entrata e in uscita;
    - nel campo oggetto si inserisce la nota: "documento pervenuto per errore";
    - la busta viene inviata alla AOO destinataria con la dicitura: "Pervenuta ed aperta per errore".

2. Busta indirizzata ad altra amministrazione:

- Se possibile, restituire tramite posta.

- Se la busta viene aperta per errore:
    - il documento viene protocollato in entrata e in uscita;
    - nel campo oggetto si inserisce la nota: “documento pervenuto per errore”;
    - la busta viene restituita al mittente con la dicitura: “Pervenuta ed aperta per errore”.

Attività di protocollazione dei documenti

Superati tutti i controlli precedenti, i documenti, informatici o analogici, sono protocollati.

Rilascio di ricevute attestanti la ricezione di documenti informatici

La ricezione dei documenti comporta l’invio automatico al mittente di due tipi di ricevute:

- Ricevuta del servizio di posta certificata (PEC)
- Ricevuta del sistema di protocollazione informatica

Tutte le ricevute sono generate automaticamente, senza necessità di intervento degli Addetti al Protocollo.

In presenza di sistemi interoperabili, il sistema provvede automaticamente all’invio di ulteriori messaggi automatici (Conferma di protocollazione, Notifica di eccezione, Annullo di protocollazione, Aggiornamento di protocollazione)

Rilascio di ricevute attestanti la ricezione di documenti analogici

Gli addetti del Servizio Protocollo non possono rilasciare ricevute per documenti non soggetti a regolare protocollazione.

Quando un documento analogico viene consegnato direttamente dal mittente o da persona incaricata al Servizio Protocollo, e viene richiesta una ricevuta cartacea attestante l’avvenuta consegna, il Servizio Protocollo è autorizzato a:

- fotocopiare la prima pagina del documento;
- apporre gli estremi della segnatura se contestualmente avviene anche la protocollazione.

In alternativa, è possibile apporre sulla copia il timbro dell’Amministrazione con data, ora di arrivo e sigla dell’operatore.

Classificazione, assegnazione e presa in carico dei documenti

Gli addetti del Servizio Protocollo classificano il documento secondo il titolario adottato dalla AOO e lo inviano al responsabile del procedimento di destinazione, che:

- verifica la congruità del documento in base alle proprie competenze;
- in caso di errore, lo restituisce al Servizio Protocollo di origine;
- in caso di verifica positiva, prende in carico il documento e, se necessario, lo smista internamente.

Archiviazione dei documenti informatici

I documenti informatici sono archiviati automaticamente mediante le applicazioni e gli spazi di archiviazione forniti dal Fornitore, in modalità non modificabile e a norma di legge, garantendo integrità e immodificabilità contestualmente alle operazioni di registrazione e segnatura di protocollo.

Conservazione delle rappresentazioni informatiche di documenti analogici

I documenti ricevuti su supporto analogico, dopo la registrazione di protocollo, vengono acquisiti in formato digitale mediante scansione, a cui segue l'apposizione della segnatura elettronica.

Secondo l'art. 4 del CAD, le copie informatiche dei documenti analogici, formate secondo l'art. 22, commi 1, 1-bis, 2 e 3, sostituiscono a tutti gli effetti l'originale cartaceo e sono valide per adempiere agli obblighi di conservazione previsti dalla legge, salvo quanto indicato al comma 5.

Dopo la riproduzione digitale e la conservazione a norma, l'originale analogico può essere:

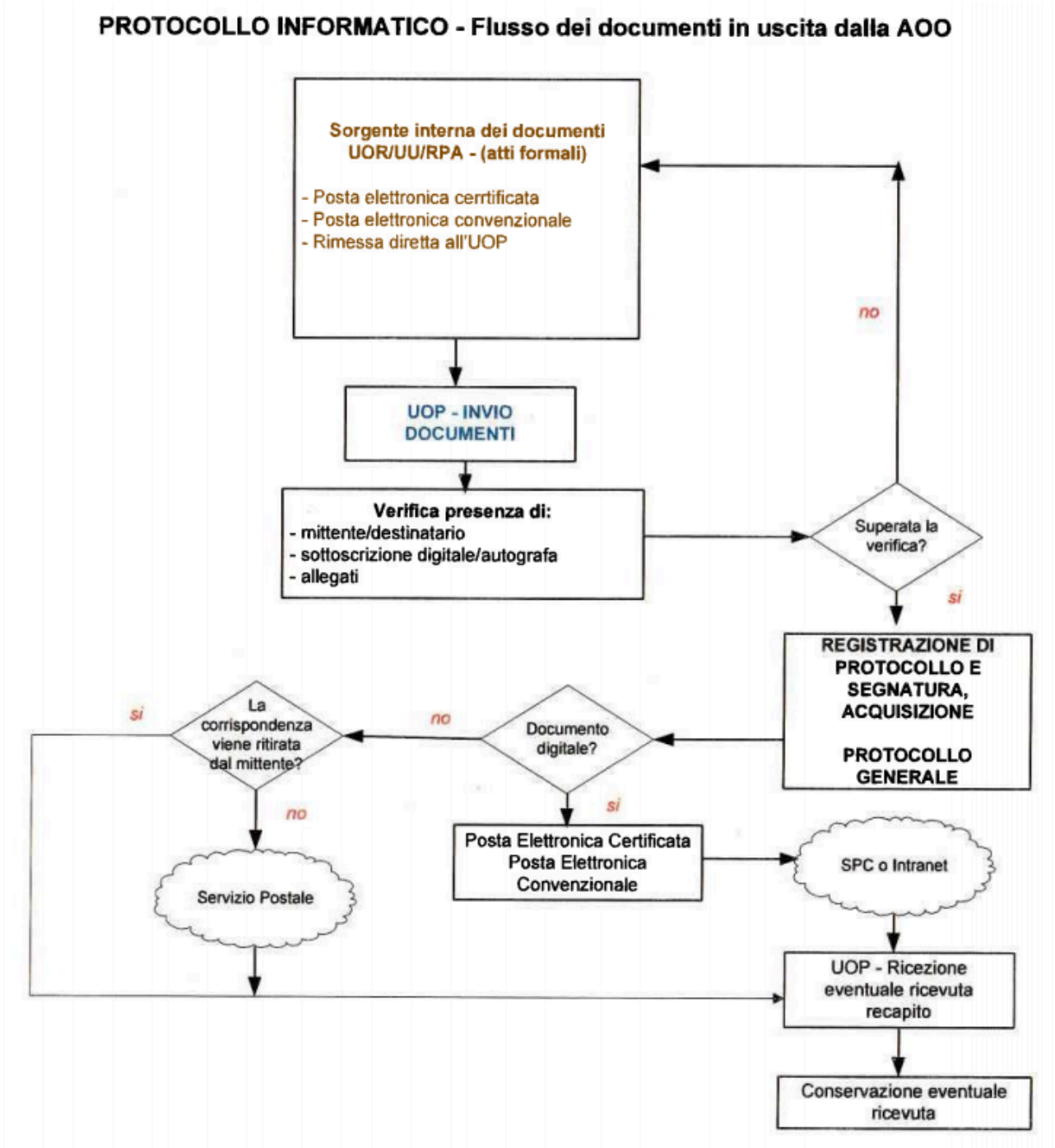
- distrutto, solo dopo il completamento della procedura di conservazione a norma;
- conservato agli atti.

Se l'originale cartaceo viene conservato, occorre allegare la prima pagina del documento scansionato, sulla quale è riportata la segnatura elettronica.

Conservazione dei documenti nell'archivio corrente

Durante l'ultima fase del flusso di lavorazione della corrispondenza in ingresso viene svolta l'attività di fascicolazione del documento secondo le procedure previste dalla AOO.

Flusso dei documenti inviati dalle AOO



Sorgente interna dei documenti

Nel grafico del paragrafo precedente, per sorgente interna dei documenti si intende qualunque UOR (Unità Organizzativa Responsabile) interna alla AOO che invia formalmente la propria corrispondenza tramite il RPA al Servizio Protocollo della AOO, per la successiva trasmissione, nelle modalità più opportune, ad altra amministrazione, altra AOO dell'Ente o ad altro ufficio della stessa AOO.

Per documenti in uscita si intendono quelli prodotti dal personale della AOO nell'esercizio delle proprie funzioni, aventi rilevanza giuridico-probatoria e destinati ad altra amministrazione, altra AOO dell'Ente o altro ufficio della stessa AOO.

Di norma i documenti sono informatici, formati secondo gli standard illustrati nei capitoli precedenti e trasmessi tramite posta elettronica, preferibilmente certificata.

Se gli allegati superano la capienza della casella di posta elettronica, si procede a un riversamento su supporto rimovibile da consegnare al destinatario o, preferibilmente, tramite strumenti di condivisione sicura (ad es. GDrive).

Solo per i cittadini privati che non siano Imprese o Professionisti e non dispongano di un indirizzo email, diventa necessario produrre il documento in formato analogico e inviarlo tramite posta cartacea.

Verifica formale dei documenti

Tutti i documenti originali da spedire, sia informatici sia analogici, sono inoltrati al Servizio Protocollo:

- documenti informatici – trasmessi nella casella di posta interna dedicata ai documenti da inviare.
- documenti analogici – consegnati in busta aperta per le operazioni di protocollazione e segnatura, eccetto quelli contenenti dati sensibili o giudiziari, che devono essere inviati in busta chiusa.

Il Servizio Protocollo verifica la conformità della documentazione allo standard formale previsto: correttezza di mittente e destinatario, sottoscrizione digitale o autografa, presenza di allegati dichiarati.

Se il documento è completo, viene registrato nel protocollo generale e gli viene apposta la segnatura secondo la tipologia. Se manca qualche elemento, il documento è restituito al proponente con le relative osservazioni.

Registrazione di protocollo e segnatura

Le operazioni di registrazione e di apposizione della segnatura dei documenti in partenza sono effettuate presso il Servizio Protocollo. Gli operatori non sono autorizzati a riservare numeri di protocollo per documenti non ancora disponibili.

La spedizione verso un'altra AOO, sia interna all'Ente sia di altra PA, deve avvenire esclusivamente tramite PEC in interoperabilità.

I documenti firmati digitalmente non devono mai essere stampati e devono essere protocollati con la segnatura elettronica.

Trasmissione di documenti informatici

Le modalità di composizione e scambio dei messaggi, il formato di codifica e le misure di sicurezza sono conformi all'allegato 6 delle Linee Guida.

I documenti informatici sono inviati all'indirizzo elettronico dichiarato dai destinatari, interno o esterno alla AOO, abilitato alla ricezione telematica.

Per la spedizione, l'AOO utilizza il servizio di Posta Elettronica Certificata (PEC). La PEC garantisce sicurezza del canale, certezza della data di spedizione e di consegna tramite le ricevute elettroniche.

Tutte le Imprese e i Professionisti sono obbligati ad avere un indirizzo PEC. Se non fornito, può essere reperito nell'archivio INI-PEC (https://www.inipec.gov.it), il registro ufficiale degli indirizzi PEC, permettendo l'invio tramite PEC invece della posta cartacea.

Gli addetti alla trasmissione telematica dei documenti non possono accedere al contenuto della corrispondenza, duplicarla o divulgarla a terzi, neppure in forma sintetica o parziale, salvo informazioni destinate alla pubblicazione o espressamente autorizzate dal mittente.

Trasmissione di documenti analogici a mezzo posta

I singoli cittadini privati diversi dalle Imprese e dai Professionisti non hanno ancora l'obbligo di dotarsi di un indirizzo PEC per cui, qualora non dispongano almeno di un indirizzo email, diventa inevitabile stampare la nota ed inviarla loro mediante posta cartacea.

Il Servizio Protocollo provvede direttamente a tutte le operazioni di spedizione della corrispondenza provvedendo anche all'affrancatura, alla ricezione e alla verifica delle distinte di raccomandate compilate dagli uffici.

Documenti in partenza per posta convenzionale con più destinatari

Se un documento deve essere inviato per posta convenzionale a più destinatari, l'UOR produce un unico documento originale e invia ai destinatari le copie di quell'originale.

Inserimento delle ricevute di trasmissione nel fascicolo

La minuta del documento analogico spedito ovvero le ricevute informatiche del sistema di posta certificata utilizzata per lo scambio dei documenti informatici, sono conservate all'interno del relativo fascicolo.

Modalità di correzione in caso di invio errato di documenti informatici

Se una comunicazione inviata tramite PEC risulta errata, occorre inviare una nuova PEC di errata corrige con un nuovo numero di protocollo.

Il protocollo della prima comunicazione non va annullato; nelle annotazioni va indicato che l'invio è errato e che è stato sostituito da una nuova comunicazione.

Deve essere creato un allegato interno che colleghi il vecchio protocollo a quello corretto, in modo che chi visualizza il protocollo errato possa aprire direttamente quello corretto dalla sezione "Allegati Interni".

Se il documento principale è corretto ma gli allegati sono errati, si reinvia la stessa comunicazione sostituendo solo gli allegati. In questo caso si mantiene lo stesso numero di protocollo e si indica nelle annotazioni che il nuovo invio sostituisce il precedente.

6. Regole di smistamento e assegnazione dei documenti ricevuti

Tutta la corrispondenza in arrivo viene esaminata e smistata dal Servizio Protocollo, previa consultazione del Dirigente/Responsabile dell'AOO o del Responsabile della gestione in caso di dubbi.

Lo smistamento consiste nell'inviare il documento protocollato e segnato all'UOR o ai dipendenti competenti, sulla base della classificazione del titolario dell'AOO.

