



Manuale di gestione documentale – Approvazione

Il Consiglio di Amministrazione nella riunione del 23 giugno 2025 ha adottato all'unanimità dei presenti la seguente deliberazione n. **24/2025**

### **IL CONSIGLIO DI AMMINISTRAZIONE**

VISTO il Decreto Legislativo 31 dicembre 2009, n. 213 “Riordino degli Enti di Ricerca in attuazione dell’art. 1 della Legge 27 settembre 2007, n. 165”;

VISTO lo Statuto dell’Istituto Italiano di Studi Germanici (IISG), emanato con delibera del CdA n. 16/2021 del 30/4/2021;

VISTO il Regolamento di funzionamento e organizzazione approvato con Decreto del 15 marzo 2006;

VISTO il Regolamento di amministrazione, finanza e contabilità dell’IISG emanato con Delibera del CdA n. 29/2021 del 24/09/2021;

VISTO il Regolamento del personale dell’IISG approvato con Delibera del CdA n. 22/2022 del 30/05/2022;

VISTO il Decreto Legislativo 25 novembre 2016, n. 218 “Semplificazione delle attività degli enti pubblici di ricerca ai sensi dell’articolo 13 della legge 7 agosto 2015, n. 124”;

VISTO il decreto legislativo 30 marzo 2001, n. 165, recante “Norme generali sull’ordinamento del lavoro alle dipendenze delle pubbliche amministrazioni”, e successive modificazioni e integrazioni;

VISTA la Legge 7 agosto 1990, n. 241 recante “Nuove norme in materia di procedimento amministrativo e di diritto d’accesso ai documenti amministrativi” e ss.mm.ii.;

VISTO il D.P.R. 28 dicembre 2000, n. 445 concernente “T.U. delle disposizioni legislative e regolamentari in materia di documentazione amministrativa” e ss.mm.ii.;



VISTO il D. Lgs. 7 marzo 2005, n. 82 concernente “Codice dell'Amministrazione Digitale” (CAD) e ss.mm.ii;

VISTO il D.L. 14 marzo 2013 n. 33 recante “Riordino della disciplina riguardante gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni” e ss.mm.ii.;

VISTO il D.lgs. 30 giugno 2003, n. 196, concernente “Codice in materia di protezione dei dati personali”;

VISTO il Regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE regolamento generale sulla protezione dei dati pubblicato sulla Gazzetta Ufficiale Europea del 4 maggio 2016 ed applicabile a decorrere dal 25 maggio 2018;

VISTO il D.lgs. 11 aprile 2006, n. 198 “Codice delle pari opportunità tra uomo e donna”, come modificato dal D.lgs. 25 gennaio 2010 n.5, in attuazione della direttiva 2006/54/CE;

VISTA la determina dell'AgID 9/9/2020 n. 407/2020, ad oggetto: “Adozione delle Linee Guida sulla formazione, gestione e conservazione dei documenti informatici”, nonché la determina 17/05/2021 n. 271/2021 di modifiche al testo e agli allegati delle Linee Guida citate e definizione della nuova versione delle Linee Guida

VISTA la presa d'atto del Collegio dei revisori dei conti nella riunione del 20/6/2025 con verbale n. 6/2025;

RITENUTA la necessità di provvedere;

### **DELIBERA**

1. Di approvare il Manuale di gestione documentale dell'Istituto Italiano di Studi Germanici di cui all'allegato 1 che costituisce parte integrante della presente deliberazione.
2. Di dare mandato al Direttore Amministrativo di porre in essere tutti gli atti conseguenti.

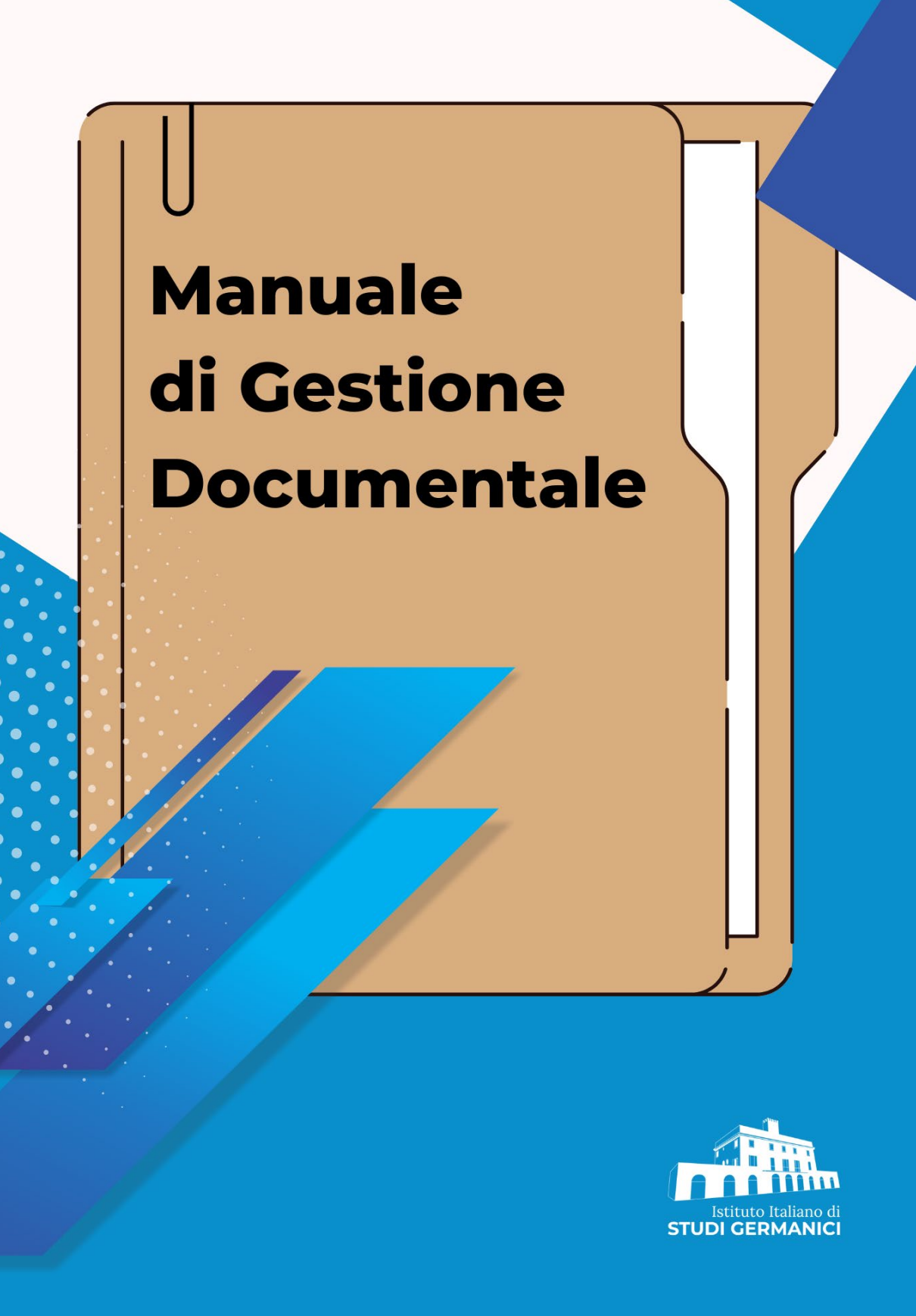


Istituto Italiano di  
**STUDI GERMANICI**

3. Di dare mandato al Responsabile della gestione documentale IISG pro-tempore di provvedere agli aggiornamenti del Manuale di gestione documentale che si rendessero necessari per l'adeguamento normativo/funzionale.

IL PRESIDENTE  
(*Prof. Luca Crescenzi*)

IL DIRETTORE AMMINISTRATIVO  
nella funzione di Segretario  
Verbalizzatore  
(*Roberto Tatarelli*)



# **Manuale di Gestione Documentale**



Istituto Italiano di  
**STUDI GERMANICI**

**Autore:** Eleonora De Longis (Responsabile Biblioteca e Archivi storici)  
**Versione:** 1.0 - Versione secondo lo schema AgID con allegati  
**Data emissione:** 16 giugno 2025

© Copyright Istituto Italiano di Studi Germanici  
Via Calandrelli, 25 00153 Roma

# **Manuale di Gestione Documentale**



Istituto Italiano di  
**STUDI GERMANICI**

---



# INDICE

## **7 Introduzione e principi generali della gestione documentale**

### **9 Il manuale di gestione**

- 9 Manuale di gestione documentale: caratteristiche e contenuti
- 10 Competenze richieste e principi guida
- 11 Integrazione con altri strumenti dell'Istituto
- 12 Modalità di pubblicità e diffusione
- 12 Principali normative di riferimento
- 14 Tutela dei dati personali: GDPR e D.Lgs 196/2003

### **17 Il quadro organizzativo istituzionale**

- 17 Area Organizzativa Omogenea e Unità Organizzativa Responsabile
- 18 Il Responsabile della Gestione Documentale
- 19 Responsabile del Servizio per la Tenuta del Protocollo Informatico, dei Flussi Documentali e degli Archivi
- 20 Funzioni del Servizio di Protocollo
- 21 Profili di Abilitazione nel Sistema di Gestione Documentale
- 21 Prassi Comportamentali per gli Utenti di Protocollo
- 22 Indirizzi di Posta Elettronica Certificata (PEC) Istituzionale
- 22 Indirizzi di Posta Elettronica Istituzionale
- 22 Responsabile della conservazione

### **23 Il documento**

- 23 Documento Informatico e Documento Analogico: Definizione e Caratteristiche
- 23 Caratteristiche del Documento Informatico
- 24 Formazione del Documento Informatico
- 25 Valore Giuridico e Probatorio
- 25 Contratti e Atti Giuridici
- 25 Formazione del Documento Amministrativo Informatico
- 26 Formazione del Documento Amministrativo Analogico
- 27 Firma Digitale e Conformità dei Documenti
- 27 Copia e Duplicato di Documenti
- 27 Posta Elettronica Certificata (PEC) e Altri Mezzi di Trasmissione
- 28 Formati di Documenti e Conservazione

