

Manuale di gestione dell'Ente Regionale per il Diritto allo Studio Universitario di Sassari (E.R.S.U.)



INDICE

1. Principi generali	p. 4
a. 1.1 Premessa	p. 4
b. 1.2 Norme di riferimento	p. 5
c. 1.3 Glossario	p. 7
d. 1.4 Acronimi e sigle	p. 10
e. 1.5 Eliminazione dei protocolli diversi da quello generale	p. 11
2. Aspetti organizzativi	p. 12
a. 2.2 Modello organizzativo	p. 12
b. 2.3 Il responsabile della Gestione documentale	p. 14
c. 2.4 Il responsabile della Conservazione	p. 15
d. 2.5 Utenti interni abilitati al sistema documentale	p. 16
3. Gestione dei documenti	p. 17
a. 3.1 Il documento informatico	p. 17
b. 3.2 Copie per immagine su supporto informatico dei documenti analogici	p. 18
c. 3.3 Duplicati, copie ed estratti informatici di documenti cartacei	p. 19
d. 3.4 Il documento amministrativo informatico	p. 20
e. 3.5 Formati di firma digitale	p. 21
f. 3.6 Formati dei documenti	p. 21
4. Il protocollo informatico	p. 22
a. 4.1 La registrazione di protocollo	p. 22
b. 4.2 La segnatura di protocollo	p. 22
c. 4.3 Allegati alla registrazione	p. 23
d. 4.4 Registrazione delle informazioni annullate o modificate	p. 23
e. 4.5 Registro di emergenza	p. 24
f. 4.6 Documenti esclusi dalla registrazione di protocollo	p. 26
g. 4.7 Differimento dei termini di protocollazione	p. 27
5. Classificazione e fascicolazione	p. 28
a. 5.1 Piano di classificazione	p. 28
b. 5.2 Aggregazioni documentali (fascicoli)	p. 28
c. 5.2.1 Tipologie di fascicolo	p. 29
6. Flussi di lavoro	p. 30

a. 6.1 Documenti in entrata	p. 30
b. 6.2 Documenti in uscita	p. 32
c. 6.3 Documenti interni	p. 34
d. 6.4 Documenti soggetti a registrazione di Repertorio	p. 34
e. 6.5 Documenti riservati	p. 35
7. Misure di sicurezza	p. 36
8. Archivio	p. 37
a. 8.1 La conservazione dei documenti digitali	p. 37
b. 8.2 Conservazione della documentazione cartacea	p. 37
c. 8.3 Scarto documentale	p. 39
d. 8.4 Accesso all'archivio analogico	p. 40
9. Allegati	p. 41

1. PRINCIPI GENERALI

1.1 Premessa

Accogliendo i principi apportati nel 2021 nelle Linee Guida AgID (Agenzia per l'Italia Digitale) sulla formazione, gestione e conservazione dei documenti informatici e a seguito dell'entrata in vigore del Regolamento UE sulla privacy n. 679/2016 (GDPR), l'ERSU Sassari ha redatto il presente Manuale di Gestione con l'obiettivo di descrivere il sistema di gestione dei documenti, anche ai fini della conservazione, e di fornire le istruzioni per il corretto funzionamento del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi.

Il Manuale di gestione ha una duplice finalità: disciplinare il sistema di gestione documentale dell'Ente, e rappresentare le funzionalità disponibili per tutti gli utenti, interni ed esterni, che interagiscono con l'ERSU.

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'ente.

Il presente strumento è pubblicato sul sito internet istituzionale dell'ERSU (<https://ersusassari.it/it/>) all'interno della Sezione "Amministrazione trasparente" nella sottosezione "Disposizioni Generali" sottosezione "Atti Generali", sotto la voce "Regolamenti e manuali".

Il Manuale deve essere oggetto di costante aggiornamento e ciò in funzione dell'evoluzione tecnologica e dell'obsolescenza degli oggetti e strumenti utilizzati. Allo stesso modo anche i processi e le attività inerenti alle attività di formazione dei documenti devono essere sottoposti a costante valutazione e monitoraggio. Il Responsabile della Gestione Documentale (RGD) provvederà alle eventuali integrazioni o revisioni nei casi in cui lo ritenga opportuno, ad esempio a seguito di:

- ✓ modifiche normative o regolamentari sopravvenute;
- ✓ introduzione di nuove pratiche tendenti a migliorare l'operatività dell'ente in termini di efficacia, efficienza e trasparenza;
- ✓ inadeguatezza delle procedure rilevate nello svolgimento delle attività correnti;
- ✓ sostanziali modifiche apportate nell'ambito dell'architettura del sistema e delle singole componenti informatiche utilizzate.

Nel caso di avvicendamento del RGD, il nuovo Responsabile deve prendere visione del manuale di gestione e dei relativi allegati, verificare le regole in esso contenute ed eventualmente modificarle, proponendo aggiornamenti del manuale stesso.

In sintonia col Regolamento europeo per la protezione dei dati (GDPR), l'AOO impiega strumenti atti a eliminare eventuali rischi possibili derivanti dal trattamento dei dati personali. Un elevato grado di informatizzazione dei flussi documentali permette di delimitare ai soli documenti e fascicoli digitali gli obblighi di conservazione dei documenti, evitando la duplicazione della documentazione amministrativa e influenzando in modo sensibile sulla necessità di spazi fisici da destinare a depositi archivistici, sui costi di gestione degli stessi e sulla possibilità di adottare un presidio più efficace dei documenti, sia nel governo che nel controllo.

La presenza di copie e le stampe dei documenti, le copie cartacee di lavoro strettamente necessarie non devono restare incustodite sulla scrivania, per evitare indebiti accessi ai dati e alle informazioni che esse contengono, ma devono essere sottratte alla visibilità e custodite adeguatamente. Una volta terminata la loro utilità, le copie e le stampe *non devono essere archiviate*, in quanto tutti i documenti sono scansionati e

inseriti nei rispettivi fascicoli elettronici, e devono essere distrutte senza formalità. La documentazione presente all'interno di cartelle condivise utilizzate dalla AOO deve essere eliminata una volta che sono cessate le esigenze istruttorie, in particolare per quanto riguarda i dati personali contenuti.

Il personale identificato nel complesso della gestione dei flussi documentali deve essere profilato nel sistema di gestione documentale, con chiara indicazione dei livelli di accesso e delle responsabilità da esso derivanti, seguendo le indicazioni del dirigente. Coerentemente con le funzioni assegnate e con le abilitazioni ad essi fornite i dipendenti sono incaricati del Trattamento dei dati e per questo motivo devono possedere una formazione idonea in merito loro relative responsabilità, ricevendo una continua e adeguata formazione.

1.2 Norme di riferimento

Il 10 settembre 2020 sono entrate in vigore le "Linee Guida sulla formazione, gestione e conservazione dei documenti informatici" (di seguito, "Linee Guida") emanate dall'Agenzia per l'Italia Digitale (di seguito: AGID): la cui applicazione è stata prevista a partire dal duecentosettantesimo giorno successivo alla loro entrata in vigore. Tuttavia, con la determinazione Agid n. 371/2021 la data di applicazione delle Linee Guida e dei relativi allegati, precedentemente fissata al 7 giugno 2021 è stata posticipata al 1° gennaio 2022. Inoltre, con la predetta Determinazione sono state apportate alcune modifiche al testo delle Linee Guida e ai seguenti allegati, approvati con la Determinazione Agid n. 407/2020:

- ✓ Modifica dell'Allegato 5 - Metadati alle Linee Guida per la formazione, gestione e conservazione dei documenti informatici;
- ✓ Modifica dell'Allegato 6 - Comunicazione tra AOO di Documenti Amministrativi Protocollati alle Linee Guida per la formazione, gestione e conservazione dei documenti informatici;
- ✓ Correzione di taluni errori materiali contenuti nel testo delle Linee Guida;
- ✓ Approvazione di un documento contenente la sintesi delle suddette modifiche.

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

- ✓ Decreto del Presidente del Consiglio dei Ministri 13 novembre 2014, recante "Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici";
- ✓ Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013, recante "Regole tecniche in materia di sistema di conservazione".

Per quanto concerne il Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013, recante "Regole tecniche per il protocollo informatico", a partire dalla data di applicazione delle Linee Guida sono abrogate tutte le disposizioni, fatte salve le seguenti:

- ✓ Art. 2 comma 1: "Oggetto e ambito di applicazione";
- ✓ Art. 6: "Funzionalità";
- ✓ Art. 9: "Formato della segnatura di protocollo";
- ✓ Art. 18: "Modalità di registrazione dei documenti informatici" (limitatamente ai commi 1 e 5);
- ✓ Art. 20: "Segnatura di protocollo dei documenti trasmessi";
- ✓ Art. 21: "Informazioni da includere nella segnatura".

Dalla data di attuazione delle nuove Linee Guida, la circolare n. 60 del 23 gennaio 2013 dell'AGID in materia di "Formato e definizione dei tipi di informazioni minime ed accessorie associate ai messaggi scambiati tra le Pubbliche Amministrazioni" è abrogata e sostituita dall'allegato 6 delle Linee Guida denominato "Comunicazione tra AOO di documenti amministrativi protocollati".

Sarà cura dell'ERSU attuare le attività volte ad adeguare i propri sistemi informatici nonché le procedure amministrative per garantire la piena applicazione delle Linee Guida.

Si precisa che nel presente Manuale, quando si impiegherà il termine "Linee Guida" si farà riferimento alle nuove disposizioni.

Oltre alle Linee Guida e ai Decreti del Presidente del Consiglio dei Ministri sopra citati si riportano le principali disposizioni in materia:

- ✓ Regio Decreto n. 1163/1911: "Regolamento per gli archivi di Stato";
- ✓ Legge n. 241/1990: "Nuove norme sul procedimento amministrativo";
- ✓ Decreto del Presidente della Repubblica n. 445/2000: "Testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa";
- ✓ Decreto Legislativo n. 196/2003: "Codice in materia di protezione dei dati personali recante disposizioni per l'adeguamento dell'ordinamento nazionale al 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";
- ✓ Decreto Legislativo n. 42/2004: "Codice dei beni culturali e del paesaggio, ai sensi dell'articolo 10 della legge 6 luglio 2002, n. 137";
- ✓ Decreto Legislativo n. 82/2005: "Codice dell'amministrazione digitale";
- ✓ Decreto Legislativo n. 104/2010: "Attuazione dell'articolo 44 della legge 18 giugno 2009, n. 69, recante delega al governo per il riordino del processo amministrativo";
- ✓ Decreto Legislativo n. 33/2013: "Riordino della disciplina riguardante il diritto di accesso civico e gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni";
- ✓ Decreto del Presidente del Consiglio dei Ministri del 21 marzo 2013: "Individuazione di particolari tipologie di documenti analogici originali unici per le quali, in ragione di esigenze di natura pubblicistica, permane l'obbligo della conservazione dell'originale analogico oppure, in caso di conservazione sostitutiva, la loro conformità all'originale deve essere autenticata da un notaio o da altro pubblico ufficiale a ciò autorizzato con dichiarazione da questi firmata digitalmente ed allegata al documento informatico, ai sensi dell'art. 22, comma 5, del Codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82 e successive modificazioni";
- ✓ Regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE - Regolamento eIDAS;
- ✓ Circolari 40 e 41 del 14 dicembre 2015 della Direzione generale degli archivi: "Autorizzazione alla distruzione di originali analogici riprodotti secondo le regole tecniche di cui al DPCM 13.11.2014 e conservati secondo le regole tecniche di cui al DPCM 13.12.2013";
- ✓ Regolamento (UE) n. 679/2016 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE;
- ✓ Circolare 18 aprile 2017, n. 2/2017 dell'Agenzia per l'Italia Digitale: "Misure minime di sicurezza ICT per le pubbliche amministrazioni".