Con l'assegnazione:

- si conferisce la responsabilità del procedimento amministrativo a un soggetto fisico;
- si trasmette il materiale documentario oggetto di lavorazione.

L'assegnazione può essere effettuata anche per sola conoscenza ad altri soggetti presenti nel titolario. Il Responsabile del procedimento può ulteriormente inviare l'assegnazione ad altri soggetti dell'UOR.

Il Responsabile del Procedimento prende in carico il documento assegnato. I termini per la definizione del procedimento decorrono:

- dalla data di protocollazione per i documenti cartacei o informatici;
- dalla data di accettazione del server per i documenti ricevuti via PEC.

Il sistema di gestione informatica registra tutti i passaggi, memorizzando per ciascuno l'identificativo dell'utente, la data e l'ora di esecuzione. Questa traccia definisce i tempi del procedimento e i relativi riflessi sulla responsabilità.

La visibilità dei documenti nel sistema di protocollo è definita dall'AOO tramite il funzionigramma, stabilendo chi può visualizzare o intervenire sui documenti.

Ogni dipendente deve aprire quotidianamente l'applicazione di protocollo per verificare eventuali assegnazioni.

Modifica delle assegnazioni

In caso di assegnazione errata, l'UOR o la persona destinataria del documento, se abilitata allo smistamento, lo invia all'UOR competente. Se non è abilitata, segnala l'errore al Servizio Protocollo che ha effettuato l'assegnazione, il quale provvede a riassegnare correttamente il documento.

Il sistema di protocollo informatico registra tutti i passaggi, memorizzando per ciascuno l'identificativo dell'utente, la data e l'ora dell'operazione.

Corrispondenza di particolare rilevanza

Se il documento ricevuto è di particolare rilevanza, va inviato preliminarmente in visione al Dirigente/Responsabile dell'AOO, che deciderà il workflow da seguire per la protocollazione e l'eventuale inoltro ad un'altra AOO.

7. Modalità di produzione e di conservazione delle registrazioni di protocollo informatico

Nell'ambito dell'AOO il registro di protocollo è unico e la numerazione progressiva delle registrazioni di protocollo è unica per tutta la AOO.

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

Il numero di protocollo individua un unico documento e, di conseguenza, ogni documento reca un solo numero di protocollo.

Non è consentita l'identificazione dei documenti mediante l'assegnazione manuale di numeri di protocollo che il sistema informatico ha già attribuito ad altri documenti, anche se questi documenti sono strettamente correlati tra loro.

Non è pertanto consentita in nessun caso la cosiddetta registrazione "a fronte", cioè l'utilizzo di un unico numero di protocollo per il documento in arrivo e per il documento in partenza.

La documentazione che non è stata registrata al protocollo viene considerata giuridicamente inesistente presso l'amministrazione.

Non è consentita la protocollazione di un documento già protocollato.

Il registro di protocollo è un atto pubblico originario che fa fede della tempestività e dell'effettivo ricevimento e spedizione di un documento, indipendentemente dalla regolarità del documento stesso, ed è idoneo a produrre effetti giuridici.

Il registro di protocollo è soggetto alle forme di pubblicità e di tutela di situazioni giuridicamente rilevanti previste dalla normativa vigente.

Registro giornaliero di protocollo

Il registro giornaliero di protocollo viene prodotto in maniera automatica dalla procedura di Protocollo Informatico e riversato automaticamente, entro la giornata lavorativa successiva, al sistema di conservazione a norma, tenuto dal Fornitore.

Registrazione di protocollo

Su ogni documento ricevuto o spedito dalla AOO è effettuata una registrazione di protocollo con il sistema di gestione del protocollo informatico, consistente nella memorizzazione dei dati obbligatori.

Tale registrazione è eseguita in un'unica operazione, senza possibilità per l'operatore di inserire le informazioni in più fasi successive.

Ciascuna registrazione di protocollo contiene i dati obbligatori secondo la normativa vigente.

Elementi aggiuntivi delle registrazioni di protocollo

Il Coordinatore della Gestione documentale, con proprio provvedimento e al fine di migliorare l'efficacia e l'efficienza dell'azione amministrativa, può decidere di fare aggiungere alla maschera di protocollo dei campi specifici.

Segnatura di protocollo dei documenti

L'operazione di segnatura di protocollo è effettuata contemporaneamente all'operazione di registrazione di protocollo.

La segnatura di protocollo è l'apposizione o l'associazione all'originale del documento, in forma permanente non modificabile, delle informazioni riguardanti il documento stesso.

Essa consente di individuare ciascun documento in modo inequivocabile.

Documenti informatici

I dati della segnatura di protocollo di un documento informatico sono contenuti, un'unica volta nell'ambito dello stesso messaggio, in un file conforme alle specifiche *dell'Extensible Markup Language* (XML).

Le informazioni incluse nella segnatura sono quelle di seguito elencate:

- codice identificativo dell'amministrazione;
- codice identificativo dell'area organizzativa omogenea;
- data e numero di protocollo del documento.

La struttura ed i contenuti del file di segnatura di protocollo di un documento informatico sono conformi alle disposizioni tecniche vigenti.

Documenti analogici

In caso di documento cartaceo in entrata, il medesimo viene scansionato e protocollato mediante segnatura elettronica.

L'originale cartaceo è conservato con le modalità usuali insieme alla stampa della prima pagina del documento scansionato, in cui è riportata la segnatura elettronica.

I documenti in uscita sono formati digitalmente e sottoscritti con firma digitale e inviati al destinatario mediante mail o PEC.

Nel solo caso di documenti da inviare a privati cittadini che non dispongano di casella mail o di posta certificata, il documento firmato digitalmente viene stampato ed inoltrato mediante posta cartacea.

Poiché, una volta stampata, la firma digitale perde ogni valore e di conseguenza il documento stampato ha il valore di una semplice copia, per attribuire validità a tale copia, secondo la normativa vigente, il protocollo viene gestito secondo una delle due modalità alternative:

1 - apposizione sulla stampa della seguente dicitura: "*Il documento informatico, da cui la presente copia è tratta, è stato predisposto come documento nativo digitale ed è disponibile presso l'amministrazione (art. 3-bis comma 4-ter del D.Lgs n. 82/2005)*";

oppure

2 - apposizione sulla stampa della seguente dicitura: "*Si attesta che la presente copia analogica è conforme all'originale digitale (art. 23 comma 1 del D.Lgs n. 82/2005)*". La dicitura è seguita dalla firma apposta manualmente.

Annullamento delle registrazioni di protocollo

La necessità di modificare - anche un solo campo tra quelli obbligatori della registrazione di protocollo, registrati in forma non modificabile - per correggere errori verificatisi in sede di immissione manuale di dati o attraverso l'interoperabilità dei sistemi di protocollo mittente e destinatario, comporta l'obbligo di annullare l'intera registrazione di protocollo.

Le informazioni relative alla registrazione di protocollo annullata rimangono memorizzate nel registro informatico del protocollo per essere sottoposte alle elaborazioni previste dalla procedura, ivi comprese le visualizzazioni e le stampe, nonché la data, l'ora e l'autore dell'annullamento e gli estremi dell'autorizzazione all'annullamento del protocollo rilasciata dal Responsabile della gestione documentale.

In tale ipotesi la procedura riporta la dicitura "annullato" in posizione visibile e tale, da consentire la lettura di tutte le informazioni originarie. Il sistema registra l'avvenuta rettifica, la data ed il soggetto che è intervenuto.

Gli operatori di protocollo possono annullare e solo il Responsabile della gestione documentale può confermare l'annullamento;

Circolari e disposizioni generali

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

Fatture passive

Le fatture passive provenienti dallo SDI vengono protocollate in automatico.

Documenti non firmati

L'operatore di protocollo registra per ogni documento la data, la forma e la provenienza.

Le lettere anonime devono comunque essere protocollate, indicando "Mittente sconosciuto o anonimo" e "Documento non sottoscritto".

Anche le lettere con mittente ma prive di firma vengono protocollate e segnalate come tali.

Sarà poi l'UOR competente, e in particolare il RPA, a valutare se il documento privo di firma debba essere considerato valido e quindi trattato come tale.

Tempestività delle registrazioni

Le registrazioni di protocollo dei documenti pervenuti presso l'amministrazione destinataria sono effettuate nella giornata di arrivo e comunque non oltre le 48 ore dal ricevimento di detti documenti.

Qualora non sia possibile effettuare la registrazione di protocollo nei tempi ordinari, si provvede prioritariamente a protocollare i documenti di particolare rilevanza, previa autorizzazione motivata del Responsabile della gestione documentale. Il provvedimento deve formalmente autorizzare l'addetto al protocollo a differire temporaneamente le operazioni relative agli altri documenti, che dovranno comunque essere registrati non appena possibile.

Corrispondenza personale o riservata

La corrispondenza è consegnata in busta chiusa al destinatario, il quale, dopo averne preso visione, se reputa che i documenti ricevuti devono essere comunque protocollati provvede a trasmetterli al più vicino ufficio abilitato alla registrazione di protocollo dei documenti in arrivo.

Integrazioni documentarie

L'addetto al protocollo non è tenuto a controllare la completezza formale e sostanziale della documentazione pervenuta, ma è tenuto a registrare in ogni caso il documento ed eventuali allegati.

Tale verifica spetta al Responsabile del Procedimento Amministrativo che, qualora reputi necessario acquisire documenti che integrino quelli già pervenuti, provvede a richiederli al mittente indicando con precisione l'indirizzo al quale inviarli e specificando che la mancata integrazione della documentazione pervenuta comporta l'interruzione o la sospensione del procedimento.

I documenti pervenuti ad integrazione di quelli già disponibili sono protocollati e inseriti nel fascicolo relativo.

8. Servizio di Conservazione elettronica dei documenti

Il servizio di Conservazione elettronica assicura il trasferimento su supporto informatico, in forma immodificabile, anche dei documenti gestiti dal protocollo informatico e del registro di protocollo.

A questo servizio è preposto il Responsabile per la Conservazione, cui spettano compiti e responsabilità previsti dall'art. 44 del Codice e dalle Linee Guida sulla conservazione. Il ruolo di pubblico ufficiale per la chiusura dei pacchetti di conservazione è svolto dal Responsabile stesso o da soggetti da lui formalmente delegati.

Il legale rappresentante dell'Ente, con apposito atto, ha affidato la gestione informatica del processo di conservazione al Fornitore, incaricandolo formalmente delle attività e vietandogli la comunicazione o la diffusione, anche accidentale, dei dati personali eventualmente presenti negli archivi.

Il Responsabile della Conservazione, secondo norma, può delegare parte delle proprie attività a uno o più dipendenti dei Sistemi Informativi che, per competenza ed esperienza, ne garantiscono la corretta esecuzione.

Archiviazione dei documenti analogici

Il Coordinatore della gestione documentale, valutati i costi e i benefici, può proporre l'operazione di conservazione a norma dei documenti analogici su supporti di memorizzazione sostitutivi dell'analogico in conformità alle disposizioni vigenti.

In questi casi, il Responsabile della gestione documentale è autorizzato a sottoscrivere digitalmente la dichiarazione di conformità all'originale analogico, da allegare alla copia informatica, come previsto dall'art. 22, comma 2, del CAD. L'archiviazione seguirà le modalità indicate nel successivo paragrafo.

Resta fermo quanto previsto dall'art. 22, comma 3, del CAD: le copie per immagine su supporto informatico di documenti originariamente analogici hanno la stessa efficacia probatoria degli originali, salvo che la conformità non venga espressamente disconosciuta.

In caso di necessità di dematerializzare grandi quantità di documenti analogici, si potranno utilizzare strumenti automatizzati, anche parziali, se consentito dalla normativa e dalle tecnologie disponibili, previa valutazione costi/benefici da parte del Coordinatore della gestione documentale.

Archiviazione dei documenti informatici

Il processo di conservazione a norma dei documenti informatici è svolto dal sistema di conservazione, gestito dal Fornitore accreditato. Esso garantisce la memorizzazione su supporti non modificabili e, in fase di chiusura dei pacchetti, l'apposizione automatica della firma digitale e del riferimento temporale, attestando l'immodificabilità e l'integrità dei documenti.

Il processo di riversamento dei documenti informatici avviene mediante memorizzazione su nuovi supporti e si conclude con la generazione, sempre da parte del sistema, di evidenze informatiche contenenti le impronte dei documenti, corredate da firma digitale e riferimento temporale.

Il Responsabile della conservazione vigila sul corretto svolgimento dei processi, fermo restando che le operazioni tecniche sono eseguite automaticamente dal sistema.

Solo nei casi previsti dalla normativa (ad esempio nel riversamento sostitutivo di documenti firmati digitalmente) è richiesta l'apposizione della firma digitale e del riferimento temporale da parte di un pubblico ufficiale per attestare la conformità rispetto al documento originario.

9. Elenco dei documenti esclusi dalla protocollazione

Sono esclusi dalla registrazione di protocollo tutti i documenti di cui all'art. 53 comma 5 del Testo unico:

- Le seguenti tipologie di documenti non sono oggetto di registrazione obbligatoria:
- Gazzette ufficiali.
- Bollettini ufficiali e notiziari della pubblica amministrazione.
- Note di ricezione delle circolari e altre disposizioni.
- Materiali statistici.
- Atti preparatori interni.
- Giornali, riviste, libri, materiali pubblicitari.
- Inviti a manifestazioni.
- Tutti i documenti già soggetti a registrazione particolare.