### **29 I metadati**

- 29 Definizione e funzioni
- 29 Categorie di Metadati
- 30 Metadati Archivistici
- 31 Metadati di Registrazione a Protocollo
- 31 Metadati del Fascicolo Informatico
- 31 Metadati del Registro Giornaliero

### **33 Il fascicolo**

- 33 Fascicolo Analogico
- 34 Fascicolo Informatico
- 35 Fascicolo Ibrido
- 35 Altre Aggregazioni Documentali Informatiche
- 31 Metadati di Registrazione a Protocollo
- 31 Metadati del Fascicolo Informatico

### **37 L'archivio corrente**

- 37 Definizione e Attività
- 38 Strumenti dell'Archivio Corrente: Registri, Repertori, Titolare
- 39 Registro Giornaliero di Protocollo Informatico
- 39 Registrazione e Classificazione
- 39 Segnatura
- 40 Registrazione Differita e Annullamento
- 40 Ricevuta di Avvenuta Registrazione e Registro di Emergenza

### **41 Il flusso di lavorazione dei documenti**

- 41 Distinzione dei Documenti in Base allo Stato di Trasmissione
- 41 Flusso di Lavorazione del Documento Ricevuto-In Arrivo
- 41 Dettaglio delle Attività
- 42 Flusso di Lavorazione del Documento Inviato - In Partenza
- 42 Flusso di Lavorazione del Documento Interno
- 42 Flusso di Lavorazione del Documento da Altra Banca Dati/Online
- 42 Utilizzo delle Firme Elettroniche
- 42 Chiusura del Fascicolo

### **45 L'archivio di deposito**

- 45 Definizione
- 45 Trasferimento all'Archivio di Deposito
- 46 Trasferimento dei Fascicoli Informatici al Sistema di Conservazione
- 46 Elenco Topografico per l'Archivio Analogico
- 46 Registro di Carico e Scarico
- 47 Massimario di Selezione e Prontuario di Scarto
- 47 Selezione e Scarto dei Documenti Analogici
- 47 Selezione e Scarto dei Documenti Informatici
- 48 Conservazione dei Documenti

### **49 Il sistema informatico**

- 49 Definizione
- 49 Sicurezza del sistema informatico
- 49 Piano di sicurezza dei documenti informatici
- 50 Accesso al sistema informatico
- 50 Misure di sicurezza dei documenti informatici e protezione dei dati personali
- 51 Titolare del trattamento/Responsabile del trattamento/Incaricati del trattamento
- 51 Misure di sicurezza e policy

## INTRODUZIONE E PRINCIPI GENERALI DELLA GESTIONE DOCUMENTALE\*

La corretta gestione digitale dei documenti amministrativi, compresa la registrazione di protocollo, la classificazione, la fascicolazione, il reperimento e la conservazione dei documenti informatici, rappresenta una serie di attività comuni a tutte le amministrazioni pubbliche e agli enti. Questi processi sono fondamentali per garantire la continuità e l'efficienza operativa delle amministrazioni.

La gestione documentale può essere suddivisa in tre fasi principali: **formazione**, **gestione** e **conservazione**. Ogni fase prevede attività con caratteristiche specifiche, che si distinguono per la loro complessità, natura, impatto e finalità, e che possono anche avere rilevanza giuridica. Le metodologie e le prassi operative da adottare per ciascuna di queste attività devono essere adeguate alla fase corrispondente. Il sistema di gestione informatica dei documenti, che può essere delegato a terzi, deve essere presidiato da procedure e strumenti tecnologici idonei a monitorare e controllare tutte le operazioni che riguardano il ciclo di vita del documento. Inoltre, tali operazioni devono rispettare i principi generali del trattamento dei dati personali, inclusa un'adeguata analisi dei rischi.

Una corretta gestione dei documenti sin dal momento della loro creazione è essenziale per assicurare il rispetto degli obblighi amministrativi, giuridici e archivistici tipici della gestione dei documenti pubblici. Dal punto di vista archivistico, la gestione dei documenti si articola in tre fasi distinte:

**Archivio corrente:** riguarda i documenti necessari per le attività quotidiane in corso.

**Archivio di deposito:** riguarda i documenti ancora utili per finalità amministrative o giuridiche, ma che non sono più indispensabili per le attività correnti.

\*Si veda AgID, [Linee Guida sulla formazione, gestione e conservazione dei documenti informatici](#).

**Archivio storico:** include i documenti selezionati per essere conservati in modo permanente per il loro valore storico.

Nella fase di formazione dei documenti devono essere perseguiti obiettivi di qualità, efficienza, razionalità, sistematicità, accessibilità e conformità alle regole tecniche, tenendo conto delle esigenze pratiche del lavoro quotidiano. Per ottenere questi risultati, è fondamentale disporre di un valido **manuale di gestione documentale**, sistemi di **Document & Content Management** e strumenti informatici specifici per la Pubblica Amministrazione, in conformità con gli articoli 65 e 68 del **Codice dell'Amministrazione Digitale (CAD)**. Tali strumenti devono basarsi su elevati livelli di automazione e interoperabilità, operando efficacemente in ambienti digitali come il web.

La gestione dei documenti prosegue con la loro conservazione, che deve avvenire in conformità alle disposizioni del **CAD**. Il processo di conservazione è generalmente affidato a sistemi specifici dedicati a questa funzione. Tuttavia, l'attenzione agli aspetti conservativi deve essere posta fin dal momento della creazione del documento, per garantirne la corretta gestione e conservazione nel lungo termine all'interno dei sistemi informatici dedicati.

Nel corso della gestione documentale possono essere necessarie operazioni di **riversamento** dei documenti in formati diversi da quelli originali. Tali operazioni possono avvenire più volte nel ciclo di vita del documento, sia per scopi gestionali sia per esigenze di conservazione a lungo termine.

Infine, gli obblighi di pubblicazione di atti e provvedimenti amministrativi, che hanno valore di pubblicità legale o che sono richiesti dalle normative sulla trasparenza, devono essere rispettati attraverso la pubblicazione sui siti web istituzionali. Per garantire la validità legale e l'efficacia della pubblicazione online, è necessario che il processo assicuri la conformità dei documenti pubblicati all'originale, l'autorevolezza dell'ente pubblicante e la credibilità del sito web. Solo così si potrà garantire che i documenti mantengano la loro validità giuridica, la loro veridicità e la loro efficacia nel tempo.

## IL MANUALE DI GESTIONE

### *Manuale di gestione documentale: caratteristiche e contenuti*

Il **Manuale di gestione documentale** è uno strumento fondamentale di *governance* e pianificazione per l'Istituto Italiano di Studi Germanici (IISG). La sua importanza risiede nella capacità di strutturare e rendere efficiente l'intero ciclo di vita dei documenti prodotti o acquisiti dall'Istituto, che rappresentano il cuore delle attività amministrative, scientifiche e di ricerca. Ogni documento, infatti, costituisce un elemento essenziale per garantire la trasparenza, la legalità e la tracciabilità delle azioni dell'Istituto.

Il **Manuale** fornisce una serie di regole e indicazioni operative che permettono di governare tutti i processi legati alla documentazione, dal momento della sua creazione fino alla conservazione e, nel caso, alla sua eliminazione.

Il documento descrive in modo sistematico e organico le attività relative alla gestione documentale, includendo ogni fase del trattamento dei documenti: dalla **formazione e ricezione**, alla **registrazione e classificazione**, fino all'**organizzazione, assegnazione e reperimento** dei documenti stessi. Ogni passaggio è normato per garantire che i documenti, siano essi prodotti internamente o acquisiti da fonti esterne, siano trattati secondo i più alti standard archivistici e nel pieno rispetto delle normative vigenti.

Il **Manuale** non si limita a fornire una descrizione delle operazioni di routine, ma costituisce una guida essenziale per assicurare che tutte le attività documentali siano condotte in conformità con le disposizioni di legge, in particolare nel rispetto delle normative italiane in tema di gestione e conservazione dei documenti informatici. Questo aspetto diventa cruciale in un contesto, come quello dell'IISG, che non solo opera all'interno di un quadro normativo ben definito, ma che deve anche assi-

curare la **compliance** con le normative di settore e con le **best practices** internazionali per la gestione della documentazione, sia in formato analogico sia digitale.

Nell'ambito della gestione documentale, il **Manuale** svolge un ruolo di **governance informativa**, fungendo da strumento che mette ordine tra i numerosi processi documentali interni all'IISG. Esso consente di avere un controllo diretto e costante sulla documentazione, garantendo che questa venga trattata in maniera adeguata e in modo conforme alle politiche di conservazione, alla protezione dei dati personali e agli obblighi di trasparenza previsti per le Pubbliche Amministrazioni.

L'Istituto, come ogni ente pubblico, è tenuto ad adottare formalmente e a pubblicare sul proprio sito istituzionale il **Manuale di gestione documentale**, in un'apposita sezione identificabile dell'area «Amministrazione trasparente», in conformità a quanto stabilito dall'articolo **9 del d.lgs. 33/2013**. Questo obbligo di pubblicazione garantisce che il Manuale stesso sia accessibile, trasparente e utilizzabile da tutti gli utenti interessati, *stakeholders* sia interni sia esterni all'Istituto.

A partire dal 8 novembre 2023, l'Istituto Italiano di Studi Germanici ha adottato un nuovo sistema di gestione documentale, in conformità alle normative più recenti e alle innovazioni tecnologiche. Per facilitare l'adozione di questo sistema e garantire una transizione efficace dal precedente, sono state predisposte delle note operative (vedi Allegato 1), pensate per offrire una guida pratica agli utenti che si trovano ad approcciarsi al nuovo programma. Queste note, integrate al presente manuale, rappresentano un importante strumento per il corretto utilizzo del sistema.

## Competenze richieste e principi guida

La redazione del **Manuale di gestione documentale** risponde sia all'obbligo normativo sia alla necessità di soddisfare le esigenze operative dell'Istituto Italiano di Studi Germanici. Per questo motivo, il manuale è stato redatto dopo un'attenta verifica e analisi del modello organizzativo e delle procedure amministrative dell'Istituto. La stesura del documento ha seguito il modello previsto dalle **Linee Guida sulla formazione**,

**gestione e conservazione dei documenti informatici**, pubblicate dall'**AgID**, di seguito abbreviate come «Linee Guida».

