COMUNE DI CORIANO

Provincia di Rimini

MANUALE DI CONSERVAZIONE

dei documenti informatici

Redatto ai sensi del paragrafo 4.6 delle Linee Guida AGID 2021 sulla formazione, gestione e conservazione dei documenti informatici.

Approvato con Delibera di Giunta n. 121 del 22/06/2026

Indice

1. Introduzione e scopo del documento

Il presente documento rappresenta il Manuale di conservazione dei documenti informatici (di seguito anche “Manuale”) del Comune di Coriano ed è lo strumento operativo che descrive e disciplina il modello organizzativo della conservazione adottato.

In particolare, il presente Manuale, redatto secondo quanto previsto dal paragrafo 4.3 delle “*Linee Guida sulla formazione, gestione e conservazione dei documenti informatici*” adottate dalla Agenzia per l'Italia Digitale (d'ora in poi Linee Guida AgID), illustra l’organizzazione del processo di conservazione, definendo i soggetti coinvolti e i ruoli svolti dagli stessi nel modello organizzativo di funzionamento dell’attività di conservazione del Comune di Coriano come soggetto produttore (d’ora in poi **Produttore**) che intende sottoporre a conservazione digitale fascicoli, serie e aggregazioni documentali, affidando il processo di conservazione all’Istituto per i beni Artistici, Culturali e Naturali (IBACN) della Regione Emilia Romagna (d'ora in poi **Conservatore**), il quale agisce per il tramite del Polo archivistico dell’Emilia-Romagna (ParER).

L’accordo tra Titolare-Ente produttore Comune di Coriano e Conservatore (Regione Emilia-Romagna) per l’affidamento in outsourcing del processo di conservazione è stato approvato con la Delibera di Giunta Comunale n. 190 del 23/12/2014 e formalizzato mediante convenzione sottoscritta tra il Comune di Coriano e IBACN.

Il presente Manuale integra, per le parti specifiche di competenza del Produttore e per quanto riguarda i rapporti tra questi e IBACN, il Manuale di conservazione di ParER, documento di riferimento del presente documento.

Per le tipologie degli oggetti sottoposti a conservazione e i rapporti con il soggetto che realizza il processo di conservazione, il Manuale è integrato con il Disciplinare tecnico, che definisce le specifiche operative e le modalità di descrizione e di versamento nel Sistema di conservazione digitale dei Documenti informatici e delle Aggregazioni documentali informatiche oggetto di conservazione.

In osservanza di quanto stabilito dalle Linee Guida AgID il presente Manuale è approvato con Delibera di Giunta comunale ed è pubblicato nella sezione “Amministrazione trasparente” della pagina internet istituzionale del Comune di Coriano all'indirizzo:*https://amministrazionetrasparente.comune.coriano.rn.it/amministrazione-trasparente//*

1.1 Contesto normativo

Senza ripercorrere in dettaglio il complesso e frastagliato excursus legislativo inerente la conservazione dei documenti in formato digitale, si fornisce di seguito un cenno ai tre testi normativi cardine.

Caposaldo del complesso impianto normativo in materia di documentazione amministrativa analogica e digitale rimane il “Testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa”

D.P.R n° 445/2000 a cui è seguito il D.Lgs n. 82/2005 “Codice Dell’Amministrazione digitale” e sue successive integrazioni e modificazioni. Se queste due fonti normative delineano le regole generali per la conservazione dei documenti amministrativi, il DPCM 03.12.2013 “Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5-bis, 23-ter, comma 4, 43, commi 1 e 3, 44 , 44-bis e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005”, traccia le regole per la conservazione a norma.

1.2 Organizzazione del Manuale

Il Manuale è organizzato in capitoli e paragrafi: contiene una panoramica di tutte le leggi e i decreti che regolano la materia, fornisce il profilo del Comune di Coriano e il profilo di ParER, il responsabile della conservazione e l’organizzazione per la gestione della documentazione elettronica. Inoltre, riporta, cenni sui riversamenti, i riferimenti alla normativa e alla policy sulla protezione dei dati personali e ai documenti allegati e collegati al Manuale.

1.3 Definizioni

- **Accreditamento** (vd. Conservatori Accreditati): riconoscimento, da parte dell’Agenzia per l’Italia digitale, del possesso dei requisiti del livello più elevato, in termini di qualità e sicurezza ad un soggetto pubblico o privato,che svolge attività di conservazione o di certificazione del processo di conservazione
- **Archivio**: complesso organico di documenti, di fascicoli e di aggregazioni documentali di qualunque natura e formato, prodotti o comunque acquisiti da un soggetto produttore durante lo svolgimento dell’attività
- **Archiviazione** (elettronica): processo di memorizzazione, su un qualsiasi idoneo supporto, di documenti informatici, anche sottoscritti, così come individuati nella

normativa vigente,univocamente identificati mediante un codice di riferimento, antecedente all'eventuale processo di conservazione

- **Codice Amministrazione Digitale** (CAD): decreto legislativo 7 marzo 2005, n. 82 e successive modificazioni e integrazioni
- **Conservazione**: insieme delle attività finalizzate a definire ed attuare le politiche complessive del sistema di conservazione e a governarne la gestione in relazione al modello organizzativo adottato e descritto nel manuale di conservazione
- **Delegato per l'attività di conservazione** (Conservatore): la persona fisica o giuridica tenuta a svolgere le attività di conservazione dei documenti in forza di apposita delega conferita dal responsabile della conservazione
- **Documento**: rappresentazione informatica o in formato analogico di atti, fatti e dati intelligibili direttamente o attraverso un processo di elaborazione elettronica
- **Documento informatico**: rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti (art 1 lett. p del D. Lgs. n. 82/05)
- **Esibizione**: operazione che consente di visualizzare un documento conservato e di ottenerne copia
- **Fascicolo informatico**: Aggregazione strutturata e univocamente identificata di atti, documenti o dati informatici, prodotti e funzionali all'esercizio di una specifica attività o di uno specifico procedimento. Nella pubblica amministrazione il fascicolo informatico collegato al procedimento amministrativo è creato e gestito secondo le disposizioni stabilite dall'articolo 41 del Codice
- **IBACN**: Istituto per i beni Artistici, Culturali e Naturali della Regione Emilia Romagna
- **Manuale di conservazione**: strumento che descrive il sistema di conservazione dei documenti informatici ai sensi dell'articolo 9 delle regole tecniche del sistema di conservazione
- **Manuale di gestione**: documento che descrive il sistema di gestione informatica dei documenti di cui all'articolo 5 delle regole tecniche del protocollo informatico ai sensi del D.P.C.M. 31 ottobre 2000 e successive modificazioni e integrazioni
- **Marcare** (temporalmente): evidenza informatica che consente la validazione temporale
- **Pacchetto di archiviazione**: pacchetto informativo composto dalla trasformazione di uno o più pacchetti di versamento secondo le modalità riportate nel manuale di conservazione del sistema di conservazione
- **Pacchetto di distribuzione**: pacchetto informativo inviato dal sistema di conservazione all'utente in risposta ad una sua richiesta

- **Pacchetto di versamento**: pacchetto informativo inviato dall'utente al sistema di conservazione secondo un formato predefinito e concordato, descritto nel manuale di conservazione del sistema di conservazione.
- **ParER**: Polo archivistico dell'Emilia-Romagna
- **Piano di sicurezza dei documenti informatici** (Piano di Sicurezza): documento che descrive le misure di sicurezza adottate per la formazione, la gestione, la trasmissione, l'interscambio, l'accesso e la conservazione dei documenti informatici, nel rispetto anche di quanto disposto dal D. Lgs 196/2003 e Misure Minime per la sicurezza ICT per le pubbliche amministrazioni (pubblicate da AgID)
- **Processo di conservazione**: insieme delle attività finalizzate alla conservazione dei documenti informatici di cui all'articolo 10 delle regole tecniche del sistema di conservazione
- **Produttore**: persona fisica o giuridica, di norma diversa dal soggetto che ha formato il documento, che produce il pacchetto di versamento ed è responsabile del trasferimento del suo contenuto nel sistema di conservazione
- **Regole tecniche del sistema di conservazione**: le regole tecniche in materia di conservazione ai sensi degli articoli 20, commi 3 e 5-bis, 23-ter, comma 4, 43, commi 1 e 3, aa, 44 – bis e 71, comma 1, del Codice dell'Amministrazione digitale di cui al D.Lgs. n. 82 del 2005, approvate con Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013
- **Responsabile della conservazione**: soggetto che svolge le attività di conservazione avvalendosi del servizio offerto dal delegato per l'attività di conservazione, in conformità a quanto disposto dal presente manuale operativo e dalle disposizioni normative vigenti in materia (attività elencate nell'articolo 8, comma 1 delle regole tecniche del sistema di conservazione)
- **Responsabile del trattamento dei dati**: la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali
- **Sistema di conservazione** (Sistema): sistema di conservazione dei documenti informatici di cui all' articolo 44 del Codice
- **Utente**: persona, ente o sistema che interagisce con i servizi di un sistema per la conservazione dei Documenti informatici al fine di fruire delle informazioni di interesse

2. Modello organizzativo, ruoli e responsabilità

Le amministrazioni pubbliche, secondo quanto previsto dall'articolo 34, comma 1-bis del decreto legislativo 07 marzo 2005, n. 82, e successive modifiche e integrazioni (d'ora inpoi CAD), possono procedere alla conservazione dei documenti informatici:

- ➔ all'interno della propria struttura organizzativa;
- ➔ affidandola, in modo totale o parziale, nel rispetto della disciplina vigente, ad altri soggetti, pubblici o privati che possiedono i requisiti di qualità, di sicurezza e organizzazione individuati, nel rispetto della disciplina europea, nelle Linee guida di cui all'articolo 71 del CAD relative alla formazione, gestione e conservazione dei documenti informatici nonché in un regolamento sui criteri per la fornitura dei servizi di conservazione dei documenti informatici emanato da AgID, avuto riguardo all'esigenza di assicurare la conformità dei documenti conservati agli originali nonché la qualità e la sicurezza del sistema di conservazione.

2.1 Modello organizzativo dell'Ente

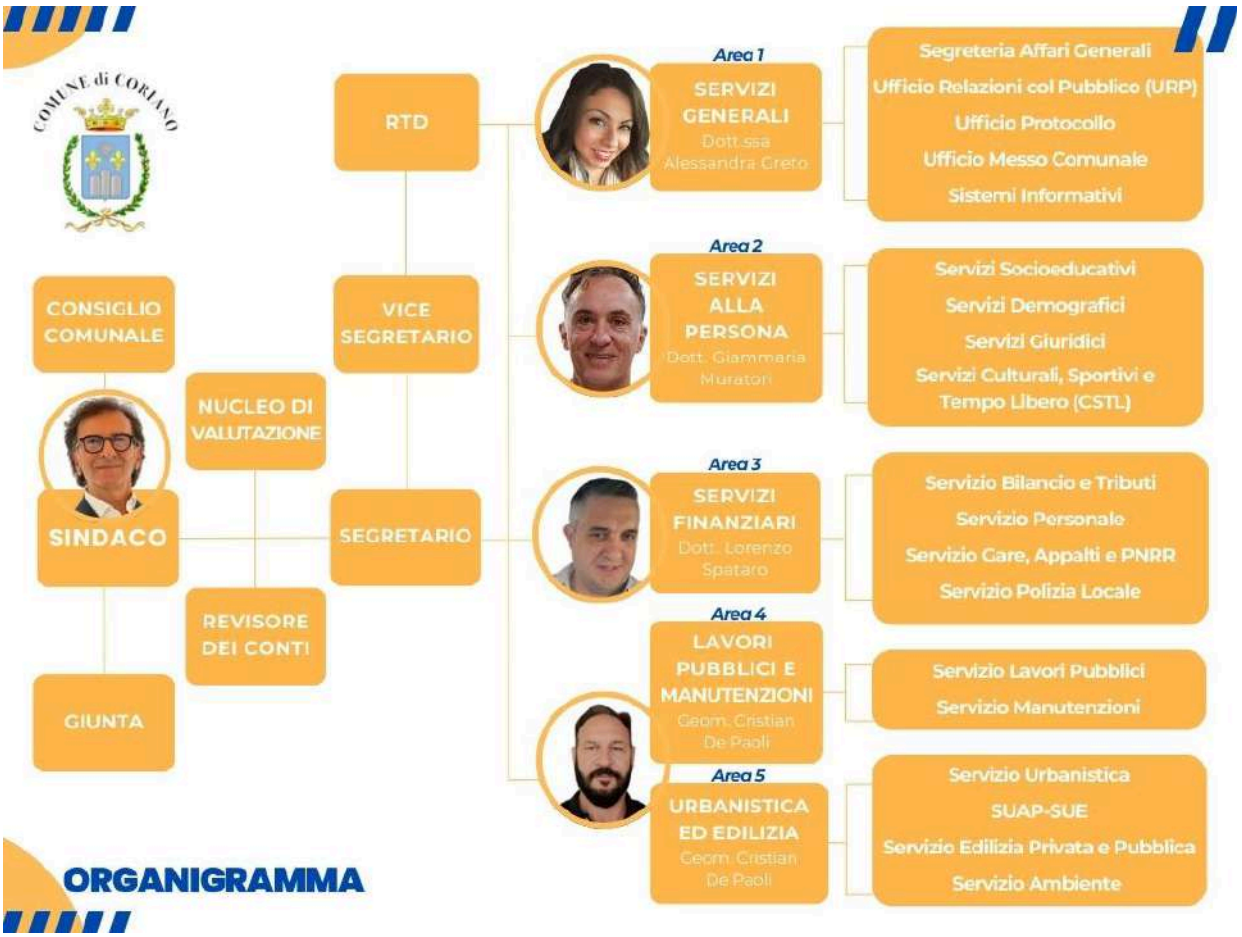
Codice IPA: c_d004

Indirizzo: P.zza Mazzini, 15 - 47853

CF: 00616520409

protocollogenerale@comune.coriano.rn.it

L'Ente è costituito in una Area Organizzativa Omogenea (AOO) denominata Comune di Coriano ed organizzata in Servizi, secondo l'Organigramma:



Il Comune di Coriano è il soggetto “Produttore” ed in quanto tale è il Titolare delle unità documentarie informatiche poste in conservazione e, attraverso il proprio Responsabile della Conservazione, definisce e attua le politiche complessive del Sistema di conservazione governando la gestione con piena responsabilità ed autonomia, in relazione al modello organizzativo di seguito adottato affida a Conservatori esterni la gestione del Servizio di Conservazione secondo quanto previsto dalla normativa in materia.

Nel Sistema di Conservazione si individuano almeno i seguenti ruoli:

- Titolare dell’oggetto della conservazione
- Produttori e Utenti abilitati
- Responsabile della Conservazione (lato produttore)
- Conservatore

Il Comune di Coriano, in quanto Titolare dell’oggetto della conservazione, ha la responsabilità, per legge, di conservare un documento o un insieme di documenti. L’Ente realizza i processi di conservazione all’interno della propria struttura

organizzativa affidandoli ad un conservatore accreditato Agid di cui all'art. 44-bis, comma 1, del Codice, fatte salve le competenze del Ministero dei beni e delle attività culturali e del turismo ai sensi del decreto legislativo 22 gennaio 2004, n. 42, e successive modificazioni.

2.1 Responsabile della conservazione

Il ruolo di Responsabile della Conservazione è stato attribuito con decreto sindacale n. 15 del 30.06.2025.

Il Responsabile della Conservazione svolge le attività elencate nel paragrafo 4.5 delle Linee Guida AgID, in particolare, definisce e attua le politiche complessive del sistema di conservazione e ne governa la gestione agendo d'intesa con il Responsabile del trattamento dei dati personali, con il Responsabile della Gestione Documentale e con il Responsabile dei Sistemi Informativi, in relazione al modello organizzativo adottato dall'Ente.

Il Responsabile della Conservazione definisce le policies di conservazione del Produttore. A tal fine, provvede alla pianificazione strategica, alla ricerca dei finanziamenti, alla revisione periodica dei risultati conseguiti e ad ogni altra attività gestionale mirata a coordinare lo sviluppo del sistema. Non risulta invece coinvolto nelle operazioni quotidiane di amministrazione del sistema, che sono a carico del soggetto incaricato della sua gestione.

Il Responsabile della Conservazione cura l'aggiornamento periodico del manuale di conservazione in presenza di cambiamenti normativi, organizzativi, procedurali o tecnologici rilevanti in collaborazione con il Responsabile della Gestione Documentale.

2.2 Delegato all'attività di conservazione (Conservatore)

Il delegato per l'attività di conservazione è il soggetto pubblico o privato nominato dal responsabile della conservazione a cui viene affidata in modo totale o parziale la conservazione dei documenti digitali.

Per il Comune di Coriano tale Ente è identificato in IBACN, che svolge tale attività principalmente tramite il proprio Servizio denominato ParER. IBACN si occupa delle politiche complessive del Sistema di conservazione e ne determina l'ambito di sviluppo e le competenze.

Gli obiettivi di ParER sono:

- ➔ garantire la conservazione, archiviazione e gestione dei Documenti informatici e degli altri oggetti digitali;

- ➔ erogare servizi di accesso basati sui contenuti digitali conservati;
- ➔ fornire supporto, formazione e consulenza al Produttore per i processi di dematerializzazione.

Di fatto, quindi (come definito dal testo della Convenzione), IBACN, tramite ParER si impegna alla conservazione dei documenti trasferiti e ne assume la funzione di Responsabile della conservazione ai sensi della normativa vigente, garantendo il rispetto dei requisiti previsti dalle norme in vigore nel tempo per i sistemi di conservazione, e svolge, tramite la struttura organizzativa e di responsabilità di ParER.

2.3 Produttori e Utenti

I ruoli di Produttore e Utente sono svolti indifferentemente da persone fisiche o giuridiche interne o esterne al sistema di conservazione, secondo il modello organizzativo scelto dal Comune di Coriano.
Il Produttore, responsabile del contenuto del pacchetto di versamento, trasmette tale pacchetto al sistema di conservazione secondo le modalità operative di versamento condivise con il delegato.
L' Utente richiede al sistema di conservazione l'accesso ai documenti per acquisire le informazioni di interesse nei limiti del livello di autorizzazione attribuito dal Responsabile della Conservazione secondo le modalità previste nel nel Disciplinare tecnico.
Il Sistema di conservazione permette ai soggetti autorizzati l'accesso diretto, anche da remoto, ai Documenti informatici conservati e consente la produzione di un Pacchetto di distribuzione direttamente acquisibile dai soggetti autorizzati.
Nel ruolo di Utente si possono definire specifici soggetti abilitati, che possono accedere esclusivamente ai documenti versati dal Produttore stesso o solo ad alcuni di essi secondo le regole di visibilità e di accesso concordate tra ParER e il Produttore.

L'abilitazione e l'autenticazione di tali operatori avviene in base alle procedure indicate nel "Piano della sicurezza" e nel rispetto delle misure di sicurezza previste negli articoli da 31 a 36 del D.lgs 30 giugno 2003, n. 196, in particolare di quelle indicate all'art. 34 comma 1 e dal Disciplinare tecnico in materia di misure minime di sicurezza di cui all'Allegato B del medesimo decreto.

2.4 Organismi di tutela e vigilanza

vd. Manuale ParER – cap. 5 "Struttura organizzativa per il Servizio di Conservazione".

3. Organizzazione del servizio di conservazione

Il servizio di conservazione dei documenti informatici del Produttore, gestito da ParER, è attivato sulla base della convenzione con IBACN.