Non devono essere protocollati i certificati medici telematici provenienti dall'INPS e disponibili sulla piattaforma dell'Istituto.

Per altri certificati medici, acquisiti nei casi previsti dalla legge o dai CCNL, si procede al protocollo scansionando l'originale cartaceo e restituendolo all'interessato, così da evitare l'archiviazione fisica.

La corrispondenza contrassegnata come riservata, personale o simili non deve essere aperta e va consegnata direttamente al destinatario.

Se il destinatario accerta che il contenuto riguarda l'attività dell'AOO, deve restituire il documento al Servizio di Protocollo per la registrazione.

10. Sistema di classificazione

Piano di organizzazione delle aggregazioni documentali

L'Amministrazione ha adottato il Piano di organizzazione delle aggregazioni documentali (POAD), redatto ai sensi delle Linee guida AgID sulla formazione, gestione e conservazione del documento informatico.

Il POAD descrive le tipologie di aggregazioni documentali utilizzate dall'Ente, le relative regole di formazione, gestione e tenuta, nonché i collegamenti con la classificazione, la fascicolazione e la conservazione.

Il Piano di organizzazione delle aggregazioni documentali è descritto in un allegato del Manuale.

Titolario

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

Il titolario è uno strumento suscettibile di aggiornamento.

Il titolario non è retroattivo: non si applica, cioè, ai documenti protocollati prima della sua introduzione.

Viene garantita la storicizzazione delle variazioni di titolario e la possibilità di ricostruire le diverse voci nel tempo mantenendo stabili i legami dei fascicoli e dei documenti con la struttura del titolario vigente al momento della produzione degli stessi.

Il titolario è riportato in allegato al Manuale.

11. Fascicolazione archivistica

La fascicolazione archivistica è il processo mediante il quale i documenti prodotti o ricevuti dall'Amministrazione vengono raggruppati in fascicoli in base alla loro funzione, oggetto o soggetto di riferimento. Questo consente di organizzare i documenti in modo coerente e facilmente reperibile, supportando la tracciabilità dei procedimenti amministrativi e garantendo una gestione ordinata e sicura delle informazioni.

La fascicolazione è parte integrante del sistema di protocollo informatico e del ciclo di vita dei documenti, dalla loro produzione o acquisizione fino alla conservazione e archiviazione finale. I fascicoli sono aperti, gestiti e chiusi in coerenza con il piano di classificazione dell'Ente, che assicura il corretto inquadramento delle funzioni e delle attività.

Piano di fascicolazione

Il Piano di fascicolazione definisce le modalità di organizzazione dei documenti nei fascicoli, stabilendo i criteri di apertura, gestione, chiusura e denominazione degli stessi, in coerenza con il piano di classificazione.

Esso assicura uniformità e tracciabilità nella gestione dei fascicoli, garantendo la corretta ricostruzione dei procedimenti e degli affari trattati.

Il Piano di fascicolazione costituisce parte integrante del sistema di gestione documentale ed è allegato al presente Manuale. Le regole di fascicolazione sono inoltre richiamate nel Piano di organizzazione delle aggregazioni documentali (POAD), di cui il Piano di fascicolazione rappresenta componente specifica.

Tipi di Fascicolo

I fascicoli possono essere distinti in cinque categorie principali:

- **Affare**
  Raccoglie documenti relativi a competenze non proceduralizzate e che non richiedono l'adozione di un provvedimento finale.
  Questi fascicoli hanno una durata limitata e sono chiusi una volta conclusa l'attività.

- **Attività**
  Contiene documenti legati a competenze proceduralizzate, senza prevedere

provvedimenti finali. Si tratta di attività amministrative ripetitive o adempimenti periodici.

- **Procedimento Amministrativo**
  Include documenti collegati tra loro e destinati a concludersi con un provvedimento amministrativo. Permette di seguire l'intero iter della pratica, dalle fasi preliminari all'atto finale.

- **Persona fisica**
  Comprende fascicoli relativi a una stessa persona fisica, contenenti più procedimenti o affari distinti ma collegati da un vincolo archivistico interno. La chiusura del fascicolo coincide con la conclusione del rapporto giuridico con l'Amministrazione.

- **Persona giuridica**
  Raccoglie i fascicoli relativi a una persona giuridica, secondo modalità analoghe a quelle dei fascicoli di persona fisica.

Aggregazioni Documentali

I fascicoli possono essere organizzati in aggregazioni più ampie:

- **Fascicolo singolo**: raggruppa documenti relativi a un'attività o procedimento specifico.

- **Serie documentale**: accorpa documenti simili per tipologia o funzione, come contratti, determinazioni o circolari.

- **Serie di fascicoli**: insieme di fascicoli raggruppati per finalità archivistiche comuni.
  Esempio: serie dei fascicoli dei dipendenti, serie dei fascicoli delle imprese o fornitori.

Le serie documentali e le serie di fascicoli contribuiscono a mantenere coerenza e facilità di consultazione all'interno dell'archivio. La descrizione completa delle aggregazioni documentali è riportata nel POAD.

Visibilità e Responsabilità

La visibilità dei fascicoli è definita dalla AOO, in base al funzionigramma, e può essere di tre tipi:

- **Completa**: accessibile a tutti gli utenti del sistema.
- **Limitata**: visibile solo agli utenti e uffici selezionati.
- **Riservata**: visibilità limitata a utenti e uffici selezionati, con indicazione di contenuto sensibile.

Il Responsabile del fascicolo (di norma il responsabile del procedimento per i fascicoli amministrativi) ha automaticamente accesso al fascicolo e ne garantisce la corretta gestione. L'assegnazione del fascicolo a un ufficio o a un operatore definisce anche la responsabilità sul procedimento correlato.

Fasi dei Procedimenti Amministrativi

Nei fascicoli relativi a procedimenti amministrativi, possono essere rilevate le seguenti sottofasi:

- **Preparatoria** – Raccolta e predisposizione dei presupposti necessari per l'adozione dell'atto amministrativo.
- **Istruttoria** – Acquisizione e valutazione degli elementi rilevanti per la decisione finale.
- **Consultiva** – Eventuale sottofase dell'istruttoria in cui si richiede il parere di uffici interni o esperti per questioni complesse.
- **Decisoria/Deliberativa** – Definizione ed emanazione del provvedimento finale. L'atto può essere considerato completo ma non sempre ancora efficace.
- **Integrazione dell'efficacia** – Eventuali adempimenti successivi, come controlli aggiuntivi o comunicazioni al destinatario prima che l'atto diventi pienamente efficace.

- *Sottofase di controllo*: verifica della correttezza dell'atto.

- *Sottofase di comunicazione*: trasmissione dell'atto al destinatario finale.

La registrazione di queste fasi nel sistema consente di documentare lo stato di avanzamento del procedimento e garantisce la tracciabilità amministrativa. I fascicoli devono essere chiusi tempestivamente al termine del procedimento o dell'attività, per consentirne il corretto versamento in conservazione.

12. Selezione e scarto dei documenti

Operazione di scarto

Nell'ambito della sezione di deposito dell'archivio viene effettuata la selezione della documentazione da conservare perennemente e lo scarto degli atti che l'amministrazione non ritiene più opportuno conservare ulteriormente, allo scopo di conservare e garantire il corretto mantenimento e la funzionalità dell'archivio, nell'impossibilità pratica di conservare indiscriminatamente ogni documento.

Un documento si definisce scartabile quando ha perso totalmente la sua rilevanza amministrativa e non ha assunto alcuna rilevanza storica.

La procedura per lo scarto dei documenti e i tempi minimi di conservazione per ciascuna tipologia documentale sono indicati nel Piano di conservazione, allegato al Manuale.

13. Rilascio delle abilitazioni di accesso alle informazioni documentali

I diversi livelli di autorizzazione, descritti nel funzionigramma, sono assegnati agli utenti dal Responsabile della gestione documentale.

Le abilitazioni all'utilizzo delle funzionalità del sistema di gestione informatica del protocollo e dei documenti, ovvero l'identificazione del personale abilitato allo svolgimento delle operazioni di registrazione di protocollo, organizzazione e tenuta dei documenti all'interno della AOO sono costantemente aggiornate a cura del Responsabile della gestione documentale.

14. Piano di sicurezza dei documenti informatici

Il Piano di Sicurezza ha lo scopo di garantire la protezione, l'affidabilità e la resilienza del sistema di gestione informatica dei documenti dell'Amministrazione.

È redatto in conformità alle Linee Guida AgID 2021 sulla formazione, gestione e conservazione dei documenti informatici e alla Circolare AgID n. 2/2017 – Misure minime di sicurezza ICT per le PA, adottando i principi e le misure previste come riferimento per la sicurezza.

Il Piano è elaborato in coerenza con le linee strategiche del Piano Triennale per l'Informatica nella Pubblica Amministrazione, per garantire un approccio unitario alla sicurezza informatica, alla continuità operativa e alla protezione del patrimonio informativo dell'Ente.

Il Piano di Sicurezza è riportato in Allegato al presente Manuale.

15. Registro di emergenza

Qualora non fosse disponibile fruire del Servizio di protocollo, per un'interruzione accidentale o programmata, l'AOO è tenuta ad effettuare le registrazioni di protocollo sul registro di emergenza. In allegato al manuale viene riportato un modello di riferimento.

Per l'apertura del registro di emergenza concorrono i diversi soggetti:

- il Responsabile della gestione documentale autorizza e supervisiona l'apertura del registro di emergenza, l'uso e la chiusura;
- il Servizio Protocollo esegue le operazioni;
- il Coordinatore della Gestione documentale viene avvisato e informa sui tempi di ripristino.

I documenti annotati nel registro di emergenza e trasferiti nel protocollo generale recano, pertanto, due numeri: il progressivo del protocollo di emergenza e quello del protocollo generale.

La data in cui è stata effettuata la protocollazione sul registro di emergenza è quella cui si fa riferimento per la decorrenza dei termini del procedimento amministrativo.

In tal modo è assicurata la corretta sequenza dei documenti che fanno parte di un determinato procedimento amministrativo.

15.1 Modalità di apertura del Registro di emergenza

Il Responsabile della gestione documentale assicura che, ogni qualvolta per cause tecniche non sia possibile utilizzare la procedura informatica, le operazioni di protocollo siano svolte manualmente sul registro di emergenza cartaceo.

Prima di avviare l'attività di protocollo sul registro di emergenza, il Responsabile della gestione documentale, avvisa, anche con sola mail, il Coordinatore della Gestione documentale, e imposta e verifica la correttezza della data e dell'ora relativa al registro di emergenza su cui occorre operare.

Sul registro di emergenza sono riportate:

a) Causa, data ed ora d'inizio dell'interruzione,

b) Data ed ora del ripristino della funzionalità del sistema,

c) Estremi del provvedimento di autorizzazione all'uso del Registro di Emergenza

Qualora l'impossibilità di utilizzare la procedura informatica si prolunghi oltre le ventiquattro ore, per cause di eccezionale gravità, il responsabile per la tenuta del protocollo autorizza l'uso del registro di emergenza per periodi successivi di non più di una settimana.

15.2 Modalità di utilizzo del Registro di emergenza

La sequenza numerica utilizzata su un registro di emergenza, anche a seguito di successive interruzioni, garantisce comunque l'identificazione univoca dei documenti registrati nell'ambito del sistema documentario della AOO.

Durante il periodo di interruzione del servizio di protocollo informatico generale, il Coordinatore della Gestione documentale (o persona da lui delegata) provvede a tenere informato il Responsabile della gestione documentale sui tempi di ripristino del servizio.

15.3 Modalità di chiusura e recupero del Registro di emergenza

È compito del Responsabile della gestione documentale verificare la chiusura del registro di emergenza.

È compito del Responsabile della gestione documentale, o suoi delegati, riportare dal registro di emergenza al sistema di protocollo generale le protocollazioni relative ai documenti protocollati fuori linea, non appena possibile successivamente al ripristino delle funzionalità del sistema.

Nella fase di ripristino, al documento è attribuito un numero di protocollo del sistema informatico ordinario, correlato attraverso un'apposita nota , al numero utilizzato in emergenza.

Ai fini giuridici ed amministrativi vale la data di registrazione riportata nel registro di emergenza; la data assegnata dal protocollo informatico indica quando il sistema ha recepito il documento.

Il Responsabile della gestione documentale provvede alla chiusura del registro di emergenza annotando sullo stesso il numero delle registrazioni effettuate e la data e ora di chiusura.

16. Approvazione e aggiornamento del Manuale, disposizioni transitorie e finali

16.1 Modalità di approvazione e aggiornamento del manuale

Il presente “Manuale di gestione” è adottato con provvedimento formale , secondo quanto previsto dalle Linee Guida sulla formazione, gestione e conservazione dei documenti informatici dell’AGID.

Il presente Manuale potrà essere aggiornato a seguito di:

- nuova normativa sopravvenuta;
- introduzione di nuove pratiche tendenti a migliorare l’azione amministrativa in termini di efficacia, efficienza e trasparenza;
- inadeguatezza delle procedure rilevate nello svolgimento delle attività correnti;

16.2 Pubblicità del presente manuale

Il Manuale è destinato alla più ampia diffusione interna ed esterna, in quanto fornisce le indicazioni per eseguire correttamente le operazioni di formazione, registrazione, classificazione, fascicolazione e archiviazione dei documenti; pertanto si rivolge non solo agli operatori di protocollo ma, in generale, a tutti i dipendenti e ai soggetti esterni che si relazionano con l’ACI.