1.3 Glossario

TERMINE	DEFINIZIONE
Archivio	<i>Complesso dei documenti prodotti o acquisiti da un soggetto pubblico o privato durante lo svolgimento della propria attività. Un archivio informatico è costituito da documenti informatici, organizzati in aggregazioni documentali informatiche</i>
Area Organizzativa Omogenea	<i>Un insieme di funzioni e di uffici individuati dall'Ente al fine di gestire i documenti in modo unitario e coordinato, secondo quanto disposto dall'art. 50 comma 4 del TUDA. Essa rappresenta il canale ufficiale per l'invio di istanze e l'avvio di procedimenti amministrativi</i>
Attestazione di conformità delle copie per immagine su supporto informatico di un documento analogico	<i>Dichiarazione rilasciata da notaio o altro pubblico ufficiale a ciò autorizzato allegata o asseverata al documento informatico</i>
Autenticità	<i>Caratteristica in virtù della quale un oggetto deve considerarsi come corrispondente a ciò che era nel momento originario della sua produzione. Pertanto un oggetto è autentico se nel contempo è integro e completo, non avendo subito nel corso del tempo o dello spazio alcuna modifica non autorizzata. L'autenticità è valutata sulla base di precise evidenze</i>
Classificazione	<i>Attività di organizzazione di tutti i documenti secondo uno schema costituito da un insieme di voci articolate in modo gerarchico e che individuano, in astratto, le funzioni, competenze, attività e/o materie del soggetto produttore</i>
Conservazione	<i>Insieme delle attività finalizzate a definire ed attuare le politiche complessive del sistema di conservazione e a governarne la gestione in relazione al modello organizzativo adottato, garantendo nel tempo le caratteristiche di autenticità, integrità, leggibilità, reperibilità dei documenti</i>
Destinatario	<i>Soggetto o sistema al quale il documento informatico è indirizzato</i>
Documento analogico	<i>Ogni rappresentazione, non informatica del contenuto di atti, anche interni, formati dalle pubbliche amministrazioni, o, comunque, da queste ultime utilizzati ai fini dell'attività amministrativa</i>
Documento amministrativo informatico	<i>Ogni rappresentazione, grafica, fotocinematografica, elettromagnetica o di qualunque altra specie, del contenuto di atti, anche interni, formati dalle pubbliche amministrazioni, o, comunque, da queste ultime utilizzati ai fini dell'attività amministrativa</i>
Documento informatico	<i>Documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti</i>
Duplicato informatico	<i>Il documento informatico ottenuto mediante la memorizzazione, sullo stesso dispositivo o su dispositivi diversi, della medesima sequenza di valori binari del documento originario</i>
Evidenza informatica	<i>Sequenza finita di bit che può essere elaborata da una procedura informatica</i>
Fascicolo informatico	<i>Aggregazione documentale informatica strutturata e univocamente identificata contenente atti, documenti o dati informatici prodotti e funzionali all'esercizio di una attività o allo svolgimento di uno specifico procedimento</i>

TERMINE	DEFINIZIONE
Formato (del documento informatico)	<i>Modalità di rappresentazione della sequenza di bit che costituiscono il documento informatico; comunemente è identificato attraverso l'estensione del file</i>
Funzione di hash crittografica	<i>Funzione matematica che genera, a partire da una evidenza informatica, una impronta crittografica o digest in modo tale che risulti computazionalmente difficile (di fatto impossibile), a partire da questa, ricostruire l'evidenza informatica originaria e generare impronte uguali a partire da evidenze informatiche differenti</i>
Gestione documentale	<i>Processo finalizzato al controllo efficiente e sistematico della produzione, ricezione, tenuta, uso, selezione e conservazione dei documenti</i>
Impronta crittografica	<i>Sequenza di bit di lunghezza predefinita, risultato dell'applicazione di una funzione di hash crittografica a un'evidenza informatica</i>
Integrità	<i>Caratteristica di un documento informatico o di un'aggregazione documentale in virtù della quale risulta che essi non hanno subito nel tempo e nello spazio alcuna alterazione non autorizzata. La caratteristica dell'integrità, insieme a quella della completezza, concorre a determinare la caratteristica dell'autenticità</i>
Interoperabilità	<i>Caratteristica di un sistema informativo, le cui interfacce sono pubbliche e aperte, e capaci di interagire in maniera automatica con altri sistemi informativi per lo scambio di informazioni e l'erogazione di servizi</i>
Leggibilità	<i>Caratteristica di un documento informatico che garantisce la qualità di poter essere decodificato e interpretato da un'applicazione informatica</i>
Manuale di conservazione	<i>Documento informatico che descrive il sistema di conservazione e illustra dettagliatamente l'organizzazione, i soggetti coinvolti e i ruoli svolti dagli stessi, il modello di funzionamento, la descrizione del processo, la descrizione delle architetture e delle infrastrutture</i>
Metadati	<i>Dati associati a un documento informatico, a un fascicolo informatico o a un'aggregazione documentale per identificarli, descrivendone il contesto, il contenuto e la struttura - così da permetterne la gestione del tempo - in conformità a quanto definito nella norma ISO 15489-1:2016 e più nello specifico dalla norma ISO 23081-1:2017</i>
Piano di classificazione (Titolario)	<i>Struttura logica che permette di organizzare documenti e oggetti digitali secondo uno schema desunto dalle funzioni e dalle attività dell'amministrazione interessata</i>
Piano di conservazione	<i>Documento, allegato al manuale di gestione e integrato con il sistema di classificazione, in cui sono definiti i criteri di organizzazione dell'archivio, di selezione periodica e di conservazione ai sensi dell'articolo 68 del TUDA</i>
Piano della sicurezza informatica	<i>Documento informatico che pianifica le attività volte alla realizzazione del sistema di protezione e di tutte le possibili azioni indicate dalla gestione del rischio nell'ambito dell'organizzazione di appartenenza</i>
Registro di protocollo	<i>Registro informatico ove sono memorizzate le informazioni prescritte dalla normativa per tutti i documenti ricevuti e spediti da un ente e per tutti i documenti informatici dell'ente stesso</i>
Regolamento eIDAS	<i>L'acronimo significa: electronic IDentification Authentication and Signature. È il Regolamento (UE) № 910/2014 del Parlamento Europeo e del Consiglio, del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE</i>

TERMINE	DEFINIZIONE
Repertorio dei fascicoli	<i>Registro su cui vengono annotati con un numero progressivo i fascicoli secondo l'ordine cronologico in cui si costituiscono all'interno delle suddivisioni del piano di classificazione</i>
Responsabile della conservazione	<i>Soggetto che definisce e attua le politiche complessive del sistema di conservazione e ne governa la gestione con piena responsabilità ed autonomia</i>
Responsabile della gestione documentale	<i>Soggetto responsabile della gestione del sistema documentale o responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi, ai sensi dell'articolo 61 del TUDA</i>
Responsabile della protezione dei dati	<i>Persona con conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, in grado di assolvere ai compiti di cui all'articolo 39 del Regolamento (UE) 2016/679</i>
Riferimento temporale	<i>Insieme di dati che rappresenta una data e un'ora con riferimento al Tempo Universale Coordinato (UTC)</i>
Scarto	<i>Operazione con cui si eliminano definitivamente, secondo quanto previsto dalla normativa vigente, i documenti ritenuti non più rilevanti ai fini giuridico-amministrativo e storico-culturale</i>
Sigillo elettronico	<i>Dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati in forma elettronica, per garantire l'origine e l'integrità di questi ultimi</i>
Sistema di conservazione	<i>Insieme di regole, procedure e tecnologie che assicurano la conservazione dei documenti informatici in attuazione a quanto previsto dall'art. 44, comma 1, del CAD</i>
Sistema di gestione informatica dei documenti	<i>Insieme delle risorse di calcolo, degli apparati, delle reti di comunicazione e delle procedure informatiche utilizzate dalle organizzazioni per la gestione dei documenti. Nell'ambito della pubblica amministrazione è il sistema di cui all'articolo 52 del TUDA</i>
Servizi aziendali	<i>Gli uffici dell'AOO che utilizzano i servizi messi a disposizione dal sistema di protocollo informatico</i>
Utente abilitato	<i>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</i>

1.4 Acronimi e sigle

ACRONIMO	DEFINIZIONE
AOO	Area Organizzativa Omogenea, struttura individuata dall'Amministrazione, che opera su tematiche omogenee e presenta l'esigenza di gestire la documentazione in modo unitario e coordinato
CAD	Decreto Legislativo 7 marzo 2005 n. 82 recante "Codice dell'amministrazione digitale"
GDPR	Regolamento UE n. 679/2016 del Parlamento Europeo e del Consiglio, del 27 aprile 2016 ("General Data Protection Regulation"), relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE
IPA	Indice delle Pubbliche Amministrazioni
PdV	Pacchetto di Versamento - un pacchetto informativo inviato dal produttore al sistema di conservazione secondo un formato predefinito e concordato descritto nel manuale di conservazione
RCD	Responsabile della conservazione digitale
RGD	Responsabile della gestione documentale
RPA	Responsabile Procedimento Amministrativo - il personale che ha la responsabilità dell'esecuzione degli adempimenti amministrativi e/o degli affari
TUDA	Il Decreto del Presidente della Repubblica 20 dicembre 2000 n. 445 recante "Testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa"
UOR	Unità organizzativa responsabile - un insieme di uffici che, per tipologia di mandato istituzionale e competenza, di funzione amministrativa perseguita, di obiettivi e di attività svolta, presentano esigenze di gestione della documentazione in modo unitario e coordinato
PdV	Pacchetto di Versamento - un pacchetto informativo inviato dal produttore al sistema di conservazione secondo un formato predefinito e concordato descritto nel manuale di conservazione
SdP	Sistema Informativo del Protocollo
SIBAR	Sistema documentale informatico adottato dall'Ente

1.5 Eliminazione dei protocolli diversi da quello generale

Conformemente con quanto programmato e illustrato dal presente Manuale, tutti i documenti inviati e ricevuti dall'Ente devono essere registrati ESCLUSIVAMENTE all'interno del registro ufficiale di protocollo informatico, con unica eccezione per la documentazione esclusa dalla protocollazione soggetta a registrazione particolare.

A tal punto infatti si dispone che tutti gli eventuali registri di protocollo interni -diversi dal registro ufficiale di protocollo informatico- siano soppressi ad eccezione dei seguenti repertori:

Decreti;

Determinazioni;

Delibere CdA;

Contratti;

Verbali del Consiglio di Amministrazione;

Verbali del Collegio dei Revisori;

Verbali OIV;

Verbali degli accertamenti delle dichiarazioni sostitutive degli studenti.

2 ASPETTI ORGANIZZATIVI

2.1 Modello organizzativo

Ai fini della gestione documentale l'ERSU Sassari identifica un'unica Area Organizzativa Omogenea. All'interno di essa il sistema per la Protocollazione è unico. Pertanto la documentazione diretta all'esterno (documenti in "uscita"), la documentazione ricevuta (documenti "in entrata") e la corrispondenza interna è gestita attraverso un unico sistema di protocollazione informatico (SIBAR).

In ottemperanza ai previsti adempimenti previsti, l'Ente è accreditato presso l'Indice delle Pubbliche Amministrazioni (IPA), strumento pubblico dove sono riportate le informazioni che individuano l'amministrazione e l'articolazione della sua AOO. Il codice IPA dell'Ente è: **erids_ss**.

I riferimenti registrati sull'IPA sono i seguenti:

Nome esteso	Ente Regionale per Il Diritto allo Studio Universitario di Sassari
Sito istituzionale	www.ersusassari.it
Indirizzo	Via Michele Coppino, 18 - 07100 Sassari (SS)
Cod IPA	erids_ss
Codice Fiscale	80000880908
Tipologia	Pubbliche Amministrazioni
Categoria	Agenzie, Enti e Consorzi Pubblici per il Diritto allo Studio Universitario
Natura Giuridica	Ente avente personalità giuridica di diritto pubblico (L.R. n. 37 del 14 settembre 1987)
Attività Ateco	Attività di supporto all'istruzione
Indirizzo PEC primario	affarigenerali@pec.ersusassari.it
Altre e-mail	affarigenerali@ersusassari.it segreteria.direzione@ersusassari.it
Data Accreditamento	01/06/2010
Acronimo	ERSU - SS

L'IPA è fruibile attraverso la consultazione del proprio sito internet da parte di soggetti pubblici e privati. L'ERSU provvede ad inoltrare all'IPA eventuali successive modifiche dei propri dati aziendali e della propria organizzazione.

L'aggiornamento è curato dal relativo servizio aziendale, individuato dall'atto di organizzazione aziendale, che alla data della redazione della presente versione del Manuale corrisponde al Settore AAGG, RU, Anticorruzione e trasparenza.

L'AOO è ripartita in Unità organizzative responsabili (UOR), ossia gli uffici che, per tipologia di mandato istituzionale e competenza, di funzione amministrativa, e di attività svolta, svolgono compiti di gestione della documentazione unitari e coordinati.

Le UOR costituenti l'ERSU sono individuate come segue:

UOR	Codice univoco
Servizio Amministrativo	050H64
Servizio Utenze	BC9M7G
U.O. Affari Generali e Risorse Umane	4690H6
U.O. Diritto allo Studio, Attività Culturali e Comunicazione	F84K01
U.O. Alloggio e Servizi ricettivi	FLFL2C
U.O. Contabilità Bilancio e Controllo di Gestione	J843NI
U.O. Appalti Contratti ed Economato	KEC9JE
U.O. Mensa Magazzino e Controllo Qualità	L2CGE7
Ufficio per la transizione al Digitale	TWFPOK

Le figure coinvolte nella gestione operativa dei flussi documentali sono le seguenti:

- ✓ il Responsabile della gestione documentale (di seguito RGD) ed eventualmente un suo sostituto, in caso di assenza e impedimento;
- ✓ gli utenti interni appartenenti all'Ente, abilitati all'utilizzo del sistema di gestione informatica dei documenti;
- ✓ il Responsabile della conservazione digitale (RCD).