3.1 Gestione del Sistema di conservazione

Il Sistema di conservazione garantisce l'autenticità, l'integrità, l'affidabilità, la leggibilità e la reperibilità degli oggetti conservati dal momento della loro presa in carico dal Produttore, fino all'eventuale scarto indipendentemente dall'evolversi del contesto tecnologico e organizzativo.
Il versamento in conservazione dei documenti informatici gestiti nella fase corrente del Produttore è effettuato unicamente dagli Operatori abilitati dal Produttore (indicati nel Disciplinare Tecnico) utilizzando la modalità automatica con il connettore (tra il sistema di gestione documentale del Produttore e il sistema di conservazione) o gli strumenti messi a disposizione da ParER.

ParER, in qualità di soggetto delegato alla gestione del servizio di conservazione del Produttore, svolge le seguenti attività:

- ➔ acquisizione, verifica e gestione dei pacchetti di versamento presi in carico e generazione del rapporto di versamento
- ➔ preparazione e gestione del pacchetto di archiviazione
- ➔ preparazione e gestione del pacchetto di distribuzione ai fini dell'esibizione e della produzione di duplicati e copie informatiche su richiesta
- ➔ scarto dei pacchetti di archiviazione
- ➔ chiusura del servizio di conservazione (al termine del contratto).

ParER, tramite il responsabile dei sistemi informativi per la conservazione, svolge inoltre le seguenti attività:

- ➔ conduzione e manutenzione del sistema di conservazione
- ➔ monitoraggio del sistema di conservazione
- ➔ change management
- ➔ verifica periodica di conformità a normativa e standard di riferimento.

3.2 Struttura Organizzativa per il Servizio di conservazione

vd. Manuale ParER.

4. Oggetti sottoposti a conservazione

4.1 Documenti informatici e aggregazioni documentali informatiche

Il Sistema di conservazione gestito da ParER, conserva documenti informatici, in particolare documenti amministrativi informatici, con i metadati ad essi associati e le loro Aggregazioni documentali informatiche. Inoltre il Sistema gestisce l'organizzazione e la descrizione dei Documenti informatici e delle Aggregazioni documentali informatiche in Serie.
I Documenti informatici e le loro Aggregazioni documentali informatiche sono trattati nel sistema nella forma di Unità documentarie e Unità archivistiche, e sono inviati in conservazione sotto forma di Pacchetti di versamento (SIP), che contengono sia i documenti che i relativi metadati.
Per mantenere anche nel Sistema le informazioni relative alla struttura dell'archivio e dei relativi vincoli archivistici, le Unità documentarie sono versate corredate di un set di metadati di Profilo archivistico.
I Documenti informatici (Unità documentarie) sono suddivisi in tipologie documentarie, che identificano gruppi documentali omogenei per natura e funzione giuridica, modalità di registrazione o di produzione. Tale suddivisione è funzionale all'individuazione, per ogni singola tipologia documentaria, di set di metadati standard e di articolazioni o strutture di composizione omogenee.
Per le tipologie documentarie, l'Area Servizi archivistici di ParER elabora dei documenti di studio ed analisi ad uso interno, che definiscono per ogni tipologia documentaria:

- ➔ il set dei metadati descrittivi da inserire nei SIP, ritenuti essenziali per la corretta conservazione dei documenti;
- ➔ l'articolazione o struttura di riferimento della corrispondente Unità documentaria ai fini della predisposizione del SIP per l'invio al Sistema di conservazione;
- ➔ le indicazioni operative per la produzione del SIP e l'invio dello stesso al Sistema.

Da tali documenti di analisi sono derivate le specifiche operative per la creazione e trasmissione dei SIP relativi alle varie tipologie documentarie contenute nel Disciplinare tecnico concordato con il Produttore.
Si rimanda al "Disciplinare Tecnico" per la descrizione delle tipologie documentarie gestite e conservate dal sistema.

4.2 Unità archivistiche e unità documentarie

I Documenti informatici e le loro Aggregazioni documentali informatiche sono trattati nel Sistema nella forma di Unità documentarie e Unità archivistiche, specificamente descritte nel paragrafo 6.1.1 del capitolo 6 ”Oggetti sottoposti a conservazione” del Manuale di Conservazione ParER al quale si rimanda per approfondimenti. , e sono inviati in conservazione sotto forma di Pacchetti di versamento (SIP), che contengono sia i documenti che i relativi metadati.

4.3 Formati

Secondo quanto stabilito dal paragrafo 6.1.1 del capitolo del Manuale di conservazione ParER il Sistema tratta i formati descritti nell’Allegato 2 alle Linee guida e, inoltre, è in grado di trattare, su richiesta del Comune di Coriano, anche formati non compresi nel suddetto elenco ma che l’Ente utilizza nei propri sistemi e che ritiene di dover conservare.

Tutti i formati trattati sono elencati e descritti in un registro interno al Sistema denominato “Registro dei formati” in cui ogni formato è corredato da informazioni relative a estensioni e mimetype. Inoltre, ogni formato è classificato in base alla sua idoneità a essere conservato a lungo termine in riferimento alle indicazioni fornite per la classificazione di formati dal citato Allegato 2 e all’indice di interoperabilità introdotto nel paragrafo 3.2 di detto Allegato.

Sulla base di questa suddivisione i formati si dividono in:

- Formati idonei: sono i formati che per le loro caratteristiche di standardizzazione, di apertura, di sicurezza, di portabilità, di immodificabilità, di staticità e di diffusione sono reputati idonei alla conservazione a lungo termine;
- Formati gestiti: sono i formati leggibili e accessibili ma potenzialmente soggetti a obsolescenza tecnologica e che, in caso di necessità, possono essere opportunamente migrati in Formati idonei con idonee procedure;
- Formati deprecati: sono formati ritenuti non idonei per la conservazione a lungo termine e che al contempo non possono essere migrati in Formati idonei, per i quali, quindi, non è possibile assicurare la conservazione a lungo termine.

Si rimanda al paragrafo 6.1.2 “Formati” del capitolo “Oggetti sottoposti a conservazione” del Manuale di conservazione ParER per approfondimenti.

4.4 Metadati

Si rimanda al Manuale ParER – paragrafo 6.1.3 ”Metadati” del cap. 6 ”Oggetti sottoposti a conservazione”

4.5 Pacchetto di versamento (SIP)

Si rimanda al Manuale ParER – paragrafo 6.2 ”Pacchetto di versamento” del cap. 6 ”Oggetti sottoposti a conservazione”

4.6 Pacchetto di archiviazione (AIP)

Si rimanda al Manuale ParER – paragrafo 6.3 ”Pacchetto di archiviazione” del cap. 6 ”Oggetti sottoposti a conservazione”

4.1 Pacchetto di distribuzione (DIP)

Si rimanda al Manuale ParER – paragrafo 6.4 ”Pacchetto di distribuzione” del cap. 6 ”Oggetti sottoposti a conservazione”

5. Processo di conservazione

5.1 Acquisizione dei pacchetti di versamento (SIP)

Il processo di conservazione è stato attivato sulla base della convenzione stipulata tra il Comune di Coriano e la Regione Emilia-Romagna, in qualità di soggetto che svolge attività di conservazione per l'Ente.

Le procedure per l'attivazione del processo di conservazione sono indicate nella Convenzione e nel Manuale di ParER che disciplina anche la chiusura del servizio in caso di recesso o scadenza della Convenzione stessa, con le modalità operative descritte nel paragrafo 7.9 "Predisposizione di misure a garanzia dell'interoperabilità e trasferibilità ad altri conservatori".

Per attestare l'avvenuta acquisizione e presa in carico del SIP, per ogni pacchetto accettato il Sistema genera automaticamente un Rapporto di versamento che viene memorizzato nel Sistema e associato al SIP cui si riferisce. Il Rapporto di versamento contiene l'Identificativo univoco del Rapporto, il Riferimento temporale relativo alla sua creazione (specificato con riferimento al tempo UTC), l'impronta dell'Indice del SIP e le impronte degli Oggetti-dati che ne fanno parte, oltre alla descrizione sintetica del contenuto del SIP acquisito. La descrizione analitica del Rapporto di versamento e la relativa struttura dati è contenuta nel documento Specifiche tecniche dei servizi di versamento.

Il Riferimento temporale contenuto nel Rapporto di versamento è generato dal Sistema (con le modalità definite dal Conservatore, vd. Manuale ParER – cap."Processo di Conservazione") ed è da considerarsi opponibile ai terzi in base a quanto previsto dal comma 4, lettera b) dell'art. 41 del DPR 22 febbraio 2013.

Il Rapporto di versamento è reso disponibile al Produttore il quale lo rende visibile all'interno del sistema di gestione documentale.

5.2 Preparazione e Gestione del Pacchetto di archiviazione (AIP)

Si rimanda al Manuale ParER – cap. "Processo di conservazione".

5.3 Preparazione e Gestione del Pacchetto di distribuzione (DIP)

Si rimanda al Manuale ParER – cap. "Processo di conservazione".

5.4 Produzione di copie, di riproduzioni e di duplicati

Si rimanda al Manuale ParER – cap. ”Processo di conservazione”.

5.5 Monitoraggio e risoluzione delle anomalie

L’azione di monitoraggio può essere svolta, secondo la natura delle attività e le fasi del processo di conservazione:

- da operatori di ParER, per il complesso degli oggetti conservati;
- dagli utenti del Produttore, limitatamente agli oggetti di propria pertinenza;

Il monitoraggio consente di avere una vista complessiva, suddivisa per fasce temporali, sull’acquisizione dei SIP, sul rifiuto dei SIP, sui tentativi falliti di versamento e sulle eventuali anomalie, mettendo a disposizione degli operatori tutte le informazioni necessarie a verificare tanto le anomalie che hanno impedito il versamento dei SIP nel Sistema, quanto tutti gli elementi relativi ai SIP versati e agli AIP generati o aggiornati a seguito di tali versamenti.

In particolare, sono evidenziati, in tabelle sintetiche complessive o per singola Struttura:

- i versamenti di SIP normalizzati svolti con successo, cioè che hanno generato un Rapporto di versamento;
- l’inserimento o meno dei SIP in Elenchi di versamento;
- versamenti rifiutati;
- i tentativi di versamento falliti, che non hanno attivato il processo di acquisizione.

Dalle tabelle sintetiche è possibile scendere fino al dettaglio dei singoli versamenti, evidenziando nel caso dei versamenti rifiutati, opportuni codici d’errore, che consentono agli operatori di individuare le soluzioni necessarie alla risoluzione delle anomalie riscontrate.

Le più comuni azioni di risoluzione delle anomalie prevedono:

- Utilizzo di parametri di forzatura dei versamenti: nel caso in cui i controlli sulle firme, sui formati o sui collegamenti presenti sul SIP non vadano a buon fine e il versamento del SIP fallisca, i SIP rifiutati possono essere versati nuovamente in conservazione forzando i controlli precedentemente falliti. Tali forzature, che sono operate dal Produttore valorizzando appositi parametri presenti nel SIP, consentono di portare in conservazione i SIP anche in presenza delle anomalie che inizialmente ne avevano pregiudicato l’acquisizione. In questi casi, il

Sistema segnala al Produttore nell'Esito versamento che il SIP è stato acquisito a seguito di forzatura. Le casistiche e le modalità con cui tali forzature operano sono configurate nel Sistema e descritte in dettaglio nel Disciplinare tecnico;

- Modifica di dati non corretti presenti nel SIP: nel caso in cui il SIP non superi i controlli a causa di alcuni dati non corretti nel SIP stesso, gli operatori di ParER in sede di Monitoraggio segnalano l'anomalia al Produttore, che provvede alla correzione dei dati indicati e a effettuare nuovamente il versamento;
- Modifica delle configurazioni del Sistema: nel caso in cui il versamento del SIP non vada a buon fine per la presenza nel SIP stesso di dati non corrispondenti con i valori configurati nel Sistema, ParER può procedere, d'accordo con il Produttore, a modificare di conseguenza le configurazioni. Di tale modifica ne viene data comunicazione al Produttore che provvede a inviare nuovamente in conservazione il SIP;
- Versamenti rifiutati e non risolubili: nel caso in cui un versamento sia stato rifiutato per la presenza di anomalie che il Produttore giudica non risolubili, della circostanza viene data comunicazione a ParER che provvede a marcare sul Sistema quel versamento come non risolubile e ad escluderlo, di conseguenza, da futuri controlli;
- Annullamento di versamenti effettuati: nel caso in cui un versamento andato a buon fine sia stato effettuato per errore, il Produttore ne dà comunicazione a ParER che provvede, utilizzando apposite funzionalità del Sistema, ad annullare il versamento. Il SIP, e il relativo AIP eventualmente generato, non sono cancellati dal Sistema, ma marcati come Annullati. I SIP e gli AIP annullati sono esclusi dai risultati delle ricerche effettuate sul Sistema, ma richiamabili solo se esplicitamente indicato nei filtri di ricerca.

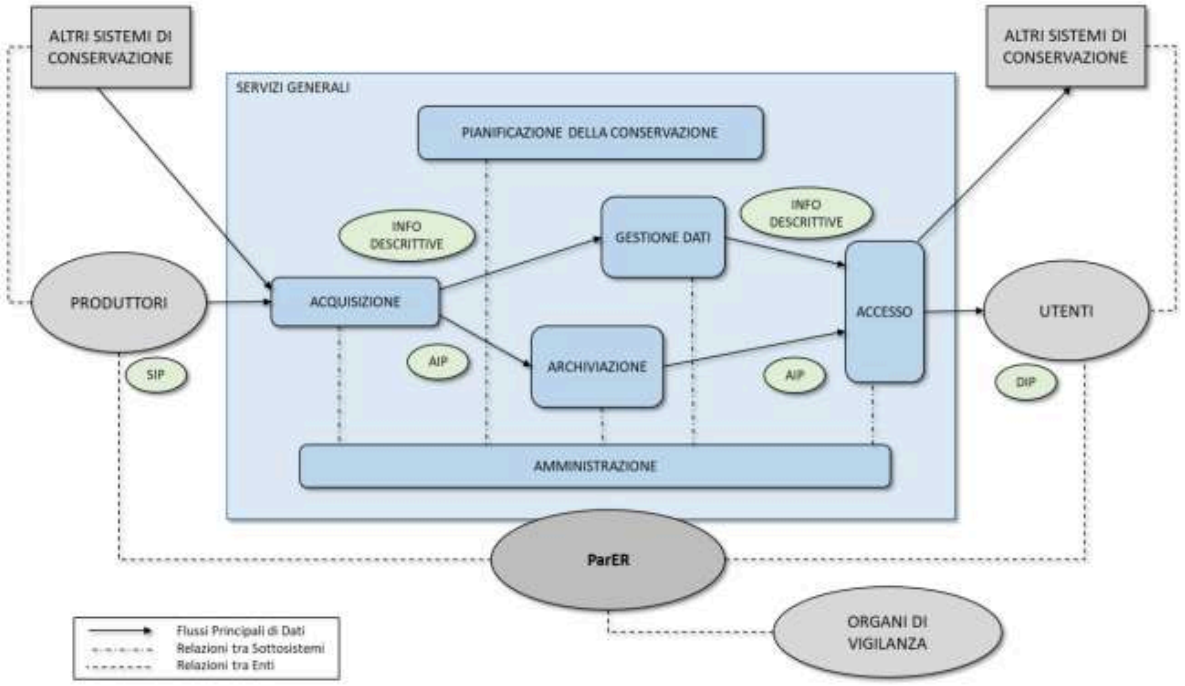
Il modulo di Monitoraggio, inoltre, fornisce accesso alle statistiche dei sistemi, del Data Base, dei versamenti, ecc., mettendo a disposizione degli operatori report sia sintetici che analitici.

vd. Manuale ParER – cap."Processo di conservazione".

6. Descrizione del sistema di conservazione

6.1 Componenti logiche

Il Manuale di Conservazione ParER schematizza dal punto di vista logico le principali componenti del Sistema di conservazione di ParER e le principali relazioni con i soggetti interessati dal processo di conservazione attraverso il seguente diagramma.



Si rimanda al paragrafo 8.1. “Componenti logiche” del capitolo 8 ”Il Sistema di Conservazione” del Manuale di Conservazione ParER per approfondimenti.

6.2 Componenti tecnologiche

Il Sistema di conservazione è costituito da diversi moduli software che interagiscono tra loro per la gestione dell’intero processo di conservazione. Il Sistema, inoltre, si avvale di ulteriori componenti applicative esterne con funzioni di supporto al processo.

Si rimanda al paragrafo 8.2. “Componenti tecnologiche” del capitolo 8 ”Il Sistema di Conservazione” del Manuale di Conservazione ParER per approfondimenti.

6.3 Componenti fisiche

Dal punto di vista tecnico il Sistema di conservazione è progettato e realizzato in maniera da fornire un'elevata continuità di servizio, garantire l'integrità degli oggetti conservati, gestire grandi volumi di dati, mantenere performance stabili indipendentemente dai volumi di attività ed assicurare la riservatezza degli accessi. Il Sistema è sviluppato con tecnologie di larga diffusione open source o comunque di libero utilizzo, a parte i sistemi di memorizzazione di dati, per i quali si utilizzano prodotti proprietari, che dispongono però di interfacce standard de facto o de jure.

Si rimanda al paragrafo 8.3. "Componenti fisiche" del capitolo 8 "Il Sistema di Conservazione" del Manuale di Conservazione ParER per approfondimenti.

6.4 Procedure di gestione e di evoluzione

La gestione del Sistema di conservazione è affidata a diversi gruppi di operatori di ParER, secondo la natura delle attività da svolgere; tali attività includono la gestione operativa del sistema in esercizio, l'avviamento di nuovi enti e di nuovi servizi di conservazione e le eventuali successive modifiche, e infine la gestione dei malfunzionamenti e degli incidenti di sicurezza.

Si rimanda al paragrafo 8.4 "Procedure di gestione e di evoluzione" del capitolo 8 "Il Sistema di Conservazione" del Manuale di Conservazione ParER per approfondimenti.

7. Strategie adottate a garanzia della conservazione

Nel Manuale di conservazione ParER è dichiarato che “ParER svolge diverse attività a garanzia dell'integrità e della fruibilità degli archivi nel lungo periodo per mantenere la loro leggibilità e reperibilità, anche nella prospettiva della futura fruizione come archivi storici.

7.1 Misure a garanzia della intelligibilità, della leggibilità e della reperibilità nel tempo

Si rimanda al Manuale ParER – cap. ”Monitoraggio e controlli - Funzionalità per la verifica e il mantenimento dell’integrità degli archivi”.

7.2 Misure a garanzia dell'interoperabilità e della trasferibilità ad altri conservatori

Si rimanda al Manuale ParER – cap. ”Processo di conservazione - Predisposizione di misure a garanzia dell'interoperabilità e trasferibilità ad altri conservatori”.

7.3 Monitoraggio e soluzioni adottate in caso di anomalie

Si rimanda al Manuale ParER – cap. ”Monitoraggio e controlli”.

8. Approvazione e aggiornamento del Manuale

Il Comune di Coriano adotta il presente Manuale su proposta del Responsabile della Conservazione, allegando il documento tecnico del Conservatore accreditato, che è parte integrante del manuale.

Il Manuale potrà essere aggiornato a seguito di:

- Normativa sopravvenuta
- Introduzione, nell'Ente, di nuove pratiche finalizzate al miglioramento dell'attività amministrativa in termini di efficacia, efficienza e trasparenza
- Sostituzione del conservatore
- Altri motivi di natura tecnica o organizzativa dell'Ente

Il presente Manuale è operativo dalla data di esecutività della deliberazione di approvazione.

Con l'entrata in vigore del presente Manuale sono abrogati tutti i regolamenti dell'Ente nelle parti contrastanti con lo stesso.