Il Manuale, a tal fine, è adottato e pubblicato sul proprio sito istituzionale. La pubblicazione è realizzata in una parte chiaramente identificabile dell’area “Amministrazione trasparente” prevista dall’art. 9 del d.lgs. 33/2013.

ALLEGATI

Fac-simile della nomina di Responsabile o Vicario della Gestione documentale

DIREZIONE / UNITÀ TERRITORIALE

Sig. xxxxxxx

OGGETTO: Incarico di "Responsabile/Vicario della Gestione documentale" (Cap. 3, par. 3.1.2 lett. b, delle Linee Guida sulla formazione, gestione e conservazione dei documenti informatici)

L'ACI, secondo a quanto disposto dal Capo IV (S*istema di gestione informatica dei documenti*) del DPR n. 445/2000 (Testo Unico in materia di documentazione amministrativa) e dalle "Linee Guida sulla formazione, gestione e conservazione dei documenti informatici di maggio 2021", ha individuato questo Ufficio/Servizi/Direzione come Area Organizzativa Omogenea (AOO) dell'Ente.

All'interno della presente AOO, secondo l'art. 61 del citato DPR, è istituito un "Servizio" per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi, al quale deve essere preposta una figura professionale che possieda idonei requisiti per l'espletamento delle attività di interesse.

In considerazione di quanto sopra indicato, Le conferisco l'incarico di Responsabile della Gestione documentale presso la predetta AOO, ai sensi e per gli effetti del citato art. 61, commi 2 e 3, del DPR n. 445/2000 e Cap. 3, par. 3.1.2 lett. b, delle Linee Guida.

Nell'ambito dell'incarico conferitoLe, Ella è altresì:

- incaricata di garantire che le caselle di posta elettronica certificata, associate al protocollo informatico della presente AOO, siano opportunamente presidiate;

- autorizzata a certificare la conformità all'originale delle copie informatiche per immagine su supporto informatico di documenti analogici anche unici, secondo le modalità di cui all'art. 22, comma 2, del decreto legislativo 7 marzo 2005, n. 82 e s.m.i.

- responsabile della tenuta degli archivi documentali analogici.

Nello svolgimento del presente incarico Ella garantirà il rispetto delle richiamate disposizioni, anche avvalendosi del Referente per i Sistemi Informativi sul territorio, nella sua qualità di esperto in materia e di auditor per la verifica dei sistemi di sicurezza adottati nella presente AOO.

Si prega di restituire copia della presente firmata per accettazione.

IL DIRETTORE TERRITORIALE

All. 2

Registro di emergenza di Protocollo

Data **AOO**

Motivazione dell'interruzione del servizio:
Data ed ora d'inizio dell'interruzione:
Data ed ora del ripristino della funzionalità del sistema:
Estremi del provvedimento di autorizzazione all'uso del Registro di Emergenza:

Protocollo	E/U	Mittente/Destinatario	Oggetto del Documento

Firma del Responsabile

All. 3 Titolario

TITOLO	CLASSE	SOTTOCLASSE
TASSE AUTOMOBILISTICHE	CIRCOLARI	
TASSE AUTOMOBILISTICHE	COMUNICAZIONI CON DELEGAZIONI	
TASSE AUTOMOBILISTICHE	CONTENZIOSO	
TASSE AUTOMOBILISTICHE	ESAZIONI	
TASSE AUTOMOBILISTICHE	ESENZIONI CONCESSIONARI	
TASSE AUTOMOBILISTICHE	ESENZIONI DISABILI	
TASSE AUTOMOBILISTICHE	ESENZIONI VEICOLI STORICI	
TASSE AUTOMOBILISTICHE	SERVIZI ESENTI	
TASSE AUTOMOBILISTICHE	GESTIONE CARTELLE ESATTORIALI	
TASSE AUTOMOBILISTICHE	INSOLUTI TASSE	
TASSE AUTOMOBILISTICHE	RADIAZIONI D'UFFICIO	
TASSE AUTOMOBILISTICHE	RETTIFICHE RUOLO REGIONALE	
TASSE AUTOMOBILISTICHE	RICHIESTA ATTI	
TASSE AUTOMOBILISTICHE	RIEPILOGHI DELEGAZIONI	
TASSE AUTOMOBILISTICHE	RIMBORSI	
TASSE AUTOMOBILISTICHE	CONVENZTASSE COMUNICAZIONI CONTRIBUENTI	
TASSE AUTOMOBILISTICHE	CONVENZTASSE COMUNICAZIONI REGIONALI	
TASSE AUTOMOBILISTICHE	COMUNICAZIONI CON AGENZIE	
TASSE AUTOMOBILISTICHE	SERVIZI ESENTI BOLLO	
TASSE AUTOMOBILISTICHE	RIEPILOGHI AGENZIE	
PUBBLICO REGISTRO AUTOMOBILISTICO	ATTI FALSIFICATI	
PUBBLICO REGISTRO AUTOMOBILISTICO	CIRCOLARI E MESSAGGI PRA	
PUBBLICO REGISTRO AUTOMOBILISTICO	COMUNICAZIONI	

PUBBLICO REGISTRO AUTOMOBILISTICO	COMUNICAZIONI ATTI	
PUBBLICO REGISTRO AUTOMOBILISTICO	COMUNICAZIONI DTT	
PUBBLICO REGISTRO AUTOMOBILISTICO	COMUNICAZIONI STUDI CONSULENZA DELEGAZIONI	
PUBBLICO REGISTRO AUTOMOBILISTICO	CONCESSIONARI	
PUBBLICO REGISTRO AUTOMOBILISTICO	DEMOLITORI AUTORIZZATI	
PUBBLICO REGISTRO AUTOMOBILISTICO	DICHIARAZIONI SOSTITUTIVE	
PUBBLICO REGISTRO AUTOMOBILISTICO	GESTIONE ARCHIVIO CARTACEO	
PUBBLICO REGISTRO AUTOMOBILISTICO	IMPOSTA PROVINCIALE	
PUBBLICO REGISTRO AUTOMOBILISTICO	INSOLUTI AGSTA	
PUBBLICO REGISTRO AUTOMOBILISTICO	NORMATIVA PRA	
PUBBLICO REGISTRO AUTOMOBILISTICO	PRIVATI	
PUBBLICO REGISTRO AUTOMOBILISTICO	RICHIESTA RETTIFICHE	
PUBBLICO REGISTRO AUTOMOBILISTICO	RICHIESTA INFORMAZIONI FORMALITA'	
PUBBLICO REGISTRO AUTOMOBILISTICO	SPORTELLO TELEMATICO	
PUBBLICO REGISTRO AUTOMOBILISTICO	CERTIFICATO CRONOLOGICO DA VOLUME CARTACEO E MISTO	
PUBBLICO REGISTRO AUTOMOBILISTICO	CERTIFICATO DELLO STATO GIURIDICO ATTUALE	
PUBBLICO REGISTRO AUTOMOBILISTICO	RICHIESTA COPIA O VISURA ATTI, NOTE E DOCUMENTI	
PUBBLICO REGISTRO AUTOMOBILISTICO	FORMALITÀ	
PUBBLICO REGISTRO AUTOMOBILISTICO	VISURA A VOLUME CARTACEO	
PUBBLICO REGISTRO	VISURA NOMINATIVA	

AUTOMOBILISTICO		
PUBBLICO REGISTRO AUTOMOBILISTICO	Fermi amministrativi	
PUBBLICO REGISTRO AUTOMOBILISTICO	Provvedimenti giudiziari e amministrativi	
PUBBLICO REGISTRO AUTOMOBILISTICO	Richiesta rettifiche	
PUBBLICO REGISTRO AUTOMOBILISTICO	Sequestro fascicoli originali	
PUBBLICO REGISTRO AUTOMOBILISTICO	VERIFICA AUTOCERTIFICAZIONI DA PARTE DI ALTRE PPAA	
PUBBLICO REGISTRO AUTOMOBILISTICO	MONITORAGGI	
GESTIONE RISORSE UMANE	COMUNICAZIONI CON LA DIREZIONE RISORSE UMANE E ORGANIZZAZIONE	Infortuni e malattie professionali
GESTIONE RISORSE UMANE	COMUNICAZIONI CON LA DIREZIONE RISORSE UMANE E ORGANIZZAZIONE	Tutte le altre comunicazioni
GESTIONE RISORSE UMANE	CONTRATTI DI LAVORO E RELAZIONI SINDACALI	Contratti, Accordi, Protocolli d'Intesa e atti applicativi
GESTIONE RISORSE UMANE	CONTRATTI DI LAVORO E RELAZIONI SINDACALI	Atti relativi alle relazioni sindacali
GESTIONE RISORSE UMANE	FORMAZIONE	Comunicazioni relative alla formazione
GESTIONE RISORSE UMANE	FORMAZIONE	Formazione in materia di salute e sicurezza nei luoghi di lavoro
GESTIONE RISORSE UMANE	GESTIONE DELLE PRESENZE	Comunicazioni varie relative alle presenze
GESTIONE RISORSE UMANE	GESTIONE DELLE PRESENZE	Accoglimento di permessi, aspettative, congedi
GESTIONE RISORSE UMANE	GESTIONE DELLE PRESENZE	Verbali ex L. 104/1992
GESTIONE RISORSE UMANE	GESTIONE DELLE PRESENZE	Certificati medici
GESTIONE RISORSE UMANE	PROCEDIMENTI DISCIPLINARI	
GESTIONE RISORSE UMANE	SALUTE E SICUREZZA SUL LAVORO	Corrispondenza sulla salute e sicurezza sul lavoro
GESTIONE RISORSE UMANE	SALUTE E SICUREZZA SUL	Verbali ispettivi e DVR

	LAVORO	
GESTIONE RISORSE UMANE	SALUTE E SICUREZZA SUL LAVORO	visite mediche e certificati di idoneità
GESTIONE RISORSE UMANE	TIROCINI EXTRA- CURRICULARI	
GESTIONE RISORSE UMANE	TRATTAMENTO ECONOMICO	
GESTIONE RISORSE UMANE	TRASFERTE (MISSIONI)	Autorizzazioni e ordini di movimento
GESTIONE RISORSE UMANE	TRASFERTE (MISSIONI)	Documentazione a supporto della liquidazione
GESTIONE RISORSE UMANE	VISITE FISCALI	Richiesta visita fiscale
GESTIONE RISORSE UMANE	VISITE FISCALI	Comunicazione assenza a visita fiscale
GESTIONE RISORSE UMANE	TEMPORANEA ASSEGNAZIONE	
DIREZIONE	CHIUSURA SPORTELLI (PROCURA GEN)	
DIREZIONE	COMUNICAZIONI SEGRETARIO GENERALE	
DIREZIONE	COMUNICAZIONI VARIE	
DIREZIONE	CORRISPONDENZA DIREZIONI CENTRALI	
DIREZIONE	DELIBERE	
DIREZIONE	INCARICHI	
DIREZIONE	PROCEDIMENTI GIUDIZIARI	
DIREZIONE	PROGETTI	
DIREZIONE	RITIRO AUTORIZZAZIONIPROVINCIA AG	
DIREZIONE	SEGNALAZIONI AUTORITA' PS	
DIREZIONE	ISPEZIONI	
DIREZIONE	INVENTARIO	
DIREZIONE	PATRIMONIO RICHIESTE MATERIALE	
DIREZIONE	PROTOCOLLO INFORMATICO	
DIREZIONE	PROCEDURE DI GARA	
CONTABILITA' CICLO PASSIVO	ANTICIPO MISSIONI	
CONTABILITA' CICLO PASSIVO	CARTELLE ESATTORIALI UTENZE	
CONTABILITA' CICLO PASSIVO	CIRCOLARI	

CONTABILITA' CICLO PASSIVO	COMUNICAZIONI	
CONTABILITA' CICLO PASSIVO	ORDINI PREVENTIVI	
CONTABILITA' CICLO PASSIVO	PAGAMENTI CONSEGNA MATERIALE	
CONTABILITA' CICLO PASSIVO	RECUPERO IPT	
CONTABILITA' CICLO PASSIVO	VERIFICHE CASSA	
CONTABILITA' CICLO PASSIVO	FATTURE	
CONTABILITA' CICLO ATTIVO	ISTANZE DI RIMBORSO	
CONTABILITA' CICLO ATTIVO	COMUNICAZIONI IPT	
CONTABILITA' CICLO ATTIVO	COMUNICAZIONI VARIE	
CONTABILITA' CICLO ATTIVO	INSOLUTI PRA	
CONTABILITA' CICLO ATTIVO	VERIFICHE CASSA	
CONTABILITA' CICLO ATTIVO	VERSAMENTO CONTANTI	
CONTABILITA' CICLO ATTIVO	RECUPERO IPT	
TRASPARENZA E ANTICORRUZIONE	NORME e DISPOSIZIONI	
TRASPARENZA E ANTICORRUZIONE	RAPPORTI ORGANISMI/AUTORITA'/MINISTERI	
TRASPARENZA E ANTICORRUZIONE	AGGIORNAMENTO PIANO/MAPPATURA PROCESSI	
TRASPARENZA E ANTICORRUZIONE	MONITORAGGI	
TRASPARENZA E ANTICORRUZIONE	SISTEMA DEI CONTROLLI	
RELAZIONI CON IL PUBBLICO	RICEZIONE/INOLTRO/RISCONTRO RICHIESTE UTENZA ESTERNA	
RELAZIONI CON IL PUBBLICO	GESTIONE ACCESSO DOCUMENTALE	
ACCESSO CIVICO	RICEZIONE/INOLTRO/ RISCONTRO RICHIESTE ACCESSO CIVICO	
PROTEZIONE DATI PERSONALI	ISTRUZIONI OPERATIVE GESTIONE DATI PERSONALI	
PROTEZIONE DATI PERSONALI	GESTIONE RICHIESTE INTERESSATI EX ARTT15-22 GDPR	