Oltre alle figure citate, le funzionalità per la gestione documentale possono essere eseguite automaticamente mediante cooperazione software con applicativi terzi. Le attività eseguite in cooperazione applicativa devono sempre essere governate, rintracciabili e autorizzate previo parere del RGD e del Responsabile per la Transizione al Digitale (RTD).

2.2 Il Responsabile della Gestione Documentale (RGD)

Il Responsabile della gestione documentale -istituito presso l'AOO- è preposto al Servizio di tenuta del protocollo informatico, della gestione documentale e degli archivi dell'ERSU.

Egli viene nominato con specifica determinazione del Direttore Generale che individua in un dirigente ovvero funzionario un soggetto in possesso di comprovate competenze giuridiche, informatiche ed archivistiche. Al pari indica anche un suo vicario che esercita le medesime funzioni nei casi di impedimento o assenza. Sia per l'RGD che per il suo vicario è prevista una formazione obbligatoria e continua, a seguito di aggiornamenti normativi e di evoluzione tecnologica, ai sensi dell'art. 61, comma 2, del TUDA.

Non è prevista la figura del Coordinatore della Gestione documentale in quanto l'ERSU è dotato di un'unica AOO.

Il RGD in ottemperanza alle disposizioni delle Linee Guida AGID (§ 3.4) dispone:

- ✓ la stesura del “Manuale di gestione documentale relativo alla formazione, alla gestione, alla trasmissione, all'interscambio, all'accesso ai documenti informatici” nel rispetto della normativa in materia di trattamenti dei dati personali ed in coerenza con quanto previsto nel manuale di conservazione. Ciò avviene in sintonia con il RCD, il Responsabile per la transizione digitale di cui all'art. 17 del CAD previa acquisizione del parere del responsabile della protezione dei dati personali;
- ✓ organizza, in collaborazione col Responsabile del Servizio ICT, il piano per la sicurezza informatica;
- ✓ controlla l'avvenuta eliminazione dei protocolli di settore, dei protocolli multipli e, più in generale, dei protocolli diversi dal protocollo informatico previsto dal TUDA.

Sono ugualmente attribuiti al RGD e al suo vicario i seguenti compiti di:

- ✓ assegnazione, sospensione e disabilitazione delle credenziali di accesso al sistema di gestione informatica dei documenti sia per gli utenti interni all'AOO che per eventuali utenti esterni;
- ✓ conferimento del livello di autorizzazione per l'accesso al sistema di gestione informatica dei documenti, differenziando tra abilitazioni alla consultazione e abilitazioni all'inserimento e alla modifica delle informazioni;
- ✓ definizione dei criteri uniformi di trattamento del documento informatico e, in particolare, di classificazione ed archiviazione;
- ✓ garanzia della corretta produzione e conservazione del registro di protocollo giornaliero e annuale;
- ✓ controllo e garanzia del buon funzionamento degli strumenti e dell'organizzazione delle attività di registrazione di protocollo e di gestione dei documenti e dei flussi documentali, ivi comprese le funzionalità di accesso di cui agli artt. 59 e 60 del TUDA e le attività di gestione degli archivi di cui agli artt. 67, 68 e 69 del TUDA;
- ✓ autorizzazione delle eventuali operazioni di annullamento delle registrazioni di protocollo;
- ✓ accertamento del ripristino delle funzionalità del sistema in caso di guasti e anomalie; tale ripristino deve avvenire entro ventiquattro ore dal blocco delle attività e in ogni modo nel più breve tempo possibile. In caso di prolungata inattività derivante da malfunzionamento del sistema deve prontamente informare il Direttore generale, eventualmente autorizzando il prosieguo dell'impiego del registro di emergenza fino al ripristino della consueta operatività;
- ✓ assicurazione della leggibilità nel tempo di tutti i documenti trasmessi o ricevuti dalla AOO attraverso l'adozione dei formati standard previsti dalla normativa vigente e l'impiego delle prescritte attività di

migrazione, in conformità all'Allegato 2 al documento Formati di file e riversamento delle citate Linee Guida AGID;

- ✓ accertamento della conformità e sicurezza dei luoghi ove sono custodite le copie di salvataggio delle informazioni del sistema di protocollo, del registro di emergenza nonché le copie di cui agli articoli 62 e 63 del TUDA;
- ✓ autorizzazione all'apertura e alla chiusura del registro di emergenza nei casi sopra palesati;
- ✓ predisposizione di periodici controlli a campione sulla congruità delle registrazioni, sulla corretta sequenza della "filiera di produzione documentale" e sull'impiego di un unico registro informatico, effettuando tramite verifiche *ad hoc* il corretto rispetto della classificazione e della fascicolazione archivistica;
- ✓ deve offrire garanzia che le operazioni di registrazione e di segnatura di protocollo si svolgano nel rispetto delle disposizioni del TUDA;
- ✓ deve permettere, su richiesta del Direttore generale o di un Dirigente di Settore, l'abilitazione di eventuali utenti alla protocollazione di documenti informatici sul registro di protocollo generale (ed eventualmente su altri repertori) in aggiunta agli operatori autorizzati.

2.3 Il Responsabile della Conservazione (RCD)

Il Responsabile della conservazione (RCD) è previsto dall'art. 44 (comma 1-quater) del CAD; tale figura, ai sensi del par. 4.5 delle Linee Guida AGID, può coincidere con quella del Coordinatore della gestione documentale, ove nominato.

Egli definisce e attua le politiche complessive del sistema di conservazione e ne governa la gestione con piena responsabilità ed autonomia. Sotto la propria responsabilità, può affidare lo svolgimento delle proprie attività o parte di esse a uno o più soggetti, che all'interno della struttura organizzativa, abbiano specifiche competenze ed esperienze. Tale mandato deve indicare le specifiche funzioni e competenze delegate.

Rientrano tra i compiti del RCD:

- ✓ la designazione ed attuazione delle politiche complessive del sistema di conservazione;
- ✓ la definizione delle politiche di conservazione e i requisiti funzionali del sistema di conservazione, in conformità alla normativa vigente e nel rispetto totale degli standard internazionali, in funzione delle specificità degli oggetti digitali da mandare in conservazione, della natura delle attività che il Titolare dell'oggetto di conservazione svolge e delle caratteristiche del sistema di gestione informatica adottato;
- ✓ la gestione del processo di conservazione e la conformità alla normativa vigente;
- ✓ la generazione e la relativa sottoscrizione del rapporto di versamento, secondo le modalità previste dal Manuale di conservazione;
- ✓ la generazione e la relativa sottoscrizione di un pacchetto di distribuzione con firma digitale o firma elettronica qualificata, nei casi previsti dal Manuale di conservazione;
- ✓ il controllo della corretta funzionalità del Sistema di conservazione;
- ✓ il controllo regolare, con cadenza non superiore ai cinque anni, dell'integrità e della leggibilità dei documenti informatici e delle aggregazioni documentarie degli archivi;

- ✓ la segnalazione subitanea di un possibile degrado dei sistemi di memorizzazione e delle registrazioni e, ove necessario, per ripristinare la corretta funzionalità, onde garantire una corretta conservazione e accesso ai documenti informatici;
- ✓ l'adozione di idonee misure di controllo circa l'obsolescenza dei formati, in sintonia con le disposizioni AGID;
- ✓ la produzione di copie di documenti informatici in relazione all'evolversi del contesto tecnologico, secondo quanto previsto dal Manuale di conservazione;
- ✓ la predisposizione di idonei provvedimenti necessari a garantire la sicurezza fisica e logica del Sistema di conservazione, come previsto dalle Linee Guida;
- ✓ l'assicurazione della presenza di un pubblico ufficiale, nei casi in cui sia richiesto il suo intervento, per l'esplicitazione di determinate procedure documentali, garantendo allo stesso l'assistenza e le risorse necessarie per l'espletamento delle attività al medesimo attribuite;
- ✓ il periodico versamento dei documenti;
- ✓ la predisposizione del Manuale di conservazione, favorendone un periodico aggiornamento in presenza di mutamenti normativi, organizzativi, procedurali o tecnologici di un certo rilievo.

Nel caso in cui il servizio di conservazione venga affidato ad un conservatore qualificato esterno, le attività sopra elencate o alcune di esse (ad esclusione della predisposizione del Manuale di conservazione), potranno essere assegnate al responsabile del Servizio di conservazione, rimanendo in ogni caso inteso che la responsabilità giuridica generale sui processi di conservazione, non essendo delegabile, rimane in capo al Responsabile della conservazione, chiamato anche a svolgere le necessarie attività di verifica e controllo in ossequio alle norme vigenti sui servizi affidati in *outsourcing* dalle PA.

2.4 Utenti interni abilitati al sistema documentale

L'ERSU è suddiviso nella Direzione Generale e due Servizi, il Servizio Amministrativo e il Servizio Utenze e ciascuno di essi è costituito da una pluralità di Settori come da atto di organizzazione aziendale.

Il RGD cura e aggiorna l'elenco degli utenti interni abilitati all'accesso al sistema di gestione documentale, i permessi applicativi e la visibilità dei dati.

Tutti gli utenti interni sono tenuti a consultare con elevata frequenza i documenti assegnati e nel caso ricoprano posizioni apicali o di coordinamento devono curarne lo smistamento ai propri collaboratori o verosimilmente ad altri soggetti aziendali cui i documenti siano di competenza.

L'utente interno, se responsabile di procedimenti amministrativi (RPA), è autorizzato a effettuare la classificazione e la fascicolazione archivistica, secondo quanto stabilito col piano di organizzazione delle aggregazioni documentali allegato al presente manuale.

L'utente interno con qualifica di Dirigente e Coordinatore di Settore è abilitato alla protocollazione interna e in partenza.

L'utente interno con profilo di Funzionario è abilitato alla protocollazione.

Tutti gli utenti interni possono predisporre un protocollo in uscita e indirizzarlo alla registrazione del protocollo: le operazioni obbligatorie e preliminari all'invio di un protocollo in uscita sono la classificazione da realizzare secondo il piano di classificazione e la fascicolazione da realizzare secondo il piano di organizzazione delle aggregazioni documentali.

3 GESTIONE DEI DOCUMENTI

3.1 Il documento informatico

Come riportato nelle Linee Guida AGID (§2.1.1) il documento informatico è formato mediante una delle seguenti modalità:

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

Il documento informatico deve essere identificato in modo univoco e persistente. Nel caso della Pubblica Amministrazione, l'identificazione dei documenti oggetto di registrazione di protocollo è rappresentata dalla segnatura di protocollo univocamente associata al documento. L'identificazione dei documenti non protocollati è affidata alle funzioni del sistema di gestione informatica dei documenti. In alternativa l'identificazione univoca può essere realizzata mediante associazione al documento di una sua impronta crittografica basata su funzioni di *hash* che siano ritenute crittograficamente sicure, e conformi alle tipologie di algoritmi previsti nell'allegato 6 delle linee guida nella tabella 1 del paragrafo 2.2 regole di processamento.

Le stesse Linee stabiliscono, per ogni punto sopra esplicitato, quali siano le operazioni da effettuarsi sul documento informatico per garantire l'immodificabilità e l'integrità:

Modalità di formazione del documento informatico	Attività da attuare sul documento informatico
a)	apposizione di una firma elettronica qualificata, di una firma digitale o di un sigillo elettronico qualificato o firma elettronica avanzata
	memorizzazione su sistemi di gestione documentale che adottino idonee misure di sicurezza ai sensi del paragrafo 3.9 delle Linee Guida
	trasferimento a soggetti terzi attraverso un servizio di posta elettronica certificata o un servizio elettronico di recapito certificato qualificato, come definito dal Regolamento (UE) 23 luglio 2014 n. 910 del Parlamento europeo e del Consiglio in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno (regolamento eIDAS), valido ai fini delle comunicazioni elettroniche aventi valore legale
	versamento ad un sistema di conservazione

b)	apposizione di una firma elettronica qualificata, di una firma digitale o di un sigillo elettronico qualificato o firma elettronica avanzata
	memorizzazione su sistemi di gestione documentale che adottino idonee misure di sicurezza ai sensi del paragrafo 3.9 delle Linee Guida
	versamento ad un sistema di conservazione
c)	apposizione di una firma elettronica qualificata, di una firma digitale o di un sigillo elettronico qualificato o firma elettronica avanzata
	registrazione nei log di sistema dell'esito dell'operazione di formazione del documento informatico, compresa l'applicazione di misure per la protezione dell'integrità delle basi di dati e per la produzione e conservazione dei log di sistema
	produzione di una estrazione statica dei dati e il trasferimento della stessa nel sistema di conservazione
d)	apposizione di una firma elettronica qualificata, di una firma digitale o di un sigillo elettronico qualificato o firma elettronica avanzata
	registrazione nei log di sistema dell'esito dell'operazione di formazione del documento informatico, compresa l'applicazione di misure per la protezione dell'integrità delle basi di dati e per la produzione e conservazione dei log di sistema
	produzione di una estrazione statica dei dati e il trasferimento della stessa nel sistema di conservazione

Quando si attua la formazione di un documento informatico immutabile è necessario generare e associare in modo stabile e permanente ad esso i relativi metadati.