Il Manuale è pubblicato sul sito istituzionale dell'Ente nella sezione "Amministrazione trasparente", sottosezione "Atti Generali".

MANUALE DI CONSERVAZIONE

Codice documento	ManualeConservazione
Versione	3.1

	Data	*Nominativo*	*Funzione*
Redazione	15/11/2024	Camilla Broccoli	Responsabile Servizi di conservazione digitali
		Cristiano Casagni	Responsabile Sistemi di conservazione
Verifica	15/11/2024	Riccardo Righi	Responsabile funzione archivistica di conservazione
Approvazione	21/11/2024	Elena Boni	Responsabile della Conservazione per l'Ente Regione Emilia-Romagna e dell'archivio storico
Approvazione	21/11/2024	Giuliano Franceschi	Responsabile dell'Area Sviluppo applicazioni, Polo Archivistico e gestione documentale

REGISTRO DELLE VERSIONI

Versione	Variazioni	Data
1.0	Prima emissione	30/11/2020
1.1	Aggiornamenti e correzioni minori	28/12/2021
2.0	Aggiornamenti a seguito della riorganizzazione regionale	17/06/2022
3.0	Aggiornamenti a seguito della riorganizzazione regionale e correzioni minori. Sono stati specificamente aggiornati: • Paragrafo 4.4 • Capitolo 5: revisione completa • Paragrafo 7.5 • Paragrafo 8.4 • Paragrafi 9.4, 9.5, 9.6 • Capitolo 10	19/05/2023
3.1	Aggiornamenti a seguito della riorganizzazione regionale e correzioni minori, Cap. 5 Rivisitazione paragrafo 7.8 Aggiornamenti minori al paragrafo 7.7 Revisione Cap. 10	15/11/2024

SOMMARIO

1 SCOPO E AMBITO DEL DOCUMENTO

Il presente documento redatto secondo quanto previsto dalle Linee Guida sulla formazione, gestione e conservazione dei documenti informatici (d'ora in poi Linee Guida) descrive il sistema di conservazione applicato dalla Regione Emilia-Romagna sia all'interno della sua organizzazione che per altri soggetti pubblici che sottoscrivono apposito accordo di collaborazione. Per la Regione Emilia-Romagna questo documento svolge il compito di *Manuale di conservazione* ed è predisposto dal Polo Archivistico regionale dell'Emilia-Romagna (d'ora in poi ParER), che realizza e gestisce il *processo di conservazione*.

In particolare, il presente Manuale descrive il modello organizzativo della conservazione adottato e illustra nel dettaglio l'organizzazione della struttura che realizza il *Processo di conservazione*, definendo i soggetti coinvolti e i ruoli svolti dagli stessi nel modello organizzativo di funzionamento dell'attività di *conservazione*. Descrive inoltre il processo, le architetture e le infrastrutture utilizzate, le misure di sicurezza adottate e ogni altra informazione utile alla gestione e alla verifica del funzionamento, nel tempo, del *Sistema di conservazione*.

Gli elementi illustrati e descritti sono validi e rilevanti per Regione Emilia-Romagna e per tutti gli enti per i quali Regione Emilia-Romagna svolge la funzione di *conservazione* e realizza e gestisce il *processo di conservazione* ai sensi della normativa nazionale e regionale, secondo il modello organizzativo descritto al paragrafo 4.1.
In riferimento a quanto indicato nel paragrafo 4.3 delle Linee Guida il processo di conservazione viene svolto all'interno della struttura organizzativa dell'ente Regione, che si definisce costituito dalla Regione Emilia-Romagna (nelle sue articolazioni di Giunta regionale, comprese le Agenzie senza personalità giuridica, e Assemblea legislativa) e dalle seguenti Agenzie regionali con personalità giuridica: Agenzia Regionale per le Erogazioni in Agricoltura; Agenzia Regionale per la sicurezza territoriale e la Protezione Civile; Agenzia Regionale per lo Sviluppo dei Mercati Telematici. mentre viene svolta anche per altri soggetti all'esterno, quali gli enti e gli organismi regionali non precedentemente indicati e le aziende del Servizio Sanitario Regionale, oltre che gli enti del territorio regionale che hanno sottoscritto apposito organo di collaborazione.

Per le tipologie degli oggetti sottoposti a *conservazione* e i rapporti con i *Produttori* il presente Manuale è integrato da un ***Disciplinare tecnico*** specifico generato e aggiornato direttamente dal sistema di conservazione per ogni *Produttore*, che definisce le specifiche operative e le modalità di descrizione e di versamento nel *Sistema di conservazione* digitale dei *Documenti informatici* e delle *Aggregazioni documentali informatiche* oggetto di *conservazione*.

In osservanza di quanto stabilito dalle Linee Guida il presente Manuale di conservazione è adottato con provvedimento formale (Determina dirigenziale) e pubblicato sul sito istituzionale della Regione Emilia-Romagna.
La documentazione di riferimento sia tecnica (p.e. specifiche tecniche di versamento, modelli di *pacchetti informativi*) che amministrativa (p.e. modulistica e informazioni relative all'iter per avviare la collaborazione) ed altra eventuale documentazione di analisi di interesse generale sono pubblicate nel sito di ParER: https://poloarchivistico.regione.emilia-romagna.it/.

[Torna al Sommario]

2 TERMINOLOGIA (GLOSSARIO, ACRONIMI)

Per i termini utilizzati nel presente Manuale si rimanda al Glossario di cui all'Allegato 1 delle Linee Guida e alle definizioni del D.lgs. 82/2005 e del DPR 445/2000 e loro successive modificazioni e integrazioni. In generale la terminologia utilizzata si riferisce alle norme citate o a standard nazionali e internazionali.
Le definizioni riportate in ordine alfabetico in questo capitolo riguardano termini impiegati ripetutamente nel testo non presenti nelle fonti citate di cui si ritiene necessario fornire una definizione. Inoltre, sono riportate le definizioni sintetiche usate nel testo per citare la normativa e gli standard di riferimento, con la descrizione completa della fonte citata.
Nel testo del Manuale sono riportati in *corsivo* i termini riferiti al Glossario delle Linee Guida e in ***corsivo grassetto*** i termini contenuti nel presente capitolo.

Accordo: accordo di collaborazione tra il *Produttore* e ParER per lo svolgimento della funzione di conservazione dei documenti informatici, che regola i rapporti tra le parti, e più precisamente: le attività rispettivamente svolte, le responsabilità delle parti e le condizioni economiche, oltre agli strumenti di consultazione e controllo. Con il termine "Accordo" vengono ricomprese anche le convenzioni sottoscritte con gli Enti del territorio dell'Emilia-Romagna.

Allegato: ***Documento*** che compone l'***Unità documentaria*** per integrare le informazioni contenute nel ***Documento principale***. È redatto contestualmente o precedentemente al ***Documento principale***.

Annesso: ***Documento*** che compone l'***Unità documentaria***, generalmente prodotto e inserito nell'***Unità documentaria*** in un momento successivo a quello di creazione dell'***Unità documentaria***, per fornire ulteriori notizie e informazioni a corredo del ***Documento principale***.

Annotazione: ***Documento*** che compone l'***Unità documentaria*** riportante gli elementi identificativi del ***Documento*** e del suo iter documentale (un tipico esempio di Annotazione è rappresentato dalla segnatura di protocollo).

Applet: programma che viene eseguito come "ospite" nel contesto di un altro programma, detto per questo container, su un computer client [...]. In altre parole, un applet è un programma progettato per essere eseguito all'interno di un programma-container; ne consegue che l'applet non può essere eseguito indipendentemente da un altro programma. (Fonte: Wikipedia)

Appliance: particolare dispositivo elettronico hardware provvisto di un software integrato con funzione di sistema operativo, utilizzato per eseguire particolari complesse e massicce funzioni applicative software. La differenza sostanziale con i normali server o le normali apparecchiature di rete è che l'appliance non è progettato per essere flessibile alle modifiche del software o dell'hardware successive alla configurazione e installazione fatta per la sua specifica funzione applicativa. (Fonte: Wikipedia)

Application server: tipologia di server che fornisce l'infrastruttura e le funzionalità di supporto, sviluppo ed esecuzione di applicazioni nonché altri componenti server in un contesto distribuito. Si tratta di un complesso di servizi orientati alla realizzazione di applicazioni ad architettura multilivello ed enterprise, con alto grado di complessità, spesso orientate per il web (applicazioni web). (Fonte: Wikipedia)

Archiving: processo di spostamento di dati, che non sono utilizzati frequentemente, su un dispositivo che ne garantisce la memorizzazione nel lungo periodo.

Autenticazione forte: procedura basata sull'utilizzo di due o più dei seguenti elementi […] (i) qualcosa che solo l'utente conosce, p.e. una password […] (ii) qualcosa che solo l'utente possiede, p.e. […] un telefono cellulare (iii) qualcosa che caratterizza l'utente, p.e. […] un'impronta digitale. (Fonte: Traduzione di citazione di Wikipedia inglese di un testo della Banca Centrale Europea)

Backup: replicazione, su un qualunque supporto di memorizzazione, di materiale informativo archiviato nella memoria di massa dei computer, al fine di prevenire la perdita definitiva dei dati in caso di eventi malevoli accidentali o intenzionali. (Fonte: Wikipedia)

Bilanciatore di carico: tecnica informatica che consiste nel distribuire il carico di elaborazione di uno specifico servizio tra più server. Si aumentano in questo modo la scalabilità e l'affidabilità dell'architettura nel suo complesso. (Fonte: Wikipedia)

BLOb: acronimo per Binary Large object; tipo di dato usato nei database per la memorizzazione di dati di grandi dimensioni in formato binario. (Fonte: Wikipedia)

Business intelligence (BI)**:** un'applicazione di BI è uno strumento software che, acquisendo e manipolando masse di dati presenti su database o anche archivi de-strutturati, fornisce report, statistiche, indicatori, grafici costantemente aggiornati, facilmente adattabili e configurabili. (Fonte: Wikipedia)

Client: componente del sistema che accede ai servizi o alle risorse di un altro componente, detto ***server***. Il termine client indica anche il software usato sul computer client per accedere alle funzionalità offerte dal ***server***. (Fonte: Wikipedia)

Cloud computing: paradigma di erogazione di servizi offerti su richiesta da un fornitore a un cliente finale attraverso la rete internet (come l'archiviazione, l'elaborazione o la trasmissione dati), a partire da un insieme di risorse preesistenti, configurabili e disponibili in remoto sotto forma di architettura distribuita. (Fonte: Wikipedia)

Cloud Marketplace di AgID: piattaforma che espone i servizi e le infrastrutture qualificate da AgID secondo quanto disposto dalle Circolari AgID n. 2 e n.3 del 9 aprile 2018. A decorrere dal 1 aprile 2019, le Amministrazioni Pubbliche possono acquisire esclusivamente servizi qualificati da AgID e pubblicati nel Cloud Marketplace. (Fonte: AgID)

Cluster: insieme di dispositivi di elaborazione connessi in maniera più o meno stretta che operano insieme in modo tale da poter essere considerati un unico sistema. (Fonte: Wikipedia)

Componente: elemento che compone il ***Documento*****.** Generalmente è un file, ma può essere anche composto solo da *metadati*.

Comunità di riferimento: un gruppo ben individuato di potenziali *Utenti* che dovrebbero essere in grado di comprendere un particolare insieme di informazioni. La Comunità di riferimento può essere composta da più comunità di *Utenti*. [Fonte: ***OAIS***]

Contenuto informativo: l'insieme delle informazioni che costituisce l'obiettivo originario della *conservazion*e. È composto dall'***Oggetto-dati*** e dalle ***Informazioni di rappresentazione***. [Fonte: ***OAIS***]

Continuità Operativa (Business Continuity)**:** capacità di un'organizzazione di continuare a erogare prodotti o servizi a livelli predefiniti accettabili a seguito di un incidente. Si tratta di una disciplina di gestione che consente all'organizzazione - privata o pubblica che sia - di diventare più resiliente agli incidenti che potrebbero causarne l'interruzione delle attività o addirittura minacciarne l'esistenza. [...] Erroneamente, viene spesso confusa con il ***Disaster Recovery*** che è solo una parte specifica della business continuity, relativa in particolare ai processi informatici. La continuità operativa ha un campo di applicazione più ampio e si riflette anche su persone, siti, risorse e fornitori dell'organizzazione.

Data Center: struttura utilizzata per ospitare computer e componenti associati, quali dispositivi di telecomunicazioni e di ***storage***, in generale con adeguati livelli di prestazioni e di sicurezza. (Fonte: Wikipedia)

Data Breach: violazione di sicurezza che comporta - accidentalmente o in modo illecito - la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati. Una violazione dei dati personali può compromettere la riservatezza, l'integrità o la disponibilità di dati personali. (Fonte: GarantePrivacy)

Data Guard: estensione del database Oracle che consente di mantenere dei database secondari allineati ad un database primario**.** (Fonte: Wikipedia)

DICOM (Digital Imaging and COmmunications in Medicine**):** standard che definisce i criteri per la comunicazione, la visualizzazione, l'archiviazione e la stampa di informazioni di tipo biomedico quali ad esempio immagini radiologiche. (Fonte: Wikipedia)

Disaster recovery: insieme delle misure tecnologiche e logistico / organizzative atte a ripristinare sistemi, dati e infrastrutture necessarie all'erogazione di servizi di business per imprese, associazioni o enti, a fronte di gravi emergenze che ne intacchino la regolare attività. (Fonte: Wikipedia)

Disciplinare tecnico: documento redatto con ogni *Produttore*, che definisce le specifiche operative e le modalità di descrizione e di versamento nel *Sistema di conservazione* digitale dei *Documenti informatici* e delle *Aggregazioni documentali informatiche* oggetto di *conservazione*.

DNS (Domain Name System**):** sistema utilizzato per la risoluzione di nomi dei nodi della rete in indirizzi IP e viceversa. (Fonte: Wikipedia)

Documenti di conservazione: evidenze informatiche prodotte nel corso del processo di conservazione o da altri *sistemi di conservazione*.

Documento: nell'uso del presente Manuale, elemento dell'***Unità documentaria***. Si distingue in ***Documento principale, Allegato, Annesso, Annotazione.*** Si tratta comunque di un ***Documento archivistico (Record)***.

Documento archivistico (Record)**:** Informazioni memorizzate su qualsiasi supporto o tipologia documentaria, prodotte o ricevute e conservate da un ente o da una persona nello svolgimento delle proprie attività o nella condotta dei propri affari. [fonte: ***ISAD***]

Documento principale: ***Documento*** che deve essere obbligatoriamente presente nell'***Unità documentaria***, della quale definisce il contenuto primario.

EJB (Enterprise JavaBean): componenti software che implementano, lato server, la logica di business di un'applicazione web all'interno della piattaforma ***J2EE***. (Fonte: Wikipedia)

Elenco di versamento: documento in formato XML in cui sono indicati i *Documenti informatici* e le *Aggregazioni documentali informatiche* acquisiti dal *Sistema di conservazione* e una serie di informazioni relative alle verifiche a cui sono stati sottoposti durante il processo di acquisizione e *presa in carico*.

Esito versamento: documento in formato XML prodotto al termine delle verifiche in fase di ***versamento***, memorizzato nel *Sistema di conservazione* e inviato al sistema versante.

File system: meccanismo con il quale i file sono posizionati e organizzati o su un dispositivo di archiviazione o su una memoria di massa, come un disco rigido o un CD-ROM e, in casi eccezionali, anche sulla RAM. (Fonte: Wikipedia)

Firma detached: firma digitale che è tenuta separata dai dati firmati, a differenza della firma digitale completa, che è inglobata nel file stesso. Ciò permette di poter lavorare con il file originale senza dover aprire un file firmato digitalmente, ma, ovviamente, qualsiasi modifica al file originale interrompe lo stretto legame con la firma, nel senso che un file differente non possiederà la medesima firma. (Fonte: Wikipedia)

Firewall: componente di difesa perimetrale di una rete informatica, che può anche svolgere funzioni di collegamento tra due o più tronconi di rete, garantendo dunque una protezione in termini di sicurezza informatica della rete stessa. (Fonte: Wikipedia)

Framework di sviluppo: architettura logica di supporto su cui un software può essere progettato e realizzato, spesso facilitandone lo sviluppo da parte del programmatore. (Fonte: Wikipedia)

FTP (File Transfer Protocol): protocollo per la trasmissione di dati tra host (client) e server, particolarmente adatto al trasferimento di file di grandi dimensioni. (Fonte: Wikipedia)

FTPS (File Transfer Protocol Secure): estensione del protocollo ***FTP*** con utilizzo di protocolli criptografici. (Fonte: traduzione di Wikipedia inglese)

FTP server: programma che permette di accettare connessioni in entrata e di comunicare con un ***client*** attraverso il protocollo ***FTP***. (Fonte: Wikipedia)

GDPR: Regolamento (UE) del 27 aprile 2016, n. 679, del Parlamento europeo e del Consiglio, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati), noto con l'acronimo GDPR (General Data Protection Regulation).

Grant: istruzione SQL utilizzata per fornire a uno specifico utente o ruolo o a tutti gli utenti i privilegi necessari per eseguire delle azioni su oggetti di data base. (Fonte: tradotto da Oracle inglese)

HSM (Hardware Security Module): dispositivo fisico che garantisce e gestisce chiavi digitali per l'***autenticazione forte*** e realizza processi di crittografia. Questi moduli in generale hanno la forma di una scheda o di un dispositivo esterno che si connette a un computer o a un server di rete (Fonte: tradotto da Wikipedia inglese)

HTTP (HyperText Transfer Protocol): principale protocollo utilizzato per la trasmissione d'informazioni sul web. (Fonte: Wikipedia)

HTTPS (HyperText Transfer Protocol over Secure Socket Layer): risultato dell'applicazione di un protocollo di crittografia al protocollo di trasmissione ***HTTP***. (Fonte: Wikipedia)

IdP (Identity Provider): strumento per rilasciare le informazioni di identificazione di tutti i soggetti che cercano di interagire con un sistema. Ciò si ottiene tramite un modulo di autenticazione che verifica un token di sicurezza come alternativa all'autenticazione esplicita di un utente all'interno di un ambito di sicurezza. (Fonte: Wikipedia)

Incidente di sicurezza delle informazioni: evento o serie di eventi relativo alla sicurezza delle informazioni, non voluti o inattesi, che hanno una probabilità significativa di compromettere le attività istituzionali o di affari e di minacciare la sicurezza delle informazioni. (Def. 2-36 STD ISO27000:2014).

Indice dell'AIP: file XML che contiene tutti gli elementi del *Pacchetto di archiviazione*, derivati sia dalle informazioni contenute nel SIP (o nei SIP) trasmessi dal *Produttore*, sia da quelle generate dal *Sistema di conservazione* nel corso del *processo di conservazione*.

Indice del SIP: file XML che contiene i *metadati* e la struttura del *Sistema di versamento*, nonché i riferimenti ai file dei ***Componenti***.

Indirizzo IP: etichetta numerica che identifica univocamente un dispositivo detto host collegato a una rete informatica che utilizza l'Internet Protocol come protocollo di rete. (Fonte: Wikipedia)

Informazioni descrittive: descrivono il *pacchetto informativo* e consentono di ricercarlo nel *sistema di conservazione*. In base alle caratteristiche della tipologia di oggetto contenuto nel Pacchetto, tali informazioni possono essere un sottoinsieme di quelle presenti nel *pacchetto informativo*, possono coincidere o possono anche essere diverse.