Inoltre, la redazione del **Manuale** richiede competenze interdisciplinari, che comprendono l'informatica, l'informatica giuridica, il diritto amministrativo, l'archivistica, la sicurezza e la privacy.

A tal fine, l'Istituto adotta un piano di formazione obbligatoria e periodica per il personale coinvolto nella gestione documentale, comprensivo di aggiornamenti su:

- normativa vigente (CAD, GDPR, Linee Guida AgID),
- strumenti digitali e pratiche archivistiche,
- sicurezza informatica e protocolli di emergenza.

La formazione sarà documentata e verificata con cadenza almeno annuale.

La conformità alle normative vigenti, in particolare per quanto riguarda la gestione documentale e la protezione dei dati, è assicurata dall'adozione di strumenti e procedure che rispettano pienamente le disposizioni del **Regolamento Generale sulla Protezione dei Dati (GDPR)**.

Il **Manuale** rappresenta un passo importante per l'IISG verso l'attuazione dei principi guida dell'azione amministrativa, che comprendono **efficacia, efficienza, economicità e trasparenza**, così come richiesto dalle normative italiane, in particolare il **d.lgs. 33/2013**.

Il documento presente rappresenta una sintesi armonica di normative nazionali e specifiche esigenze dell'IISG. Integra la disciplina archivistica, le procedure operative degli uffici dell'Istituto e il sistema informatico utilizzato, garantendo al contempo la piena **compliance** con gli standard più avanzati di gestione documentale.

## ***Integrazione con altri strumenti dell'Istituto***

Il **Manuale** di gestione documentale si integra perfettamente con altri strumenti e regolamenti già adottati dall'Istituto Italiano di Studi Germanici, come il **manuale di conservazione**, il **piano di sicurezza dei dati**, le **linee guida per la pubblicazione delle informazioni**, il **piano triennale anticorruzione** e

il **regolamento per l'accesso agli atti amministrativi**. Questi strumenti, insieme al **Manuale**, assicurano una gestione integrata e coordinata della documentazione, garantendo che l'IISG operi in modo trasparente, sicuro ed efficiente.

In definitiva, l'IISG, grazie all'adozione del **Manuale di gestione documentale** e degli strumenti correlati, si impegna a mantenere elevati standard di **compliance**, fornendo al contempo un modello organizzativo che risponde pienamente alle esigenze normative e operative della Pubblica Amministrazione.

### **Modalità di pubblicità e diffusione**

Il manuale è reso pubblico mediante la pubblicazione sul sito istituzionale <https://www.studigermanici.it/> nella sezione «**Amministrazione trasparente**». Sarà inoltre distribuito a tutte le unità organizzative dell'Area Organizzativa Omogenea (AOO) dell'Istituto Italiano di Studi Germanici, al fine di garantire una completa diffusione delle nozioni e delle procedure documentali.

È prevista una revisione almeno annuale del contenuto pubblicato, a cura del Responsabile della gestione documentale, per garantire che la versione online sia sempre aggiornata e conforme alle modifiche normative e organizzative. Eventuali revisioni sono accompagnate da un registro delle versioni, allegato al documento stesso, e da una determina interna che ne autorizza la pubblicazione aggiornata.

### **Principali normative di riferimento**

Riferimenti normativi contenuti nel **Manuale**:

**CAD** = *D.lgs. 82/2005 e ss.mm.ii., Codice dell'amministrazione digitale;*

**TUDA**= *D.P.R. 445/2000, Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa;*

**Linee Guida** = *Linee Guida sulla formazione, gestione e conservazione dei documenti informatici 2020 – 2021, Legge 241;*

**CC** = *Codice Civile;*

**Codice dei beni culturali** = *D. lgs 42/2004, Codice dei beni culturali e del paesaggio, ai sensi dell'articolo 10 della legge 6 luglio 2002, n. 137;*

Inoltre:

**Decreto legislativo n. 196 del 30 giugno 2003** - *Codice in materia di protezione dei dati personali;*

**Decreto del 2 novembre 2005 – MIT** – *Regole tecniche per la formazione, la trasmissione e la validazione anche temporale della posta elettronica certificata;*

**DPR 633/1972 art.39 in vigore dal 1 gennaio 2013**  
–**Modificato da: Legge del 24/12/2012 n. 228 Art. 1** – *Le fatture elettroniche in formato elettronico e quelle cartacee possono essere conservate elettronicamente;*

**Decreto del Presidente del Consiglio dei Ministri (DPCM) del 22 febbraio 2013** - *Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali, ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma 3, lettera b), 35, comma 2, 36, comma 2, e 71;*

**DPCM del 3 dicembre 2013** -

*Regole tecniche per il protocollo informatico (Artt. 40 bis, 41, 47 e 71 del CAD)*

*Regole tecniche in materia di sistema di conservazione (Artt. 20 c.3 e c.5-bis, 23-ter, comma 4, 43, c. 1 e 3, 44, 44-bis e 71 c. 1)*

**DPCM del 13 novembre 2014** – *Regole tecniche in materia di formazione / trasmissione / copia / duplicazione / riproduzione e validazione temporale dei documenti informatici delle Pubbliche amministrazioni;*

**Regolamento generale per la protezione dei dati personali n. 2016/679, (General Data Protection Regulation o GDPR) - Normativa europea in materia di protezione dei dati del 24/05/2016.**

**Tutela dei dati personali: GDPR e D.Lgs. 196/2003**

L'Istituto Italiano di Studi Germanici (IISG) è un Ente Pubblico di Ricerca e, pertanto, nella gestione dei documenti amministrativi contenenti dati sensibili è tenuto a rispettare il Regolamento Generale sulla Protezione dei Dati Personali (GDPR), al momento della protocollazione. Gli operatori abilitati ad accedere al sistema di protocollo informatico (i protocollatori), nominati dal Responsabile della Gestione Documentale, devono osservare comportamenti adeguati previsti dal loro incarico, come riservatezza, uso di credenziali personali e non condivisibili, bloccare il computer in caso di assenza, evitare di diffondere informazioni personali riservate, ecc. Inoltre, l'IISG assicura che i documenti trasmessi contengano esclusivamente le informazioni richieste dalla legge e dai regolamenti, necessarie per le finalità perseguite.

Per quanto riguarda la protezione dei dati personali trattati, l'IISG afferma di aver rispettato quanto stabilito dal GDPR e dal D.Lgs. 196/2003:

- Nominare un Responsabile della Protezione dei Dati (Data Protection Officer), incaricato di facilitare l'attuazione del regolamento da parte del titolare del trattamento dei dati;
- Garantire la riservatezza dei dati, impedendo l'accesso a persone non autorizzate;
- Seguire procedure di sicurezza standard e verificare le misure tecniche implementate per assicurare l'integrità dei sistemi e dei servizi di trattamento;
- Ripristinare prontamente la disponibilità e l'accesso ai dati personali in caso di incidenti fisici o tecnici, informando immediatamente il Garante Privacy in caso di violazione o attacco informatico (data breach);
- Effettuare la valutazione dell'impatto delle violazioni (Data Protection Impact Assessment);
- Tenere un registro delle attività di trattamento.

Secondo l'art. 5 del GDPR e considerando che le Pubbliche Amministrazioni devono avere un sistema documentale conforme ai requisiti del Regolamento Europeo e al principio di tracciabilità dell'azione amministrativa, è necessario:

- Assegnare un'identificazione univoca a ciascun documento creato o acquisito, attraverso la registrazione di informazioni descrittive e la sua classificazione per facilitare il recupero e provare la sua esistenza (elementi presenti nel sistema di protocollo informatico);
- Definire i diritti di accesso ai documenti in base ai dati personali trattati, stabilendo specifici permessi per ogni utente del protocollo;
- Determinare i tempi di conservazione a partire dalla creazione del documento, mediante un piano di conservazione;
- Garantire la tracciabilità dei dati e dei documenti attraverso un'infrastruttura informatica avanzata.

In conformità agli articoli 5, 25 e 30 del GDPR, nonché al D.Lgs. 196/2003, l'Istituto definisce in modo esplicito:

- i **tempi di conservazione** dei dati personali associati ai documenti amministrativi, in coerenza con il piano di conservazione e con il massimario di selezione approvato;
- le **modalità di cancellazione, anonimizzazione o pseudonimizzazione** dei dati alla scadenza del periodo di conservazione previsto, inclusi i meccanismi automatici ove supportati dal sistema informatico;
- la **documentazione dei trattamenti** tramite un **registro delle attività**, aggiornato con cadenza almeno semestrale dal Responsabile della Protezione dei Dati (DPO);
- la **valutazione dell'impatto sulla protezione dei dati (DPIA)** nei casi in cui il trattamento documentale possa comportare rischi elevati per i diritti e le libertà degli interessati;
- la **formazione obbligatoria del personale autorizzato al trattamento**, con tracciamento delle attività formative e aggiornamento annuale dei contenuti in collaborazione con il DPO;
- l'adozione di misure tecniche e organizzative che garantiscano **riservatezza, integrità, disponibilità e resilienza dei dati**, inclusi:
  - sistemi di controllo degli accessi e logging;
  - segmentazione degli ambienti informatici;

- backup e piani di continuità operativa in caso di data breach o incidente.

Infine, è importante ricordare che i sistemi di gestione documentale adottati sono progettati per limitare i rischi che possono minacciare i dati contenuti nei documenti amministrativi. Tali misure sono applicate anche ai sistemi di conservazione, per garantire la rintracciabilità, l'integrità e la riservatezza dei documenti, in conformità ai principi stabiliti dal Regolamento Europeo.

## IL QUADRO ORGANIZZATIVO ISTITUZIONALE

### ***Area Organizzativa Omogenea e Unità Organizzativa Responsabile***

L'Area Organizzativa Omogenea (AOO), secondo quanto definito dall'art. 50, comma 4, e dall'art. 61 del DPR 445/2000 (TUDA), rappresenta un insieme di unità organizzative all'interno di un'amministrazione che utilizzano in modo uniforme e coordinato i servizi informatici per la gestione dei flussi documentali. Ogni AOO fornisce un servizio di protocollo per la registrazione e gestione dei documenti in entrata e in uscita, utilizzando una sequenza numerica unica e specifica per ciascuna AOO, nonché strumenti per la gestione elettronica dei documenti.