PROTEZIONE DATI PERSONALI	RICHIESTE DI PARERE FORMALE AL DPO	
PROTEZIONE DATI PERSONALI	COMUNICAZIONI CON LA STRUTTURA CENTRALE DI SUPPORTO AI REFERENTI	
PROTEZIONE DATI PERSONALI	INFORMATIVE E CONSENSI	
PROTEZIONE DATI PERSONALI	MISURE DI SICUREZZA	
PROTEZIONE DATI PERSONALI	REGISTRO DEI TRATTAMENTI E VALUTAZIONE D'IMPATTO (DPIA)	
PROTEZIONE DATI PERSONALI	NOMINE AI RUOLI PRIVACY	
PROTEZIONE DATI PERSONALI	VIOLAZIONE DEI DATI PERSONALI (DATA BREACH)	
CONTRATTI	PROGRAMMAZIONE	
CONTRATTI	CENTRALE ACQUISTI	
CONTRATTI	PROCEDURA NEGOZIALE	
CONTRATTI	VICENDE CONTRATTUALI	
CONTRATTI	CIRCOLARI	
GESTIONE IMMOBILE	CIRCOLARI	
GESTIONE IMMOBILE	CONTRATTI LOCAZIONE	
GESTIONE IMMOBILE	MANUTENZIONE	
GESTIONE IMMOBILE	SERVIZI CONDOMINIALI	
GESTIONE BENI	INVENTARIO E GESTIONE BENI MOBILI	
GESTIONE BENI	CIRCOLARI	

All. 4 - Manuale di conservazione

Il Manuale di conservazione, da considerarsi quale allegato al presente Manuale di gestione documentale, è pubblicato nella sezione Amministrazione Trasparente del sito dell'Automobile Club d'Italia all'indirizzo: Amministrazione trasparente / Disposizioni generali / Atti generali.

All. 5

Figure Responsabili

Ruoli	**Nominativo**
Coordinatore della gestione documentale	**Vincenzo Pensa**
Vicario del Coordinatore della gestione documentale	**Tiziana Santucci**
Responsabile della Conservazione	**Vincenzo Pensa**
Vicario del Responsabile della Conservazione	**Tiziana Santucci**
Responsabile della gestione documentale	**Gianna Guiducci**
Vicario delle gestione documentale	**Tiziana Magrini**

All. 6

Glossario

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 di un documento informatico che garantisce di essere ciò che dichiara di essere, senza aver subito alterazioni o modifiche. L'autenticità può essere valutata analizzando l'identità del sottoscrittore e l'integrità del documento informatico

Classificazione: attività di organizzazione logica di tutti i documenti secondo uno schema articolato in voci individuate attraverso specifici metadati

Copia analogica del documento informatico: documento analogico avente contenuto identico a quello del documento informatico da cui è tratto

Documento analogico: rappresentazione non informatica di atti, fatti o dati giuridicamente rilevanti (i documenti cartacei, le registrazioni su nastro - audio e video e le fotografie). All'interno del manuale sarà considerato solo il documento formato su supporto cartaceo prodotto con strumenti analogici (es. documento scritto a mano o a macchina da scrivere) o con strumenti informatici (es. documento prodotto con un sistema di videoscrittura e stampato)

Documento informatico: rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti in contrapposizione al documento analogico

Fascicolo informatico: Aggregazione strutturata e univocamente identificata di atti, documenti o dati informatici, prodotti e funzionali all'esercizio di una specifica attività o di uno specifico procedimento. Nella pubblica amministrazione il fascicolo informatico collegato al procedimento amministrativo è creato e gestito secondo le disposizioni stabilite dall'articolo 41 del CAD

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

Immodificabilità: caratteristica che rende il contenuto del documento informatico non alterabile nella forma e nel contenuto durante l'intero ciclo di gestione e ne garantisce la staticità nella conservazione del documento stesso

Integrità: insieme delle caratteristiche di un documento informatico che ne dichiarano la qualità di essere completo ed inalterato

Interoperabilità: capacità di un sistema informatico di interagire con altri sistemi informatici analoghi sulla base di requisiti minimi condivisi

Leggibilità: insieme delle caratteristiche in base alle quali le informazioni contenute nei documenti informatici sono fruibili durante l'intero ciclo di gestione dei documenti

Memorizzazione: processo di trasposizione su un qualsiasi idoneo supporto, attraverso un processo di elaborazione, di documenti analogici o informatici

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 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

Processo di conservazione: insieme delle attività finalizzate alla conservazione dei documenti informatici secondo la normativa vigente

Registro di protocollo: registro informatico di atti e documenti in ingresso e in uscita che permette la registrazione e l'identificazione univoca del documento informatico all'atto della sua immissione cronologica nel sistema di gestione informatica dei documenti

Riferimento temporale: informazione contenente la data e l'ora con riferimento al Tempo Universale Coordinato (UTC), della cui apposizione è responsabile il soggetto che forma il documento

Scarto: operazione con cui si eliminano, secondo quanto previsto dalla normativa vigente, i documenti ritenuti privi di valore amministrativo e di interesse storico culturale

Segnatura di protocollo: s'intende l'apposizione all'originale del documento, in forma permanente e non modificabile, delle informazioni riguardanti il documento stesso: numero di protocollo, data di protocollo, indicazione o codice dell'amministrazione o dell'AOO.

Sistema di classificazione: strumento che permette di organizzare tutti i documenti secondo un ordinamento logico con riferimento alle funzioni e alle attività dell'amministrazione interessata

Sistema di conservazione: sistema di conservazione dei documenti informatici di cui all'articolo 44 del Codice

Sistema di gestione informatica dei documenti: nell'ambito della pubblica amministrazione è il sistema di cui all'articolo 52 del Testo unico.

Figure di riferimento

Area organizzativa omogenea (AOO): un insieme di funzioni e di strutture, individuate dall'amministrazione, che opera su tematiche omogenee e che presenta esigenze di gestione della documentazione in modo unitario e coordinato secondo l'articolo 50, comma 4, del Testo unico

Coordinatore della Gestione Documentale: responsabile della definizione di criteri uniformi di classificazione ed archiviazione nonché di comunicazione interna tra le AOO secondo quanto disposto dall'articolo 50 comma 4 del Testo unico nei casi di amministrazioni che abbiano istituito più Aree Organizzative Omogenee e dal Capitolo 3, par. 3.1.2 lett. c).

Destinatario: identifica il soggetto/sistema al quale il documento informatico è indirizzato

Fornitore del Servizio: quando non diversamente specificato, s'intende la società ACI Informatica S.p.A.

Produttore: persona fisica o giuridica, 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

Responsabile della gestione documentale: dirigente o funzionario, comunque in possesso di idonei requisiti professionali o di professionalità tecnico archivistica, preposto al servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi, secondo l'articolo 61 del Testo unico.

Responsabile della conservazione: soggetto responsabile dell'insieme delle attività elencate nel par. 4.5 delle "Linee Guida sulla formazione, gestione e conservazione dei documenti informatici" di maggio 2021

Responsabile del Procedimento Amministrativo (RPA): il dirigente o il dipendente individuato dall'amministrazione, cui è attribuita la responsabilità dell'istruttoria, dell'adozione di tutti gli atti endoprocedimentali e del corretto e tempestivo svolgimento del procedimento, fino alla sua conclusione con il provvedimento finale.

Responsabile del trattamento dei dati: la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali

Responsabile della sicurezza: soggetto incaricato di garantire la sicurezza fisica e logica del sistema di gestione informatica dei documenti e degli archivi, mediante l'adozione e il monitoraggio delle misure tecniche ed organizzative necessarie a tutelare l'integrità, la disponibilità e la riservatezza delle informazioni, in coerenza con le disposizioni del CAD, delle Linee guida AgID e delle misure minime di sicurezza ICT per le pubbliche amministrazioni.

Servizio Protocollo Informatico: il reparto che cura le attività di ricezione, spedizione, registrazione, classificazione e archiviazione della corrispondenza in entrata e uscita; può essere costituita da più unità di protocollo;

Unità Organizzativa Responsabile (UOR): riferito ad un'area organizzativa omogenea, un ufficio dell'area stessa che utilizza i servizi messi a disposizione dal Servizio Protocollo Informatico;

Utente: persona, ente o sistema che interagisce con i servizi di un sistema di gestione informatica dei documenti e/o di un sistema per la conservazione dei documenti informatici, al fine di fruire delle informazioni di interesse

Per tutte le altre definizioni è necessario fare riferimento al glossario di cui all'allegato 1 "Linee Guida sulla formazione, gestione e conservazione dei documenti informatici" di maggio 2021, da cui le presenti sono state tratte.

Allegato al Manuale di gestione documentale

Piano di Organizzazione delle Aggregazioni Documentali

1. Premessa

Nell' Allegato 1 delle Linee Guida AGID il "Piano di Organizzazione delle Aggregazioni Documentali" viene definito come: *"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".*

Si intende, pertanto, come uno strumento archivistico integrato che accorpi il Piano di classificazione, il Piano di fascicolazione, il Piano di conservazione, strumenti archivistici tradizionali, fornendo inoltre informazioni sugli applicativi che concorrono alla formazione dell'archivio, sull'eventuale presenza di sistemi di gestione federati e sulla pubblicazione dei documenti e delle aggregazioni documentali che costituiscono l'archivio dell'Ente.

Il presente Piano di Organizzazione delle Aggregazioni Documentali è redatto in ottemperanza alle disposizioni del Decreto Legislativo 7 marzo 2005, n. 82 e successive modificazioni (Codice dell'Amministrazione Digitale - CAD) e delle Linee Guida sulla formazione, gestione e conservazione dei documenti informatici di maggio 2021 (Linee Guida AgID 2021).

Il documento ha la finalità di descrivere le aggregazioni documentali adottate dall'Ente e le relative modalità di formazione, gestione e conservazione. Il Piano di Organizzazione delle Aggregazioni Documentali si integra con il Manuale di Gestione Documentale dell'Automobile Club d'Italia, il quale descrive il sistema di gestione informatica dei documenti e fornisce le istruzioni per il corretto uso del protocollo informatico, la gestione dei flussi documentali e degli archivi. Il Piano di Conservazione, allegato al Manuale di Gestione Documentale, definisce i tempi e i criteri per la selezione e lo scarto dei documenti.

2. Definizioni e principi generali

Per gli scopi del presente Piano, si intende per:

- **Aggregazione documentale:** un insieme strutturato e univocamente identificato di atti, documenti o dati informatici. Nel contesto dell'Ente, le tipologie di aggregazioni documentali attualmente adottate sono i fascicoli e il Registro delle Determine.
- **Fascicolo informatico:** un'aggregazione strutturata e univocamente identificata di atti, documenti o dati informatici, prodotti e funzionali all'esercizio di una specifica attività o di uno specifico procedimento. Nella pubblica amministrazione, il fascicolo informatico è creato e gestito secondo le disposizioni stabilite dall'articolo 41 del CAD. Le tipologie di fascicoli possono includere fascicoli di affare, di procedimento, di attività, di persona fisica o di persona giuridica.

- **Classificazione:** l'attività di organizzazione logica di tutti i documenti secondo uno schema articolato in voci individuate attraverso specifici metadati. Si avvale del piano di classificazione (titolario), che mappa le funzioni dell'ente su più livelli gerarchici.
- **Protocollo informatico:** il registro informatico di atti e documenti in ingresso e in uscita che permette la registrazione e l'identificazione univoca del documento informatico all'atto della sua immissione cronologica nel sistema di gestione informatica dei documenti. Le registrazioni di protocollo si integrano con il piano di organizzazione delle aggregazioni documentali.

3. Aggregazioni documentali adottate dall'Ente

L'Automobile Club d'Italia adotta le seguenti aggregazioni documentali:

3.1 Fascicoli

I flussi documentali dei documenti soggetti a protocollo sono gestiti mediante fascicoli informatici predisposti secondo il piano di classificazione e relativo piano di fascicolazione ai sensi del par. 3.3.1 delle Linee Guida AGID in ottemperanza a quanto disposto dall'art. 64 del TUDA. Detti fascicoli sono gestiti direttamente dal sistema di protocollo informatico dell'Ente. La fascicolazione archivistica è, quindi, parte integrante del sistema di protocollo informatico e del ciclo di vita dei documenti, dalla loro produzione o acquisizione fino alla conservazione e archiviazione finale.

- **Tipologie di fascicoli:** L'Ente utilizza diverse tipologie di fascicoli per organizzare la documentazione in base alla funzione, all'oggetto o al soggetto di riferimento:
    - **Fascicoli di Affare:** raggruppano documenti relativi a competenze non proceduralizzate e che non richiedono l'adozione di un provvedimento finale.
    - **Fascicoli di Attività:** contengono documenti legati a competenze proceduralizzate, senza prevedere provvedimenti finali, per attività amministrative ripetitive o adempimenti periodici.
    - **Fascicoli di Procedimento Amministrativo:** includono documenti collegati tra loro e destinati a concludersi con un provvedimento amministrativo, permettendo di seguire l'intero iter della pratica.
    - **Fascicoli di Persona Fisica e Persona Giuridica:** comprendono documenti relativi a una stessa persona fisica o giuridica, raggruppati per finalità archivistiche comuni e la cui chiusura coincide con la conclusione del rapporto giuridico con l'Amministrazione.