Informazioni sulla conservazione (PDI): informazioni necessarie a conservare il ***Contenuto informativo*** e a garantire che lo stesso sia chiaramente identificato e che sia chiarito il contesto in cui è stato creato. Sono costituite da *metadati* che definiscono la provenienza, il contesto, l'identificazione e l'*integrità* del ***Contenuto informativo*** oggetto della *conservazione*. [Fonte: ***OAIS***]

Informazioni sulla rappresentazione: informazioni che associano un ***Oggetto-dati*** a concetti più significativi. [Fonte: ***OAIS***]

Informazioni sull'impacchettamento (PI): informazioni che consentono di mettere in relazione nel *Sistema di conservazione*, in modo stabile e persistente, il ***Contenuto informativo*** con le relative ***Informazioni sulla conservazione***. [Fonte: ***OAIS***]

ISAD: ICA - ISAD (G): General International Standard Archival Description - Second Edition - Adopted by the Committee on Descriptive Standards Stockholm, Sweden, 19-22 September 1999.

Istanza: copia dell'applicativo dedicata ad uno scopo specifico.

JAVA: piattaforma software che ha come caratteristica peculiare il fatto di rendere possibile la scrittura e l'esecuzione di applicazioni scritte in linguaggio Java, che siano indipendenti dall'hardware sul quale poi sono eseguite. (Fonte: Wikipedia)

J2EE (Java Platform, Enterprise Edition): specifica le cui implementazioni vengono principalmente sviluppate in linguaggio di programmazione Java e ampiamente utilizzata nella programmazione Web. Ha come scopo la separazione delle funzionalità relative alla visualizzazione delle pagine web da quelle per la gestione della logica di business e del salvataggio delle informazioni sulla base dati. (Fonte: Wikipedia)

Lepida: rete delle Pubbliche Amministrazioni dell'Emilia-Romagna istituita dalla legge regionale n. 11/2004, principalmente costituita da collegamenti in fibra ottica ed estesa nel territorio appenninico attraverso dorsali radio in tecnologia Hyperlan. (Fonte: sito di Lepida s.c.p.a.)

Linee Guida: Linee Guida sulla formazione, gestione e conservazione dei documenti informatici pubblicate da AgID

Magic number: sequenza di bit, normalmente posta prima della sequenza di dati, che serve per definire il formato in cui i dati sono memorizzati. [...] Oggi la maggior parte dei formati del file hanno un magic number, costituito da un numero di byte variabile (solitamente da 2 a 10). I file immagine GIF, per esempio, cominciano sempre con la stringa ASCII GIF87a o GIF89a che definisce lo standard al quale il file aderisce. [...] I file PDF iniziano con "%PDF". (Fonte: Wikipedia)

Marca temporale: sequenza di caratteri che rappresentano una data e/o un orario per accertare l'effettivo avvenimento di un certo evento. La data è di solito presentata in un formato compatibile, in modo che sia facile da comparare con un'altra per stabilirne l'ordine temporale. La pratica dell'applicazione della marca temporale è detta *timestamping*. (Fonte: Wikipedia)

Massimario di scarto: vedi ***Piano di Conservazione***.

Microservizi: approccio architetturale alla realizzazione di applicazioni caratterizzata dalla suddivisione dell'applicazione nelle sue funzioni di base. Ciascuna funzione, denominata servizio, può essere compilata e implementata in modo indipendente. Pertanto, i singoli servizi possono funzionare, o meno, senza compromettere gli altri (Fonte: RedHat)

Migrazione: procedimento atto a trasformare il software, l'hardware, oppure i dati nell'ambito di un sistema informativo o nel passaggio da un sistema ad un altro.

Mimetype: identificatore standard utilizzato su internet per indicare il tipo di dati contenuti in un file. I mimetype sono definiti in un Registro ufficiale gestito dalla Internet Assigned Numbers Authority (IANA). (Fonte: Wikipedia)

Multi-tenant: architettura software in cui una singola istanza del software è eseguita da un server ed è fruita da diverse organizzazioni che, ciascuna con le sue peculiarità ambientali, che costituiscono concettualmente uno specifico tenant, vedono il software come a loro utilizzo esclusivo. (Fonte: Wikipedia)

Near-line: termine usato in informatica per descrivere un tipo intermedio di archiviazione dati che rappresenta un compromesso tra lo storage on-line (con accesso ai dati frequente, molto rapido) e storage/archiviazione off-line (usato ad esempio per i backup, con accesso infrequente ai dati). (Fonte: Wikipedia)

NOC (Networking Operations Center): sito (o insieme di siti) da cui viene effettuato il controllo dell'operatività di una rete di apparecchiature informatiche e di server (Fonte: tradotto da Wikipedia inglese)

NTP (Network Time Protocol): protocollo per sincronizzare gli orologi dei computer all'interno di una rete. (Fonte: Wikipedia)

OAIS: ISO 14721:2012: Space data and information transfer systems -- Open archival information system - Reference model, OAIS (Open Archival Information System), Sistema informativo aperto per l'archiviazione.

Object storage: architettura di calcolatori dedicati alla memorizzazione di dati, che gestisce i dati come oggetti, anziché come gerarchia di file, come fanno invece i file system; ogni oggetto contiene i dati, una quantità variabile di metadati e un identificatore univoco. (Fonte: tradotto da Wikipedia inglese)

Oggetto-dati: un oggetto composto da un insieme di sequenze di bit. [Fonte: ***OAIS***]

PACS: acronimo anglosassone di Picture Archiving and Communication System (Sistema di archiviazione e trasmissione di immagini). Consiste in un sistema hardware e software dedicato all'archiviazione, trasmissione, visualizzazione e stampa delle immagini diagnostiche digitali. (Fonte: Wikipedia)

Partitioning: suddivisione di un database o dei suoi costituenti in parti indipendenti; viene utilizzata per ragioni di performance, gestibilità e disponibilità dei dati. (Fonte: tradotto da Wikipedia inglese)

Penetration test: processo operativo di valutazione della sicurezza di un sistema o di una rete che simula l'attacco di un utente malintenzionato. (Fonte: Wikipedia)

Persistenza: possibilità di far sopravvivere delle strutture dati all'esecuzione di un singolo programma, salvando i dati in uno storage non volatile, come su un *file system* o su un database. (Fonte: Wikipedia)

Piano di conservazione: l'art. 68 del DPR 445/2000 (Disposizioni per la conservazione degli archivi), prevede la dotazione da parte dell'ente di un piano di conservazione degli archivi, che

deve consentire di selezionare i documenti destinati alla conservazione permanente e di identificare quelli passibili di scarto, secondo quanto indicato nel Massimario di Scarto, nel rispetto delle disposizioni vigenti in materia di tutela dei beni culturali.

Protocollo di rete: descrizione a livello logico del processo di comunicazione (meccanismi, regole o schema di comunicazione) tra terminali e apparati preposto al funzionamento efficace della comunicazione in rete. (Fonte: Wikipedia)

Proxy: un server proxy è un server (inteso come sistema informatico o applicazione), che funge da intermediario per le richieste da parte dei client alla ricerca di risorse su altri server, disaccoppiando l'accesso al web dal browser. Un client si connette al server proxy, richiedendo qualche servizio (ad esempio un file, una pagina web o qualsiasi altra risorsa disponibile su un altro server), e quest'ultimo valuta ed esegue la richiesta in modo da semplificare e gestire la sua complessità. (Fonte: Wikipedia)

RAC: in un ambiente Oracle RAC due o più computer, ognuno con un'istanza del software accedono contemporaneamente allo stesso database. Ciò consente a un'applicazione o a un utente di connettersi a ambedue i computer, mantenendo un accesso coordinato ai dati. (Fonte: tradotto da Wikipedia inglese)

Raccolta di archiviazione (AIC): *Pacchetto di archiviazione* (AIP), il cui contenuto informativo è costituito da un insieme di altri Pacchetti di archiviazione, in particolare aggregazione di AIP delle singole unità documentarie appartenenti all'aggregazione. [Fonte:***OAIS***]

Regione: Regione Emilia-Romagna, nelle sue articolazioni di Giunta regionale, comprese le Agenzie senza personalità giuridica, e l'Assemblea legislativa

Release: specifica versione di un software resa disponibile ai suoi utenti finali. La release è univocamente identificata da un numero in modo da distinguerla dalle precedenti e future altre release del software. Convenzionalmente si distinguono release maggiori, dette *major release*, quando le differenze dalla release precedente riguardano sostanziali evoluzioni delle funzionalità del software, e release minori, dette *minor release*, quando le differenze riguardano principalmente correzioni di malfunzionamenti del software. (Fonte: Wikipedia)

ReST (REpresentational State Transfer): insieme di principi di architetture di rete, i quali delineano come le risorse sono definite e indirizzate. Il termine è spesso usato nel senso di descrivere ogni semplice interfaccia che trasmette dati su ***HTTP*** senza un livello opzionale. (Fonte: Wikipedia)

S3: Servizio di ***Object storage*** accessibile via web fornito da Amazon; per l'accesso al servizio da parte degli applicativi Amazon mette a disposizione funzionalità di interfaccia che sono diventate uno standard de facto, accettato da molti dei sistemi di ***Object storage*** presenti sul mercato.

SaaS (Software as a Service): modello di distribuzione del software applicativo dove un produttore di software sviluppa, opera e gestisce un'applicazione web, che mette a disposizione dei propri clienti via Internet; spesso si tratta di un servizio di **cloud computing**. (Fonte: Wikipedia)

SCP (Secure Copy): protocollo per trasferire in modo sicuro un file tra un computer locale ed un host remoto o tra due host remoti. (Fonte: Wikipedia)

Serie: ***Unità Archivistiche*** o ***Unità Documentarie*** ordinate secondo un *sistema di classificazione* o conservati insieme perché:

- sono il risultato di un medesimo processo di sedimentazione o archiviazione o di una medesima attività;
- appartengono ad una specifica ***tipologia documentaria***;
- sussiste qualche altra relazione derivante dalle modalità della loro produzione, acquisizione o uso.

(fonte: ***ISAD***)

Server: componente o sottosistema informatico di elaborazione e gestione del traffico di informazioni che fornisce, a livello logico e fisico, un qualunque tipo di servizio ad altre componenti (tipicamente chiamate ***client***) che ne fanno richiesta attraverso una rete di computer, all'interno di un sistema informatico o anche direttamente in locale su un computer. (Fonte: Wikipedia)

Servlet container: componente di un web server che interagisce con i servlet, ovvero con programmi in linguaggio Java atti alla generazione dinamica di pagine web. (Fonte: tradotto da Wikipedia inglese)

SGI: Sistema di Gestione Integrato, che armonizza il Sistema di Gestione della Qualità **(*SGQ*)**, il Sistema di Gestione della Sicurezza delle Informazioni **(*SGSI*)** e il Sistema di Gestione Anticorruzione.

SGQ (Sistema di Gestione della Qualità): insieme formalizzato delle attività collegate e interdipendenti che influenzano la qualità di un prodotto o di un servizio. Documenta i processi, le procedure ISO 9001 e le responsabilità per il raggiungimento delle politiche della qualità e degli obiettivi della qualità.

SGSI (Sistema di Gestione della Sicurezza delle Informazioni): strumento che permette di controllare in modo sistematico e continuativo i processi che riguardano la sicurezza di tutto il patrimonio informativo aziendale, non solo dal punto di vista informatico, ma anche e soprattutto dal punto di vista gestionale ed organizzativo, definendo ruoli, responsabilità e procedure formali per l'operatività dell'organizzazione.

SIEM (Security Information and Event Management): le soluzioni rientranti in questa categoria di sistemi sono contraddistinte dalla capacità di effettuare analisi anche real-time degli allarmi di sicurezza generati dagli apparati hardware di rete e dalle applicazioni software di gestione e monitoraggio. Le soluzioni SIEM sono anche impiegate per effettuare il log delle informazioni di sicurezza e generare dei report funzionali alle tematiche di rispetto delle norme e degli standard. (Fonte: Wikipedia)

SID (Settore Innovazione Digitale, dati, tecnologia e polo archivistico): Settore, appartenente alla Direzione Generale Risorse, Europa, Innovazione e Istituzioni, che si occupa della progettazione e gestione dei Servizi IT, del presidio della Sicurezza informatica, della Statistica e della Conservazione.

SOC (Security Operation Center): centro da cui vengono forniti servizi finalizzati alla sicurezza dei sistemi informativi dell'azienda stessa o di clienti esterni.
Un SOC fornisce tre tipologie di servizi:

- di gestione: tutte le attività di gestione delle funzionalità di sicurezza legate all'infrastruttura IT (rete, sistemi ed applicazioni) sono centralizzate dal SOC;
- di monitoraggio: l'infrastruttura IT e di Sicurezza vengono monitorate in tempo reale al fine di individuare tempestivamente tentativi di intrusione, di attacco o di uso malevolo dei sistemi;
- proattivi: sono servizi finalizzati a migliorare il livello di protezione dell'organizzazione.

(Fonte: Wikipedia)

Sotto componente: ***Componente*** di un ***Componente***. Per esempio, sono Sotto componenti la ***marca temporale*** (se detached) o la Firma digitale (sempre se detached) di un determinato ***Componente***.

SPID: (Sistema Pubblico di Identità Digitale) è il Sistema Pubblico di Identità Digitale che garantisce a tutti i cittadini e le imprese un accesso unico, sicuro e protetto ai servizi digitali della Pubblica Amministrazione e dei soggetti privati aderenti. (Fonte: AgID)

Storage: dispositivo per memorizzare i dati in formato digitale, quale un dispositivo a cassette o un dispositivo a disco.

Struttura versante (o Struttura)**:** ripartizione dell'**Ente produttore** identificativa della specifica funzione di produzione dei documenti versati, in genere coincidente con l*a funzione organizzativa omogenea*.

Tape library: sistema automatico composto da alloggiamenti contenenti cassette magnetiche, dispositivi di lettura/scrittura delle cassette stesse e dispositivi di riconoscimento automatico delle cassette. (Fonte: Wikipedia)

Tempo UTC (Tempo coordinato universale): fuso orario di riferimento da cui sono calcolati tutti gli altri fusi orari del mondo. Esso è derivato dal tempo medio di Greenwich (in inglese Greenwich Mean Time, GMT), con il quale coincide a meno di approssimazioni infinitesimali, e perciò talvolta è ancora chiamato, sia pure impropriamente, GMT. (Fonte: Wikipedia)

Tipologia documentaria: categoria di ***Documenti*** omogenei per natura e funzione giuridica, modalità di registrazione o di produzione, che hanno comuni caratteristiche formali e/o intellettuali; nel sistema SacER, che fa riferimento al più complesso concetto di ***Unità Documentaria***, anziché di Documento, si preferisce parlare di "Tipo di Unità Documentaria"

Trouble ticket: sistema informatico che registra e gestisce liste di richieste di assistenza o di problemi, organizzato secondo le necessità di chi offre il servizio. […] Un ticket serve per mantenere la sequenza di attività derivate di una richiesta. Ad ogni ticket corrisponde un identificativo univoco, che ne consente l'archiviazione e la consultazione in qualunque momento da parte del personale coinvolto nella sua gestione. I ticket vengono 'creati' o 'aperti', all'atto della ricezione di una nuova richiesta, e l'obiettivo è di 'chiuderli' o 'risolverli', fornendo la soluzione al problema segnalato. (Fonte: Wikipedia)

Unità archivistica: insieme organizzato di ***Unità documentarie*** o ***Documenti*** raggruppati dal *Produttore* per le esigenze della sua attività corrente in base al comune riferimento allo stesso

oggetto, attività o fatto giuridico. Può rappresentare una unità elementare di una ***Serie***. [Fonte: ***ISAD***]

Unità di archiviazione (AIU): *Pacchetto di archiviazione* (AIP) elementare, il cui contenuto informativo non è ulteriormente decomposto in altri contenuti informativi. Definisce un AIP di ***Unità documentaria***. [Fonte: ***OAIS***]

Unità documentaria (*item)*: aggregato logico costituito da uno più ***Documenti*** che sono considerati come un tutto unico. Costituisce l'unità elementare in cui è composto l'*archivio,* cioè l'unità minima, concettualmente non divisibile, di cui è composto un archivio o, in altri termini, la più piccola distinta unità di ***Documenti*** gestita come entità. Può contenere ***Componenti***, come ad esempio una e-mail con allegati; comunque, i ***Componenti*** dell'Unità documentaria sono gestiti come una singola entità nel sistema. [Fonte: ***ISAD e ISO 23081***]

Versamento: azione di *trasferimento* di SIP dal ***Produttore*** al *Sistema di conservazione*.

Versamento anticipato: *versamento* nel *Sistema di conservazione* di *Documenti informatici* che si trovano ancora nella fase attiva del loro ciclo di vita.

Versamento in archivio: *versamento* nel Sistema di *Aggregazioni documentali informatiche* nella loro forma stabile e definitiva (principalmente Fascicoli chiusi e ***Serie*** annuali complete), ovvero che hanno esaurito il loro ciclo di vita attivo per entrare in quello semi-attivo**.**

Vulnerabilità: componente di un sistema, in corrispondenza del quale le misure di sicurezza sono assenti, ridotte o compromesse, il che rappresenta un punto debole del sistema e consente a un eventuale aggressore di compromettere il livello di sicurezza dell'intero sistema. (Fonte: Wikipedia)

Vulnerability assessment: processo che porta a identificare, quantificare, valutare la priorità (o l'importanza) delle ***vulnerabilità*** in un sistema. (Fonte: tradotto da Wikipedia inglese)

Web Server: applicazione software che, in esecuzione su un server, è in grado di gestire le richieste di trasferimento di pagine web di un ***client***, tipicamente un web browser, tramite il protocollo ***HTTP*** o eventualmente la versione sicura ***HTTPS***. (Fonte: Wikipedia)

Web Service: un sistema software progettato per supportare l'*interoperabilità* tra diversi sistemi in una medesima rete oppure in un contesto distribuito. (Fonte: Wikipedia)

ZIP: formato di compressione dei dati molto diffuso nei computer con sistemi operativi Microsoft e supportato di default nei computer con sistema operativo Mac OS X. Supporta vari algoritmi di compressione. (Fonte: Wikipedia)

[Torna al Sommario]

3 NORMATIVA E STANDARD DI RIFERIMENTO

3.1 Normativa di riferimento

Le normative in vigore nei luoghi dove sono conservati i documenti, cioè la normativa europea, nazionale italiana e regionale dell'Emilia-Romagna e gli standard di riferimento sono riportati in modo più dettagliato e secondo la gerarchia delle fonti nell'Allegato 1 "Normativa e standard di riferimento" che viene mantenuto costantemente aggiornato e pubblicato on-line sul sito di ParER.

Alla data di approvazione del presente manuale l'elenco dei principali riferimenti normativi italiani in materia, ordinati secondo il criterio della gerarchia delle fonti, è costituito da:

Codice Civile [Libro Quinto Del lavoro, Titolo II Del lavoro nell'impresa, Capo III Delle imprese commerciali e delle altre imprese soggette a registrazione, Sezione III Disposizioni particolari per le imprese commerciali, Paragrafo 2 Delle scritture contabili], articolo 2215 bis - Documentazione informatica.

Legge del 7 agosto 1990, n. 241 e s.m.i. – Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi.

Decreto del Presidente della Repubblica del 28 dicembre 2000, n. 445 e s.m.i. – Testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa.

Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 23 luglio 2014 (EIDAS) rinnovato dal **Regolamento (UE) 2024/1183 del Parlamento Europeo e del Consiglio dell'11 aprile 2024 (EIDAS 2)** relativo all'identificazione elettronica pubblica e sicura, ivi incluse le firme digitali interoperabili, che garantisca alle persone il controllo della loro identità e dei loro dati online e consenta l'accesso a servizi digitali pubblici, privati e transfrontalieri.