Le AOO sono fondamentali per garantire l'efficienza della gestione documentale in un'ottica coordinata e unitaria, assicurando criteri uniformi di classificazione, protocollazione e archiviazione dei documenti, sia analogici che digitali. Questo modello organizzativo permette alle amministrazioni di mantenere standard uniformi tra le diverse AOO, facilitando la comunicazione interna e garantendo il rispetto delle normative in materia di gestione documentale.

Nell'ambito dell'Istituto Italiano di Studi Germanici (IISG), è stato adottato un modello organizzativo basato su un'AOO, con codice univoco A69665C, descritta nell'[Indice dei domicili digitali delle Pubbliche Amministrazioni \(IPA\)](#). Il Servizio per la tenuta del protocollo informatico e per la gestione dei flussi documentali e degli archivi è collocato sotto la responsabilità diretta della stessa AOO.

L'AOO si avvale di 2 Unità Organizzative (UO), che rappresentano un complesso di risorse umane e strumentali a cui è affidata la gestione specifica di affari e procedimenti amministrativi: «Uff\_eFatturaPA», con codice univoco UFS25E, e «Ufficio per la transizione al Digitale» con codice univoco

ZRRVBI (nell'[Indice dei domicili digitali delle Pubbliche Amministrazioni, IPA](#)).

Questo sistema garantisce che le operazioni di protocollazione e gestione dei documenti avvengano in modo coordinato e conforme alle disposizioni normative, preservando l'integrità e la sicurezza delle informazioni trattate, nel rispetto dei criteri di tracciabilità e trasparenza amministrativa.

## ***Il Responsabile della Gestione Documentale***

Il Responsabile della Gestione Documentale (nel seguito RGD), secondo quanto stabilito dall'art. 61, comma 3, del DPR 445/2000 e dall'art. 4 del DPCM del 3 dicembre 2013 sul protocollo informatico (ad esclusione della lettera c del comma 1 e del comma 2), ha il compito di:

- Definire i livelli di autorizzazione per l'accesso alle funzioni del sistema, distinguendo tra abilitazioni alla consultazione e abilitazioni all'inserimento e modifica delle informazioni;
- Assicurare che le operazioni di registrazione e segnatura di protocollo siano conformi alle normative vigenti;
- Conservare le copie di backup previste dagli articoli 62 e 63 del DPCM del 3 dicembre 2013;
- Garantire il corretto funzionamento degli strumenti e dell'organizzazione per la gestione dei documenti e dei flussi documentali;
- Autorizzare eventuali operazioni di annullamento;
- Verificare il rispetto delle disposizioni del manuale di gestione da parte del personale autorizzato.

Al fine di assicurare una gestione coerente, è opportuno che i ruoli del RGD, del Responsabile della Conservazione e del Responsabile del Trattamento dei Dati siano affidati a soggetti diversi, come indicato nelle Linee Guida AGID, per garantire indipendenza e presidio dei rispettivi ambiti di competenza.

Per garantire che il sistema documentale sia conforme alla normativa europea, il Responsabile deve definire i diritti di accesso ai documenti in base ai dati personali trattati. A tal fine, è necessario stabilire regole precise per tutti coloro che trattano dati personali, in conformità al GDPR e al Codice di compor-

tamento per i dipendenti delle Pubbliche Amministrazioni (art. 54 comma 5 del D.Lgs. 165/2001).

Tra le responsabilità del Responsabile rientrano anche:

- Implementare meccanismi adeguati per la tracciabilità dei flussi documentali;
- Nominare e gestire gli addetti al trattamento dei dati, rispettando criteri di trasparenza e principi etici, con la formalizzazione della nomina per gli addetti al protocollo (come indicato nell'Allegato 3);
- Formare e informare i collaboratori sulle procedure operative per il trattamento dei dati, trasferendo conoscenze e consapevolezza riguardo ai rischi;
- Redigere l'informativa sul trattamento dei dati registrati (Allegato 4).

### ***Responsabile del Servizio per la Tenuta del Protocollo Informatico, dei Flussi Documentali e degli Archivi***

Il Responsabile, come previsto dall'art. 61 del **TUDA**, è la figura incaricata di tutte le operazioni di registrazione, protocollo, organizzazione e gestione dei documenti all'interno dell'Area Organizzativa Omogenea (AOO). Questo responsabile ha il compito di garantire che il sistema di Protocollo Informatico, implementato all'interno dell'AOO, funzioni correttamente e nel rispetto delle normative vigenti, a beneficio non solo dell'amministrazione interna ma anche nei confronti di cittadini, imprese e altre amministrazioni pubbliche.

Le funzioni svolte sono regolate dagli art. 61 e 62 del **TUDA**, dall'art. 5 della Deliberazione CNIPA n. 11/2004 e dalle Regole Tecniche previste **CAD**.

Le principali attività che rientrano in questo ambito includono:

- Lo sviluppo e la gestione del protocollo informatico e del sistema di gestione documentale;
- L'analisi e gestione dei flussi documentali;
- La conservazione a norma della documentazione amministrativa;
- La gestione degli archivi.

Queste attività sono descritte nel dettaglio nei capitoli successivi del manuale.

## **Funzioni del Servizio di Protocollo**

Considerate le ridotte dimensioni dell'Ente le funzioni sono svolte dal RGD che cura la tenuta del protocollo informatico, la gestione dei flussi documentali e degli archivi e ha il compito di assicurare la corretta gestione e conservazione dei documenti durante l'intero ciclo di vita. Oltre a curare le operazioni di registrazione e archiviazione, si assicura che la normativa in materia di gestione documentale venga rispettata in ogni fase del processo.

Le principali funzioni includono:

- Attribuire i livelli di autorizzazione per l'accesso alle diverse funzioni del sistema, distinguendo tra autorizzazioni per la consultazione e quelle per l'inserimento o modifica delle informazioni;
- Garantire che le operazioni di registrazione e segnatura di protocollo vengano effettuate nel pieno rispetto delle disposizioni normative vigenti;
- Assicurare la corretta produzione e conservazione del registro giornaliero di protocollo;
- Ripristinare le funzionalità del sistema entro 24 ore in caso di guasti o anomalie, o comunque nel minor tempo possibile;
- Conservare copie dei documenti in luoghi sicuri e separati;
- Garantire il buon funzionamento degli strumenti e dell'organizzazione delle attività di protocollo, gestione documentale e flussi documentali, comprese le funzionalità di accesso ai documenti e la gestione degli archivi;
- Autorizzare eventuali operazioni di annullamento;
- Vigilare sull'osservanza delle normative vigenti da parte del personale incaricato.

Infine, è responsabile dell'adeguamento del sistema di gestione documentale in caso di modifiche all'organigramma o al funzionigramma dell'Istituto.

## ***Profili di Abilitazione nel Sistema di Gestione Documentale***

Presso l'IISG, il sistema di gestione documentale prevede la differenziazione dei profili utente tra:

- **Responsabile della Gestione Documentale:** con funzioni decisionali e di delega;
- **Amministratore di sistema:** con funzioni gestionali, subordinate alle decisioni del Responsabile della Gestione Documentale;
- **Utente di Protocollo o Protocollatore:** con funzioni operative;
- **Consultatore:** con funzioni di sola visualizzazione.

La protezione dei dati personali e sensibili è garantita.

## ***Prassi Comportamentali per gli Utenti di Protocollo***

Gli utenti di protocollo devono rispettare specifiche prassi comportamentali, tra cui:

- Non trasferire, comunicare o diffondere dati personali al di fuori della propria sede, salvo disposizioni normative specifiche;
- Operare esclusivamente sugli applicativi a cui hanno legittimo accesso, utilizzando gli strumenti forniti dall'amministrazione;
- Osservare rigorosamente gli obblighi di riservatezza riguardo ai dati personali;
- Non comunicare a terzi le proprie credenziali di accesso ai sistemi di protocollo o altri applicativi;
- Verificare, in caso di assenza temporanea dalla postazione di lavoro, che i dati personali non siano accessibili a terzi, adottando misure di sicurezza per i documenti sia analogici che informatici;
- Assicurarsi, durante le operazioni di registrazione, che nessuno possa visualizzare documenti riservati sullo schermo;
- Segnalare al Direttore o al Responsabile eventuali rischi per la sicurezza dei dati, come violazioni delle password o tentativi di accesso non autorizzato;
- Informare tempestivamente il Direttore o il Responsabile in caso di sospetta o confermata violazione dei dati personali.

## ***Indirizzi di Posta Elettronica Certificata (PEC) Istituzionale***

L'AOO mantiene le caselle PEC associate al registro di protocollo. In particolare, nel portale dell'indice dei domicili digitali delle Pubbliche Amministrazioni e dei gestori di pubblici servizi (IPA) è presente la PEC dell'Ente: <https://indicepa.gov.it/ipa-portale/consultazione/pec/ricerca-pec-ente/scheda-ente/12758>.

## ***Indirizzi di Posta Elettronica Istituzionale***

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

## ***Responsabile della conservazione***

Il sistema di conservazione della documentazione si basa su modelli organizzativi chiari, definiti e separati dal sistema di gestione documentale. Il Responsabile della conservazione collabora con il Responsabile del trattamento dei dati personali e con il Responsabile della sicurezza, oltre che con il Responsabile della gestione documentale. Per le funzioni e le attività relative alla conservazione della documentazione amministrativa, si fa riferimento al Manuale della Conservazione, come stabilito dalla normativa vigente.

# IL DOCUMENTO

## *Documento Informatico e Documento Analogico: Definizione e Caratteristiche*

Il **documento informatico** è un documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti. Si tratta di un file digitale, costituito da una sequenza di valori binari, indipendentemente dal supporto fisico utilizzato per la sua memorizzazione. Ogni documento informatico deve essere identificato in modo univoco e persistente; per i documenti protocollati, l'identificazione è garantita dalla segnatura di protocollo, mentre per i documenti non protocollati si utilizza un ID univoco assegnato dal sistema di gestione informatica.