3.2 Copie per immagine su supporto informatico di documenti analogici

La copia per immagine su supporto informatico di un documento analogico è generata mediante processi e strumenti che assicurino che il documento informatico presenti contenuto e forma identici a quelli del documento analogico da cui è tratto, previo raffronto dei documenti o, nel caso di esigenze di dematerializzazione massiva di documenti analogici, attraverso opportuna certificazione di processo nei casi in cui siano adottate tecniche in grado di garantire la corrispondenza della forma e del contenuto dell'originale e della copia.

I requisiti tecnici per la certificazione di processo sono individuati nell'allegato 3 "Certificazione di Processo" delle Linee Guida.

Fermo restando quanto previsto dall'art. 22, comma 3, del CAD nel caso in cui non vi sia l'attestazione di un pubblico ufficiale, la conformità della copia per immagine ad un documento analogico è garantita mediante l'apposizione della firma digitale o firma elettronica qualificata o firma elettronica avanzata o altro tipo di

firma ai sensi dell'art. 20, comma 1 bis, ovvero del sigillo elettronico qualificato o avanzato da parte di chi effettua il raffronto.

Laddove richiesta dalla natura dell'attività, l'attestazione di conformità delle copie per immagine su supporto informatico di un documento analogico può essere inserita nel documento informatico contenente la copia per immagine o essere prodotta come documento informatico separato contenente un riferimento temporale e l'impronta di ogni copia per immagine. Il documento informatico contenente l'attestazione è sottoscritto con firma digitale o firma elettronica qualificata o avanzata del notaio o del pubblico ufficiale a ciò autorizzato.

La distruzione degli originali analogici potrà essere effettuata in accordo con le previsioni di cui all'art. 22, commi 4 e 5 del CAD.

3.3 Duplicati, copie ed estratti informatici di documenti informatici

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

La copia di un documento informatico è un documento il cui contenuto è il medesimo dell'originale, ma con una diversa evidenza informatica rispetto al documento da cui è tratto.

L'estratto di un documento informatico è una parte del documento con una diversa evidenza informatica rispetto al documento da cui è tratto. Tali documenti hanno lo stesso valore probatorio dell'originale da cui hanno origine se la stessa conformità non viene espressamente disconosciuta. In particolare, la validità del documento informatico per le copie e/o estratti di documenti informatici è consentita mediante uno dei due metodi:

- raffronto dei documenti
- certificazione di processo.

I requisiti tecnici per la certificazione di processo sono individuati nell'allegato 3 - "Certificazione di Processo" delle Linee Guida.

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

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

Laddove richiesta dalla natura dell'attività, l'attestazione di conformità delle copie o estratti informatici di documenti informatici può essere inserita nel documento informatico contenente la copia o l'estratto.

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

3.4 Il documento amministrativo informatico

Al documento amministrativo informatico si applicano le stesse regole valide per il documento informatico.

Il documento amministrativo informatico assume le caratteristiche di immodificabilità e di integrità, oltre che con le modalità di cui al precedente paragrafo, anche con la sua registrazione nel registro di protocollo, negli ulteriori registri, nei repertori, negli albi, negli elenchi, negli archivi o nelle raccolte di dati contenute nel sistema di gestione informatica dei documenti.

Al documento amministrativo informatico viene associato l'insieme dei metadati previsti per la registrazione di protocollo ai sensi dell'art. 53 del TUDA, nonché i metadati relativi alla classificazione, ai sensi dell'articolo 56 del TUDA, e ai tempi di conservazione, in coerenza con il piano di conservazione, e quelli relativi alla relazione con l'aggregazione documentale informatica d'appartenenza.

Al documento amministrativo informatico sono associati ulteriori metadati rilevanti ai fini amministrativi o per finalità gestionali o conservative, definiti, per ogni tipologia di documento, nell'ambito del contesto a cui esso si riferisce, secondo quanto previsto dall'Allegato 5 alle Linee Guida.

Sono inclusi i documenti soggetti a registrazione particolare, come identificati nel presente Manuale, che comunque devono contenere al proprio interno o avere associati l'insieme minimo dei metadati previsti per il documento amministrativo informatico.

In applicazione dell'art.23-ter, comma 5 bis, del CAD, i documenti amministrativi informatici devono essere accessibili secondo le regole previste dall'art. 11 della legge n. 4/2004.

Laddove possibile, qualsiasi documento amministrativo informatico, compresi gli allegati, deve essere convertito e gestito sul sistema documentale in formato PDF/A.

Sui documenti amministrativi informatici deve essere apposta la firma digitale avendo cura di verificare la validità della firma attraverso una delle diverse applicazioni disponibili.

Ogni documento, formato per essere inoltrato all'esterno o all'interno in modo formale, deve indicare:

- ✓ la corretta indicazione del settore o della sede che ha prodotto il documento;
- ✓ la corretta indicazione del servizio che ha prodotto il documento;
- ✓ il numero degli allegati, qualora siano presenti;
- ✓ l'oggetto del documento;
- ✓ la sottoscrizione;
- ✓ le modalità di spedizione;
- ✓ la classificazione.

Non è consentita la produzione di documenti con sottoscrizioni "ibride" (ovvero corredate di firma autografa + firma digitale).

Per i documenti acquisiti come copia di documenti analogici (con e senza firma analogica) occorre mantenere l'originale cartaceo e attenersi a quanto disposto nella sezione 2.2 delle Linee guida: "Copie per immagine su supporto informatico di documenti analogici".

3.5 Formati di firma digitale

I formati di firma digitale previsti sono essenzialmente 3:

A) **PADES**. La firma PAdES (acronimo di PDF Advanced Electronic Signature) permette di firmare esclusivamente file in formato PDF. Il documento mantiene il proprio nome, il suo formato e la sua estensione, anche dopo essere stato sottoscritto digitalmente. La busta crittografica che sarà generata avrà sempre l'estensione “.pdf” e il certificato di firma viene incorporato direttamente nel file “.pdf”, rimanendo associato al documento firmato. Questi documenti possono essere aperti e letti con un qualsiasi lettore di file PDF e possono riportare una firma visibile. Può essere utilizzato (ed è consigliato) solo per i documenti con estensione .pdf.

B) **CAdES**. La firma CAdES (acronimo di Cryptographic Message Syntax Advanced Electronic Signature) permette la firma di qualsiasi tipologia di file (PDF, fogli Word, immagini, fogli di calcolo). Il documento, una volta firmato con questa modalità, modifica il suo nome. Si crea infatti una “busta crittografica” (cioè un nuovo file, che ha una sua estensione specifica e che al proprio interno contiene il documento da firmare) avente come estensione “.p7m”, che racchiude sia il file firmato sia la sua impronta cifrata col certificato privato di firma. Bisogna rilevare che l'estensione “.p7m”, può essere letta solo attraverso un apposito software di firma digitale. Infine si ricorda come tutte le firme CAdES non sono visibili graficamente.

C) **XAdES**. Il formato XAdES (XML Advanced Electronic Signature) è lo standard per la sottoscrizione elettronica dei documenti in formato XML. Grazie a questa modalità è possibile firmare agendo sui “metadati” del documento, ossia su quelle informazioni sul documento scritto in XML. Come per il formato PAdES, il certificato di firma viene incapsulato all'interno del file “.xml” che, pertanto, manterrà la medesima estensione anche dopo la sottoscrizione digitale.

È tuttavia preferibile ricondurre l'uso di firma digitale ai soli formati descritti ai punti A e B.

3.6 Formati dei documenti

I formati da utilizzare sono quelli previsti dall'Allegato 2 “Formati di file e riversamento” delle Linee Guida. Nel prediligere i formati di file, da utilizzare per i propri documenti informatici, sono scelti formati aperti, non proprietari, standard *de iure*, estendibili, parlanti, completamente robusti, indipendenti dal dispositivo.

Il formato raccomandato per la produzione di documenti informatici (ovvero non più modificabili) è il PDF/A. Si tratta di uno standard internazionale (ISO19005), sottoinsieme dello standard PDF, appositamente pensato per l'archiviazione nel lungo periodo di documenti elettronici.

È uno standard che garantisce la visualizzazione di un documento sempre allo stesso modo, anche a distanza di tempo e con programmi software diversi. Inoltre il PDF/A contiene le sole informazioni necessarie per visualizzare il documento come nel momento in cui è stato formato. Tutto il contenuto visibile del documento deve essere incluso, come il testo, le immagini, vettori grafici, fonts, colori e altro. Non può contenere macro-istruzioni o riferimenti ad elementi od informazioni (come i font) non contenuti nel file stesso.

Il PDF/A è il formato migliore per registri e documenti firmati digitalmente perché consente di apporre una firma elettronica specificando solo alcuni requisiti minimi. In questo modo i registri e i documenti potranno essere firmati in modo digitale anche in futuro, utilizzando le nuove tecnologie che si svilupperanno.

Il formato PDF/A si basa sulla versione originale PDF 1.4 e ha due livelli di conformità:

- Il **PDF/A-1a** è conforme al Livello A e soddisfa tutti i requisiti specificati. Consente al software di tecnologia assistiva di migliorare l'accessibilità per utenti con disabilità fisiche.
- Il **PDF/A-1b** ha un livello di conformità inferiore con requisiti minimi, al fine di garantire che l'aspetto visivo del file sia preservato nel tempo.

Per le esigenze dell'Ente non è necessario utilizzare formati diversi da quelli elencati nell'Allegato 2 "Formati di file e riversamento" delle Linee Guida. Pertanto, ai sensi di quanto previsto al paragrafo 3.1 del suddetto Allegato 2, non vi è l'obbligo annuale della valutazione di interoperabilità.

4. IL PROTOCOLLO INFORMATICO

4.1 Le registrazioni di protocollo

La registrazione di protocollo è l'insieme dei metadati che il registro di protocollo deve memorizzare per tutti i documenti ricevuti o spediti e per tutti i documenti informatici che non rientrano tra le tipologie specificate dall'art. 53 del TUDA e che non sono oggetto di registrazione particolare, al fine di garantirne l'identificazione univoca e certa.

Il Registro di protocollo è il registro informatico ove sono memorizzate le informazioni prescritte dalla normativa per tutti i documenti ricevuti e spediti da un ente e per tutti i documenti informatici dell'ente stesso. Le informazioni contenute nel registro di protocollo sono quelle previste dall'art. 53 comma 1 del TUDA.

La numerazione delle registrazioni di protocollo è unica per tutti i settori che compongono l'Ente ed è rigidamente progressiva, senza distinzione fra documenti ricevuti, spediti e interni. Essa si chiude il 31 dicembre di ogni anno e viene rinnovata all'inizio di ogni anno solare.

Il numero di protocollo è univoco e conseguentemente 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 collegati tra loro.

La produzione delle registrazioni di protocollo informatico, l'operazione di "segnatura" delle stesse e le modalità di registrazione delle informazioni annullate o modificate nell'ambito di ogni sessione di attività di registrazione sono demandate al Sistema Informativo del Protocollo (SdP). Il sistema di sicurezza del SdP garantisce la protezione di tali informazioni, operando controlli d'accesso e i livelli di autorizzazione realizzati.

È vietata la registrazione di protocollo senza associare il documento a cui si riferisce.

Non è consentita la protocollazione di un documento che sia già stato protocollato.

La registrazione di protocollo, per ogni documento ricevuto o spedito, è effettuata mediante la memorizzazione nel sistema delle seguenti informazioni, obbligatorie ed immutabili:

- ✓ numero di protocollo del documento generato automaticamente dal sistema, come da segnatura;
- ✓ data di registrazione di protocollo, come da segnatura;
- ✓ il corrispondente, ovvero il mittente per il documento in entrata, il destinatario per il documento in uscita;
- ✓ l'oggetto;
- ✓ l'impronta del documento informatico (costituita dalla sequenza di simboli binari in grado di identificarne univocamente il contenuto, registrata in forma non modificabile);
- ✓ allegati della registrazione di protocollo in arrivo e in partenza (o di repertorio) con indicazione del numero e con descrizione sinottica;
- ✓ Le informazioni obbligatorie e immutabili sono: oggetto, classificazione, destinatario, dell'assegnatario per competenza;
- ✓ Unità organizzativa responsabile del procedimento/affare/attività (UOR);
- ✓ Responsabile del procedimento amministrativo (RPA);
- ✓ Classificazione archivistica;
- ✓ Fascicolo

Le informazioni non obbligatorie e modificabili sono tutte le altre tipologie di annotazione e nota che integrano la registrazione.