Regolamento (UE) 20164/910 del Parlamento Europeo e del Consiglio del 27 aprile 2016 (GDPR) relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).

Decreto Legislativo 10 agosto 2018, n. 101 che ha dettato disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016.

Decreto Legislativo del 30 giugno 2003, n. 196 e s.m.i. – Codice in materia di protezione dei dati personali.

Decreto Legislativo del 22 gennaio 2004, n. 42 e s.m.i. – Codice dei Beni Culturali e del Paesaggio.

Decreto Legislativo del 7 marzo 2005 n. 82 e s.m.i – Codice dell'amministrazione digitale (CAD).

Decreto del Presidente del Consiglio dei Ministri del 22 febbraio 2013 – Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma3, lettera b), 35, comma 2, 36, comma 2, e 71.

Decreto del Ministero dell'Economia e delle Finanze del 17 giugno 2014 - Modalità di assolvimento degli obblighi fiscali relativi ai documenti informatici ed alla loro riproduzione su diversi tipi di supporto - articolo 21, comma 5, del decreto legislativo n. 82/2005.

Circolare AgID del 9 aprile 2018, n. 2 – Criteri per la qualificazione dei Cloud Service Provider per la PA

Circolare AgID del 9 aprile 2018, n. 3 – Criteri per la qualificazione di servizi SaaS per il Cloud della PA

Linee Guida sulla formazione, gestione e conservazione dei documenti informatici, pubblicate da AgID nel settembre 2020 e aggiornate nel maggio 2021, con relativi allegati

Regolamento sui criteri per la fornitura dei servizi di conservazione dei documenti informatici pubblicato da AgID nel giugno 2021 e aggiornato nel dicembre 2021, con relativi allegati

[Torna al Sommario]

3.2 Standard di riferimento

ICA - ISAD (G): General International Standard Archival Description - Second Edition -Adopted by the Committee on Descriptive Standards Stockholm, Sweden, 19-22 September 1999. Traduzione italiana a cura di Stefano Vitali, con la collaborazione di Maurizio Savoja, Firenze 2000. Standard dell'ICA (International Council on Archives – Conseil International des Archives) che fornisce delle norme generali per l'elaborazione di descrizioni archivistiche.

ISO 14721:2012 – Open Archival Information System (**OAIS**) – Reference model (CCSDS 650.0-M-2, Recommend Practice, Magenta Book June 2012): definisce concetti, modelli e funzionalità inerenti agli archivi digitali e ciò che è richiesto per garantire una conservazione permanente, o per un lungo termine indefinito, di informazioni digitali. Questa versione sostituisce la prima (ISO 14721:2003 - CCSDS 650.0-B-1 – Blue Book, January 2002) di cui è disponibile una traduzione in italiano (Sistema informativo aperto per l'archiviazione: traduzione italiana: *OAIS. Sistema informativo aperto per l'archiviazione,* a cura di Giovanni Michetti, Roma, ICCU 2007).

ISO 15836:2009 - Information and documentation – The Dublin Core metadata element set. Sistema di metadati del Dublin Core (questa versione sostituisce la precedente: ISO 15836:2003).

ISO 16363:2012 - Space data and information transfer systems - Audit and certification of trustworthy digital repositories (CCSDS 652.0-M-1 Recommend Practice, Magenta Book September 2011).

ISO 17025:2018 - General requirements for the competence of testing and calibration laboratories. Norma che esprime i "Requisiti generali per la competenza dei laboratori di prova e di taratura".

ISO 23081-1:2006 - Information and documentation – Records management processes – Metadata for records – Part 1- Principles. Quadro di riferimento per lo sviluppo di un Sistema di metadati per la gestione documentale.

ISO/TS 23081-2:2007: - Information and documentation – Records management processes – Metadata for records – Part 2- Conceptual and implementations issues. Guida pratica per l'implementazione.

ISO 23081-2:2009: - Information and documentation – Managing Metadata for records – Part 2- Conceptual and implementations issues. Guida pratica per l'implementazione.

LTO6: LTO (Linear Tape Open) è uno standard "open" sviluppato alla fine del 1990 come tecnologia di storage dei dati su nastro. La versione 6 è stata definita alla fine del 2012.

PREMIS: Data Dictionary for Preservation Metadata. Risultato dell'attività di un gruppo di lavoro transnazionale costituito nel 2003, definisce l'insieme essenziale di metadati necessari per tracciare il processo di conservazione. La versione 3.0 è stata definita nel giugno del 2105 e rivista nel novembre 2015.

SQL: (Structured Query Language) è un linguaggio standardizzato per database basati sul modello relazionale (RDBMS).

UNI 11386:2020: - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali (UNI SInCRO): Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali: definisce la struttura dell'insieme di dati a supporto del processo di conservazione e recupero degli oggetti digitali, individuando gli elementi informativi necessari alla creazione dell'indice di conservazione e descrivendone sia la semantica sia l'articolazione per mezzo del linguaggio formale XML.

UNI ISO 15489-1:2006: Informazione e documentazione – Gestione dei documenti di archivio – Principi generali sul record management.

UNI ISO 15489-2:2007: Informazione e documentazione – Gestione dei documenti di archivio – Linee guida sul record management.

ISO/IEC 9001:2015: requisiti per la realizzazione all'interno di un'organizzazione di un sistema di gestione della qualità.

ISO/IEC 27001:2013: Information technology -- Security techniques -- Information security management systems -- Requirements. Requisiti di un ISMS (Information Security Management System).

ISO/IEC 27017:2015: Codice di condotta per i controlli di sicurezza delle informazioni per i servizi in cloud.

ISO/IEC 27018:2014: - Codice di condotta per la protezione delle informazioni di identificazione personale (PII) in cloud pubblici.

ISO 22301:2012: Societal security -- Business continuity management systems --- Requirements.

ISO 37001:2016: Sistemi di gestione per la prevenzione della corruzione - Requisiti e guida all'utilizzo.

ETSI TS 101 533-1 v1.3.1 (2012-04) - Electronic Signatures and Infrastructures (ESI); Data Preservation Systems Security; Part 1: Requirements for Implementation and Management. Requisiti per realizzare e gestire sistemi sicuri e affidabili per la conservazione elettronica delle informazioni.

ETSI TR 101 533-2 v1.3.1 (2012-04) - Technical Report, Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part 2: Guidelines for Assessors. Linee guida per valutare sistemi sicuri e affidabili per la conservazione delle informazioni.

[Torna al Sommario]

4 RUOLI E RESPONSABILITÀ

4.1 Modello organizzativo

La Regione Emilia-Romagna con la legge regionale 24 maggio 2004 n. 11 (Sviluppo regionale della società dell'informazione e sue successive modificazioni[1]) ha definito la propria declinazione del modello organizzativo per la conservazione stabilendo, all'art. 2 comma 4bis, che:
La Regione, anche in collaborazione con le altre pubbliche amministrazioni interessate, favorisce […] lo sviluppo integrato della conservazione digitale dei documenti informatici e, nel rispetto dei principi di efficacia, efficienza ed economicità, svolge, con le modalità previste dalle disposizioni vigenti, le funzioni di archiviazione e conservazione digitale dei documenti informatici anche a rilevanza fiscale, prodotti o ricevuti dalla Regione e dagli altri soggetti di cui all'articolo 19, comma 5, lettera a) della legge regionale 24 maggio 2004, n. 11 nonché, mediante apposito accordo, dei documenti informatici prodotti o ricevuti dai soggetti di cui all'articolo 19, comma 5, lettera b) della medesima legge e da altri soggetti pubblici".

I soggetti indicati al citato articolo 19 sono rispettivamente:

a) *la Regione, gli enti e gli organismi regionali, le loro associazioni e consorzi, quali le agenzie, le aziende egli istituti, anche autonomi, nonché gli enti e le aziende del Servizio sanitario regionale, ed inoltre gli organismi di diritto pubblico e le società strumentali partecipate in misura totalitaria o maggioritaria dai soggetti precedenti;*
b) *gli Enti locali, i loro enti e organismi, le loro associazioni, unioni e consorzi, quali le aziende e gli istituti, anche autonomi, le istituzioni, gli organismi di diritto pubblico e le società strumentali partecipate in misura totalitaria o maggioritaria da tali soggetti, ed inoltre gli istituti di istruzione scolastica e universitaria presenti e operanti nel territorio regionale.*

I soggetti elencati al punto a), ai sensi del comma 3 dell'art. 16 della L.R. 11/2004 sono "obbligati" ad utilizzare le funzioni di archiviazione e conservazione digitale dei documenti informatici svolte dalla Regione Emilia-Romagna. Invece quelli elencati al punto b) hanno la facoltà di utilizzare le funzioni di conservazione svolte dalla Regione Emilia-Romagna.

Riassumendo si può dire che il modello organizzativo definito dalla Regione Emilia-Romagna è che la **Regione Emilia-Romagna stessa svolga le funzioni di archiviazione e conservazione digitale per la Regione e gli altri enti sopracitati, in particolare gli enti e le aziende del Servizio sanitario regionale, nella logica di sviluppo integrato della conservazione digitale dei documenti informatici nel rispetto dei principi di efficacia, efficienza ed economicità**.

Il modello rientra in quanto previsto dall' articolo 34 comma 1 bis del CAD, ma si tratta di un modello rafforzato da una norma di legge regionale ed inserito in una più ampia visione di sistema regionale allargato. Infatti, per garantire risparmi ed efficienza si concentra in un soggetto specializzato una funzione complessa come quella della conservazione degli oggetti digitali.

[1] L'ultima con Legge Regionale 26 novembre 2020 n. 7.

La Regione Emilia-Romagna, ai sensi del citato art. 2 comma 4bis della L.R. 11/2004 può inoltre collaborare con pubbliche amministrazioni interessate di tutto il territorio nazionale.

L'idea progettuale di realizzare centri di conservazione digitale, cioè "strutture dedicate alla conservazione della memoria digitale di più soggetti *Produttori*, dotate di personale archivistico e informatico altamente qualificato" era già presente nel progetto DOCAREA, presentato ed attuato nell'ambito del piano nazionale di e-government su iniziativa e coordinamento della Provincia di Bologna[2].

All'interno di tale progetto si era infatti maturata l'idea che il complesso delle attività da svolgere, i requisiti giuridici da soddisfare e le competenze professionali necessarie per la corretta conservazione degli *archivi informatici* non fossero alla portata della maggior parte delle pubbliche amministrazioni, richiedendo risorse – finanziarie, umane e strumentali – troppo elevate per ogni singola organizzazione. Di qui la concezione di un polo di conservazione digitale, concepito come archivio unico di concentrazione servente più *Produttori*, che si proponesse di offrire una soluzione condivisa, affidabile e tempestiva al problema della conservazione dei documenti informatici delle pubbliche amministrazioni.

Questa struttura, inizialmente pensata a livello provinciale e denominata Archive Service Center (ASC), già durante lo svolgimento del progetto DOCAREA venne portata, proprio per il livello di complessità e di risorse richieste, ad una dimensione regionale assumendo la denominazione di Polo archivistico regionale dell'Emilia-Romagna (ParER).

Al termine della fase di progettazione nel luglio 2009 il Polo archivistico era stato costituito come struttura operativa presso l'Istituto dei Beni artistici, culturali e naturali della Regione Emilia-Romagna. Ora, a seguito della chiusura di detto Istituto[3], tale struttura è ricompresa nella organizzazione interna della Regione Emilia-Romagna.

ParER ha tutte le caratteristiche istituzionali, giuridiche e tecniche indispensabili al corretto svolgimento del proprio ruolo di *archivio* cioè, per utilizzare i termini di ***OAIS***, una struttura organizzata di persone e sistemi che accetta la responsabilità di conservare documenti informatici e renderli disponibili ad una ***Comunità di riferimento***.

Infatti, la Regione Emilia-Romagna ha dotato ParER di una specifica struttura tecnologica e di un organico con professionalità qualificate, che assommano conoscenze di natura archivistica, informatica, organizzativa e giuridica.

In particolare, in ParER si ritiene fondamentale promuovere l'incontro tra le professionalità archivistiche e informatiche, in quanto la collaborazione tra archivisti e informatici rappresenta, e si rivela sempre più, una risorsa strategica e una condizione, se non sufficiente, sicuramente necessaria per affrontare le sfide poste dalla conservazione digitale.

Le logiche organizzative di ParER e i suoi rapporti con i *Produttori* fanno riferimento come modello concettuale alle risultanze del progetto internazionale sulla conservazione InterPARES e al

[2] Una scheda sul progetto si trova nella Appendice B di S. Pigliapoco, *La memoria digitale delle amministrazioni pubbliche*, cit., p. 225 - 236

[3] Disposta con L.R. 26 novembre 2020 n. 7 "Riordino istituzionale e dell'esercizio delle funzioni regionali nel settore del patrimonio culturale. Abrogazione delle leggi regionali 10 aprile 1995, N. 29 e 1° dicembre 1998 e modifica di leggi regionali".

modello Open Archival Information System (***OAIS***), certificato standard ISO 14721 nel 2003 e successivamente aggiornato nel 2012 (ISO 14721:2012).

Il *Sistema di conservazione* opera secondo modelli organizzativi esplicitamente definiti che garantiscono la sua distinzione logica dal sistema di gestione documentale.

Seguendo quanto indicato dalle ***Linee Guida*** e sulla base dello stesso modello ***OAIS*** si possono identificare i seguenti ruoli fondamentali: ***Produttore*** (o **Ente produttore**, che racchiude i ruoli di *Titolare dell'oggetto della conservazione* e di *produttore dei Pacchetti di Versamento*), *Utente (o Utente abilitato)*, *Responsabile della conservazione e/o Conservatore*.

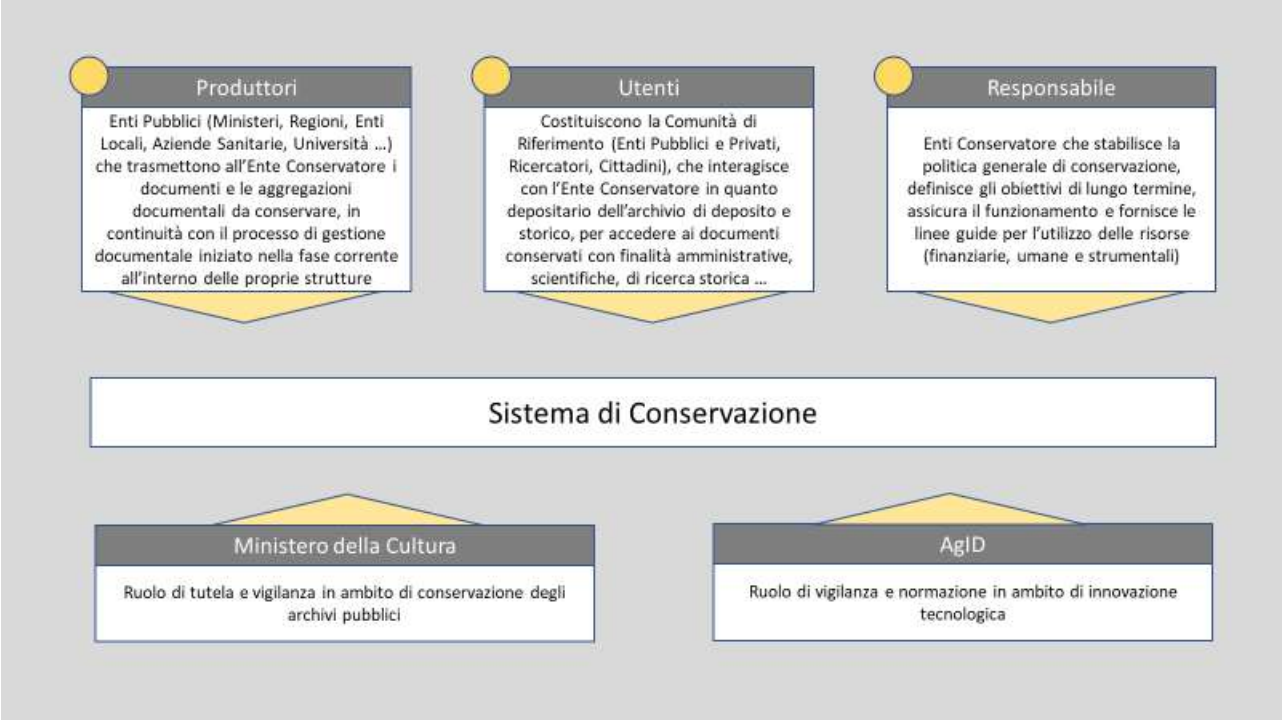


Figura 1 - Sistema e attori

[Torna al Sommario]

4.2 Titolare e Produttore

Le **Linee Guida,** tra i ruoli individuati nel processo di conservazione al primo punto definisce il *titolare dell'oggetto della conservazione*, cioè, in senso archivistico, il soggetto produttore degli oggetti di conservazione, come da definizione contenuta nel Glossario allegato alle **Linee Guida.**

Nello specifico lo si indentifica per la gestione interna della conservazione nella Regione, mentre nel caso di conservazione esterna è il soggetto che affida la conservazione dei propri documenti informatici alla Regione Emilia-Romagna, denominato nell'**Accordo** "Ente Produttore".

Nel ruolo del *Produttore* possono essere definiti tutti gli enti pubblici che hanno sottoscritto accordi di collaborazione e versano i *Documenti informatici* e le *Aggregazioni documentali informatiche* da conservare con gli opportuni *metadati*, in continuità con il processo di gestione documentale iniziato nella fase corrente all'interno delle strutture di produzione.

I rapporti tra la Regione Emilia-Romagna, tramite ParER, e i *Produttori* vengono formalizzati e regolati per mezzo di due documenti fondamentali: l'**Accordo** ed il ***Disciplinare tecnico*[4].**

L'**Accordo** regola i rapporti di collaborazione tra il *Produttore* e ParER, e, più precisamente, le attività svolte e gli obblighi delle parti, definendo gli strumenti di consultazione e controllo. Gli attuali ***Accordi*** prevedono che la funzione di conservazione dei documenti informatici sia svolta a titolo gratuito per gli enti dell'Emilia-Romagna (Enti locali, Aziende sanitarie, Università) e a titolo oneroso per gli enti di altre regioni.

Il *Produttore*, secondo quanto previsto nell'**Accordo**, si impegna a depositare i *Documenti informatici* e le loro *Aggregazioni documentali informatiche* nei modi e nelle forme definite dalla Regione Emilia-Romagna, tramite ParER, garantendone l'*autenticità* e l'*integrità* nelle fasi di produzione e di archiviazione corrente, effettuata nel rispetto delle norme sulla formazione e sui sistemi di gestione dei documenti informatici. In particolare, garantisce che il trasferimento dei documenti informatici venga realizzato utilizzando formati compatibili con la funzione di conservazione e rispondenti a quanto previsto dalla normativa vigente. Si impegna inoltre a depositare e mantenere aggiornati, nei modi e nelle forme definite tramite ParER dalla Regione Emilia-Romagna, gli strumenti di ricerca e gestione archivistica elaborati a supporto della formazione dei documenti e della tenuta degli *archivi*.
Il *Produttore* mantiene la titolarità e la proprietà dei documenti depositati.

Le ***tipologie documentarie*** da trasferire, le modalità di versamento e i *metadati* sono concordati e specificati nel ***Disciplinare tecnico***.