- **Modalità di apertura, gestione e chiusura dei fascicoli:**
    - **Apertura:** i fascicoli sono aperti secondo le procedure definite nel sistema di gestione documentale, in coerenza con il titolario di classificazione.
    - **Gestione:** la gestione dei fascicoli informatici avviene nel rispetto di quanto stabilito dagli articoli 65 del TUDA e 41 del CAD. Il sistema di gestione informatica dei documenti permette la produzione, il mantenimento e l'uso dei fascicoli informatici.

- **Chiusura:** la chiusura del fascicolo avviene una volta conclusa l'attività o il procedimento amministrativo di riferimento, o la conclusione del rapporto giuridico con l'Amministrazione.
- **Ruoli e responsabilità:** il Responsabile del fascicolo, di norma il Responsabile del Procedimento Amministrativo (RPA), ha automaticamente accesso al fascicolo e ne garantisce la corretta gestione. L'assegnazione del fascicolo a un ufficio o a un operatore definisce anche la responsabilità sul procedimento correlato. La visibilità dei documenti all'interno del sistema di protocollo è definita dall'AOO tramite il funzionigramma.

3.2 Registro delle Determine

Le Determine dirigenziali rappresentano una tipologia documentale specifica e peculiare all'interno della gestione documentale dell'Amministrazione. Non vengono inserite nel protocollo generale, ma sono soggette a una registrazione dedicata, conforme all'articolo 53 del DPR 445/2000.

- **Scopo:** La registrazione dedicata garantisce tracciabilità, validità formale e ordinamento cronologico interno all'Area Organizzativa Omogenea (AOO).
- **Funzionamento:** Le Determine sono registrate mediante un'applicazione specifica che ne verifica automaticamente la completezza formale (ad esempio, la presenza della firma digitale o autografa). Durante la registrazione, l'applicazione attribuisce un numero progressivo univoco per ciascuna AOO, che costituisce l'identificativo ufficiale del documento all'interno dell'Amministrazione.

Assenza di altre aggregazioni: Si conferma che, al momento della redazione del presente Piano, non risultano altre tipologie documentali o aggregazioni documentali adottate dall'Ente oltre a quelle sopra descritte.

4. Regole di gestione e tenuta delle aggregazioni

La gestione e la tenuta delle aggregazioni documentali sono improntate ai principi di unicità, integrità, immodificabilità e reperibilità, garantendo la piena efficacia giuridica e probatoria dei documenti.

Identificazione univoca delle aggregazioni:

Le aggregazioni documentali sono strutturate e univocamente identificate. L'identificazione è garantita dall'associazione di un insieme minimo di metadati, come definito nell'Allegato 5 delle Linee Guida AgID 2021.

Per i documenti soggetti a registrazione di protocollo (inclusi quelli che compongono i fascicoli), l'identificazione univoca è rappresentata dalla segnatura di protocollo, che è apposta o associata all'originale del documento in forma permanente e non modificabile. La segnatura include il codice identificativo dell'amministrazione, dell'AOO, la data e il numero

di protocollo del documento, ecc… secondo quanto disposto in merito dall'art. 55 del TUDA e dall'Allegato 6 delle Linee Guida AGID.

Il numero di protocollo è progressivo, unico per l'AOO e rinnovato ogni anno solare. Non è consentita la cosiddetta registrazione "a fronte" o la protocollazione di un documento già protocollato.

Per il Registro delle Determine, l'identificazione avviene tramite un numero progressivo univoco assegnato per ciascuna AOO dall'applicazione specifica.

Responsabili della creazione e cura:

- Il **Responsabile della gestione documentale (RGD)** è preposto al Servizio per la gestione del protocollo informatico, dei flussi documentali e degli archivi. Il RGD garantisce il buon funzionamento degli strumenti e dell'organizzazione delle attività di registrazione di protocollo, di gestione dei documenti e dei flussi documentali, inclusa la gestione degli archivi.
- Il **Coordinatore della gestione documentale** è responsabile della definizione di criteri uniformi di classificazione e archiviazione per tutte le AOO dell'Automobile Club d'Italia.
- **Collegamento con il ciclo di vita dei documenti:** la gestione documentale è un processo che si articola in tre fasi principali: formazione, gestione e conservazione. La fascicolazione è parte integrante del sistema di protocollo informatico e del ciclo di vita dei documenti, dalla loro produzione o acquisizione fino alla conservazione e archiviazione finale. Il sistema di gestione informatica dei documenti supporta la produzione, la gestione e l'uso delle aggregazioni documentali informatiche.

5. Collegamenti con conservazione e scarto

La conservazione e lo scarto delle aggregazioni documentali avvengono in conformità alla normativa vigente, garantendo la tutela del patrimonio informativo.

Modalità di riversamento delle aggregazioni nel sistema di conservazione:

Il registro informatico di protocollo viene generato automaticamente dal sistema e trasmesso al sistema di conservazione, che ne garantisce l'immodificabilità.

Gli obblighi di conservazione e di esibizione di documenti sono soddisfatti a mezzo di documenti informatici, se le relative procedure sono conformi alle Linee Guida.

Il sistema di gestione informatica dei documenti trasferisce al sistema di conservazione i fascicoli informatici chiusi e le serie informatiche chiuse dall'archivio corrente o di deposito. Possono essere trasferiti anche i documenti contenuti in fascicoli o serie non ancora chiuse, sulla base di specifiche esigenze dell'ente, per prevenire rischi di obsolescenza tecnologica.

Il sistema di conservazione, logicamente distinto dal sistema di gestione, assicura, dalla presa in carico fino all'eventuale scarto, le caratteristiche di autenticità, integrità, affidabilità, leggibilità e reperibilità dei documenti e delle aggregazioni documentali informatiche, inclusi i metadati associati.

Il processo di conservazione è gestito dal Responsabile della conservazione dell'Ente, anche avvalendosi di un fornitore esterno accreditato. Le Determine, essendo soggette a registrazione dedicata, rientreranno anch'esse nel processo di conservazione per garantirne la validità e la tracciabilità nel tempo.

Destinazione finale: conservazione permanente o scarto selettivo

La selezione e lo scarto dei documenti informatici e delle aggregazioni documentali informatiche sono effettuati nel rispetto della normativa sui beni culturali.

Un documento è considerato scartabile quando ha perso completamente la sua rilevanza amministrativa e non ha acquisito alcuna rilevanza storica.

Le procedure per lo scarto dei documenti e i tempi minimi di conservazione per ciascuna tipologia documentale sono indicati nel Piano di conservazione, allegato al Manuale di Gestione Documentale.

Il **Responsabile della conservazione** è incaricato di generare l'elenco dei pacchetti di archiviazione contenenti i documenti destinati allo scarto, verificando il rispetto dei termini temporali stabiliti dal piano di conservazione e comunicandolo al Responsabile della gestione documentale.

Lo scarto dei documenti è effettuato previa autorizzazione della Soprintendenza Archivistica e Bibliografica, secondo quanto previsto dalla normativa vigente.

6. Aggiornamento e manutenzione del Piano di Organizzazione delle Aggregazioni Documentali

Il presente Piano sarà oggetto di revisione periodica, e comunque ogni qualvolta intervengano cambiamenti significativi a livello normativo, organizzativo o tecnologico.

Ruolo del Responsabile: Il Coordinatore della gestione documentale verifica periodicamente la rispondenza del piano di classificazione ai procedimenti amministrativi e agli affari in essere e procede al suo aggiornamento. Egli coordina inoltre la pubblicazione delle versioni aggiornate del Manuale di gestione documentale (di cui il Piano di Organizzazione delle Aggregazioni Documentali fa parte) da parte di ciascuna AOO sul sito istituzionale dell'Ente.

Modalità di comunicazione delle modifiche: Le modifiche e gli aggiornamenti del Piano di Organizzazione delle Aggregazioni Documentali saranno pubblicati sul sito istituzionale dell'Ente, in una parte chiaramente identificabile dell'area "Amministrazione trasparente", come previsto dall'articolo 9 del d.lgs. 33/2013, al fine di garantirne la massima diffusione e conoscibilità interna ed esterna.

Allegato al Manuale di gestione documentale

PIANO PER LA SICUREZZA INFORMATICA

1. Premessa e Obiettivi

Il presente Piano per la Sicurezza Informatica costituisce parte integrante del Manuale di Gestione Documentale, in ottemperanza alle disposizioni vigenti in materia di gestione e conservazione dei documenti informatici.

La sua redazione è prevista dalle Linee Guida sulla formazione, gestione e conservazione dei documenti informatici, emanate da AgID. Nello specifico, il paragrafo 3.4, "Compiti del responsabile della gestione documentale", stabilisce che il responsabile della gestione documentale (o il coordinatore, ove nominato) ha il compito di predisporre il Manuale di gestione documentale, il quale "conterrà inoltre, come parte integrante dello stesso, il piano per la sicurezza informatica, per la quota parte di competenza". Tale previsione è ulteriormente dettagliata nel paragrafo 3.9, "Misure di sicurezza", che ribadisce i requisiti per tale piano.

Il Piano di Sicurezza ha lo scopo di garantire la protezione, l'affidabilità e la resilienza del sistema di gestione informatica dei documenti dell'Amministrazione. In particolare, il Piano è finalizzato a:

- contrastare le minacce di natura informatica (ICT) che possono compromettere l'integrità, la disponibilità e la riservatezza delle informazioni;
- assicurare la protezione dei dati personali trattati nell'ambito della gestione documentale, in conformità alla normativa vigente;
- tutelare la corretta formazione, gestione, accessibilità e conservazione dei documenti informatici, quale patrimonio informativo dell'Amministrazione.

Il Piano è redatto in conformità alle Linee Guida sulla formazione, gestione e conservazione dei documenti informatici emanate da AgID, nonché alla Circolare AgID n. 2/2017 – Misure minime di sicurezza ICT per le pubbliche amministrazioni, adottando i principi e le misure ivi previsti come quadro di riferimento per la sicurezza.

Il documento si colloca nell'ambito del più ampio Piano generale di sicurezza dell'Amministrazione, con il quale è integrato e coordinato. Esso è inoltre elaborato in coerenza con le linee di indirizzo strategiche del Piano Triennale per l'Informatica nella Pubblica Amministrazione vigente, al fine di assicurare un approccio unitario e armonizzato alla gestione della sicurezza informatica, alla continuità operativa e alla protezione del patrimonio informativo dell'Ente.

2. Ruoli e Responsabilità

La predisposizione, l'attuazione e il monitoraggio del presente Piano di Sicurezza coinvolgono diversi soggetti dell'Amministrazione, ciascuno con compiti e responsabilità specifiche nell'ambito della gestione documentale e della sicurezza delle informazioni.

<u>Coordinatore della gestione documentale</u>

Assicura l'applicazione del Piano di Sicurezza nell'ambito delle attività di formazione, registrazione, classificazione, archiviazione e conservazione dei documenti informatici.

Coordina le attività con i responsabili delle altre funzioni, al fine di garantire un approccio unitario alla sicurezza.

Responsabile della conservazione

Vigila sul corretto trasferimento, archiviazione e conservazione dei documenti informatici e dei fascicoli digitali.

Verifica che le misure di sicurezza adottate garantiscano integrità, leggibilità, reperibilità e protezione dei documenti nel lungo periodo.

Responsabile per la transizione digitale (RTD)

Assicura la coerenza del Piano di Sicurezza con le strategie generali di digitalizzazione dell'Amministrazione.

Coordina le azioni di sicurezza ICT in sinergia con i responsabili dei sistemi informativi e con i referenti di ACI Informatica.

Responsabile della protezione dei dati personali (DPO)

Esprime parere sul Piano di Sicurezza, verificandone la conformità al Regolamento UE 679/2016 (GDPR) e alla normativa nazionale in materia di protezione dei dati personali.

Fornisce indicazioni operative per garantire il rispetto dei principi di minimizzazione, proporzionalità e accountability.

Titolare e Responsabile del trattamento dei dati

Ai sensi dell'art. 28 del Regolamento UE 679/2016:

- Automobile Club d'Italia (ACI) è individuato quale Titolare del trattamento (art. 4 GDPR).
- ACI Informatica S.p.A. è individuata quale Responsabile del trattamento (art. 28 GDPR), per le attività di gestione tecnica e manutenzione dei sistemi informatici .

ACI Informatica

Partner tecnologico di ACI, responsabile della gestione dell'intero ciclo di vita degli incidenti di sicurezza delle informazioni e dell'implementazione del sistema di Business Continuity.