L'assegnazione delle informazioni nelle operazioni di registrazione di protocollo è effettuata dal sistema in unica soluzione, con esclusione di interventi intermedi, anche indiretti, da parte dell'operatore, garantendo la completezza dell'intera operazione di modifica o registrazione dei dati.

Ogni utente adibito al servizio di protocollo è autorizzato dal RGD a svolgere attività di protocollazione e segnatura su tutta la corrispondenza in uscita e in arrivo per il proprio ambito (sia in formato cartaceo che telematico).

4.2 La segnatura di protocollo

La segnatura di protocollo è l'apposizione o l'associazione all'originale del documento, in forma permanente, non modificabile, delle informazioni riguardanti la registrazione di protocollo. Essa consente di individuare ciascun documento in modo inequivocabile; viene effettuata contemporaneamente all'operazione di registrazione di protocollo.

La registrazione e la segnatura costituiscono un'operazione unica e contestuale avente entrambe la natura di atto pubblico. Non potranno, quindi, essere effettuate registrazioni di protocollo senza disporre del documento a cui la registrazione si riferisce.

Le informazioni minime apposte od associate al documento mediante l'operazione di segnatura sono quelle riportate all'art. 55 del TUDA:

- ✓ il progressivo di protocollo (composto da n. 7 cifre + anno es. 0000001/21);
- ✓ la data di protocollo;
- ✓ l'identificazione in forma sintetica dell'AOO (ERSU SASSARI) e il codice IPA.

L'azione di segnatura di protocollo può includere il codice identificativo del settore cui il documento è assegnato o il codice del settore che ha prodotto il documento, l'indice di classificazione del documento e ogni altra informazione utile o necessaria, qualora tali informazioni siano disponibili già al momento della registrazione di protocollo.

4.3 Allegati alla registrazione

Il peso massimo di ogni allegato che può essere associato ad una bozza di documento o ad una registrazione è di 100 mega; il sistema avvisa l'utente dell'impossibilità di inserimento di un allegato che ecceda tale limite.

Per la spedizione PEC dal sistema Sibar è necessario non superare il limite di 100 mega, ottenuto moltiplicando il peso complessivo degli allegati per il numero dei destinatari.

Le operazioni di registrazione indicate all'articolo 53 del DPR 445/2000 e le operazioni di segnatura di protocollo di cui all'articolo 55 dello stesso DPR nonché le operazioni di classificazione sono operazioni necessarie e sufficienti per la tenuta del sistema di gestione informatica dei documenti da parte delle pubbliche amministrazioni.

4.4 Registrazione delle informazioni annullate o modificate

L'articolo 54 del D.P.R. 445/2000 Informazioni annullate o modificate indica che le informazioni non modificabili di cui all'articolo 53 lett. a), b), c), d) e) ed f), in quanto registrate in forma non modificabile, sono annullabili con l'utilizzo di una procedura di annullamento di seguito analizzata, secondo cui le informazioni annullate devono rimanere memorizzate nella base di dati per essere sottoposte alle elaborazioni previste dalla procedura.

L'annullamento riporta, secondo i casi, una dicitura o un segno in posizione sempre visibile e tale, comunque, da consentire la lettura di tutte le informazioni originarie unitamente alla data, all'identificativo dell'operatore ed agli estremi del provvedimento d'autorizzazione. In ottemperanza al paragrafo 3.1.5 delle Linee guida AgID, il sistema SIBAR impiegato dall'ERSU impedisce la modifica dei dati essenziali di una registrazione di protocollo, oltre alla sostituzione del documento principale e degli allegati, successivamente alla registrazione.

Bisogna differenziare la bozza di documento, che non è registrata con un numero di protocollo, ma ha associato solo un numero identificativo (ID) attribuito dal sistema, dal documento protocollato, a cui si applica il disposto dell'articolo 54 già riportato:

Documento in bozza: all'eliminazione delle bozze di documenti può provvedere autonomamente il creatore o l'assegnatario della bozza attraverso il tasto *Elimina* nella scheda *Dettaglio* del documento;

Documento protocollato: per l'annullamento di documenti registrati a protocollo ma non ancora spediti, inclusi i documenti relativi alle serie tipologiche (es. determinazione, contratto, decreto, ecc.) la richiesta va inoltrata attraverso il pulsante *Invia in annullamento* nella scheda *Dettaglio* del documento, motivando in modo preciso la ragione della richiesta e selezionando un utente abilitato all'annullamento, che ha sul sistema SIBAR il profilo di Responsabile della gestione documentale.

L'annullamento può avvenire:

Per errore materiale: registrazione in uscita anziché in entrata, mancata valorizzazione della serie tipologica o errore nella valorizzazione della serie tipologica, utilizzo della funzionalità *Nuovo protocollo* al posto di *Nuovo documento*, doppia registrazione di un documento già protocollato;

In seguito ad analisi del contenuto da parte della struttura che ha prodotto il documento: ragioni di opportunità, necessità, autotutela, errore, ecc.

Il sistema memorizza la registrazione originaria annullata contrassegnando il documento con la specifica dicitura *Annullato* e ne consente la visibilità. Se il documento di cui si intende richiedere l'annullamento è stato spedito, con successivo atto della stessa tipologia deve essere data comunicazione ai destinatari originari unitamente con le ragioni dell'annullamento.

4.5 Registro di emergenza

Qualora si verifichi la presenza di problemi tecnici che renda indisponibile il sistema (come per esempio il mancato funzionamento del sistema stesso, una mancanza del collegamento di rete, una interruzione di energia elettrica et al.), il Responsabile della gestione documentale o il suo vicario, per le registrazioni che non è possibile rimandare al momento del ripristino del sistema, attivano il registro di emergenza, della cui conservazione e gestione sono responsabili.

Il registro si apre a partire dalla giornata in cui il sistema non è operativo e si chiude al termine del disservizio; al termine dell'emergenza, ad ogni registrazione effettuata sul registro viene attribuito un nuovo numero di protocollo generale, continuando la numerazione raggiunta al momento dell'interruzione del servizio. A questa registrazione è associato anche il numero di protocollo e la data di registrazione riportati sul protocollo di emergenza.

Le operazioni da effettuare al ripristino consisteranno, inoltre, nella stampa dell'etichetta e nella scansione dei documenti (se trattasi di documenti cartacei) o nell'importazione del documento e apposizione della segnatura elettronica (se trattasi di documenti informatici).

I documenti annotati nel registro di emergenza e che successivamente sono trasportati nel protocollo generale presenteranno dunque doppia numerazione, una riferibile al protocollo di emergenza e un'altra al protocollo generale. La data in cui è stata effettuata la protocollazione sul registro di emergenza è quella a cui

si fa riferimento per la decorrenza dei termini del procedimento amministrativo: così facendo sarà assicurata la corretta sequenza dei documenti che fanno parte di un determinato procedimento amministrativo.

Se si verifica un perdurare della condizione di inagibilità del sistema, comunque entro le ventiquattro ore, per cause di eccezionale gravità, il RGD autorizza l'uso del registro di emergenza per periodi successivi di non più di una settimana.

Per ogni giornata in cui si impiega la registrazione di emergenza viene indicato sul relativo registro il numero totale di operazioni registrate manualmente.

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 dell'AOO.

Di seguito sono riportati i campi da compilare nel registro di emergenza presenti nel file *excel*, allegato del presente *Manuale*.

- ✓ Data documento¹;
- ✓ Data arrivo²;
- ✓ Data di protocollo³;
- ✓ Numero⁴;
- ✓ Anno⁵;
- ✓ Repertorio⁶;
- ✓ Numero Repertorio⁷;
- ✓ Numero di protocollo⁸;
- ✓ Ufficio⁹;
- ✓ Data registro¹⁰;
- ✓ Ora registro¹¹;
- ✓ Classificazione¹²;
- ✓ Oggetto¹³;
- ✓ Allegati¹⁴.

¹ È la data del protocollo del mittente, se disponibile.

² È la data di arrivo del documento ricevuto, se disponibile.

³ È la data di protocollo del mittente, se disponibile.

⁴ È il numero di protocollo del mittente, se disponibile.

⁵ È l'anno del protocollo del mittente, se disponibile.

⁶ È la serie di repertorio del documento ricevuto, se presente.

⁷ È il numero di repertorio del documento ricevuto, se presente.

⁸ È il numero di protocollo di emergenza, progressivo per anno.

⁹ È l'ufficio che effettua la registrazione di emergenza (numero di CDR della AOO).

¹⁰ È la data della registrazione di emergenza.

¹¹ È l'ora della registrazione di emergenza (hh/mm).

¹² È la classificazione archivistica del documento.

¹³ È l'oggetto del documento. Si ricorda che l'oggetto è la sintesi dei contenuti di carattere giuridico, amministrativo e narrativo di un documento, e che oltre a costituire un ambito per la ricerca del documento, ha la fondamentale funzione di contribuire a identificarlo e a definirne la relazione con il fascicolo e con gli altri elementi del contesto documentario a cui appartiene.

¹⁴ Indica numero di allegati presenti (eventualmente con annotazione riassuntiva della loro tipologia).

Sul registro sono riportate la causa, la data e l'ora di inizio dell'interruzione del funzionamento del protocollo generale.

4.6 Documenti esclusi dalla registrazione di protocollo

Si ricorda come l'art. 53 comma 5 del TUDA stabilisce come siano «oggetto di registrazione obbligatoria i documenti ricevuti e spediti dall'amministrazione e tutti i documenti informatici. Ne sono esclusi le gazzette ufficiali, i bollettini ufficiali e i notiziari della pubblica amministrazione, le note di ricezione delle circolari e altre disposizioni, i materiali statistici, gli atti preparatori interni, i giornali, le riviste, i libri, i materiali pubblicitari, gli inviti a manifestazioni e tutti i documenti già soggetti a registrazione particolare dell'amministrazione».

A tal fine, essendo soggette a registrazione particolare sul sistema di gestione informatica dei documenti, non sono protocollate le seguenti tipologie documentali¹⁵:

- Deliberazioni del Consiglio di Amministrazione;
- Determinazioni del Direttore generale;
- Determinazioni dei Dirigenti di settore;
- Decreti del Presidente;
- Decreti del Commissario straordinario;
- Verbali del Consiglio di Amministrazione;
- Verbali del Collegio dei Revisori;
- Verbali dell'Organismo Indipendente di Valutazione;
- Verbali di accertamento di veridicità delle autocertificazioni;
- Contratti.

Sono inoltre indicate, a seguire, ulteriori tipologie documentarie non soggette a protocollazione:

- certificazioni e attestazioni esistenti nelle banche dati dell'Agenzia delle Entrate, dell'INPS, dei Comuni e di altre PP.AA. (in riferimento all'attività di accertamento di veridicità delle dichiarazioni sostitutive di certificazione presentate dai richiedenti i benefici erogati dal Diritto allo Studio Universitario);
- gli estratti conto bancari e postali;
- i bollettini di conto corrente postale;
- gli allegati e tutti i documenti che, essendo corredati da lettera di trasmissione, non hanno bisogno di ulteriore protocollazione;
- gli avvisi di ricevimento delle raccomandate e degli atti giudiziari, spediti tramite servizio postale o corriere, nonché le comunicazioni di avvenuto deposito di raccomandate e atti giudiziari in caso di impossibilità di recapito degli stessi;
- gli atti riservati personali, quali corrispondenza e modelli fiscali (730, CUD, F24, 770, cedolini, etc.);
- le copie dei telegrammi inviati a mezzo telefono o a mezzo web;
- gli originali dei documenti pervenuti anticipatamente via fax, e-mail, PEC o altro mezzo e già protocollati: in questo caso, sull'originale dovrà essere riportato lo stesso numero e la stessa data attribuiti in precedenza;
- i contratti, gli accordi e le intese soggette a diversa repertoriazione;

¹⁵ Devono però essere inserite nei rispettivi repertori e comunque collegate al Sistema.

- i documenti non indirizzati all'ERSU o comunque ad alcuna sua struttura;
- la corrispondenza privata, pervenuta a mezzo posta o corriere tramite busta o plico che riporta solo nome e cognome del destinatario;
- la corrispondenza privata, pervenuta a mezzo posta o corriere tramite busta o plico che riporta le diciture: «riservato», «personale», «s.p.m.», etc.;
- la corrispondenza privata, pervenuta a mezzo posta o corriere tramite busta o plico che hanno carattere di corrispondenza privata (ad es. busta particolare).

Infine la corrispondenza privata non deve essere aperta per motivi di riservatezza e privacy ma consegnata ai destinatari che, verificato il contenuto, potranno richiederne la registrazione.

4.7 Differimento dei termini di protocollazione

Solitamente la registrazione di protocollo deve essere effettuata in giornata e, comunque, entro le 24 ore lavorative successive alla ricezione della corrispondenza.