Il responsabile di riferimento del *Produttore* è di norma il *Responsabile della gestione documentale*, il *Responsabile della conservazione* o il responsabile di specifici sistemi di produzione documentale, quali quelli di produzione di documentazione sanitaria. Se nominato, può essere anche il *Coordinatore della gestione documentale.*

Come indicato nel paragrafo 4.4 delle **Linee Guida** il *Responsabile della gestione documentale* o, se nominato, il *Coordinatore della gestione documentale,* svolge il ruolo di *produttore dei PdV* (Pacchetti di Versamento) e assicura la trasmissione dei pacchetti di versamento al sistema di conservazione in coerenza con le modalità operative definite nel presente manuale di conservazione. Inoltre, verifica il buon esito della operazione di versamento in particolare tramite la verifica della produzione del *rapporto di versamento* da parte del sistema di conservazione.

[4] Per il dettaglio delle operazioni preliminari all'avvio in produzione di un ente, sia dal punto di vista amministrativo sia tecnico-operativo si vedano le pagine del sito di ParER specificamente dedicate alla attività di conservazione per gli enti; lo schema di Accordo è approvato con apposita delibera della Giunta della REGIONE EMILIA-ROMAGNA e periodicamente aggiornato; i Disciplinari Tecnici specifici sono presenti nel sistema di conservazione per ogni produttore.

Il *Produttore* resta il responsabile del contenuto del *Pacchetto di Versamento* (d'ora in poi SIP) ed è obbligato a trasmetterlo al servizio di conservazione secondo le modalità operative descritte a grandi linee nel presente Manuale e in dettaglio nel ***Disciplinare tecnico*** e nella documentazione tecnica di riferimento.

Il soggetto che materialmente versa i SIP nel sistema di conservazione è identificato con il termine "Versatore". Normalmente coincide con il *Produttore*, ma in alcuni casi, generalmente per motivi tecnico-organizzativi, quest'ultimo può incaricare un altro Versatore di versare in conservazione i suoi documenti.
Se il Versatore non è un *Produttore* (e in questo caso prende il nome di Versatore esterno), non può versare i SIP direttamente nel sistema - in quanto non può essere titolare di una Struttura versante – ma può versare oggetti per conto del *Produttore* nel sistema di preacquisizione (vedi paragrafo 7.1.1).

Il *Produttore*, nella sua attività di produzione e versamento in conservazione dei SIP, può essere coadiuvato da utenti esterni appartenenti ad altre organizzazioni, definite "Fornitori esterni", che sono normalmente le software house che gestiscono i sistemi di produzione e/o versamento dei documenti.

Il personale dei Fornitori esterni può operare sul Sistema per finalità di supporto tecnico e organizzativo alle attività di conservazione su esplicita autorizzazione del *Produttore*.

Come indicato nel paragrafo 4.3, il *Produttore* ha l'accesso presso la propria sede al *Sistema di conservazione* per la parte relativa alla sua documentazione conservata.

[Torna al Sommario]

4.3 Utente abilitato

In base alla definizione del glossario allegato alle **Linee Guida** si indentifica come *Utente abilitato* una persona, ente o sistema che interagisce con i servizi di un sistema per la conservazione dei *Documenti informatici* al fine di fruire delle informazioni di interesse.

L'*Utente* richiede al *Sistema di conservazione* l'*accesso* ai documenti per acquisire le informazioni di interesse nei limiti previsti dalla legge. Il *Sistema di conservazione* permette ai soggetti autorizzati l'*accesso* diretto, anche da remoto, ai *Documenti informatici* conservati e consente la produzione di un *Pacchetto di Distribuzione* direttamente acquisibile dai soggetti autorizzati.

In termini ***OAIS*** la comunità degli *Utenti* può essere definita come ***Comunità di riferimento***.

Nel ruolo dell'*Utente* si possono definire al momento solo specifici soggetti abilitati dei *Produttori*, in particolare gli operatori indicati dal *Produttore* che possono accedere esclusivamente ai documenti versati dal *Produttore* stesso o solo ad alcuni di essi secondo le regole di visibilità e di *accesso* concordate tra ParER e il *Produttore*
L'abilitazione e l'autenticazione di tali operatori avviene in base alle procedure di gestione utenze indicate nel *Piano della sicurezza del sistema di conservazione* e nel rispetto delle misure di sicurezza previste negli articoli da 31 a 36 del D.lgs. 30 giugno 2003, n. 196, in particolare di

quelle indicate all'art. 34 comma 1 e dal Disciplinare tecnico in materia di misure minime di sicurezza di cui all'Allegato B del medesimo decreto.
In prospettiva si possono definire *Utenti* potenzialmente tutti coloro che potranno interagire con ParER, quale conservatore e custode di archivi di deposito e storici, per accedere ai documenti conservati per finalità amministrative, scientifiche e di ricerca storica in relazione alle ***tipologie documentarie*** conservate e nel rispetto delle normative vigenti in materia di tutela dei beni culturali e di tutela dei dati personali.

[Torna al Sommario]

4.4 Responsabile della conservazione

In base alla normativa vigente il *Responsabile della conservazione* per le pubbliche amministrazioni è identificato con un dirigente o un funzionario formalmente designato e può identificarsi con il *Responsabile della gestione documentale* o, se nominato, con il *Coordinatore della gestione documentale.*
La Regione Emilia-Romagna con Determinazione dirigenziale n. 24766 del 30 dicembre 2021 del Direttore Generale della Direzione Generale Risorse, Europa, innovazioni e istituzioni ha individuato il Responsabile della Conservazione all'interno del Servizio Polo Archivistico e gestione documentale.
A seguito delle successive variazioni organizzative, il ruolo è ora interno all'Area sviluppo applicazioni, Polo archivistico e gestione documentale del Settore Innovazione Digitale, dati, tecnologie e Polo archivistico della Direzione Generale Risorse, Europa, innovazioni e istituzioni che ha funzioni di Direzione Generale trasversale, finalizzata alla programmazione, organizzazione e gestione di funzioni, processi e servizi di supporto e integrazione dei servizi necessari al funzionamento dell'Ente Regione.
Con determinazione n. 24946 del 20/12/2022 è stata istituita una specifica posizione di Elevata Qualificazione Q0001725 "Responsabile della Conservazione e dell'archivio storico" che svolge la funzione di Responsabile della Conservazione per i documenti informatici della Regione Emilia-Romagna.
I compiti di tale responsabile, oltre a quanto previsto dalle Linee Guida, sono i seguenti:

- Svolge la funzione di Responsabile della Conservazione per i documenti informatici della Regione Emilia-Romagna;
- Monitora il processo di conservazione dei documenti e delle aggregazioni informatiche dell'Amministrazione regionale;
- Gestisce l'archivio di deposito, predisponendo e monitorando i piani di trasferimento dei dati e dei documenti da e verso altri depositi digitali e i piani di informatizzazione dei documenti e degli archivi cartacei della Regione Emilia-Romagna;
- Gestisce l'Archivio storico della Regione Emilia-Romagna di San Giorgio di Piano assicurando il servizio di accesso ai documenti conservati da parte degli utenti esterni;
- Promuove la redazione di strumenti di corredo di tipo archivistico finalizzati all'accesso di natura storico-culturale e propone nuove funzionalità del sistema di conservazione per i medesimi fini;
- Presidia i rapporti con le strutture del Ministero della Cultura per quanto di competenza gestendo le procedure di scarto dei documenti della Regione Emilia-Romagna;

- Fornisce, relativamente all'ambito di competenza, assistenza specialistica di 2º livello, presidia la gestione tecnica dei contratti monitorando i livelli di servizio e promuove valutazioni sull'impatto della propria attività.

4.5 Conservatore

Il modello organizzativo precedentemente descritto al paragrafo 4.1, ai sensi dell'articolo 34, comma 1 bis, lettera b) del CAD**,** prevede che il titolare o soggetto produttore affidi la conservazione e il processo di conservazione ad un soggetto conservatore esterno specificamente individuato nella Regione Emilia-Romagna.

La responsabilità del Sistema di conservazione e del servizio di conservazione come soggetto che svolge attività di conservazione è in capo alla Regione Emilia-Romagna, che individua al suo interno nel Polo Archivistico Regionale (ParER) lo specifico soggetto conservatore articolato come descritto nel capitolo 5 nell'ambito delle strutture organizzative regionali.
Il ruolo di ParER come responsabile del servizio di conservazione e del *Sistema di conservazione* va inquadrato alla luce dell'art. 2 della L.R. 11/2004, ossia nel contesto di un più generale impegno, da parte della Regione Emilia-Romagna – nel rispetto delle competenze dello Stato e di concerto con il sistema degli Enti locali – per assicurare a cittadini, imprese ed enti condizioni di sviluppo delle loro attività e relazioni, promuovendo le potenzialità delle tecnologie informatiche nella prestazione di servizi e nell'accessibilità e scambio di dati. In particolare, la Regione persegue lo sviluppo delle reti strumentali, organizzative ed operative e lo sviluppo integrato dei servizi attivi sulla rete della pubblica amministrazione attraverso la collaborazione con le amministrazioni periferiche dello Stato, il sistema delle autonomie locali e, più in generale, tutti i soggetti pubblici e privati e le organizzazioni sociali operanti sul territorio.

Nello specifico, la Regione, anche in collaborazione con le altre pubbliche amministrazioni interessate, favorisce lo sviluppo integrato della *conservazione* dei *Documenti informatici* e, nel rispetto dei principi di efficacia, efficienza ed economicità, svolge le funzioni di archiviazione e *conservazione* digitale dei *Documenti informatici.*

In quanto soggetto responsabile la Regione Emilia-Romagna si occupa delle politiche complessive del *Sistema di conservazione* e ne determina l'ambito di sviluppo e le competenze. A tal fine, in coerenza con ***OAIS***, provvede alla pianificazione strategica, alla individuazione ed erogazione dei finanziamenti, alla revisione periodica dei risultati conseguiti e ad ogni altra attività gestionale mirata a coordinare lo sviluppo del sistema. Non risulta invece coinvolta nelle operazioni quotidiane di amministrazione del sistema che sono totalmente a carico del soggetto incaricato della sua gestione, cioè il Settore Innovazione Digitale, Dati, Tecnologie e Polo Archivistico (SID), in particolare l'Area sviluppo applicazioni, Polo Archivistico e gestione documentale, il cui dirigente è specificamente individuato come Responsabile del servizio di conservazione.

La missione di ParER è essere l'*archivio informatico* della Pubblica Amministrazione per la conservazione e l'accesso dei *Documenti informatici* e in generale di ogni oggetto digitale a supporto dei processi di innovazione e semplificazione amministrativa, con gli obiettivi di:

- garantire la conservazione, archiviazione e gestione dei *Documenti informatici* e degli altri oggetti digitali;
- erogare servizi di accesso basati sui contenuti digitali conservati;

- fornire supporto, formazione e consulenza ai Produttori per i processi di dematerializzazione.[5]

Di fatto, quindi (come definito dal testo dell'**Accordo**, art. 3, comma 1), la Regione Emilia-Romagna, tramite ParER, si impegna alla *conservazione* dei documenti trasferiti e ne assume la funzione di *Responsabile del servizio di conservazione* ai sensi della normativa vigente, garantendo il rispetto dei requisiti previsti dalle norme in vigore nel tempo per i sistemi di conservazione, e svolge, tramite la struttura organizzativa e di responsabilità di ParER, l'insieme delle attività in capo al *Responsabile della conservazione* elencate nel paragrafo 4.5 delle ***Linee Guida***, in particolare quelle indicate alle lettere a), b), c), d), e), f), g), h), i), j), k).
Il *Responsabile del servizio di conservazione* a cui sono affidate tali attività è individuato nel responsabile dell'Area sviluppo applicazioni, Polo Archivistico e gestione documentale (ParER) all'interno del Settore "Innovazione digitale, Dati, Tecnologie e Polo archivistico" della Direzione Generale Risorse, Europa, innovazioni e istituzioni. Nello svolgimento di tali attività è coadiuvato dal *Responsabile della funzione archivistica di conservazione*, individuato nel funzionario incaricato della posizione di Elevata Qualificazione Q0001003 "Responsabile della funzione archivistica di Conservazione".

Per la descrizione nel dettaglio della struttura organizzativa e di responsabilità si veda il capitolo 5 e per i dati dei soggetti che nel tempo hanno assunto la responsabilità del *Sistema di conservazione* l'Allegato 2 "Registro dei responsabili".
Nell'Allegato, che verrà mantenuto costantemente aggiornato, sono riportati i dati delle persone fisiche che, in base ai loro ruoli in Regione Emilia-Romagna, nel tempo hanno esercitato la rappresentanza del conservatore tramite specifiche azioni e/o eventuali sottoscrizioni. In particolare, il Responsabile del Servizio di Conservazione ed il Responsabile della Funzione Archivistica di Conservazione a cui sono assegnate le funzioni di sottoscrizione previste nell'ambito del *processo di conservazione* e le funzioni di rappresentanza nei rapporti con il MiC e gli altri enti di vigilanza per quanto di competenza.

In taluni casi l'**Accordo** può prevedere che, per semplificare le attività di avviamento e di gestione ordinaria della funzione diconservazione, il rapporto tra il *Produttore* e il Conservatore sia mediato da un ente, chiamato nel sistema di conservazione "Ente gestore", che, pur non assumendo la responsabilità diretta del processo di conservazione, che resta in capo al conservatore, agisce come facilitatore del processo medesimo, svolgendo attività di gestione (quali configurazioni di sistema, definizione di modalità comuni di versamento, monitoraggio) e coordinamento (gestione delle utenze, formazione, supporto di primo livello) rispetto ad un gruppo definito di *Produttori*.
Il ruolo di Gestore è concordato tramite apposito accordo da una parte con il Conservatore, dall'altra parte con i *Produttori*: il Gestore stipula con il Conservatore un accordo generale, cui gli enti Produttori possono aderire, semplificando notevolmente i processi correlati. Il ruolo di gestore viene normalmente svolto da enti territoriali che svolgono servizi per gli enti del proprio territorio.

[Torna al Sommario]

[5] Da Relazione sulle attività realizzate per gli anni 2009 – 2012 approvata dalla Delibera di Giunta regionale Emilia-Romagna del 01 ottobre 2012, n. 1428.

4.6 Organismi di tutela e vigilanza

Il Ministero della Cultura (MiC) esercita funzioni di tutela e vigilanza dei sistemi di conservazione degli archivi di enti pubblici o di enti privati dichiarati di interesse storico particolarmente importante e autorizza le operazioni di *scarto* e trasferimento della documentazione conservata ai sensi del D.Lgs 42/2004[6].
La tutela e vigilanza sugli archivi di enti pubblici non statali è esercitata dal MiC, tramite le Soprintendenze archivistiche e bibliografiche competenti per territorio.
"Lo spostamento, anche temporaneo dei beni culturali mobili" compresi gli archivi storici e di deposito è soggetto ad autorizzazione della Soprintendenza archivistica (D.lgs 22 gen. 2004, n. 42, art. 21, c. 1, lettera b).
Anche "Il trasferimento ad altre persone giuridiche di complessi organici di documentazione di archivi pubblici, nonché di archivi di privati per i quali sia intervenuta la dichiarazione ai sensi dell'articolo 13", sia che comporti o non comporti uno spostamento, rientra tra gli interventi soggetti ad autorizzazione della Soprintendenza archivistica (D.lgs 22 gen. 2004, n. 42, art.21, c. 1, lettera e).
La disposizione si applica anche:

- all'affidamento a terzi dell'archivio (outsourcing), ai sensi del D.lgs 22 gen. 2004, n. 42, art.21, c. 1, lettera e)
- al trasferimento di archivi informatici ad altri soggetti giuridici, nell'ottica della conservazione permanente sia del documento sia del contesto archivistico[7].

La Soprintendenza archivistica e bibliografica può, in seguito a preavviso, effettuare ispezioni per accertare lo stato di conservazione e custodia degli archivi e può emettere prescrizioni per la tutela degli archivi.
Secondo quanto disposto dall'art. 44, comma 2 lettera a) del recente regolamento di organizzazione del MiC (DPCM 2 dicembre 2019, n. 169, pubblicato sulla GU n. 16 del 21 gennaio 2020, vigente dal 5 febbraio 2020), il Soprintendente archivistico e bibliografico "svolge, sulla base delle indicazioni e dei programmi definiti dalla competente Direzione generale, attività di tutela dei beni archivistici e librari presenti nell'ambito del territorio di competenza nei confronti di tutti i soggetti pubblici e privati, ivi inclusi i soggetti di cui all'articolo 44-bis del Codice dell'amministrazione digitale di cui al decreto legislativo 7 marzo 2005, n. 82,", cioè i conservatori esterni.
In aderenza con le funzioni di tutela sopra indicate è stato stipulato un accordo di collaborazione con la Soprintendenza archivistica e Bibliografica dell'Emilia-Romagna, valido fino al 31 dicembre 2033 che prevede tra i punti più qualificanti:

- la semplificazione delle procedure di autorizzazione al trasferimento mediante l'approvazione preventiva dello schema di ***Accordo***;
- l'agevolazione dell'attività ispettiva;
- il supporto e consulenza ai *Produttori.*

In particolare, la Soprintendenza archivistica per l'Emilia-Romagna (ora Soprintendenza Archivistica e Bibliografica dell'Emilia-Romagna) svolge un ruolo di vigilanza del *Sistema di conservazione* per verificare che il *processo di conservazione* avvenga in modo conforme alla

[6] Si fa riferimento in particolare agli art. 4, 10, 18 e 21 del citato Decreto legislativo. Il mantenimento delle competenze del MiC in materia di tutela dei sistemi di conservazione degli archivi pubblici è ribadito in diversi paragrafi delle **Linee Guida,**in particolare i paragrafi 4.3 e 3.8

[7] Dal sito della Soprintendenza archivistica per l'Emilia-Romagna, Soprintendenza archivistica e bibliografica dell'Emilia-Romagna: Spostamento e trasferimento (cultura.gov.it)

normativa e ai principi di corretta e ininterrotta custodia, senza però accedere a informazioni personali / sensibili contenute nei documenti o nel sistema.

In base a tale accordi e secondo quanto indicato nell'**Accordo**, ParER consente alla Soprintendenza archivistica e bibliografica dell'Emilia-Romagna l'*accesso* ai propri sistemi per rendere possibile e operativo lo svolgimento della funzione di vigilanza e tutela prevista dalla legge ed effettuare le opportune verifiche sul corretto svolgimento dell'attività di *conservazione,* in particolare lo svolgimento dell'attività ispettiva, finalizzata ad accertare lo stato di conservazione e di custodia degli archivi, ai sensi e nel rispetto di quanto previsto dall'articolo 19 del D.lgs. n. 42/2004, con "*modalità concordate che consentano lo svolgimento e la documentazione di tale attività in modalità interamente digitali all'interno del sistema di conservazione sviluppato dalla Regione Emilia-Romagna*".
La profilazione dell'utente Soprintendente non consente l'accesso ai contenuti dei documenti conservati e ai dati personali / sensibili presenti nei documenti e nei metadati.

Bisogna ricordare che, ai sensi del DPR del 1° novembre 1973 n. 690, le attribuzioni degli organi centrali e periferici dello Stato in materia di ordinamento, tutela, vigilanza, conservazione, custodia e manutenzione del patrimonio storico artistico e popolare sono esercitate, per il rispettivo territorio, dalle province autonome di Trento e di Bolzano. Per la provincia di Trento tali attribuzioni riguardano anche gli archivi e i documenti della provincia, dei suoi enti funzionali, dei comuni e degli altri enti locali, degli altri enti pubblici per le materie di competenza della provincia, nonché gli archivi e i documenti dei privati.