2. Norme di Riferimento

Il Piano di Sicurezza si basa e si conforma alle seguenti norme e direttive principali:

- Decreto Legislativo 7 marzo 2005, n. 82 (C.A.D.) e successive modifiche e integrazioni, con particolare riferimento all'Art. 14-bis (funzioni di AgID in materia di sicurezza informatica), all'Art. 51 (sicurezza e disponibilità dei dati, dei sistemi e delle infrastrutture delle pubbliche amministrazioni) e all'Art. 71 (Linee Guida AgID).
- Direttiva del Presidente del Consiglio dei Ministri 1° agosto 2015, che impone l'adozione di standard minimi di prevenzione e reazione ad eventi cibernetici.
- Circolare AGID 18 aprile 2017, n. 2/2017 (già n. 1/2017 del 17 marzo 2017), che indica le misure minime di sicurezza ICT per le pubbliche amministrazioni.
- DPCM 17 febbraio 2017, recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali (Piano nazionale per la protezione cibernetica e la sicurezza informatica).
- Regolamento UE 2016/679 (GDPR), relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, in particolare gli Artt. 25 (Protezione dei dati fin dalla progettazione), 28 (Responsabile del trattamento), 32 (Sicurezza del trattamento), 33 (Notifica di una violazione dei dati personali all'autorità di controllo) e 34 (Comunicazione di una violazione dei dati personali all'interessato).
- Linee guida EDPB 4/2019 sull'articolo 25 Protezione dei dati fin dalla progettazione e per impostazione predefinita.
- Linee guida EDPB 9/2022 sulla notifica delle violazioni dei dati personali ai sensi del regolamento generale sulla protezione dei dati (GDPR).
- UNI CEI EN ISO/IEC 27001:2017 (Sistemi di Gestione della Sicurezza delle Informazioni – Requisiti), come standard di riferimento per la gestione della sicurezza IT.
- UNI EN ISO 22301:2019 (Sistemi di gestione della continuità operativa – Requisiti), per il sistema di gestione della Business Continuity.
- ISO/IEC 20000-1:2018 ("Tecnologie informatiche - Gestione del servizio - Parte 1: Requisiti per un sistema di gestione del servizio").
- UNI EN ISO 9001:2015 (Sistemi di gestione per la qualità – Requisiti).
- Linee Guida sulla formazione, gestione e conservazione dei documenti informatici (AgID, Maggio 2021).
- DPR 445/2000 (Testo Unico sulla Documentazione Amministrativa - TUDA), in particolare gli articoli relativi al sistema di gestione informatica dei documenti e del protocollo.
- SANS 20 / CCSC «CIS Critical Security Controls for Effective Cyber Defense» versione 6.0 di ottobre 2015, utilizzato come base per le misure minime di sicurezza.
- ITIL v3 – Service Operations e altre best practice di settore come ENISA e SANS Institute per la gestione degli incidenti.

3. Documenti di Riferimento

Il presente Piano di Sicurezza si integra con e fa riferimento ai seguenti documenti interni ed esterni:

- Politiche di Sicurezza dei Sistemi e delle Informazioni.
- Regolamento Data Breach – Violazioni dei Dati Personali.
- Manuale della Business Continuity.
- Business Impact Analysis (BIA), che identifica i servizi essenziali e i relativi tempi di recupero.
- Manuale di gestione documentale
- Manuale di conservazione.

- Piano Triennale per l'Informatica nella Pubblica Amministrazione.

4. Analisi del Rischio e Misure di Sicurezza

Analisi del rischio

L'Amministrazione adotta una metodologia strutturata di analisi e gestione del rischio, basata sui principi delle norme internazionali in materia di sicurezza delle informazioni (ISO/IEC 27001, ISO/IEC 27701 e ISO/IEC 27005), nonché sui criteri indicati dalle Linee Guida AgID e dall'ACN (Agenzia per la Cybersicurezza Nazionale).

L'analisi è finalizzata a:

- identificare i beni informativi e i processi critici relativi alla gestione documentale;
- valutare le minacce e le vulnerabilità cui i sistemi sono esposti;
- stimare l'impatto potenziale su riservatezza, integrità e disponibilità delle informazioni;
- definire le misure di sicurezza necessarie per garantire un livello di protezione adeguato, in relazione alla tipologia dei dati trattati.

Particolare attenzione è riservata al trattamento delle categorie particolari di dati personali di cui agli artt. 9 e 10 del Regolamento UE 679/2016 (GDPR), che richiedono un livello di protezione rafforzato.

Misure tecniche e organizzative di sicurezza (Art. 32 GDPR)

In coerenza con l'analisi del rischio, l'Amministrazione adotta misure tecniche e organizzative idonee a garantire un livello di sicurezza proporzionato al rischio, tra cui:

- la pseudonimizzazione e la cifratura dei dati personali in transito e in conservazione, ove applicabile;
- la capacità di assicurare, su base permanente, la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
- la capacità di ripristinare tempestivamente la disponibilità e l'accesso ai dati personali in caso di incidente fisico o tecnico, attraverso procedure di backup e disaster recovery;
- l'adozione di una procedura periodica di test, verifica e valutazione dell'efficacia delle misure tecniche e organizzative implementate, mediante audit di sicurezza e simulazioni di incidente.

Misure minime di sicurezza ICT (Circolare AgID n. 2/2017)

Nel rispetto della Circolare AgID n. 2/2017, l'Amministrazione assicura l'applicazione delle misure minime di sicurezza ICT, adattandole ai tre livelli di sicurezza (Minimo, Standard, Alto) in funzione della classificazione dei dati e dei sistemi trattati. Le principali classi di misure implementate comprendono:

- Inventario dei sistemi e delle applicazioni: mantenimento di un registro aggiornato delle risorse ICT utilizzate nel sistema di gestione documentale.

- Protezione della configurazione dei sistemi: adozione di configurazioni sicure e aggiornate, con applicazione costante delle patch di sicurezza.

- Analisi delle vulnerabilità: monitoraggio periodico delle vulnerabilità e applicazione di misure correttive tempestive.

- Gestione degli utenti e privilegi di accesso: applicazione del principio del "minimo privilegio", con controlli specifici sugli utenti con funzioni di amministrazione.

- Difesa contro i malware: utilizzo di strumenti di protezione avanzata e aggiornamenti automatici delle definizioni antivirale/antimalware.

- Copie di sicurezza: esecuzione regolare di backup, custoditi in ambienti protetti e verificati periodicamente per garantirne l'efficacia in caso di ripristino.

- Protezione dei dati rilevanti: applicazione di misure di prevenzione e rilevamento contro i rischi di esfiltrazione o perdita di dati sensibili.

<u>Modulo di implementazione</u>

Per ciascuna delle misure sopra indicate, l'Amministrazione predispone un apposito modulo di implementazione, contenente:

- descrizione della misura;

- livello di sicurezza applicato (Minimo, Standard, Alto);

- modalità di attuazione tecnica e organizzativa;

- periodicità dei controlli e dei test;

- referenti responsabili dell'attuazione.

5. Sicurezza del Sistema di Protocollo Informatico

Il sistema di protocollo informatico rappresenta un elemento centrale della gestione documentale dell'Amministrazione, in quanto assicura la registrazione, la classificazione e la tracciabilità dei

documenti. Per tale ragione, esso è soggetto a requisiti di sicurezza specifici, volti a garantire l'affidabilità, la protezione e la conformità normativa del trattamento delle informazioni.

I principali requisiti minimi di sicurezza previsti sono:

Univoca identificazione ed autenticazione degli utenti

Ogni utente è identificato in maniera univoca mediante credenziali personali non condivisibili. L'accesso al sistema avviene attraverso procedure di autenticazione sicura, basate su nome utente e password complesse o, ove previsto, su sistemi di autenticazione a più fattori.

Gestione dei profili di accesso

L'accesso alle risorse e alle funzioni del sistema è consentito esclusivamente agli utenti abilitati, sulla base di profili predefiniti che distinguono i livelli di autorizzazione. I profili di accesso sono configurati in modo da consentire a ciascun utente soltanto le operazioni necessarie allo svolgimento delle proprie attività, garantendo la separazione dei compiti e la protezione dei dati sensibili.

Tracciamento e audit delle operazioni

Il sistema assicura il tracciamento permanente di tutte le operazioni rilevanti, comprese la registrazione, la modifica, la cancellazione e la consultazione dei documenti. Ogni evento è registrato nei log di sistema, con l'indicazione dell'utente autore dell'operazione, della data e dell'ora, nonché della tipologia di azione compiuta.

I registri di tracciamento sono protetti da alterazioni e conservati per un periodo adeguato, al fine di consentire eventuali verifiche, audit interni e controlli di conformità.

6. Gestione degli Incidenti di Sicurezza e Violazioni dei Dati Personali (Data Breach)

Il presente piano descrive le procedure da adottarsi per la gestione di eventi e incidenti di sicurezza delle informazioni, con particolare enfasi sulle violazioni dei dati personali (Data Breach), in conformità agli Artt. 33 e 34 del Regolamento UE 679/2016 (GDPR) e alle Misure Minime di Sicurezza ICT emanate dall'AgID con Circolare n. 2/2017. L'obiettivo è garantire un approccio strutturato e sistematico per minimizzare i rischi per le operazioni, i sistemi e i dati personali, assicurando tempestività, efficacia e conformità normativa.

6.1. Scopo e Principi Guida

Obiettivo primario: Implementare politiche e controlli per la gestione degli incidenti di sicurezza e delle violazioni dei dati personali, allineandosi agli standard e alle best practice internazionali di settore (es. ISO/IEC 27035:2016, SANS Institute).

Ambito di applicazione: Le politiche e le procedure si applicano a tutti gli eventi e agli incidenti di sicurezza delle informazioni che possono impattare la riservatezza, l'integrità e la disponibilità del patrimonio informativo dell'Amministrazione, coinvolgendo tutto il personale e le terze parti che hanno accesso a tale patrimonio.

6.2. Definizioni Chiave

Evento di Sicurezza: ogni occorrenza che indichi una potenziale infrazione di una policy, il fallimento di un controllo o una situazione precedentemente ignota e potenzialmente rilevante per la tutela delle informazioni.

Incidente di Sicurezza delle Informazioni: uno o più eventi di sicurezza indesiderati che comportano una significativa probabilità di compromissione delle operazioni di business e della sicurezza delle informazioni (integrità, disponibilità e riservatezza). Un incidente può essere deliberato (es. malware, infrazioni intenzionali) o accidentale (es. errori umani, fenomeni naturali).

Non tutti gli incidenti costituiscono una violazione dei dati personali.

Violazione dei Dati Personali (Data Breach): una violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati. Le violazioni possono essere classificate in base alla compromissione di:

- Riservatezza: divulgazione o accesso non autorizzato o accidentale ai dati personali.
- Integrità: modifica non autorizzata o accidentale dei dati personali.
- Disponibilità: perdita o distruzione accidentale o non autorizzata dei dati personali.

Una violazione può riguardare contemporaneamente la riservatezza, l'integrità e la disponibilità dei dati personali, nonché qualsiasi combinazione delle stesse.

6.3. Ruoli e Responsabilità nella Gestione degli Incidenti

I principali attori coinvolti e le loro responsabilità sono:

- Utenti (personale interno e terze parti): richiesti a segnalare tempestivamente qualsiasi evento o punto di debolezza relativo alla sicurezza delle informazioni osservato o sospettato nei sistemi o servizi. Le segnalazioni di tentativi sospetti di accesso indebito devono essere indirizzate alla casella cybersecurity@aci.it (o equivalente). In caso di sospetta violazione dei dati personali, la segnalazione deve essere inviata senza ritardo al Titolare del trattamento (es. privacy@aci.it) e al DPO (es. m.annibalidpo@aci.it).

- ACI Informatica (o soggetto tecnico/responsabile esterno del trattamento): è responsabile per la gestione dell'intero ciclo di vita degli incidenti di sicurezza delle informazioni. Le attività includono il monitoraggio proattivo, la presa in carico delle segnalazioni, la classificazione degli incidenti, le attività di analisi e risposta, nonché la comunicazione e il reporting verso la Direzione per lo Sviluppo, la Gestione, la Sicurezza dei Sistemi Informativi e l'Innovazione digitale di ACI e l'attivazione delle procedure di escalation (es. Crisis Management, fornisce i dati e gli elementi necessari per la gestione di eventuali Data Breach). Insieme alla Funzione per i Sistemi Informativi, opera come Unità Tecnologica del Comitato di Crisi, individuando le azioni di risposta.

- Direzione per lo Sviluppo, la Gestione, la Sicurezza dei Sistemi Informativi e l'Innovazione digitale (DSII): Coinvolta con ruolo consultivo e autorizzativo nella gestione

degli incidenti di particolare severità. Collabora con ACI Informatica per la revisione della reportistica periodica e per l'identificazione di incidenti che possono portare alla dichiarazione dello stato di crisi.

- Responsabile della Sicurezza Informatica: valuta la gravità degli incidenti e, in caso di potenziale data breach, informa immediatamente il DPO e il Direttore Centrale Organizzazione e Gestione della Privacy e Monitoraggio dei Sistemi di Qualità dell'Ente.

- Data Protection Officer (DPO): è componente del Comitato di Crisi. Conduce la verifica post-incidente per valutare l'efficacia della risposta, l'adeguatezza delle misure preventive e identificare eventuali lacune, informandone il Comitato di Crisi. È parte integrante del Comitato di Crisi per l'adozione delle conseguenti misure.

- Comitato di Crisi: organismo interno preposto a fronteggiare tempestivamente e in modo coordinato situazioni di emergenza che comportano rischi e minacce per la gestione dei dati personali. È responsabile della gestione strategica e tattica della crisi, definendo priorità e risorse. Se la violazione di dati personali comporta un rischio elevato per i diritti e le libertà delle persone, fornisce al Titolare, per il tramite della Struttura di privacy compliance, gli elementi per la notifica all'Autorità di controllo nei termini di legge e indicazioni per l'eventuale comunicazione agli interessati. Redige il Piano di risposta agli incidenti (Remediation plan).

- Responsabile della gestione documentale: in accordo con il responsabile della conservazione, il responsabile per la transizione digitale e acquisito il parere del DPO, predispone il piano della sicurezza del sistema di gestione informatica dei documenti, che include le procedure per la gestione delle violazioni dei dati personali.