Al contrario, il **documento analogico** rappresenta atti, fatti o dati rilevanti in formato non informatico, come ad esempio documenti cartacei. Pertanto, qualsiasi documento non digitale viene classificato come analogico.

### **Documento Amministrativo Informatico**

Il documento amministrativo informatico è una rappresentazione digitale, che può essere grafica, elettromagnetica o di altra natura, del contenuto di atti prodotti o utilizzati dalle pubbliche amministrazioni per finalità amministrative. La creazione di un documento amministrativo informatico richiede che siano rispettate le caratteristiche di immodificabilità e integrità, spesso garantite dalla registrazione nel registro di protocollo.

## *Caratteristiche del Documento Informatico*

**Riconducibilità all'Autore:** Per garantire la certezza dell'autore di un documento, è necessario che vi sia la possibilità di associare in maniera certa e permanente il soggetto che lo

ha sottoscritto. In assenza di prova contraria, si presume che l'uso di un dispositivo di firma sia riconducibile al suo titolare.

**Forma e Validità Giuridica:** Il documento informatico, come il documento analogico, deve soddisfare determinati requisiti giuridici per essere valido. La validità giuridica del documento informatico è legata alla pluralità di firme elettroniche che possono essere apposte: firma elettronica semplice, qualificata, digitale o avanzata. La firma elettronica non rappresenta una semplice trasposizione grafica della firma tradizionale, ma un meccanismo di associazione che garantisce la responsabilità giuridica del firmatario.

Quando la legge richiede espressamente la forma scritta, il documento informatico può soddisfare questo requisito solo se firmato con firma elettronica qualificata, digitale o avanzata. Negli altri casi, la validità del documento è soggetta alla valutazione del giudice, che considera la sicurezza, integrità e immodificabilità del documento stesso.

**Immodificabilità e Integrità:** Un documento informatico è considerato immodificabile se la sua memorizzazione digitale non permette alterazioni nel corso dell'accesso, gestione e conservazione. L'integrità, invece, implica che il documento resti completo e non alterato nel tempo. La data e l'ora di creazione sono opponibili a terzi se stabilite secondo le Linee Guida vigenti, mentre la sicurezza dipende dalla protezione contro modifiche non autorizzate e dall'assenza di codice maligno.

## **Formazione del Documento Informatico**

Il processo di formazione di un documento informatico può avvenire in diverse modalità:

- **Creazione mediante strumenti software o servizi cloud:** La produzione del documento deve seguire regole precise di interoperabilità. L'integrità e l'immodificabilità sono garantite da una o più operazioni, come l'apposizione di firme elettroniche qualificate o l'uso di sistemi di gestione documentale sicuri.

- **Acquisizione di documenti preesistenti:** Include l'acquisizione di documenti tramite modalità telematica, la conversione di documenti analogici in formato digitale o l'acquisizione di copie informatiche. Anche in questo caso, la sicurezza è garantita da firme elettroniche o memorizzazione in sistemi di gestione documentale conformi alle Linee Guida.
- **Memorizzazione su supporto informatico:** Include la registrazione di dati generati da transazioni o processi informatici. L'immodificabilità è garantita da processi di sicurezza che comprendono la firma elettronica qualificata, la conservazione in sistemi idonei e la registrazione dei log di sistema.

## **Valore Giuridico e Probatorio**

Il valore probatorio del documento informatico dipende dalla tipologia di firma utilizzata. Un documento firmato digitalmente soddisfa il requisito della forma scritta e ha piena validità giuridica, opponibile fino a querela di falso. Quando la forma scritta è richiesta dalla legge, come nei contratti immobiliari o in atti di grande rilevanza giuridica, la mancanza di una firma qualificata o digitale può determinare la nullità del documento. Tuttavia, anche documenti non firmati digitalmente possono essere valutati in giudizio, considerando sicurezza e integrità.

## **Contratti e Atti Giuridici**

Devono essere stipulati in forma scritta, pena la nullità, i contratti che coinvolgono beni immobili, usufrutti, servitù, diritti di superficie e altri diritti reali immobiliari. Anche i contratti che conferiscono godimenti di beni immobili devono rispettare tale requisito, soprattutto se hanno una durata superiore ai nove anni o sono di natura perpetua.

## **Formazione del Documento Amministrativo Informatico**

Il documento amministrativo informatico è soggetto alle stesse regole del documento informatico, con alcune specifiche parti-

colari. L'Istituto Italiano di Studi Germanici forma gli originali dei propri documenti utilizzando strumenti informatici oppure acquisendo istanze, dichiarazioni e comunicazioni previste dalla legge. I documenti formati digitalmente, insieme ai dati detenuti in formato informatico, costituiscono l'informazione primaria e originale da cui è possibile effettuare duplicazioni e copie. Questi documenti, così come le comunicazioni previste dalla normativa, devono essere registrati tramite il protocollo, repertoriati, segnati e fascicolati per garantire tracciabilità e sicurezza.

Il documento amministrativo informatico deve garantire caratteristiche di **immodificabilità** e **integrità**. Tali caratteristiche possono essere assicurate non solo attraverso la firma elettronica, ma anche tramite la registrazione nel registro di protocollo per ciascuna Area Organizzativa Omogenea (AOO), così come nei repertori, albi e archivi istituzionali. Di norma, il documento deve includere informazioni dettagliate come la denominazione dell'Istituto, l'indicazione dell'AOO/UOR, la data, la classificazione, il numero di allegati, l'oggetto, il destinatario, il testo, la sottoscrizione e gli elementi identificativi del responsabile del procedimento.

### **Formazione del Documento Amministrativo Analogico**

Nell'ambito amministrativo, il documento analogico è generalmente un documento prodotto su supporto cartaceo, utilizzando strumenti tradizionali (ad esempio, scrittura a mano) o sistemi informatici (ad esempio, stampa di un documento redatto digitalmente). L'originale analogico è la versione definitiva, completa di tutti gli elementi formali e sostanziali, tra cui sigilli, carta intestata e firme autografe. Di norma, i documenti analogici destinati a terzi sono prodotti in due copie: un originale per il destinatario e una minuta per la conservazione negli archivi dell'Istituto.

I documenti amministrativi analogici in uscita devono essere redatti su carta intestata e contenere le stesse informazioni dettagliate richieste per i documenti informatici. La sottoscrizione deve avvenire prima della protocollazione, e la data di firma e di protocollo coincidono solitamente.

## ***Firma Digitale e Conformità dei Documenti***

L'IISG ha dotato tutti i dipendenti di firma digitale, inclusi il Presidente, il Direttore Amministrativo. La firma digitale, così come altre forme di firme elettroniche qualificate o avanzate, garantisce la validità giuridica del documento informatico, rendendolo opponibile fino a querela di falso.

Le **copie di documenti informatici** devono mantenere la stessa efficacia probatoria dell'originale se la loro conformità è attestata da un pubblico ufficiale o se non viene contestata. In caso di assenza di attestazione ufficiale, la conformità può essere garantita da firme digitali o sigilli elettronici qualificati. Laddove richiesto, l'attestazione di conformità può essere inclusa nel documento informatico stesso o prodotta come documento separato con riferimento temporale.

## ***Copia e Duplicato di Documenti***

**Copie di Documenti Informatici:** Le copie hanno la stessa efficacia probatoria dell'originale se la conformità è garantita da un raffronto o da una certificazione di processo.

**Duplicati di Documenti Informatici:** Sono identici all'originale, mantenendo la stessa sequenza di valori binari, e non richiedono attestazioni di conformità per avere valore giuridico.

**Copie di Documenti Analogici:** Si distinguono in copia semplice, imitativa e conforme. La copia conforme è quella certificata da un pubblico ufficiale come autentica.

## ***Posta Elettronica Certificata (PEC) e Altri Mezzi di Trasmissione***

La **Posta Elettronica Certificata (PEC)** è uno strumento che garantisce la trasmissione legale di documenti, equivalente a una raccomandata con ricevuta di ritorno. La PEC consente di certificare l'invio e la consegna di un messaggio, inclusa la

data certa di spedizione e ricezione, rendendo i documenti trasmessi opponibili in giudizio. In caso di invio di documenti ufficiali tramite PEC, è consigliabile utilizzare un'unica PEC per ciascun documento da protocollare.

L'Istituto ha attivato specifiche caselle PEC associate al registro di protocollo e per la gestione della fatturazione elettronica.

## **Formati di Documenti e Conservazione**

L'IISG utilizza specifici formati standard per la creazione e gestione dei documenti, assicurando la leggibilità e la conservabilità nel tempo. Tra questi formati troviamo:

- **Documenti impaginati:** PDF, PDF/A, OOXML (.docx), ODT.
- **Dati strutturati:** SQL, CSV, JSON.
- **Posta elettronica:** EML, MBOX.
- **Presentazioni:** PPTX, ODP.
- **Immagini e multimedia:** JPEG, PNG, TIFF, MPEG4, FLAC.

La scelta dei formati è orientata verso standard aperti e ampiamente diffusi, in conformità all'art. 68 del CAD. L'Istituto si impegna a garantire, attraverso aggiornamenti periodici del piano dei formati, la preferenza per soluzioni open source e interoperabili, evitando l'utilizzo di formati proprietari non documentati, al fine di assicurare la piena portabilità e sostenibilità archivistica.

# I METADATI

## *Definizione e funzioni*

I **metadati** sono dati associati a un documento informatico, a un fascicolo o a un'aggregazione documentale, che servono a identificarli descrivendone contesto, contenuto e struttura. Questi dati sono fondamentali per gestire le informazioni nel tempo e facilitare l'interoperabilità e la ricerca. La definizione di metadati segue le linee guida stabilite dalle norme internazionali, come la **ISO 15489-1:2016** e la **ISO 23081-1:2017**, che specificano criteri di gestione e conservazione. La codifica dei caratteri utilizzata nei metadati può seguire standard come la **ISO 8859-1**, utilizzata per rappresentare alfabeti latini in contesti globali, garantendo compatibilità nei sistemi di scambio dati.