Il servizio di conservazione agli Enti Produttori viene erogato in base al *Regolamento sui criteri per la fornitura dei servizi di conservazione dei documenti informatici* pubblicato da AgID nel giugno 2021 ed aggiornato il 17 dicembre 2021. AgID stessa può esercitare le funzioni di vigilanza previste in detto Regolamento o da altra normativa vigente.
La disciplina per la vigilanza e per l'esercizio del potere sanzionatorio previsto all'art. 32-bis del CAD da parte di AgID è oggetto del "Regolamento recante le modalità per la vigilanza ai sensi dell'art. 14-bis comma 2, lett. i) e per l'esercizio del potere sanzionatorio ai sensi dell'art. 32-bis del d. lgs. 7 marzo 2005, n. 82 e successive modificazioni"

[Torna al Sommario]

5 STRUTTURA ORGANIZZATIVA PER IL SERVIZIO DI CONSERVAZIONE

5.1 Organigramma

La Regione Emilia-Romagna è articolata a livello di macro-organizzazione interna in Direzioni Generali e Settori. Al loro interno, tali strutture organizzative possono essere articolate in:
a) Posizioni di livello dirigenziale, definite Aree di lavoro dirigenziali;
b) Posizioni di livello non dirigenziale, definite Posizioni di Elevata qualificazione.
La Direzione generale è l'unità organizzativa di massima dimensione dell'Ente che può articolarsi in Settori, che a loro volta possono ricomprendere al loro interno Aree di lavoro assegnate a responsabilità dirigenziali e Posizioni Organizzative, secondo raggruppamenti di competenza adeguati all'attività che svolgono.
Al Settore sono assegnate funzioni e attività caratterizzate da elementi di omogeneità con l'obiettivo di perseguire livelli ottimali di efficacia ed efficienza.
La Regione Emilia-Romagna ha individuato all'interno della *Direzione Generale Risorse, Europa, innovazioni e istituzioni* il Settore Innovazione digitale, dati, tecnologia e polo archivistico come settore di riferimento per il Polo archivistico (ParER), ponendo nella specifica Declaratoria tra le responsabilità del Settore la progettazione, sviluppo e manutenzione del servizio di conservazione **in qualità di Polo Archivistico Regionale (ParER)** e la cura dello svolgimento dei processi di conservazione e di riversamento sostitutivo dei documenti informatici della Regione e degli Enti sottoscrittori di accordi di collaborazione, raccordandosi con analoghe iniziative a livello nazionale ed europeo.

Si riporta nella figura seguente l'organigramma regionale evidenziando il Settore Innovazione digitale, dati, tecnologia e polo archivistico.

Figura 2 - Organizzazione della DGREI

All'interno del Settore Innovazione digitale, dati, tecnologia e polo archivistico si individuano due strutture organizzative dirigenziali: *Area sviluppo applicazioni, Polo archivistico e gestione documentale* e *Area Infrastrutture e Sicurezza*, che collaborano alla cura del processo di conservazione e all'evoluzione tecnologica del sistema.

[Torna al Sommario]

5.2 Struttura organizzativa

All'interno del Settore "Innovazione digitale, Dati, Tecnologie e Polo archivistico**"**, si presenti due strutture dirigenziali a livello di Area, che collaborano nell'ambito della gestione del sistema di conservazione e di erogazione del Servizio di conservazione:

- Area sviluppo applicazioni, Polo archivistico e gestione documentale;
- Area Infrastrutture e sicurezza.

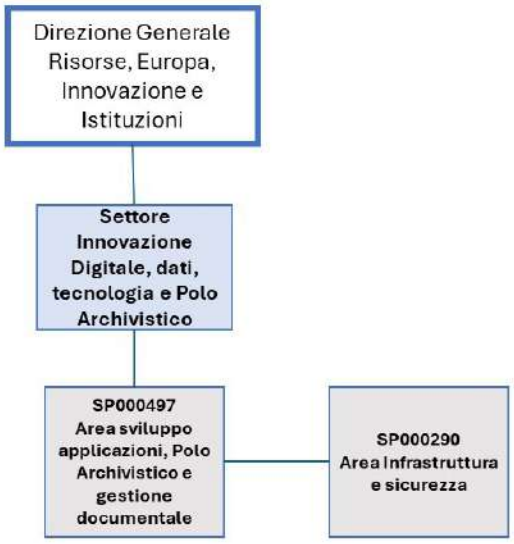


Figura 3 – Dettaglio organizzazione Settore Innovazione Digitale, dati, tecnologia e Polo Archivistico

Le attività che seguono, gestite dalle due Aree del Settore di cui sopra, sono svolte anche in relazione al Servizio di Conservazione.
In particolare, in una prospettiva di promozione della dematerializzazione e della conservazione digitale, l'Area sviluppo applicazioni, Polo archivistico e gestione documentale ha tra le proprie attività, definite in declaratoria, le seguenti:

- gestisce ed eroga i servizi per il trattamento e la trasmissione tra Pubbliche Amministrazioni dei documenti informatici e multimediali per la Regione e gli Enti in accordo;

- assicura il mantenimento dei requisiti e delle certificazioni necessarie per ottenere e mantenere le qualificazioni per poter erogare i servizi di conservazione digitale alle Pubbliche Amministrazioni;
- definisce standard e linee guida per la progettazione, gestione e manutenzione del sistema di conservazione digitale Polo Archivistico regionale e il suo aggiornamento in conformità agli standard internazionali di riferimento e ai cambiamenti normativi in materia;
- realizza, gestisce e garantisce la manutenzione della piattaforma tecnologica del sistema di conservazione digitale Polo Archivistico regionale;
- promuove e realizza interventi finalizzati ad assicurare l'integrazione tra i sistemi informativi verticali e i sistemi di gestione della documentazione con il sistema di conservazione;
- cura le relazioni con i livelli interregionali, nazionali ed internazionali sulle materie di competenze, partecipando ad iniziative e gruppi di lavoro;
- partecipa all'analisi dei costi dei servizi IT e alla pianificazione del budget, contribuisce alla stesura dei capitolati di gara per l'acquisizione di beni e servizi IT di competenza, contribuisce alla stesura dei documenti di programmazione e ne monitora l'attuazione, formula proposte per progetti di innovazione, coordina personale e risorse coinvolte nei progetti affidati anche su ambiti trasversali.

L'Area Infrastrutture e Sicurezza ha tra le proprie attività per l'Ente e quindi anche in relazione al Servizio di Conservazione, le seguenti:

- Individua soluzioni infrastrutturali a supporto dei servizi IT che ne garantiscano la disponibilità, la performance e la sicurezza nel contesto dell'assetto organizzativo dell'Ente, supportandone le sue evoluzioni in coerenza con gli obiettivi indicati negli strumenti di programmazione;
- Presidia le attività di progettazione, realizzazione e sviluppo di tutte le infrastrutture informatiche e telematiche a supporto dei servizi IT erogati tramite i datacenter regionali, anche in cloud pubblico e privato;
- Definisce gli standard tecnologici e architetturali dell'infrastruttura IT e delle architetture applicative garantendo l'operatività dei servizi IT, presidiando il monitoraggio dei livelli di servizio e gestendo il processo di presa in carico e rilascio in produzione di nuovi servizi applicativi;
- Contribuisce alla definizione e redazione delle linee guida del sistema informativo regionale, dei disciplinari tecnici e dei modelli di convenzionamento per Istituti ed Agenzie dell'Amministrazione regionale promuovendo il modello di Cloud Service Providing;
- Collabora con la struttura competente in materia di Patrimonio e Logistica al presidio e coordinamento delle attività di sviluppo e gestione della logistica e dell'impiantistica a servizio delle attrezzature informatiche e telematiche, all'interno dei datacenter regionali e presso le sedi regionali nel rispetto delle norme di protezione dei dati personali, dell'efficienza energetica ed in generale della resilienza delle componenti coinvolte;
- Presidia e coordina i processi e le attività finalizzate a garantire l'integrazione infrastrutturale ed applicativa delle soluzioni software e hardware sia nei datacenter regionali che nelle soluzioni cloud (cloud ibrido), l'integrità dei dati ed il corretto dispiegamento delle soluzioni e processi di continuità operativa (business continuity e disaster recovery);
- Presidia e coordina le attività di progettazione e sviluppo dell'infrastruttura di rete locale, geografica e di datacenter realizzando la ridondanza dei collegamenti delle sedi, dei

datacenter regionali e promuovendo soluzioni per la connettività remota e soluzioni VPN e di virtualizzazione della rete;
- Gestisce e sviluppa l'infrastruttura tecnica di rilevazione presenze dei dipendenti regionali e i sistemi di monitoraggio e controllo, anche tramite videosorveglianza attiva e passiva dei locali regionali in collaborazione con la struttura competente in materia di Patrimonio e Logistica;
- Definisce le policy di gestione della sicurezza delle informazioni assicurando l'adeguamento delle infrastrutture e le necessarie integrazioni nel rispetto delle vigenti normative; progetta e coordina il sistema di valutazione dei rischi in materia di sicurezza e cybersecurity; presidia i processi di certificazione qualità nelle aree di competenza;
- Formula proposte per la definizione dei livelli di servizio IT, individua soluzioni per problemi e incidenti che coinvolgono le infrastrutture tecnologiche, organizza servizi di assistenza specialistica all'utenza;
- Partecipa all'analisi dei costi dei servizi IT e alla pianificazione del budget, contribuisce alla stesura dei capitolati di gara per l'acquisizione di beni e servizi IT di competenza, contribuisce alla stesura dei documenti di programmazione e ne monitora l'attuazione, formula proposte per progetti di innovazione, coordina personale e risorse coinvolte nei progetti affidati anche su ambiti trasversali.

Inoltre, all'interno del citato Settore, struttura organizzativa della Regione Emilia-Romagna, si collocano le responsabilità relative al Servizio di Conservazione di seguito dettagliate.

Area sviluppo applicazioni, Polo Archivistico e Gestione documentale

Responsabile del Servizio di Conservazione: dirigente con responsabilità dei procedimenti / processi / progetti di ParER. È il dirigente responsabile dell'Area Polo archivistico e gestione documentale. Rientrano tra le sue mansioni e responsabilità, come da specifica indicazione dell'appendice all'allegato A del Regolamento sui criteri per la fornitura dei servizi di conservazione dei documenti informatici pubblicato da AgID:
- definizione e attuazione delle politiche complessive del sistema di conservazione nonché del governo della gestione del sistema di conservazione;
- definizione delle caratteristiche e dei requisiti del sistema di conservazione in conformità alla normativa vigente;
- corretta erogazione del Servizio di Conservazione, che costituisce parte del rapporto di collaborazione con l'ente produttore;
- gestione degli accordi, definizione degli aspetti tecnico-operativi e validazione dei disciplinari tecnici che specificano gli aspetti di dettaglio e le modalità operative nell'ambito della collaborazione con gli Enti produttori.

In assenza del dirigente d'Area la figura di Responsabile del Servizio di Conservazione è svolta dal dirigente responsabile del Settore Innovazione digitale, dati, tecnologia e polo archivistico

Responsabile della funzione archivistica di conservazione: è il funzionario titolare della posizione di Elevata Qualificazione responsabile del presidio della funzione archivistica di conservazione ed opera a stretto contatto con il Responsabile del Servizio di Conservazione. Rientrano tra le sue mansioni e responsabilità, quanto indicato nell'appendice all'allegato A del Regolamento sui criteri per la fornitura dei servizi di conservazione dei documenti informatici pubblicato da AgID:
- definizione e gestione del processo di conservazione, incluse le modalità di trasferimento da parte dell'ente produttore, di acquisizione, verifica di integrità e descrizione

archivistica dei documenti e delle aggregazioni documentali trasferiti, di esibizione, di accesso e fruizione del patrimonio documentario e informativo conservato;
- definizione del set di metadati di conservazione dei documenti e dei fascicoli informatici;
- monitoraggio del processo di conservazione e analisi archivistica per lo sviluppo di nuove funzionalità del sistema di conservazione;
- collaborazione con l'ente produttore ai fini del trasferimento in conservazione, della selezione e della gestione dei rapporti con il Ministero dei beni e delle attività culturali (ora Ministero della Cultura) per quanto di competenza.

Responsabile dei Servizi di Conservazione Digitale: è il funzionario titolare della posizione di Elevata Qualificazione responsabile della relazione con gli Enti che sottoscrivono accordi di collaborazione e della gestione operativa dei servizi di conservazione, che costituiscono parte della collaborazione stessa. Opera a stretto contatto con il Responsabile del Servizio di Conservazione. Rientrano tra le sue mansioni e responsabilità:
- coordinamento delle attività operative a supporto del processo di conservazione;
- coordinamento delle attività delle risorse della funzione, in modo tale da garantire adeguati livelli di servizio agli Enti che conservano presso ParER;
- gestione il ciclo di pianificazione, esecuzione e controllo delle attività,
- definizione dei processi e delle procedure operative del servizio, in coerenza con le linee guida emesse dalla Funzione Archivistica di Conservazione;
- nel caso di nuovo sviluppi applicativi, definizione dei requisiti di massima del servizio e verifica dei documenti prodotti dall'Area Sviluppo Applicazioni;

Inoltre, come Referente per la Qualità:
- si occupa della gestione delle relazioni con gli Enti Produttori, Fornitori per ciò che attiene alle problematiche della Qualità;
- monitora e misura il livello di soddisfazione degli Enti Produttori;
- controlla i livelli di Qualità nell'ambito dei processi di conservazione;
- si occupa dell'analisi dei reclami degli Enti Produttori per la gestione di azioni correttive opportune da parte del responsabile competente.

Il Responsabile dei Servizi di conservazione digitale opera in raccordo con un gruppo di archivisti, i quali analizzano le problematiche specifiche delle diverse tipologie documentarie, con particolare riferimento alla modellizzazione dei *pacchetti informativi*, avviano in conservazione nuovi Enti, estendono l'uso del servizio a nuove strutture e a nuove tipologie documentarie e aggregazioni, formano gli utenti all'utilizzo del servizio, verificano l'andamento dei versamenti e supportano gli utenti nell'utilizzo quotidiano del servizio. Gli archivisti contribuiscono inoltre allo sviluppo delle nuove applicazioni, partecipando, quando necessario, all'analisi funzionale e ai test preliminari al passaggio in produzione. È operativo un servizio di help desk curato dai medesimi archivisti, che svolge attività di supporto e assistenza, utilizzando strumenti e procedure standardizzate.

Responsabile Sistemi di conservazione[8]: è il funzionario titolare della posizione di Elevata Qualificazione responsabile che gestisce tutti gli aspetti di sviluppo, gestione e manutenzione del Sistema di Conservazione.

[8] Nel perimetro della Conservazione è anche definito Responsabile dello Sviluppo del Sistema di Conservazione

Area Infrastrutture e Sicurezza:

In questa area sono presenti le figure di **Responsabile Sicurezza Informatica e Responsabile Infrastruttura Tecnologica e Architetture Applicative** che includono tutti gli elementi relativi ai servizi di conservazione, come la sicurezza e la gestione delle infrastrutture a sostegno dell'erogazione, all'interno delle loro responsabilità come dichiarato nella Declaratoria.

Il Responsabile del trattamento dei dati personali e il Responsabile della Protezione dei Dati (DPO) sono identificati nel capitolo 10 del presente Manuale.

Nella tabella successiva è riportata la mappatura tra le attività principali del Servizio e le strutture interessate. Per la rappresentazione grafica è stato utilizzato lo schema RACI:

- **R**, Responsible: ha il compito di svolgere una particolare attività;
- **A**, Accountable: è responsabile dei risultati dell'attività o ha un ruolo di approvatore;
- **C**, Consulted: è coinvolto attivamente nel processo indirizzando le azioni da compiere o le decisioni da prendere;
- **I**, Informed: è mantenuto informato sulle azioni da compiere o sulle decisioni prese. Il soggetto informato non può influenzare il risultato.

Attività	Resp. Servizio di conservazione	Ref. Sicurezza dei Sistemi	Resp. Funzione Archivistica Conservazione	Resp. Servizi di conservazione Digitale	Ref. Servizi Tecnologici Infrastrutture	Resp. Sistemi di conservazione	DPO Regione e referente privacy del SID
Gestione degli Accordi	A		C	R			
Attivazione del servizio di conservazione	A		C	R			
Gestione e monitoraggio del processo di conservazione	A		R	I		C	
Gestione e monitoraggio Infrastruttura	I, C		I	I	A, R	I, C	
Sviluppo, manutenzione e monitoraggio del sistema	I, C		I, C	I	I, C	A, R	
Monitoraggio dei Servizi di conservazione	I		C	R		C	
Verifica di conformità a norme e std di conservazione			A, R		I	I	C
Gestione Sicurezza del sistema	I	A, R			I	I	

Attività	Resp. Servizio di conservazione	Ref. Sicurezza dei Sistemi	Resp. Funzione Archivistica Conservazione	Resp. Servizi di conservazione Digitale	Ref. Servizi Tecnologici Infrastrutture	Resp. Sistemi di conservazione	DPO Regione e referente privacy del SID
Gestione degli incidenti di sicurezza	I	A, R	I	I	C	C	I
Gestione del Cambiamento	A	C	C	C	C	R	
Gestione mal-funzionamenti	A		R	R	R	R	
Rapporti con le Autorità di vigilanza	I		A,R				
Amministrazione Processi di Certificazione	I	I	I	A,R	I	I	
Trattamento dei dati personali	I	I	R	R			A

[Torna al Sommario]

6 OGGETTI SOTTOPOSTI A CONSERVAZIONE

6.1 Oggetti conservati

Il *Sistema di conservazione* gestito da ParER (Sistema), conserva *Documenti informatici*, in particolare documenti amministrativi informatici, con i *metadati* ad essi associati e le loro *Aggregazioni documentali informatiche*, che includono i Fascicoli informatici (Fascicoli). Inoltre, il Sistema gestisce l'organizzazione e la descrizione dei *Documenti informatici* e delle *Aggregazioni documentali informatiche* in ***Serie***.

Tale modello riprende quello gerarchico di ordinamento di un *archivio*, illustrato in figura, derivata dallo schema dello standard ***ISAD***.

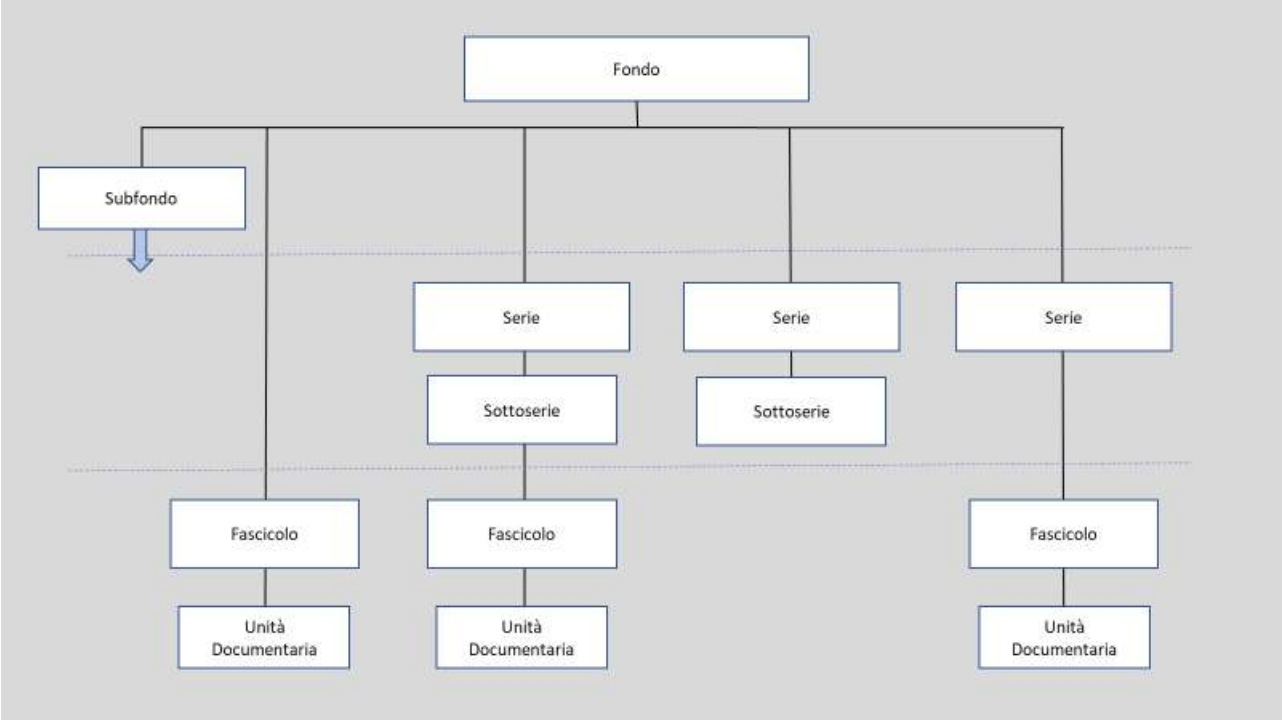


Figura 3 - Modello di ordinamento di archivio derivato da ISAD

I *Documenti informatici* e le loro *Aggregazioni documentali informatiche* (fascicoli) sono trattati nel sistema nella forma di ***Unità documentarie*** e ***Unità archivistiche***, specificamente descritte nel paragrafo 6.1.1, e sono inviati in conservazione sotto forma di *Pacchetti di versamento* (SIP), che contengono sia i documenti che i relativi *metadati*.