Tuttavia possono crearsi dei casi in cui per temporaneo ed eccezionale carico di lavoro le operazioni di protocollazione non possano oggettivamente essere effettuate nei termini di cui sopra e qualora dalla mancata registrazione a protocollo del documento nello stesso giorno di arrivo possa venire meno un diritto di terzi il differimento dei termini di registrazione a protocollo può essere autorizzato dal RGD.

Con questa autorizzazione sono indicati:

- la tipologia di documenti da ammettere alla registrazione differita di protocollo;
- le cause che determinano la necessità di procedere al differimento dei termini di registrazione;
- la durata del periodo di differimento, entro il quale tutte le registrazioni di protocollo debbono essere effettuate (massimo 3 giorni lavorativi).

In seguito, nel procedere alla registrazione di protocollo della documentazione precedentemente timbrata e siglata, l'addetto al protocollo inserisce nel sistema di gestione informatica dei documenti la data di effettivo arrivo del documento che, in tal caso, assume valore legale anche se precedente a quella di protocollo.

5. CLASSIFICAZIONE E FASCICOLAZIONE

5.1 Piano di classificazione

L'ERSU è dotato di un proprio Piano di classificazione, allegato al presente manuale, come previsto dalla normativa vigente¹⁶.

Il Piano di classificazione indica ed articola, su più livelli gerarchici, tutte le funzioni dell'Ente.

Come espresso nelle Linee guida si ricorda che la classificazione è un'attività obbligatoria nel sistema di gestione informatica dei documenti dell'AOO e si applica a tutti i documenti prodotti e acquisiti dalla stessa AOO sottoposti o meno alla registrazione di protocollo. Le informazioni relative alla classificazione nei casi dei documenti amministrativi informatici costituiscono parte integrante dei metadati previsti per la formazione dei documenti medesimi.

Il Responsabile della gestione documentale verifica periodicamente la rispondenza del piano di classificazione ai procedimenti amministrativi e agli affari in essere e procede al suo aggiornamento, curandone periodica revisione e aggiornamento.

5.2 Aggregazioni documentali (fascicoli)

La Pubblica Amministrazione documenta la propria attività Attraverso le funzioni del Sistema di gestione informatica dei documenti finalizzate alla produzione, alla gestione e all'uso delle aggregazioni documentali informatiche, corredate da opportuni metadati.

La documentazione ricevuta e prodotta deve essere tutta inserita in apposito fascicolo, in relazione al procedimento amministrativo o funzione che lo stesso rappresenta.

Infatti il fascicolo rappresenta l'unità di base dell'archivio. Ogni fascicolo contiene documenti che concorrono ad uno stesso affare, attività o procedimento, classificati in maniera omogenea, in base al contenuto e secondo il grado divisionale attribuito dal Piano di classificazione adottato.

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

Eventuali sottofascicoli, se istruiti, presentano il medesimo ordine cronologico di sedimentazione. Questa sottounità è rappresentativa di un endoprocedimento o sub-procedimento e può essere chiusa prima del fascicolo, ma non viceversa: la chiusura del fascicolo implica la chiusura dei relativi sottofascicoli. Nel sistema SIBAR tale ordine, stabilito di default, può essere modificato dall'utente, scegliendo di disporre i documenti in base all'identificativo o alla data di protocollo.

L'obbligo di fascicolatura dei documenti riguarda sia i documenti contraddistinti dalla segnatura di protocollo sia i documenti procedurali non registrati.

Sono presenti cinque tipologie di fascicolo trattate dell'Ente:

- ✓ Fascicolo per Affare: conserva i documenti relativi a una competenza non proceduralizzata né procedimentalizzata; per gli affari non esiste un termine per la conclusione previsto da norme. Ne sono esempio l'istituzione di un gruppo di lavoro, l'organizzazione di un corso di formazione (che non

¹⁶ Cfr. Linee Guida AGID, PAR. 3.2.

avvenga attraverso un affidamento), l'attività di affiancamento e coordinamento di gestione documentale;

- ✓ Fascicolo per Attività: conserva i documenti relativi a una competenza proceduralizzata, per la quale esistono documenti vincolati o attività di aggiornamento procedurale e per la quale non è comunque prevista l'adozione di un provvedimento finale. Alcuni esempi sono rintracciabili nei pareri, nelle consulenze legali, nella pubblicazioni di atti;
- ✓ Fascicolo per Procedimento amministrativo: al suo interno si sedimentano diversi documenti che rappresentano azioni amministrative omogenee e destinate a concludersi con un provvedimento finale (es. gli atti di un concorso, la costruzione di opere, l'affidamento attraverso gara, la fornitura di beni e servizi, l'approvazione bilancio);
- ✓ Fascicolo per Persona fisica: custodisce i documenti relativi a diversi procedimenti amministrativi, distinti per affari o per attività e uniti da un vincolo archivistico interno, relativo a una persona fisica determinata (es. fascicoli del Personale). La chiusura del fascicolo dipende dalla conclusione del rapporto giuridico con l'Ente;
- ✓ Fascicolo per Persona giuridica: conserva i documenti relativi a una persona giuridica con modalità simili a quelle del fascicolo di persona fisica (es. fascicoli di impresa o di associazioni).

Costituiscono altre forme di aggregazioni documentali informatiche i Repertori che raccolgono particolari tipologie documentarie (es. Pareri, Decreti, Determinazioni etc.) e i Repertori dei fascicoli. Questi sono costituiti dalle unità archivistiche create dall'AOO, ordinate all'interno di ogni classe di riferimento. Ad effettuare l'estrazione del Repertorio dei fascicoli è il Responsabile della gestione documentale o da un suo vicario.

Il sistema SIBAR consente di aprire e alimentare il fascicolo in tutte le fasi della gestione corrente del documento. Consente anche di modificarne la denominazione e di assegnarlo ad altri utenti con i quali si intendono condividere le autorizzazioni. Il numero progressivo del fascicolo è assegnato automaticamente dal sistema con riferimento all'anno; l'insieme dei fascicoli creati nella AOO costituisce il Repertorio dei fascicoli.

Il fascicolo può essere creato anche prima dell'esistenza di documenti da inserirvi, nell'imminenza dell'avvio di una attività o di un procedimento o relativamente alle serie tipologiche (determinazioni, decreti, contratti, ecc.).

Il Piano di conservazione, allegato al presente Manuale, definisce la durata dei fascicoli a seconda dell'attività, affare o procedimento al quale si riferisce. Una eventuale riapertura di un fascicolo chiuso è consentita solo al creatore della medesima unità archivistica e agli assegnatari del medesimo.

5.2.1 Tipologie di fascicolo

Attualmente l'Ente produce le seguenti tipologie di fascicolo:

- ✓ fascicoli digitali: tutta la documentazione originale della pratica è prodotta in formato elettronico. Rappresentano la maggioranza della produzione documentale;
- ✓ fascicoli ibridi: la documentazione riguardante la pratica è formata da documenti prodotti, in originale, sia in formato cartaceo che in formato elettronico. In questi casi vengono prodotti due fascicoli distinti:
 - un fascicolo cartaceo, nel quale viene raccolta la documentazione cartacea;
 - un fascicolo informatico, archiviato nel sistema di gestione documentale, nel quale sono raccolti tutti i documenti prodotti in formato elettronico e i documenti prodotti

in formato cartaceo, dei quali è prodotta copia informatica (a seguito di scansione ottica);

L'esistenza di fascicoli ibridi deve essere considerata un'eccezione. Nel caso in cui si debba procedere alla creazione di un fascicolo cartaceo, sulla copertina del fascicolo deve essere riportato il riferimento al fascicolo digitale corrispondente e, viceversa, nel Sistema SIBAR, nel campo "Descrizione del fascicolo digitale" deve essere riportato il riferimento all'esistenza di un fascicolo cartaceo.

- ✓ fascicoli cartacei: l'unica eccezione è rappresentata dalla produzione e custodia dei fascicoli del personale.

6. FLUSSI DI LAVORO

Vengono di seguito riportati i flussi di lavoro dei documenti ricevuti, inviati e interni.

6.1 Documenti in entrata.

La gestione della documentazione ricevuta dall'Amministrazione si svolge secondo le seguenti fasi:

- a) ricezione;**
- b) protocollazione;**
- c) segnatura;**
- d) assegnazione.**

a) Ricezione

I documenti in entrata possono pervenire attraverso:

- 1) caselle di posta elettronica certificata (PEC);
- 2) caselle di posta non certificata;
- 3) documenti analogici.

1). Posta elettronica certificata (PEC). Come stabilito dalle vigenti normative lo strumento di comunicazione fra gli uffici della Pubblica Amministrazione e fra la Pubblica Amministrazione e altri soggetti qualificati (società partecipate, imprese, ecc.) è la Posta Elettronica Certificata (PEC). I documenti pervenuti alle caselle di posta certificata sono gestiti attraverso il sistema SIBAR, in quanto la PEC è integrata nel sistema.

2). Posta ordinaria. Qualora vi sia la necessità di richiesta di comunicazioni informali, scambi di informazioni non soggette ordinariamente a registrazione di protocollo, possono essere impiegate esclusivamente le caselle mail istituzionali relative agli uffici o ai singoli utenti. Qualora se ne palesi la necessità, sotto valutazione della persona che cura l'istruttoria che valuta il contenuto stesso della mail, si può procedere alla protocollazione in entrata. In tal caso si salva l'intero messaggio mail in formato eml e si acquisisce a sistema. In tal caso viene indicato come "mittente" colui che ha redatto la mail.

3). Documenti analogici. Il documento analogico può giungere all'Ente anche attraverso il servizio postale o tramite consegna a mano.

Il documento cartaceo ricevuto viene sottoposto a scansione per essere in seguito allegato alla registrazione di protocollo e gestito (ovvero smistato e assegnato al dirigente/funziionario, preso in carico, fascicolato e archiviato) in formato digitale. L'originale del documento ricevuto, insieme agli eventuali allegati, deve essere consegnato al Responsabile della gestione documentale con compiti di Responsabile di protocollo, a cui fa capo l'archivio della AOO, per l'archiviazione in luogo sicuro. Sul documento principale e sugli allegati deve essere apposta la segnatura. La documentazione cartacea deve essere periodicamente esaminata ai fini della selezione.

Tutti i documenti ricevuti dall'Amministrazione -in ingresso, interni o indipendentemente dal supporto sul quale sono formati- devono essere protocollati con sistema informatizzato che ne consente l'immediata tracciabilità e reperibilità. L'unica eccezione è rappresentata dalle tipologie di documenti non soggetti a protocollazione come precisato di seguito.

b) Protocollazione

La registrazione dei documenti in ingresso in forma digitale è effettuata dall'operatore di protocollo con l'ausilio delle specifiche funzionalità del SIBAR.

I messaggi di posta elettronica certificata e di posta ordinaria oggetto di protocollazione non devono essere stampati e trasformati impropriamente in documenti analogici per l'apposizione della segnatura di protocollo.

In caso di ricezione di posta cartacea ai fini della protocollazione della stessa e successiva gestione in formato elettronico, il documento cartaceo è acquisito digitalmente attraverso scansione (nel formato PDF/A) ed è allegato alla registrazione di protocollo e gestito (smistato e assegnato al dirigente/funziionario, preso in carico, fascicolato e archiviato) in formato digitale. L'originale del documento ricevuto, insieme ai relativi eventuali allegati, deve essere consegnato al Responsabile della gestione documentale con compiti di Responsabile di protocollo, a cui fa capo l'archivio della AOO, per l'archiviazione in luogo sicuro. Sul documento principale e sugli allegati deve essere apposta la segnatura.

Le registrazioni di protocollo sono eseguite in un'unica operazione, senza possibilità per l'operatore di inserire le informazioni fondamentali - data e numero di protocollo, oggetto, generalità del mittente e/o destinatario in differenti fasi successive.

Ciascuna registrazione di protocollo, ai sensi dell'art. 53 del DPR n. 445/2000, contiene dati obbligatori e dati accessori.

c) Segnatura 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; consente di individuare ciascun documento in modo inequivocabile.

In caso di documento cartaceo, la segnatura è posta, di norma, sul fronte del documento in arrivo attraverso etichetta.

d) Assegnazione

Dopo essere stato sottoposto a registrazione di protocollo e segnatura, ogni documento viene assegnato al settore/servizio di competenza per il successivo trattamento utilizzando le funzionalità del sistema SdP in uso.

La struttura responsabile dell'istruttoria/procedimento che riceve in assegnazione i documenti, detiene, ai sensi della L. 241/90 e ai sensi dell'art. 41 del CAD, l'intero fascicolo, indipendentemente dalla sua natura digitale o cartacea, per tutta la "fase corrente dell'archivio".