Le principali funzioni dei metadati sono:

- **Ricerca:** Permettono di individuare l'esistenza di un documento.
- **Localizzazione:** Consente di rintracciare un documento specifico.
- **Selezione:** Analisi e filtro di una serie di documenti per valutarne la rilevanza.
- **Interoperabilità Semantica:** Facilitano la ricerca trasversale in ambiti disciplinari diversi, grazie all'uso di equivalenze tra descrittori.
- **Gestione delle Risorse:** Coordinano le raccolte documentali attraverso banche dati e cataloghi.
- **Disponibilità:** Forniscono informazioni sull'effettiva disponibilità di un documento.

## *Categorie di Metadati*

**Metadati Descrittivi:** Identificano e facilitano il recupero degli oggetti digitali, descrivendo i documenti originali o

digitali nativi. Sono spesso collegati ai sistemi di recupero delle informazioni (information retrieval) e sono gestiti esternamente agli archivi digitali.

**Metadati Amministrativi e Gestionali:** Indicano le modalità di archiviazione e gestione degli oggetti digitali. Questi metadati sono essenziali per la conservazione a lungo termine, documentando i processi tecnici, l'autenticità e l'integrità del contenuto, e identificando univocamente gli oggetti informativi.

**Metadati Strutturali:** Collegano le componenti di risorse digitali per una fruizione completa e mappano schemi di metadati diversi. Forniscono dati su identificazione e localizzazione del documento, come il codice identificativo e l'indirizzo del file sul server.

## *Metadati Archivistici*

Gli obiettivi dei metadati archivistici sono:

- **Identificazione Permanente:** Garantire l'univocità dei singoli oggetti informativi, utilizzando numeri di protocollo, date, autori e altri riferimenti chiave.
- **Relazioni tra Oggetti Informativi:** Mantenere traccia delle connessioni tra i documenti attraverso indici di classificazione e fascicolatura.
- **Intelligibilità:** Conservare informazioni che facilitino la comprensione dei documenti, come il procedimento amministrativo a cui sono associati.

Tutti i metadati adottati dal sistema devono essere conformi agli schemi previsti dalle Linee Guida AgID e, laddove applicabile, agli standard UNI SInCRO. La codifica, la struttura e i formati dei metadati devono garantire interoperabilità, tracciabilità e sostenibilità della conservazione a lungo termine. Il sistema deve essere in grado di esportare i metadati secondo i profili XML previsti per il versamento nei sistemi di conservazione.

## Metadati di Registrazione a Protocollo

Questi metadati includono:

- **Identificativo Unico:** Sequenza di caratteri alfanumerici che identifica in modo univoco il fascicolo o documento.
- **Denominazione dell'Ente:** Indica l'organizzazione responsabile.
- **Corrispondente (Mittente/Destinatario).**
- **Oggetto:** Descrizione del contenuto del documento.
- **Numero di Allegati** e la loro descrizione.
- **Numero di Protocollo, UOR** (Unità Organizzativa Responsabile), **RPA** (Responsabile del Procedimento Amministrativo).
- **Data di Registrazione** e **Impronta Digitale** per garantire la connessione tra documento e metadati.

## Metadati del Fascicolo Informatico

I metadati minimi necessari per la gestione di un fascicolo informatico includono:

- **Identificativo Unico e Persistente.**
- **Area Organizzativa Omogenea (AOO).**
- **Unità Organizzativa Responsabile (UOR).**
- **Responsabile del Procedimento Amministrativo (RPA).**
- **Amministrazioni Partecipanti.**
- **Oggetto del Fascicolo.**
- **Elenco dei Documenti Contenuti.**
- **Data di Apertura** e **Data di Chiusura** del fascicolo.

## Metadati del Registro Giornaliero

I metadati del registro giornaliero sono i seguenti:

- **Identificativo Unico e Persistente:** Espresso in codice IPA, denominazione dell'amministrazione, AOO, anno e altri riferimenti.
- **Data di Chiusura** del registro.
- **Operatore** che ha prodotto il registro, con nome, cognome e codice fiscale.

- **Impronta del Documento Informatico** per collegare registro e documenti.
- **Responsabile della Gestione Documentale**, con i dettagli identificativi.
- **Descrizione dell'Oggetto** del registro, come «Registro giornaliero di protocollo».
- **Numeri Progressivi** del registro, incluse data e numero della prima e ultima registrazione.

## IL FASCICOLO

L'Istituto Italiano di Studi Germanici documenta la propria attività attraverso la conservazione di documenti all'interno di fascicoli, che rappresentano l'unità di base dell'archivio corrente. Ogni fascicolo raccoglie documenti (protocollati e non) relativi a un affare, attività o procedimento, organizzati in modo omogeneo secondo il **Piano di Classificazione/Titolario** vigente (vedi Allegato). L'obiettivo principale del fascicolo è preservare il vincolo archivistico, ovvero mantenere la connessione logica e necessaria tra i documenti correlati.

All'interno di ciascun fascicolo, i documenti seguono un ordine cronologico basato sulla data di registrazione, con il documento più recente visibile per primo. In caso di necessità, i fascicoli possono essere suddivisi in sottofascicoli e inserti, rispettando l'ordine cronologico anche all'interno delle suddivisioni. I sottofascicoli, se presenti, devono essere chiusi prima del fascicolo principale, poiché rappresentano spesso subprocedimenti o fasi specifiche di un procedimento più ampio. Tutti i documenti, inclusi quelli non protocollati, devono essere classificati e inclusi nei fascicoli.

Il **Responsabile del Procedimento Amministrativo** o dell'affare a cui appartengono i documenti è incaricato di garantire la corretta gestione del fascicolo, secondo le direttive del Direttore o del Dirigente responsabile.

### *Fascicolo Analogico*

I fascicoli cartacei contengono atti, documenti e dati prodotti su supporto fisico. In questi fascicoli devono essere mantenute le caratteristiche originali del formato, ma è possibile includere copie cartacee di documenti digitali per preservare il vincolo

archivistico. Un fascicolo analogico deve riportare le seguenti informazioni:

- **Anno di Apertura.**
- **Numero del Fascicolo** con numerazione annuale sequenziale all'interno del grado divisionale finale (Titolo/Classe).
- **Oggetto del Fascicolo.**

Le convenzioni grafiche prevedono l'uso di numeri romani per i titoli e di cifre arabe per gli altri gradi divisionali, con separatori specifici: un trattino tra anno e titolo, una barretta tra titolo e gradi successivi, e un punto tra gradi divisionali e numero del fascicolo. L'oggetto del fascicolo è inserito tra virgolette caporali (« »).

Alla chiusura del procedimento o pratica, il fascicolo viene chiuso formalmente, con la data di chiusura inserita dal responsabile. I fascicoli chiusi restano conservati presso l'Ufficio produttore per almeno un anno, garantendo l'accesso ai documenti per esigenze operative, prima del trasferimento nell'archivio di deposito.

## **Fascicolo Informatico**

Nell'Istituto, i flussi documentali sono gestiti attraverso fascicoli informatici, organizzati secondo il Piano di Classificazione vigente. Un fascicolo informatico è un'aggregazione documentale digitale contenente atti e dati informatici legati a un'attività o procedimento specifico, con identificazione univoca. Ogni fascicolo informatico deve includere:

- **Amministrazione Titolare del Procedimento.**
- **Altre Amministrazioni Partecipanti.**
- **Responsabile del Procedimento** (Nome e Cognome).
- **Oggetto del Procedimento.**
- **Elenco dei Documenti Contenuti.**
- **Indice di Classificazione** (Titolo, Classe, ecc.).
- **Numero del Fascicolo**, basato su una sequenza numerica riferita al grado divisionale dell'anno di creazione.
- **Date di Apertura e Chiusura** del fascicolo.

Il fascicolo informatico viene creato dal responsabile del procedimento o da un utente abilitato e può essere modificato da operatori autorizzati. In caso di presenza di documenti cartacei, anche la «camicia» del fascicolo cartaceo deve essere rinominata per mantenere la coerenza. In un sistema completamente digitale, il fascicolo è consultabile e aggiornabile dalle amministrazioni coinvolte.

### **Fascicolo Ibrido**

Un fascicolo può contenere documenti su supporti diversi (analogici e digitali), creando un **fascicolo ibrido**. Questa combinazione implica due unità fisiche di conservazione: una cartacea e una digitale. La classificazione garantisce comunque l'integrità del fascicolo grazie agli elementi identificativi (anno, titolo, numero, oggetto), assicurando la gestione coerente anche durante la fase di versamento nell'archivio storico. Se necessario, è consigliabile digitalizzare i documenti cartacei per unificare il formato del fascicolo.

In questi casi, è obbligatorio assicurare l'integrità e la coerenza logica dell'aggregazione documentale. Il fascicolo deve essere dotato di metadati comuni e aggiornati in entrambi i supporti, e la versione analogica deve essere digitalizzata con modalità tali da garantirne la conformità. È fortemente raccomandata, dove possibile, la progressiva dematerializzazione per l'uniformità della conservazione nel sistema digitale.

### **Altre Aggregazioni Documentali Informatiche**

L'Istituto gestisce anche **serie documentarie** e **serie di fascicoli**, che raccolgono documenti o fascicoli in base a criteri funzionali e classificatori. Queste serie, organizzate per tipologia o classe, possono collegare fascicoli diversi e sono gestite attraverso il sistema di gestione documentale dell'AOO, seguendo le indicazioni del Piano di Classificazione o del sistema di fascicolatura.



# L'ARCHIVIO CORRENTE

## *Definizione e Attività*

L'archivio corrente raccoglie i documenti relativi ad affari, attività e procedimenti amministrativi in fase di istruttoria o trattazione, o per i quali esiste ancora un interesse non concluso. Le attività principali dell'archivio corrente comprendono la registrazione informatica dei documenti, la loro classificazione e la fascicolazione.

La **registrazione informatica** è un'attività di certificazione svolta dall'operatore di protocollo, che, in qualità di pubblico ufficiale, garantisce data certa e provenienza del documento, rendendolo una prova affidabile e opponibile a terzi. Questo processo implica l'associazione di un insieme di dati in formato elettronico al documento, al fine di assicurarne l'identificazione univoca. Questi dati includono la classificazione e sono integrati nel piano di organizzazione delle aggregazioni documentali.