6.4. Fasi del Processo di Gestione degli Incidenti e Data Breach

Il processo è articolato nelle seguenti attività:

1. Monitoraggio e Rilevazione degli Eventi di Sicurezza:

- Attività continuative (H24 7x7) di monitoraggio, rilevazione e analisi di eventi anomali attraverso dispositivi informatici di monitoraggio e analisi periodica dei log.

- Raccolta e valutazione delle segnalazioni di comportamenti anomali o sospetti provenienti da utenti, amministratori di sistema o fonti esterne autoritative (es. alert, bollettini di sicurezza).

2. Segnalazione e Prima Classificazione:

L'incidente viene segnalato dagli utenti o dai sistemi di monitoraggio.

Ogni incidente che determina una violazione dei dati personali deve essere registrato e documentato senza ritardo nell'apposito "Registro delle violazioni" (Allegato al Regolamento Data Breach). Il Registro è detenuto dalla Struttura di privacy compliance dell'Ente e deve essere costantemente aggiornato e mantenuto in sicurezza.

Gli eventi vengono valutati per stabilire se classificarli come incidenti di sicurezza dei dati e delle informazioni, con i risultati registrati per il riesame di misure tecnico-organizzative migliorative.

3. Assessment e Valutazione della Gravità:

- ACI Informatica (o soggetto analogo) esegue un assessment per valutare la gravità e l'impatto dell'incidente.

- Se l'incidente è considerato grave o potenzialmente a rischio, il Responsabile della Sicurezza Informatica informa la Direzione per lo Sviluppo, la Gestione, la Sicurezza dei Sistemi Informativi e l'Innovazione digitale che ne dà notizia al Titolare ai fini dell'attivazione del Comitato di crisi.

- Valutazione Data Breach: Se l'assessment conferma un potenziale data breach, viene attivata la procedura di gestione delle violazioni dei dati. Il Responsabile della Sicurezza Informatica informa immediatamente il Titolare, il Direttore della Struttura di privacy compliance e il DPO.

- Valutazione del rischio e analisi delle conseguenze: Il DPO dell'ACI coordina una valutazione del rischio per determinarne l'entità e le conseguenze (es. tipologia e volume dei dati compromessi, categorie di interessati, effetti a lungo termine). Tale valutazione viene effettuata utilizzando strumenti standardizzati (es. diagramma di flusso operativo fornito dall'EDPB nelle apposite Linee Guida) e include la classificazione della gravità dell'incidente.

4. Contenimento, Risposta e Recupero:

Il Comitato di Crisi (o l'Unità Tecnologica del Comitato di crisi) adotta misure tecniche e organizzative immediate per limitare l'estensione della violazione, come la sospensione degli account utente compromessi o il blocco degli accessi non autorizzati.

Pianificazione e preparazione delle azioni di risposta, incluse le procedure di escalation (es. Crisis Management).

Recupero dei dati compromessi: Deve essere eseguito tempestivamente, cercando di ripristinare i dati allo stato originario precedente alla violazione.

5. Notifica all'Autorità Garante (Art. 33 GDPR) e Comunicazione agli Interessati (Art. 34 GDPR):

- Notifica al Garante: In caso di data breach che comporti un rischio per i diritti e le libertà delle persone fisiche, la violazione deve essere notificata all'Autorità di Controllo competente senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui l'Amministrazione ne è venuta a conoscenza. La notifica deve essere dettagliata e includere la natura della violazione, le categorie e il numero degli interessati, i contatti del DPO, le probabili conseguenze e le misure adottate. L'istruttoria è condotta dal Comitato di Crisi.

- Comunicazione agli Interessati: Se la violazione comporta un rischio elevato per i diritti e le libertà degli interessati, questi devono essere informati senza ingiustificato ritardo. La comunicazione deve essere chiara, concisa e facilmente comprensibile, includendo la descrizione della violazione, i contatti del DPO, le probabili conseguenze e i consigli per tutelarsi. La comunicazione non è necessaria in specifiche condizioni (es. dati cifrati, misure successive che evitano il rischio elevato, sforzi sproporzionati).

6. Chiusura, Reporting e Analisi Post-Incidente (Remediation Plan):

Al termine della gestione, si procede alla chiusura dell'evento e alla redazione di un report dettagliato sull'intero processo di gestione dell'incidente, inviato al Responsabile della Sicurezza Informatica.

Il Comitato di Crisi redige il Piano di risposta agli incidenti (Remediation Plan) che definisce le procedure specifiche per ripristinare la normale operatività e minimizzare l'impatto sugli interessati, garantendo la continuità operativa. Tale piano deve essere periodicamente testato attraverso simulazioni.

Il DPO conduce una verifica post-incidente per valutare l'efficacia della risposta, l'adeguatezza delle misure preventive esistenti e identificare eventuali lacune nei sistemi di sicurezza, informandone il Comitato di Crisi. Redige un rapporto per il Titolare.

Le politiche e le procedure interne saranno aggiornate in base ai risultati delle verifiche per migliorare la gestione dei trattamenti dei dati personali e prevenire lacune nei sistemi di sicurezza e future violazioni.

5.5. Modulo di Implementazione delle Misure Minime di Sicurezza ICT (MMS-PA)

Le modalità con cui ciascuna delle misure minime di sicurezza ICT (MMS-PA) è implementata presso l'Amministrazione devono essere sinteticamente riportate nel modulo di implementazione di cui all'allegato 2 della Circolare AgID n. 2/2017.

Tale modulo deve essere firmato digitalmente con marcatura temporale dal responsabile dell'attuazione delle misure e dal Rappresentante legale, conservato e, in caso di incidente informatico, trasmesso al CERT-PA insieme con la segnalazione dell'incidente stesso.

7. Continuità Operativa (Business Continuity - BC) e Disaster Recovery (DR)

La Continuità Operativa (Business Continuity - BC) e il Disaster Recovery (DR) sono elementi fondamentali per garantire l'erogazione dei servizi, in particolare per le Pubbliche Amministrazioni (PA), a fronte di eventi imprevisti e potenzialmente disastrosi. L'obiettivo è assicurare che l'organizzazione possa continuare a fornire prodotti o servizi a livelli predefiniti accettabili anche in seguito a interruzioni.

1. Contesto Normativo e Standard di Riferimento:

Le PA sono tenute a predisporre piani di emergenza per assicurare la continuità delle operazioni, come indicato dall'Art. 51, comma 2-quater, del Codice dell'Amministrazione Digitale (CAD). L'Agenzia per l'Italia Digitale (AgID) definisce le linee guida tecniche e verifica annualmente l'aggiornamento dei piani di Disaster Recovery.

Le Misure Minime di Sicurezza ICT per le Pubbliche Amministrazioni (MMS-PA), stabilite dalla Circolare AgID 18 aprile 2017, n. 2/2017, devono essere adottate per contrastare le minacce più comuni ai sistemi informativi e sono richiamate per l'attuazione delle Linee Guida sulla formazione, gestione e conservazione dei documenti informatici.

ACI Informatica si è dotata di un Sistema di Gestione della Continuità Operativa (BCMS) progettato e realizzato in conformità con la norma ISO 22301:2019, detenendo inoltre le certificazioni ISO 27001 (sicurezza IT), ISO 20000 (gestione servizi IT) e UNI EN ISO 9001 (qualità).

Le politiche di sicurezza sono allineate a standard e best practice internazionali come ISO/IEC 27001, ISO/IEC 27035:2016, ITIL v3, ENISA e SANS Institute, ISO/IEC 27701.

2. Obiettivi e Parametri Chiave della Continuità Operativa:

Per i servizi in ambito BC, ACI Informatica definisce e monitora i seguenti parametri:

- Recovery Time Objective (RTO): Il tempo massimo di ripristino del servizio. È fissato a 24 ore, includendo 8 ore per la dichiarazione di disastro, 6 ore per la messa a disposizione del sito di recovery e il trasferimento del personale, e 10 ore per la ripartenza delle applicazioni.

- Recovery Point Objective (RPO): Il valore massimo di perdita dei dati tollerabile. ACI Informatica mira a 0, ovvero nessuna perdita di dati.

- Maximum Tolerable Data Loss (MTDL): La massima perdita di dati tollerata, tendente al 100% di salvaguardia della coerenza e consistenza dei dati.

- Minimum Business Continuity Objective (MBCO): Il livello di servizio minimo accettabile. Si prevede un decremento massimo del 10% delle prestazioni delle applicazioni durante l'erogazione dal sito secondario.

- Maximum Tolerable DownTime (MTDT): Il massimo intervallo di tempo ammissibile di interruzione della disponibilità del sito primario, fissato a 6 mesi.

3. Struttura Organizzativa per la Gestione della Continuità Operativa:

ACI Informatica ha istituito strutture permanenti per la Business Continuity, che includono:

- Unità di Crisi: la struttura centrale per la gestione delle emergenze. Ha la responsabilità di dichiarare ufficialmente lo stato di crisi, notificare formalmente la "Dichiarazione di Disastro" ad ACI e ad Enti Esterni, attivare le procedure operative e organizzative, attivare il sito secondario e monitorare l'andamento del ripristino. Si occupa anche dell'organizzazione del rientro sul sito primario. La sua composizione include figure

apicali come il Direttore Generale, il Business Continuity Manager, il Responsabile Sicurezza Aziendale e il Responsabile Sicurezza Informatica. All'interno dell'Unità di Crisi operano una Unità Tecnologica (composta da DSII e ACI Informatica, con sede nella War Room) e una Unità Strategica (composta dai membri permanenti per le decisioni strategiche e comunicazionali).

- Gruppo di Coordinamento Squadre: Costituito dai responsabili dei settori operativi, è coinvolto sia nella gestione ordinaria del piano (aggiornamento, approvazione modifiche, pianificazione test) sia in condizioni di emergenza (valutazione del danno, coordinamento delle squadre di intervento, comunicazione con l'Unità di Crisi).

- Squadre di Intervento: Personale tecnico-operativo dell'IT Operation, dei Gruppi Applicativi e della Security Operation, organizzato in squadre e reperibile per le attività di ripristino.

- Il Responsabile della struttura per l'organizzazione, l'innovazione e le tecnologie (o dirigente designato, spesso il Responsabile per la Transizione Digitale - RTD) ha la responsabilità dell'attuazione delle MMS-PA. Il Responsabile della Sicurezza Informatica spesso svolge il ruolo di "Segretario della Business Continuity", curando la gestione operativa del piano e la distribuzione della documentazione.

4. Strategie e Misure Tecniche e Organizzative:

La definizione delle misure di protezione si basa su analisi del rischio (Risk Assessment - RA) e analisi di impatto sul business (Business Impact Analysis - BIA), che identificano servizi essenziali, impatti e tempi massimi di indisponibilità.

- Continuità sul Sito Primario: L'infrastruttura di ACI Informatica è progettata per alta affidabilità, con sistemi ridondati, distribuzione su più sale CED per resilienza, bilanciamento del carico e soluzioni di backup veloci.

- Continuità sul Sito Secondario: ACI Informatica si avvale di un data center esterno, configurato in modalità "Campus" con il primario. La soluzione tecnica prevede:

    - Replica sincrona dei dati: L'intera base informativa e di sistema è replicata in sincrono, garantendo che ogni modifica sia contemporaneamente registrata sul sito primario e sul secondario, minimizzando la perdita di dati;

    - Connettività dedicata: La comunicazione tra i due Data Center avviene tramite due circuiti in fibra scura con percorsi distinti, permanentemente attivi per la replica dei dati;

    - Risorse HW e SW disponibili: Il sito secondario dispone di hardware e software necessari per la ripartenza delle applicazioni critiche in caso di disastro;

    - Spazio logistico: È previsto uno spazio di appoggio per il personale che deve operare al sito secondario.

- Gestione Quotidiana della BC: Comporta la verifica e il controllo continuo dei sistemi di storage, dell'allineamento della replica, dei collegamenti in fibra e delle configurazioni hardware e software.

- Procedure di Backup: Oltre alla replica sincrona, i salvataggi delle basi dati sul sito primario vengono copiati progressivamente, in modalità asincrona, su un Datadomain sul sito secondario. È in fase di realizzazione anche la collocazione di un terzo Datadomain, replica del primario, presso un terzo sito.

5. Il Contingency Plan:

Il Contingency Plan è l'insieme di manuali e procedure che descrivono le azioni da intraprendere prima, durante e dopo la dichiarazione dello stato di crisi. È composto dal Manuale Organizzativo (che descrive le funzioni, i ruoli e le responsabilità) e dal Manuale Tecnico (che dettaglia le operazioni tecniche di recupero). Le fasi previste sono:

- Notifica ed Attivazione: Le azioni da svolgere quando si registra o si prevede un'emergenza, allertando il personale preposto e stabilendo il danno. L'attivazione del piano avviene se la valutazione del danno indica un tempo di ripristino sul sito primario superiore alle 6 ore;
- Valutazione del Danno: L'individuazione della natura e dell'estensione del danno subito per determinare gli interventi necessari;
- Recovery sul Sito Secondario: Le procedure dettagliate per attivare i server di infrastruttura e di servizio, verificare la rete, attivare i database server (con verifica della consistenza dei dati), i web e application server e riattivare il servizio;
- Rientro sul Sito Primario: Le operazioni da eseguire al termine della fase di emergenza per ripristinare l'operatività standard, inclusa la sincronizzazione delle basi dati, le prove e lo switch back della rete.