L'assegnazione dei documenti può avvenire sia per competenza, nei riguardi del settore/servizio responsabile dell'istruttoria/procedimento, deputata alla fascicolazione ed alla conservazione, sia per conoscenza.

Nel caso di trasmissione non corretta, l'ufficio che riceve il documento lo restituisce, motivando la restituzione, alla struttura mittente, che provvederà a trasmetterlo nuovamente.

16.2 Documenti in uscita

L'elaborazione, la firma e il rispettivo invio di documenti digitali soggetti a registrazione di protocollo o diretti ad altri settori del medesimo Ente avvengono attraverso il sistema SIBAR, che gestisce anche le verifiche di avvenuto recapito dei documenti spediti.

Il ciclo di produzione dei documenti in uscita prevede le seguenti fasi di lavorazione:

- a) formazione del documento;***
- b) sottoscrizione;***
- c) registrazione di protocollo;***
- d) segnatura;***
- e) spedizione.***

a) Formazione del documento

I documenti amministrativi aventi rilevanza esterna devono avere le seguenti informazioni minime:

- Denominazione e logo ERSU Sassari;
- Indirizzo di posta elettronica certificata dell'Ufficio competente;
- Indicazione della struttura (Settore, Servizio, etc.) che ha prodotto il documento e relativi recapiti;
- Data di produzione del documento;
- Oggetto del documento;
- Sottoscrizione digitale del Dirigente/Funzionario responsabile;
- Indicazione del responsabile del procedimento (nei procedimenti amministrativi).

Le firme necessarie alla redazione e perfezione giuridica del documento in partenza vanno apposte prima della sua protocollazione.

b) Sottoscrizione

Ultimata la redazione, il documento viene sottoscritto da colui che è titolare del potere di firma o da un suo delegato, alternativamente:

- con apposizione di firma digitale, nel caso in cui il documento originale sia prodotto in forma elettronica¹⁷;

¹⁷ Si ricorda che, in sintonia coi dettami del CAD e in accordo con gli indirizzi in materia di semplificazione dell'azione amministrativa e di dematerializzazione della documentazione, i documenti devono essere firmati prioritariamente in modalità digitale.

- con apposizione firma autografa, quando l'originale del documento è prodotto in forma cartacea (in casi eccezionali).

Eventuali deleghe di firma, in forza delle quali la sottoscrizione può essere curata da un soggetto diverso dal titolare del potere di firma, devono risultare da specifici atti di delega o di attribuzioni di funzioni delegate, agli atti dell'Amministrazione.

c) Registrazione di protocollo

Tutti i documenti in uscita devono essere registrati, dopo la sottoscrizione, nel Registro Ufficiale di Protocollo, attraverso le specifiche funzionalità del SIBAR.

Ogni registrazione di protocollo deve identificare un solo documento, pertanto non è possibile, ad esempio, attribuire a un documento in uscita lo stesso numero di protocollo attribuito all'eventuale documento in entrata dal quale è scaturita la lavorazione.

La protocollazione dei documenti in uscita (sia in formato digitale che in formato cartacea) è effettuata dalle UOP con l'ausilio delle specifiche funzionalità del SIBAR.

d). Segnatura 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; consente di individuare ciascun documento in modo inequivocabile¹⁸.

e) Spedizione

Un documento sottoscritto e protocollato viene inviato al destinatario utilizzando la modalità telematica (a mezzo posta elettronica o PEC). Vi può essere anche la possibilità, del tutto straordinaria, di presiedere all'invio in modalità cartacea.

Spedizione tramite PEC

Di norma per tutti i destinatari, che devono avere obbligatoriamente un domicilio digitale, il canale di spedizione è la PEC, in grado di attestare l'invio e l'avvenuta consegna di un messaggio di posta e di fornire ricevute opponibili a terzi. La PEC certifica l'invio e la ricezione dei messaggi fornendo al mittente:

- ✓ una ricevuta che costituisce prova opponibile dell'avvenuta spedizione del messaggio (accettazione);
- ✓ una ricevuta di avvenuta (o mancata) consegna, anch'essa prova opponibile a terzi (consegna).

Si evidenzia che il SdP dispone di specifiche funzionalità per l'invio dei documenti in uscita senza necessità di ricorso a sistemi terzi, previa configurazione degli account di posta elettronica istituzionale e di posta elettronica certificata. Lo stesso Sistema gestisce le ricevute di accettazione e di consegna dei messaggi inviati tramite PEC., rendendoli in automatico allegati del documento inviato.

Le comunicazioni tramite i domicili digitali sono effettuate agli indirizzi inseriti nei seguenti elenchi:

¹⁸ L'Ente riduce al minimo la produzione di documenti analogici. Nel caso, residuale, di produzione di un documento cartaceo, la segnatura è posta, di norma, sul fronte del documento in arrivo attraverso etichetta. In tal caso, il sistema di gestione documentale provvede, una volta effettuato il caricamento della copia per immagine su supporto informatico di un documento analogico, ad apporre la segnatura di protocollo anche sul documento in formato pdf generato dal sistema a seguito di acquisizione della scansione del documento originale.

- ✓ Indice nazionale dei domicili digitali (INI-PEC) delle imprese e dei professionisti, istituito presso il Ministero per lo sviluppo economico;
- ✓ Indice degli indirizzi della pubblica amministrazione e dei gestori di pubblici servizi (indice IPA);
- ✓ Indice nazionale dei domicili digitali delle persone fisiche, dei professionisti e degli enti di diritto privato, non tenuti all'iscrizione in albi, elenchi o registri professionali o nel registro delle imprese (Indice INAD).

Le comunicazioni elettroniche trasmesse ad uno dei domicili digitali producono, quanto al momento della spedizione e del ricevimento, gli stessi effetti giuridici delle comunicazioni a mezzo di raccomandata con ricevuta di ritorno ed equivalgono alla notificazione per mezzo della posta, salvo che la legge disponga diversamente. Le suddette comunicazioni si intendono spedite dal mittente, se inviate al proprio gestore, e si intendono consegnate se rese disponibili al domicilio digitale del destinatario, salva la prova che la mancata consegna sia dovuta a fatto non imputabile al destinatario medesimo.

L'invio della documentazione in uscita in modalità digitale (ossia tramite e-mail o PEC) è effettuata dal competente Servizio.

L'invio di posta cartacea mediante servizi postali con relativa affrancatura deve considerarsi attività residuale ed è consentita solo se indirizzata a privati cittadini sprovvisti di un indirizzo digitale.

6.3 Documenti interni

Per direzione INTERNA dei documenti si intende il flusso documentale indirizzato esclusivamente agli uffici e/o a utenti interni. Per legge i documenti scambiati tra uffici interni della stessa AOO non sono soggetti all'obbligo di registrazione sul Registro Ufficiale di Protocollo, lasciando tale facoltà in capo a ciascun Responsabile.

I documenti interni possono distinguersi in documenti informali e documenti formali.

I primi sono di norma documenti di lavoro di natura non ufficiale, temporanea ed interlocutoria a carattere informativo, operativo o preparatorio (ad esempio: scambio di prime bozze di documenti senza annotazioni significative, convocazioni di incontri interni non ufficiali, memorie informali, appunti, ecc.). Si tratta di documenti che non hanno rilevanza amministrativa giuridico-probatoria e non vanno protocollati.

I documenti interni di natura formale sono tutti i documenti interni giuridicamente rilevanti, di natura prevalentemente giuridico-probatoria, e precisamente tutti gli atti redatti dal personale dell'ERSU nell'esercizio dell'espletamento delle proprie funzioni, finalizzati a documentare le attività istruttorie di competenza (ad esempio: relazioni istruttorie, pareri, nulla osta, ecc.) e dai quali possono nascere diritti, doveri o legittime aspettative di terzi.

Il sistema SIBAR permette, attraverso specifica funzione, di gestire questo tipo di comunicazione.

6.4 Documenti soggetti a registrazione di repertorio

I documenti soggetti a registrazione di repertorio devono ricevere una doppia fascicolazione: la prima nel fascicolo annuale della serie tipologica, la seconda nel fascicolo del procedimento al quale appartengono.

A seguire si propone una breve descrizione dei flussi delle serie tipologiche.

- ✓ Delibere del C.d.A.;
- ✓ Delibere del presidente d'urgenza;
- ✓ Determinazioni non contabili;

- ✓ Determinazioni elettroniche contabili;
- ✓ Verbali;
- ✓ Contratti;
- ✓ Ordini di servizio;
- ✓ Circolari;
- ✓ Note;
- ✓ Fatture;
- ✓ Documenti a firma multipla (atti legali; contratti, concessioni, protocolli d'intesa).

6.5 Documenti riservati

Fra le misure impiegate a limitare la visibilità di documenti in entrata in uscita o interni che veicolano dati personali, all'interno del sistema SIBAR è presente la modalità riservata di registrazione, che permette una limitazione dell'accesso alle informazioni ai soli soggetti coinvolti nella relativa istruttoria, i quali devono essere individuati quali assegnatari. Sono oggetto di modalità riservata:

- Documenti legati a vicende di persone o a condizioni e fatti privati.
- Rientrano in questa categoria i documenti contenenti i dati particolari, idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale.
- Inoltre vi rientrano i documenti contenenti i dati relativi alla situazione familiare e ai minori, alla residenza personale, alle assenze, ai provvedimenti disciplinari e alle sanzioni, agli infortuni, alla richiesta di orari particolari, alle relazioni sindacali, ai referti di visite fiscali e a certificati medici, alla valutazione dei dipendenti;
- Documenti di cui il mittente abbia effettuato o previsto un trattamento riservato, se valutato come tale dal ricevente;
- Documenti di carattere politico e di indirizzo di competenza del Presidente o del Direttore o di altro dirigente, che, se resi noti, potrebbero ostacolare il raggiungimento degli obiettivi prefissati;
- Documenti dalla cui contestuale pubblicità possa derivare pregiudizio a terzi o al buon andamento dell'attività amministrativa;
- Documenti relativi all'attività ispettiva;
- Documenti individuati dalla normativa vigente come riservati;
- Eventuali ulteriori tipologie di documenti soggetti a registrazione riservata individuate dal Dirigente.

7.MISURE DI SICUREZZA

Di seguito sono sommariamente indicate le misure di sicurezza impiegate sul sistema SIBAR per garantire un livello di sicurezza adatto al rischio:

- Aggiornamento periodico dell'inventario hardware, software e delle interfacce di tutti gli applicativi;
- Salvataggio giornaliero di tutti gli applicativi e relative basi dati con test periodici con cadenza almeno semestrale dell'efficacia dei backup effettuati e definizione delle procedure di ripristino prestabilite per ciascun applicativo;
- Attivazione di un Security Information and Event Management (SIEM) utilizzato per la produzione e consultazione dei log sui sistemi per la prevenzione e il monitoraggio delle intrusioni;
- Tutti gli accessi alle macchine virtuali e fisiche sulle quali sono installati gli applicativi sono possibili solo da parte di amministratori di sistema opportunamente nominati, con utenze nominative e non condivise;
- Nessun dato dell'ambiente di produzione può essere riversato negli ambienti di pre-produzione, test e/o sviluppo senza l'esplicito consenso scritto da parte del Titolare. Qualora, per esigenze legate al Titolare stesso, quanto sopra fosse effettuato, la permanenza del dato sugli ambienti non produttivi sarà limitata ad un tempo strettamente necessario alle verifiche da parte del Titolare e poi dovrà essere immediatamente cancellato tramite sovrascrittura della base dati da altro ambiente;
- L'accesso a tutti gli applicativi avviene solo tramite Rete Telematica Regionale (RTR) o VPN fornita dal Titolare. Nessun servizio è raggiungibile al di fuori delle Rete Regionale o della VPN suddette;
- L'autenticazione degli amministratori di sistema del vCenter, possibile solo dall'interno della rete regionale o tramite VPN, avviene sulla base di utenze di dominio (RS) di tipo personale;
- L'accesso ai sistemi avviene tramite un software di access manager, l'Oracle Access Manager, che gestisce il single sign on delle utenze. Le password su tale software sono cifrate con un algoritmo standard (SHA-512 - salted). È presente un blocco delle credenziali dopo 8 tentativi di accesso errati;
- Infine tutti i servizi esposti dalle applicazioni utilizzano il protocollo di comunicazione https.

8. ARCHIVIO

8.1 La conservazione dei documenti digitali

Conservare i documenti digitali significa attuare il processo informatico che consente di amministrare l'intero ciclo di vita dei documenti archiviati, certificandone il contenuto tramite apposizione di firma digitale e marca temporale, che rendono un documento imm modificabile, opponibile a terzi e non deteriorabile e disponibile nel tempo in tutta la sua integrità ed autenticità.