La **classificazione** è il processo di organizzazione dei documenti secondo uno schema gerarchico, strutturato in voci che individuano funzioni, competenze, attività o materie dell'ente produttore. Il piano di classificazione guida questa attività, mappando le funzioni dell'ente su più livelli gerarchici. La classificazione è obbligatoria per tutti i documenti prodotti o acquisiti dall'ente e costituisce una componente fondamentale dei metadati per i documenti informatici. Il Coordinatore della gestione documentale verifica regolarmente l'adeguatezza del piano di classificazione ai procedimenti in corso, procedendo a eventuali aggiornamenti.

La **fascicolazione** è l'attività di organizzazione logica (e, per i documenti cartacei, anche fisica) dei documenti all'interno

di fascicoli, mantenendo il vincolo archivistico che collega i documenti alla pratica di riferimento. Questo processo consente di strutturare i documenti in unità complesse e stabili nel tempo, facilitando l'accesso alle informazioni necessarie per le attività amministrative e per il pubblico.

## Strumenti dell'Archivio Corrente: Registri, Repertori, Titolario

La gestione del sistema documentale dell'Istituto passa attraverso strumenti specifici come registri, repertori e il titolare (piano di classificazione), che facilitano l'organizzazione e la consultazione della documentazione. Tra questi strumenti troviamo:

**Registri di Protocollo:** Questi registri gestiscono l'identificazione univoca dei documenti ricevuti e spediti tramite la registrazione di elementi specifici. Il registro di protocollo è un atto pubblico e ha funzione giuridico-probatoria, garantendo la validità giuridica dei documenti. Ogni AOO dell'ente dispone di un registro unico, con validità annuale, che viene inviato in conservazione digitale per assicurarne l'integrità. Il trasferimento avviene mediante la generazione di un pacchetto di versamento, curato dal Responsabile della conservazione.

**Repertori:** Sono registri che catalogano con numerazione progressiva le serie omogenee di documenti, differenziati per tipologia. Questi registri coprono documenti soggetti a registrazione particolare come decreti, contratti e delibere. Ogni repertorio è collegato a una specifica AOO e ha natura di atto pubblico, attestando data e descrizione degli atti registrati. La numerazione inizia il 1° gennaio e termina il 31 dicembre di ogni anno.

**Piano di Classificazione/Titolario:** Costituisce la struttura logica di riferimento per classificare i documenti, organizzato in gradi divisionali. Ogni documento, protocollato o meno, viene classificato sulla base della corrispondenza tra il suo contenuto e la voce del titolare. Il piano di classificazione garantisce il mantenimento del vincolo archivistico e viene

aggiornato periodicamente per riflettere eventuali modifiche normative o organizzative.

## **Registro Giornaliero di Protocollo Informatico**

Il registro giornaliero di protocollo informatico è lo strumento centrale per la gestione dei documenti ricevuti e spediti dall'ente, memorizzando tutte le informazioni rilevanti. Questo registro è generato automaticamente, con una struttura logica predeterminata, e viene memorizzato in modo statico e immutabile. Le informazioni registrate vengono protette contro manipolazioni e sono accessibili solo all'amministratore del sistema. Eventuali modifiche vengono tracciate in un file di log, garantendo una cronologia completa delle operazioni.

## **Registrazione e Classificazione**

La registrazione di protocollo copre tutti i documenti ricevuti e spediti dall'amministrazione, nonché i documenti informatici da cui possono derivare diritti o doveri. Ogni documento deve avere un numero di protocollo univoco e deve essere classificato, anche se non protocollato, per consentire una gestione efficace del sistema documentale. Documenti come gazzette ufficiali, materiale statistico e atti preparatori interni sono esclusi dalla registrazione di protocollo. La registrazione avviene tramite la memorizzazione di dati essenziali, inclusi numero di protocollo, data di registrazione, mittente o destinatario, oggetto e classificazione in base al titolare vigente.

## **Segnatura**

La segnatura di protocollo consiste nell'associazione permanente di dati al documento, identificandolo in modo univoco e persistente. Gli elementi della segnatura includono il progressivo di protocollo, la data di registrazione, l'identificazione dell'amministrazione e l'area organizzativa di riferimento. Per i documenti cartacei, la segnatura è apposta tramite timbro meccanico. Questo

processo garantisce la tracciabilità e la sicurezza dei documenti prodotti e scambiati tra le UOR dell'AOO.

## **Registrazione Differita e Annullamento**

La registrazione differita è consentita solo in casi eccezionali, come un carico di lavoro imprevisto, e richiede l'autorizzazione del Responsabile della gestione documentale. È possibile annullare una registrazione per motivi giustificati, previa richiesta motivata, con l'autorizzazione del Responsabile della gestione documentale. L'annullamento determina la cancellazione dell'intera registrazione, ma la traccia resta visibile nel sistema documentale.

## **Ricevuta di Avvenuta Registrazione e Registro di Emergenza**

La ricevuta di avvenuta registrazione può essere emessa su richiesta e riporta tutti i dati essenziali del documento. In caso di malfunzionamenti gravi del sistema documentale, si attiva il registro di emergenza, la cui gestione deve seguire una procedura formalizzata e approvata dal Responsabile della gestione documentale.

Il registro, redatto in formato digitale o cartaceo conforme, deve riportare:

- data e ora dell'attivazione,
- motivazione dell'interruzione,
- operatori abilitati all'utilizzo,
- modalità di reinserimento dei dati nel sistema ufficiale.

La chiusura della procedura deve essere documentata e sottoscritta dal RGD, con conservazione permanente del verbale di attivazione.

## IL FLUSSO DI LAVORAZIONE DEI DOCUMENTI

### *Distinzione dei Documenti in Base allo Stato di Trasmissione*

I documenti, che siano analogici o informatici, si distinguono in base al loro stato di trasmissione in:

**Documenti ricevuti o in arrivo:** quelli ricevuti dall'Istituto nell'esercizio delle sue funzioni.

**Documenti inviati o in partenza:** quelli prodotti e inviati dall'Istituto per svolgere le proprie attività.

**Documenti interni:** quelli scambiati tra le diverse Unità Organizzative Responsabili (UOR) all'interno della stessa Area Organizzativa Omogenea (AOO).

### *Flusso di Lavorazione del Documento Ricevuto - In Arrivo*

La gestione della corrispondenza in arrivo viene svolta dal Servizio per la tenuta del protocollo informatico e la gestione dei flussi documentali. Il Servizio per la gestione documentale si occupa di ricevere la corrispondenza, registrarne l'arrivo, classificarla, segnare i documenti e assegnarli alle unità competenti.

### *Dettaglio delle Attività*

**Ricezione della Corrispondenza:** La corrispondenza analogica viene raccolta dal personale addetto alla posta e consegnata al Servizio per la gestione documentale, che si occuperà di aprire le buste (ad eccezione di quelle contrassegnate come «riservato» o «confidenziale»). Le buste indirizzate al personale

devono essere consegnate ai destinatari, che sono tenuti a inoltrare al Servizio per la gestione documentale qualsiasi documento che necessiti di registrazione.

**Posta Elettronica Istituzionale o PEC:** Il controllo delle caselle di posta elettronica istituzionale e PEC è affidato al personale autorizzato. All'atto della lettura, è possibile modificare l'oggetto dei messaggi per chiarire eventuali ambiguità.

**Registrazione nel Protocollo Informatico:** Gli addetti provvedono alla registrazione di documenti analogici e digitali, inclusi quelli contenuti in e-mail o PEC. La registrazione deve avvenire entro la giornata di arrivo o entro 24 ore lavorative, salvo casi particolari in cui il carico di lavoro richieda il protocollo differito.

**Classificazione e Segnatura:** Dopo la registrazione, i documenti vengono classificati secondo il titolario vigente. Per i documenti analogici, viene apposta una segnatura tramite timbro e digitalizzati in PDF; per i documenti informatici, la segnatura è automatica. Successivamente, i documenti sono assegnati alla UOR o al RPA competente.

**Assegnazione:** Una volta registrato e classificato, il documento viene assegnato tramite il sistema documentale all'UOR/RPA designato, che procederà alla fascicolazione. Le regole di assegnazione sono stabilite dal Responsabile del Servizio per la gestione documentale.

## ***Flusso di Lavorazione del Documento Inviato - In Partenza***

Per la gestione dei documenti in uscita:

La registrazione e classificazione avvengono direttamente presso la UOR che si occupa anche della fascicolazione da parte degli ~~Gli~~ operatori autorizzati.

Una volta registrati, i documenti informatici possono essere inviati via e-mail o PEC, mentre i documenti analogici devono essere spediti entro il giorno lavorativo successivo alla registrazione.

### ***Flusso di Lavorazione del Documento Interno***

I documenti interni, vengono protocollati, classificati e fascicolati.

### ***Flusso di Lavorazione del Documento da Altra Banca Dati/Online***

L'interoperabilità tra sistemi è essenziale per la gestione di documenti provenienti da altre banche dati o risorse online. Questa può avvenire tramite accessi diretti ai database o attraverso processi di gestione documentale automatizzati.

### ***Utilizzo delle Firme Elettroniche***

**Firma Digitale:** Necessaria per documenti che implicano responsabilità verso l'esterno.

### ***Chiusura del Fascicolo***

Il RPA è responsabile della gestione e chiusura dei fascicoli di sua competenza, sia analogici che informatici. La chiusura avviene al termine del procedimento o attività, con riferimento alla data dell'ultimo documento inserito. Un fascicolo chiuso non può essere riaperto senza consultazione con il Responsabile della gestione documentale.



# L'ARCHIVIO DI DEPOSITO

## *Definizione*

L'archivio di deposito è lo spazio in cui vengono conservati i fascicoli relativi a pratiche concluse, che non sono più rilevanti per l'attività quotidiana. Questa fase dell'archivio, chiamata anche **«archivio intermedio»**, rappresenta un passaggio tra l'archivio corrente e quello storico. In questa fase, i documenti sono custoditi perché, nonostante appartengano a pratiche concluse, possono ancora essere utili, ad esempio, per controlli fiscali.

## *Trasferimento all'Archivio di Deposito*

Nell'archivio di deposito sono conservati fascicoli e documenti relativi a procedimenti, affari e attività conclusi, per i quali non è più necessaria una trattazione corrente, ma che potrebbero avere ancora un interesse occasionale. La conservazione dei documenti deve seguire le modalità stabilite dal Responsabile della conservazione, in collaborazione con il Responsabile della gestione documentale, rispettando l'organizzazione dei documenti dell'archivio corrente. Il Servizio per la tenuta del protocollo informatico e la gestione dei flussi documentali è responsabile della gestione dell'archivio di deposito.

Il trasferimento dei fascicoli e delle serie documentarie avviene periodicamente, almeno una volta l'anno, verso un apposito archivio di deposito istituito presso ogni amministrazione. Durante questo trasferimento, l'organizzazione dei fascicoli e delle serie deve rimanere invariata rispetto a quella dell'archivio corrente. Il Responsabile della gestione documentale è incaricato di mantenere un elenco aggiornato dei fascicoli e delle serie trasferite.

Alla consegna dei fascicoli, il Responsabile della gestione documentale verifica la corrispondenza con l'elenco di consistenza

tramite un verbale di trasferimento firmato, insieme all'elenco, anche dal RPA al momento della consegna.

### ***Trasferimento dei Fascicoli Informatici al Sistema di Conservazione***

Il Responsabile della conservazione, almeno una volta all'anno, deve generare e trasmettere al sistema di conservazione i pacchetti di versamento, seguendo le indicazioni del manuale di conservazione. Possono essere utilizzati processi di automazione del sistema documentale per agevolare il trasferimento.

Se per alcune tipologie di procedimenti o documenti sono necessarie tempistiche particolari per la conservazione, il RPA interessato deve comunicare tempestivamente al Responsabile della conservazione per concordare le modalità adeguate. Un esempio tipico è la gestione delle fatture elettroniche, che devono essere fascicolate nei fascicoli informatici pertinenti.

### ***Elenco Topografico per l'Archivio Analogico***

Dopo aver ricevuto i fascicoli e le serie documentarie, il personale dell'archivio di deposito organizza i documenti nei depositi secondo il loro ordinamento archivistico. Gli elenchi di versamento vengono integrati nell'elenco di consistenza dell'archivio, corredati di indicazioni topografiche.

### ***Registro di Carico e Scarico***

Il Responsabile della gestione documentale annota le richieste di prelievo di fascicoli dall'archivio di deposito in un registro apposito. Il registro include dati identificativi del fascicolo, l'unità organizzativa richiedente, il nome del richiedente, la motivazione della richiesta, le date di richiesta, di evasione e di restituzione, nonché eventuali note aggiuntive.

## ***Massimario di Selezione e Prontuario di Scarto***

Il **massimario di selezione**, redatto secondo i criteri stabiliti dalla Soprintendenza archivistica e validato dal Responsabile della conservazione, identifica per ogni tipologia documentale:

- la funzione e il procedimento amministrativo di riferimento;
- il tempo minimo di conservazione;
- la destinazione finale (conservazione permanente o scarto).

Il prontuario di scarto specifica le tipologie documentali destinabili all'eliminazione e i relativi termini di conservazione, in coerenza con il massimario. Le operazioni di selezione devono avvenire durante la fase di transito nell'archivio di deposito e devono essere accompagnate da un verbale e da un fascicolo di procedimento. Lo scarto è sempre subordinato ad autorizzazione della Soprintendenza archivistica e registrato nel sistema documentale dell'Istituto.

## ***Selezione e Scarto dei Documenti Analogici***

I documenti analogici possono essere sottoposti a selezione e scarto, seguendo le normative sui beni culturali. La proposta di scarto deve essere preparata dal Responsabile della gestione documentale, specificando le tipologie documentali, il periodo di riferimento, il volume in metri lineari (o in chilogrammi per i documenti analogici) e le motivazioni dell'eliminazione. Il provvedimento di scarto deve essere autorizzato dal Direttore Generale inviato alla Soprintendenza archivistica.

Dopo l'autorizzazione, il Responsabile della gestione documentale organizza il ritiro e l'eliminazione fisica dei documenti, con rilascio di un verbale di esecuzione. Il fascicolo relativo al procedimento di scarto è conservato indefinitamente.

## ***Selezione e Scarto dei Documenti Informatici***

I documenti informatici possono anch'essi essere selezionati e scartati nel sistema di conservazione, seguendo la normativa

sui beni culturali. La procedura di selezione è determinata dal Titolare dell'oggetto di conservazione, in accordo con il piano di conservazione. In caso di affidamento esterno del servizio di conservazione, le modalità operative devono essere concordate tra il Titolare e il Conservatore.

Una volta ottenuta l'autorizzazione della Soprintendenza archivistica, il Titolare dell'oggetto di conservazione procede alla distruzione dei pacchetti di archiviazione, seguendo i metadati tracciati nel sistema. In caso di documenti riservati, l'autorizzazione deve essere richiesta anche al Ministero dell'Interno. Al termine delle operazioni, viene notificato l'esito della procedura agli organi di tutela competenti.

## ***Conservazione dei Documenti***

Il Responsabile della gestione documentale garantisce la corretta conservazione della documentazione analogica e digitale. Per la documentazione analogica, è importante assicurare la sicurezza dei depositi, il controllo delle condizioni ambientali e la manutenzione periodica. Per la documentazione digitale, le modalità di conservazione vengono stabilite in collaborazione con il Responsabile della conservazione.

# IL SISTEMA INFORMATICO

## Definizione

Il sistema informatico comprende l'insieme delle risorse tecnologiche utilizzate dall'Amministrazione per gestire i documenti, tra cui risorse di calcolo, dispositivi, reti di comunicazione e procedure informatiche. La gestione dei flussi documentali, elemento fondamentale, consente di organizzare e amministrare in modo efficace tutta la documentazione, sia quella ricevuta sia quella prodotta.

## Sicurezza del sistema informatico

La sicurezza del sistema informatico si pone l'obiettivo di proteggere sia i luoghi fisici sia gli strumenti tecnologici utilizzati, riducendo i rischi e limitando eventuali conseguenze negative dovute a minacce. Questo obiettivo viene perseguito attraverso una serie di misure mirate, tra cui:

- esecuzione periodica di backup, con frequenza almeno settimanale, in ambienti distinti e protetti;
- verifica annuale del piano di disaster recovery e l'esecuzione di test di ripristino dei dati;
- definizione di una procedura per l'attivazione del registro di emergenza, da aggiornare e condividere con gli operatori almeno una volta l'anno.

## Piano di sicurezza dei documenti informatici

Il piano di sicurezza mira a garantire la protezione dei dati e a rispettare le misure minime di sicurezza previste dalla normativa. Questo strumento è fondamentale per preservare i dati dai rischi a cui possono essere esposti. Nel piano vengono definiti:

- **Ruoli e responsabilità:** Chi fa cosa nell'organizzazione, con particolare attenzione alla sicurezza.
- **Regole per l'accesso:** Norme per controllare gli accessi, sia per gli utenti interni sia per quelli esterni, utilizzando sistemi di autenticazione forte e tracciando le attività svolte.
- **Procedure per la gestione documentale:** Metodologie che garantiscono l'identificabilità di chi ha formato il documento, la sua sottoscrizione (anche con firma digitale, ove necessario), la sua leggibilità e disponibilità nel tempo, nonché l'integrità e la riservatezza.
- **Conservazione dei documenti:** Scelta di supporti adeguati per il salvataggio (dischi, applicazioni, ecc.), backup regolari (preferibilmente giornalieri) e predisposizione di piani di emergenza per assicurare la continuità operativa.

## Accesso al sistema informatico

L'accesso al sistema è regolato da credenziali personali, composte da username e password. Ogni utente viene identificato e autorizzato in base a specifici profili, che possono variare a seconda delle sue mansioni. Per assicurare la massima sicurezza:

- **Le credenziali sono personali e non condivisibili.**
- **La password deve rispettare criteri di robustezza**, ad esempio evitando riferimenti facili da indovinare e includendo caratteri speciali.
- **Le credenziali non utilizzate da più di sei mesi sono disattivate**, a meno che non siano autorizzate per scopi tecnici specifici.
- **Gli utenti possono modificare la propria password** in qualsiasi momento, soprattutto se sospettano che la sua segretezza sia stata compromessa.

In caso di necessità operative urgenti, esistono disposizioni che consentono l'accesso straordinario ai dati o agli strumenti elettronici, garantendo sempre riservatezza e sicurezza.

## Misure di sicurezza dei documenti informatici e protezione dei dati personali

Per garantire la disponibilità e la riservatezza delle informazioni, l'Amministrazione adotta specifiche politiche e procedure,

in conformità con le normative vigenti. Tra queste, particolare attenzione è dedicata alla protezione dei dati personali, mediante l'applicazione di misure tecniche e organizzative adeguate. I dati e i documenti sono resi accessibili a chiunque abbia diritto di consultarli, nel rispetto della normativa sulla trasparenza (Legge 241/1990 e D.Lgs. 33/2013) e delle disposizioni sulla privacy.

## Titolare del trattamento/Responsabile del trattamento/Incaricati del trattamento

**Titolare del trattamento:** L'Istituto Italiano di Studi Germanici (IISG), con sede a Roma, è responsabile della definizione delle finalità e dei mezzi per il trattamento dei dati personali, in linea con il Regolamento UE 679/2016.

**Responsabile del trattamento:** PADigitale gestisce l'applicativo "URBI", che consente la registrazione, la ricerca e la consultazione dei documenti trattati, garantendo la conformità alle normative.

**Incaricati del trattamento:** Soggetti autorizzati dall'Amministrazione, responsabili della gestione documentale e vincolati da obblighi di riservatezza che si estendono anche dopo la cessazione del loro incarico. Ogni accesso al sistema è supervisionato dal Coordinatore della gestione documentale, che assegna le credenziali.

## Misure di sicurezza e policy

Per proteggere i propri sistemi informativi e garantire la resilienza, l'IISG adotta:

- Le **misure minime di sicurezza ICT** previste dall'AgID (Circolare 2/2017).
- Un **manuale per la gestione di violazioni dei dati personali** (data breach), in conformità agli articoli 33-34 del Regolamento UE 679/2016.
- Una direttiva interna sull'utilizzo delle risorse informatiche, che tutela riservatezza, integrità e disponibilità delle informazioni e dei dati personali trattati.

## Note

## **Note**