Allo stato attuale il sistema SIBAR invia in conservazione le tipologie documentarie riportate nel documento DEFINITO Piano di conservazione, allegato al presente Manuale. Il sistema di conservazione assicura, dalla presa in carico fino allo scarto, la conservazione degli oggetti digitali in esso conservati, attraverso l'impiego di regole e procedure che garantiscono le caratteristiche di autenticità, integrità, affidabilità, leggibilità, reperibilità sia per i documenti amministrativi informatici che per le aggregazioni documentali informatiche (fascicoli e serie). Il sistema di conservazione garantisce l'accesso all'oggetto conservato per il periodo previsto dal Piano di fascicolazione e conservazione, indipendentemente dall'evoluzione del contesto tecnologico.

8.2 Conservazione della documentazione cartacea

Benché l'AOO gestisca i flussi documentali attraverso procedure informatiche vi è la possibilità di avere anche fascicoli cartacei (analogici) relativi ad alcune attività residuali gestite in cartaceo (es. fascicoli del Personale). Ciò determina l'attivazione di adeguate procedure di conservazione, nel rispetto della vigente normativa.

È obbligo che durante la trattazione corrente i documenti cartacei devono essere custoditi all'interno di armadi debitamente chiusi onde evitare accessi non controllati ai dati e alle informazioni ivi contenute.

Generalmente una volta all'anno si individuano i fascicoli cartacei relativi ai procedimenti conclusi o, comunque, non più necessari allo svolgimento delle attività correnti, da trasferire all'archivio di deposito. Di tale operazione è generalmente incaricato il Responsabile del Servizio.

L'archivio di deposito è costituito dai fascicoli contenenti i documenti relativi ad affari e a procedimenti amministrativi conclusi, per i quali non risulti più necessaria una trattazione giornaliera o verso i quali vi sia da parte dell'Ente un interesse amministrativo meno contingente.

Potranno essere trasferiti nell'archivio di deposito unicamente i documenti ordinati e raccolti in fascicoli; non sarà possibile depositare atti e carte sciolte che non sianostate oggetto di fascicolazione, né saranno consentiti trasferimenti di fascicoli o unità di condizionamento contenenti "miscellanee" o "varie". Sarà allo stesso modo evitato ogni deposito di materiale non archivistico (raccolte normative cartacee, libri, cataloghi et al). Il funzionario che ha creato la pratica avrà cura di verificare l'integrità del fascicolo, ispezionando l'eventuale presenza di "doppioni" o copie fotostatiche che dovranno essere rimosse.

Qualora si verificasse la mancanza di uno o più documenti per i quali non sia stato possibile il recupero, il funzionario che ha creato il fascicolo e ne ha curato la gestione richiede il trasferimento segnalando per iscritto l'incompletezza del fascicolo e l'eventuale motivo per cui è incompleto. Si avrà cura di non eliminare bozze o versioni differenti dello stesso documento che ne possano tracciare il processo di elaborazione, né materiali a stampa o di altro genere acquisiti per conoscenza nell'espletamento dell'affare. La documentazione da trasferire dovrà essere predisposta dal Servizio versante in adeguato materiale di condizionamento (cartelline, faldoni), corredato di idonee etichette con l'indicazione sulla cartella e sul dorso della busta dell'Ufficio produttore, o se differente dall'Ufficio versante, recante indicazioni degli estremi cronologici, dell'oggetto, della classificazione, del numero progressivo del faldone.

In caso vi sia un trasferimento o cessazione dal servizio dell'utente le pratiche non devono essere abbandonate ma si provvederà al trasferimento dei documenti ordinati e raccolti in fascicoli al nuovo assegnatario. Nel caso si registrino rischi di dispersione, il Responsabile della gestione documentale potrà

disporre d'ufficio il trasferimento nell'archivio di deposito della documentazione esaurita da almeno un quinquennio.

- ✓ Un eventuale spostamento della documentazione è soggetto, in alcuni casi, a comunicazione, in altri, ad autorizzazione da parte della Soprintendenza archivistica della Sardegna. In particolare:
- ✓ Lo spostamento di archivi correnti comporta l'obbligo di comunicazione alla Soprintendenza archivistica della Sardegna, ai sensi dell'art. 21, c. 3 del D. Lgs n. 42 del 2004;
- ✓ Lo spostamento, anche temporaneo, di documenti dell'archivio di deposito o dell'archivio storico da un locale ad un altro deve essere autorizzato, ai sensi dell'art. 21, c. 1, lettera b) del D. Lgs n. 42 del 2004, dalla Soprintendenza archivistica della Sardegna;
- ✓ Possibili affidamenti a terzi dell'archivio (gestione in regime di outsourcing) è soggetto ad autorizzazione della Soprintendenza archivistica ai sensi dell'art. 21, c. 1, lettera e) del D. Lgs n. 42 del 2004;
- ✓ Qualora lo spostamento si verifichi in seguito al trasferimento di dimora o di sede del detentore dell'archivio, deve preventivamente essere denunciato alla Soprintendenza che può prescrivere misure conservative a tutela del bene (art. 21, c. 2, D. Lgs n. 42 del 2004).

Nei casi di cui ai punti precedenti, il Responsabile della gestione documentale informa il Coordinatore della gestione documentale che effettua verifica preliminare dello stato dei locali di destinazione e cura i rapporti con la Soprintendenza archivistica della Sardegna.

La documentazione conservata negli archivi di deposito è consultabile dalle strutture dell'Ente che abbiano bisogno di esaminarla e di servirsene nello svolgimento delle proprie attività. Le richieste devono essere rivolte al Responsabile della gestione documentale che provvede a metterla a disposizione previa autorizzazione dei responsabili dei procedimenti competenti per materia. La documentazione conservata negli archivi di deposito è accessibile ai sensi della Direttiva in materia di diritto di accesso ai documenti amministrativi. Analoga richiesta andrà inoltrata per la consultazione di serie afferenti alla sezione storica, ovvero i documenti relativi ad affari ed a procedimenti amministrativi conclusi da un quarantennio e destinati alla conservazione permanente.

La consultazione della documentazione è libera ad eccezione di quanto previsto dall'art. 122 del D.lgs. 42/2004:

Documenti relativi alla politica interna ed estera dello Stato, dichiarati di carattere riservato dal Ministero dell'Interno d'intesa con il Ministero della cultura, diventano consultabili 50 anni dopo la loro data;

Documenti contenenti dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale) diventano consultabili 40 anni dopo la loro data;

Documenti contenenti dati personali idonei a rivelare lo stato di salute, la vita sessuale o i rapporti riservati di tipo familiare diventano consultabili 70 anni dopo la loro data;

Documenti contenenti dati giudiziari (cioè dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del D.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale) diventano consultabili 40 anni dopo la loro data.

8.3 Scarto documentale

Una periodica eliminazione dei documenti che hanno esaurito la validità giuridico-amministrativa e che si reputano privi di interesse storico consente un'ordinata gestione dell'archivio favorendo la conservazione di quanto si ritiene utile ai fini storici e di testimonianza dell'esercizio delle funzioni dell'Ente.

Si tratta com'è noto in dottrina, di un'operazione di grande rilevanza culturale poiché permette la selezione e la conservazione di quelle fonti documentarie che si ritiene di tramandare alle generazioni future.

Il piano di fascicolazione e conservazione integrato con il Titolario di classificazione, è lo strumento che consente di coordinare razionalmente lo scarto archivistico, in quanto individua le tipologie di documenti prodotti, la loro organizzazione in fascicoli e il rispettivo tempo di conservazione.

Ai fini dello scarto viene istituita una commissione, che, nella sua struttura minima, deve essere composta da:

- Responsabile della gestione documentale della AOO;
- Dirigente competente sulla documentazione da scartare;
- Funzionari con competenze archivistiche.

La Commissione è di volta in volta integrata dai funzionari responsabili della produzione della documentazione da analizzare o che abbiano competenza su di essa. La Commissione dispone l'eliminazione delle serie per le quali sia trascorso il termine di conservazione indicato nel piano di fascicolazione e conservazione. Ai fini di documentare specifiche tipologie documentarie, nonché modalità e procedure di trattamento di determinate pratiche non soggette a conservazione permanente, o per altre esigenze che si potessero determinare, la Commissione di scarto può disporre la conservazione per campione di limitate porzioni delle serie proposte per lo scarto.

Al termine dei propri lavori, la Commissione di scarto redige un verbale e una proposta di scarto (Proposta di scarto, allegata al presente Manuale) nella quale sono indicate le serie e i nuclei di documentazione da eliminare.

Come da prassi nella proposta di scarto, per ciascuno dei nuclei di documentazione individuato, viene indicato:

- ✓ Numero d'ordine;
- ✓ Indice di classificazione con la specifica del Titolario di riferimento;
- ✓ Denominazione e descrizione sommaria del contenuto con riferimento anche al procedimento cui la documentazione attiene;
- ✓ Estremi cronologici;
- ✓ Consistenza espressa in numero di pezzi metri lineari (ml);
- ✓ Motivazione dello scarto, che deve essere opportunamente argomentata;

La procedura di scarto della documentazione analogica presenta i seguenti passaggi:

1. elaborazione della proposta di scarto, compilata dalla AOO e approvata dalla Commissione di scarto nominata all'interno della struttura interessata: la proposta di scarto è inviata informalmente ai referenti dei diversi Servizi in cui si articola l'Ente;
2. richiesta di parere informale alla Soprintendenza archivistica della Sardegna;

3. predisposizione della determinazione di scarto: la struttura proponente, sulla base delle indicazioni della Soprintendenza archivistica, provvede a predisporre la determinazione di scarto (Determinazione di scarto, allegata al presente Manuale);

4. richiesta di autorizzazione alla Soprintendenza archivistica della Sardegna: al fine di ottenere l'autorizzazione ai sensi dell'art. 21 del Codice dei beni culturali, la struttura proponente invia la determinazione di scarto via PEC (indirizzo: sa-sar@pec.cultura.gov.it) alla Soprintendenza archivistica della Sardegna;

5. coordinamento delle operazioni di ritiro e distruzione della documentazione: ottenuta l'autorizzazione allo scarto si provvede alle operazioni di ritiro e distruzione della documentazione. Al momento del prelievo della documentazione viene sottoscritto in duplice copia, da un funzionario da un Funzionario dell'Ente che sovrintende alle operazioni di prelievo e da un referente della ditta incaricata, un formulario rifiuti. Successivamente alla distruzione della documentazione la cartiera consegna al Funzionario copia del formulario del referente della ditta, eventualmente integrata con l'indicazione del peso effettivo della documentazione scartata e con il timbro della cartiera, che attesta l'avvenuto conferimento. Dopo le operazioni di distruzione viene predisposto dalla cartiera un verbale di avvenuta distruzione, controfirmato da un funzionario. Tale verbale, a corredo della procedura, viene trasmesso via PEC alla Soprintendenza archivistica.

Non ricade in questa procedura l'eliminazione di materiali del tutto superflui ai bisogni ordinari dell'Ente e non necessari ai fini della ricerca storica, ovvero: stampati; modulistica non compilata; gazzette ufficiali; BURAS; periodici.

8.4 Accesso all'archivio analogico

L'accesso agli archivi di deposito è precluso al pubblico ed è limitato al personale autorizzato e avviene sotto il controllo del Responsabile della gestione documentale della AOO. È necessario comunicare al personale della vigilanza i nominativi dei dipendenti autorizzati ad accedere ai locali, poiché ne custodiscono le chiavi.

L'accesso alle pratiche depositate nell'archivio o negli arredi degli uffici afferenti ai vari Settori e l'eventuale prelievi di documentazione sarà annotato in un apposito registro dei prelevamenti e delle restituzioni

Si prelevano e si consegnano agli interessati, sia per la consultazione in loco che presso gli uffici delle AOO, soltanto interi fascicoli, registri e/o faldoni, non essendo consentita l'estrazione dai fascicoli di singoli documenti, a meno che ciò non contrasti con le esigenze di tutela della riservatezza, previste dalla normativa vigente.

La documentazione può essere movimentata solo previa compilazione di una scheda pro-memoria, copia della quale sarà lasciata al posto della documentazione presa in carico.

9 ALLEGATI

Allegato n. 1 - Organigramma [file.pdf]

Allegato n. 2 – Protocollo di emergenza [file.xlsx]

Allegato n. 3 – Formati di file [file.docx]

Allegato n. 4 - Piano di fascicolazione e conservazione [file.xlsx]

Allegato n. 5 - Metadati [file.docx]

Allegato n. 6 – Scheda Pro-memoria per il prelievo documenti analogici [file.docx]

Allegato n. 7 - Piano di Conservazione [file .docx]

Allegato n. 8 - Proposta di scarto [file.docx]

Allegato n. 9 - Determinazione di scarto [file.docx]

Allegato n. 10 – Atto di nomina del Responsabile della Gestione Documentale e Responsabile della Conservazione (Delibera Commissariale n. 16 del 18/04/2023)

Allegato n. 11 – Atto di nomina del Vicario del Responsabile della Gestione Documentale (DPU n. 2 del 20/02/2026)