Il Sistema gestisce gli oggetti sottoposti a conservazione in *archivi*, articolati in ***Strutture*** (generalmente, ma non necessariamente, corrispondenti alle Aree Organizzative Omogenee delle Pubbliche Amministrazioni) e distinti per ogni singolo *Produttore*.

Per mantenere anche nel Sistema le informazioni relative alla struttura dell'*archivio* e dei relativi vincoli archivistici, le ***Unità documentarie*** sono versate corredate di un set di *metadati* di Profilo archivistico che include gli elementi identificativi e descrittivi del Fascicolo, con riferimento alla voce di *classificazione* e l'eventuale articolazione in sottofascicoli. Inoltre, è gestita la presenza

di classificazioni, fascicoli e sotto-fascicoli secondari e collegamenti tra le diverse ***Unità archivistiche*** e documentarie presenti nel sistema.

Le ***Unità archivistiche*** e le ***Serie*** sono versate nel Sistema quando sono complete e dichiarate chiuse, descritte da un set di *metadati* che include obbligatoriamente, oltre alle informazioni di identificazione, *classificazione* e descrizione, anche il tempo di conservazione previsto. Nel caso delle ***Serie*** la chiusura avviene normalmente a cadenza annuale (o comunque secondo una definizione temporale definita dal *Produttore*) ed è da intendersi come chiusura della partizione periodica della Serie stessa (ad esempio, la partizione annuale della serie delle Determinazioni corrisponde alle determinazioni prodotte in uno specifico anno e tale partizione va ad alimentare la relativa serie).

I *Documenti informatici* (***Unità documentarie***), e, in certi casi, i Fascicoli (***Unità archivistiche***) sono suddivisi in ***tipologie documentarie*** (definite nel sistema "Tipi unità documentarie" e "Tipi fascicolo"), che identificano gruppi documentali omogenei per natura e funzione giuridica, modalità di registrazione o di produzione. Tale suddivisione è funzionale all'individuazione, per ogni singola ***tipologia documentaria***, di set di *metadati* standard e di articolazioni o strutture di composizione omogenee. Inoltre, le ***tipologie documentarie*** in molti casi individuano le ***Serie*** in cui si articola e organizza la produzione documentale del *Produttore*.

Per le principali ***tipologie documentarie***, la Funzione archivistica elabora e pubblica documenti di studio ed analisi (modelli degli AIP e dei SIP), che definiscono per ogni ***tipologia documentaria***:

- il set dei *metadati* descrittivi che le caratterizzano, ritenuti essenziali per la corretta conservazione dei documenti e delle aggregazioni documentali informatiche (vedi più avanti paragrafo 6.1.3), in coerenza con quanto stabilito nell'Allegato 5 delle ***Linee Guida***;
- la struttura in base a cui sono articolate (vedi più avanti paragrafo 6.1.1).

A titolo esemplificativo, si riportano le principali macrocategorie di ***tipologie documentarie*** gestite e conservate:

- **Documentazione amministrativa:** documenti inerenti all'attività degli organi consiliari, contratti e accordi, decreti e ordinanze, deliberazioni, determinazioni, documentazione contabile, documenti protocollati, registri, strumenti urbanistici, ecc.;
- **Documentazione sanitaria:** referti e immagini diagnostiche;
- **Documentazione scolastica:** pagelle e registri didattici;
- **Documentazione universitaria:** verbali di esame e altri documenti inerenti all'attività didattica;
- **Documenti di conservazione:** evidenze informatiche prodotte da altri *sistemi di conservazione*.

Benché il Sistema operi primariamente su *Documenti informatici* originali e su Fascicoli informatici, al fine di mantenere la completezza e la consistenza dei fascicoli, e più in generale dell'*archivio* nel suo complesso, nel caso di Fascicoli ibridi è previsto l'invio al Sistema anche delle copie per immagini di originali analogici o dei soli *metadati* relativi a documenti in originale analogico.

Stante la natura eterogenea degli *archivi* conservati da ParER, diverse sono le attività svolte a garanzia non solo della integrità ma anche della fruibilità degli *archivi* stessi nel lungo periodo,

per mantenere la loro leggibilità e reperibilità, anche nella prospettiva della futura fruizione come archivi storici.
A tal fine le strategie adottate per la conservazione a cura di ParER prevedono le seguenti azioni:

- definire con precisione la ***Comunità di riferimento*** di ogni *archivio*, in accordo con i *Produttori*;
- analizzare le caratteristiche archivistiche e tecnologiche dei documenti conservati;
- mantenere attivo un osservatorio tecnologico sulla conservazione ed effettuare sperimentazioni sulle tecnologie disponibili, con particolare riguardo alle tecnologie open source ed ai progetti nazionali e internazionali nell'area della conservazione;
- collaborare attivamente con le autorità istituzionalmente preposte alla definizione del quadro normativo e delle regole operative per la conservazione documentale e con le autorità di sorveglianza.

In ragione dei diversi fattori che influiscono sulla fruibilità degli *archivi* nel lungo periodo, ParER adotta diverse misure per garantire la reperibilità e la *leggibilità* dei documenti conservati negli *archivi*. In particolare per quanto riguarda la reperibilità dei documenti si prevedono appropriate procedure di natura archivistica (creazione di ***Serie*** e fascicoli, arricchimento di *metadati*, collegamento tra documenti interrelati, ecc.), mentre per quanto riguarda la *leggibilità* si prevedono procedure di manutenzione dei *formati*, che possono variare in ragione della ***Comunità di riferimento*** e delle caratteristiche archivistiche e tecnologiche dei documenti stessi; p.e. nel caso di studi in standard ***DICOM***, che vengono restituiti solo a sistemi ***PACS***, non vengono operate trasformazioni di *formato*, mentre nel caso di formati proprietari o deprecati di documenti amministrativi destinati ad avere ampia diffusione, si possono operare attività di trasformazione verso formati standard aperti (p.e. pdf/A); l'adozione di trasformazioni dipende dalla vita utile del documento (p.e. non vengono trasformati documenti che saranno sottoposti a *scarto* nel breve periodo), dagli accordi con il *Produttore* e da considerazioni più generali di natura tecnologica ed archivistica. Quando necessario ParER sviluppa e manutiene nel tempo appositi sistemi di accesso per specifiche ***tipologie documentarie***, a garanzia della fruibilità nel lungo periodo.

Gli oggetti sottoposti a conservazione, siano essi *Aggregazioni documentali informatiche*, *Documenti informatici*, o *metadati*, sono trasmessi dal *Produttore*, memorizzati e conservati nel Sistema e distribuiti agli *Utenti* sotto forma di *pacchetti informativi*. Il *pacchetto informativo*, a seconda sia utilizzato per versare, conservare o distribuire gli oggetti sottoposti a conservazione, assume la forma, rispettivamente, di *Pacchetto di versamento* (SIP), *Pacchetto di archiviazione* (AIP) e *Pacchetto di distribuzione* (DIP), descritti rispettivamente nei paragrafi 6.2, 6.3 e 6.4.

Il *pacchetto informativo* è un contenitore astratto che contiene due tipi di informazione: il ***Contenuto informativo*** (o Content information) e le ***Informazioni sulla conservazione*** (PDI – Preservation Description Information), la cui correlazione è identificata dalle ***Informazioni sull'impacchettamento*** (PI – Packaging information). Il *pacchetto informativo*, inoltre, è descritto e può essere ricercato nel Sistema grazie alle ***Informazioni descrittive*** (Descriptive information).
Una rappresentazione grafica del *pacchetto informativo*, ripresa dal Modello ***OAIS***, è riportata in figura.

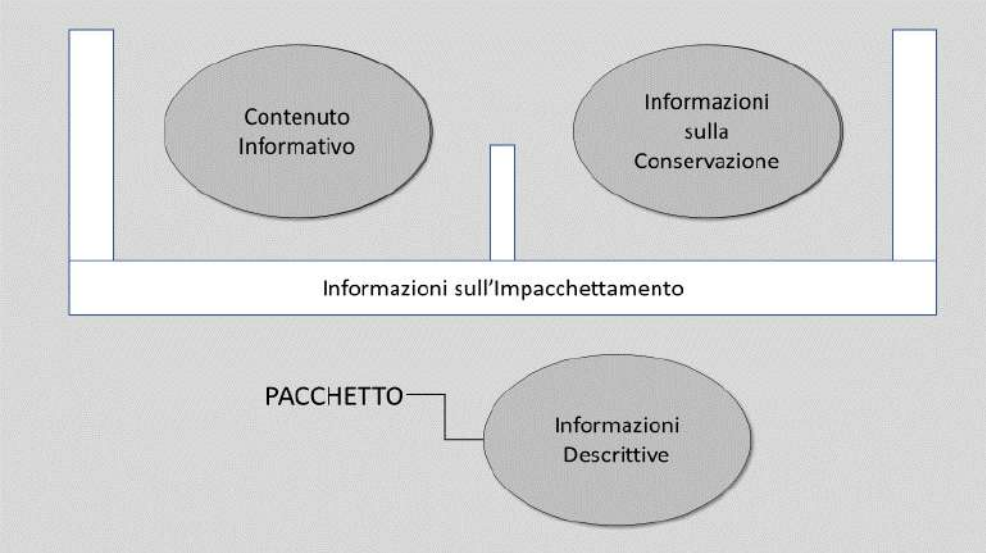


Figura 4 - Pacchetto informativo (da OAIS)

Il ***Contenuto informativo*** contiene le informazioni che costituiscono l'oggetto originario della conservazione ed è composto da due elementi:

- ***Oggetto-dati***: può assumere la forma di sequenza di bit (tipicamente un file), qualora l'oggetto sia digitale, o solo da informazioni (*metadati*), qualora sia un oggetto materiale (ad esempio, un documento analogico);
- ***Informazioni sulla rappresentazione***: costituiscono le informazioni necessarie a rendere comprensibile l'***Oggetto-dati*** agli *Utenti*. Il caso tipico di ***Informazioni sulla rappresentazione*** è costituito dalle informazioni relative al *formato* con cui la sequenza di bit è codificata, informazioni che consentono al Sistema di decodificare opportunamente la sequenza di bit per essere correttamente rappresentata e resa intelligibile agli *Utenti* del Sistema.

Le ***Informazioni sulla conservazione*** sono le informazioni necessarie a conservare il ***Contenuto informativo*** e garantiscono che lo stesso sia chiaramente identificato e che sia chiarito il contesto in cui è stato creato. Sono costituite da *metadati* che definiscono la provenienza, il contesto, l'identificazione e l'*integrità* del ***Contenuto informativo*** oggetto della conservazione.

Le ***Informazioni sull'impacchettamento*** sono informazioni che consentono di mettere in relazione nel Sistema, in modo stabile e persistente, il ***Contenuto informativo*** con le relative ***Informazioni sulla conservazione***.

Le ***Informazioni descrittive***, infine, descrivono il *pacchetto informativo* e consentono di ricercarlo nel Sistema. In base alle caratteristiche della tipologia di oggetto contenuto nel Pacchetto, tali informazioni possono essere un sottoinsieme di quelle presenti nel *pacchetto informativo*, possono coincidere o possono anche essere diverse.

[Torna al Sommario]

6.1.1 Unità archivistiche e Unità documentarie

Le ***Unità archivistiche*** contengono una o più ***Unità documentarie***, secondo le logiche di *classificazione* e fascicolazione utilizzate dal *Produttore* per organizzare i documenti prodotti nel proprio *archivio* (vedi figura 4).

L'***Unità documentaria*** rappresenta l'unità minima elementare di riferimento di cui è composto un *archivio*, pertanto rappresenta il riferimento principale per la costruzione dei *pacchetti informativi* di cui ai paragrafi 6.2, 6.3 e 6.4.
Con rifermento a quanto indicato nello standard ISO 23081-2, l'***Unità documentaria***, rappresenta la più piccola "unit of records" individuabile e gestibile come una entità singola gestita nel Sistema, anche se al suo interno contiene elementi e ***Componenti*** come, ad esempio, un messaggio di posta elettronica con i suoi allegati.
All'***Unità documentaria*** e agli elementi che la compongono sono associati set di *metadati* che li identificano e li descrivono, secondo le logiche e le articolazioni esposti al paragrafo 6.1.3.

Coerentemente con quanto sopra riportato l'Unità Documentaria è pertanto strutturata su tre livelli: Unità Documentaria, ***Documento***, ***Componente***, come rappresentato in figura***.***

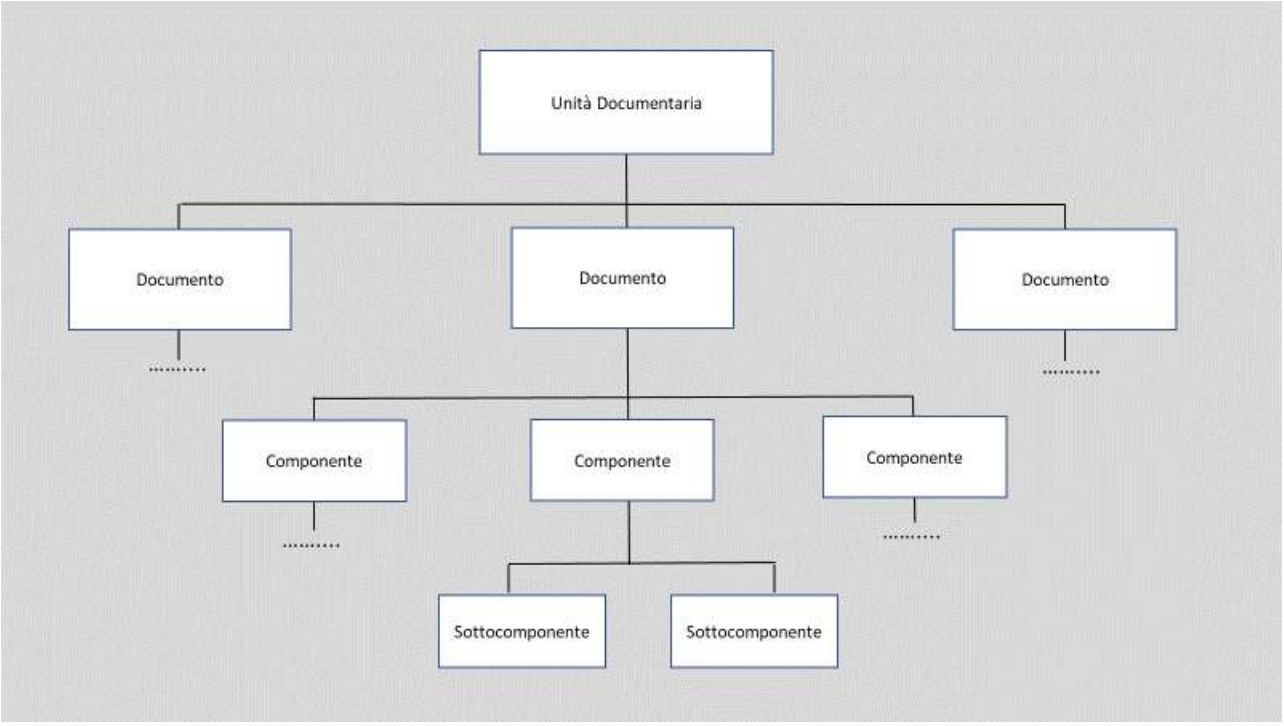


Figura 5 - Struttura dell'Unità documentaria

L'***Unità documentaria*** fa sempre riferimento a una specifica ***tipologia documentaria*** che ne determina oltre ai *metadati* di riferimento anche la struttura, in termini di definizione ed articolazione in ***Documenti*** e ***Componenti*** in essa contenuti.
I ***Documenti*** sono gli elementi dell'***Unità documentaria*** e sono identificati in base alla funzione che svolgono nel contesto dell'***Unità documentaria*** stessa, ovvero:

- ***Documento principale***: è il ***Documento*** che definisce il contenuto primario dell'***Unità documentaria***. È obbligatorio e quindi deve essere sempre presente;

- **Allegato:** è un ***Documento*** redatto contestualmente o precedentemente al ***Documento principale*** ed unito a questo, come parte integrante, per memoria, prova, chiarimento o integrazione di notizie. È facoltativo;
- **Annesso**: è un ***Documento***, generalmente prodotto e inserito nell'***Unità documentaria*** in un momento successivo rispetto a quello del ***Documento principale***, per fornire ulteriori notizie e informazioni a corredo del ***Documento principale***. È facoltativo;
- **Annotazione**: può essere costituita da quegli elementi che tradizionalmente in ambiente cartaceo venivano apposti sullo stesso supporto del ***Documento principale*** come elementi identificativi del ***Documento*** e del suo iter documentale e che in ambito informatico si sono mutati in ***Documenti*** associati al ***Documento principale*** (un tipico esempio di Annotazione è rappresentato dalla segnatura di protocollo). È facoltativa.

I ***Componenti*** individuano il contenuto del ***Documento***, che normalmente è digitale, ovvero costituito da una sequenza di bit, generalmente sotto forma di file, e i relativi *metadati*, tra cui quelli che identificano il *formato*. È possibile, però, che in taluni casi, il ***Componente*** sia espresso solo da *metadati* e sia quindi privo della sequenza di bit. Tipicamente questo avviene quando l'oggetto della conservazione non è digitale (ad esempio, documenti presenti solo in originale analogico).

Inoltre, esiste una particolare categoria di ***Componenti*** definiti ***Sotto componenti***, che contengono elementi integrativi del ***Componente*** rappresentati da sequenze di bit distinte da quelle del ***Componente*** (ad esempio, ***marche temporali detached*** o ***firma detached***). Il ***Sotto componente*** ha una struttura del tutto simile al ***Componente*** ed è associato logicamente al ***Componente*** cui fa riferimento.

[Torna al Sommario]

6.1.2 Formati

Il *Sistema* tratta i formati descritti nell'Allegato 2 alle ***Linee guida*** e, inoltre, è in grado di trattare, su richiesta del *Produttore*, anche *formati* non compresi nel suddetto elenco, ma che il *Produttore* utilizza nei propri sistemi e che ritiene di dover conservare.

Tutti i formati trattati sono elencati e descritti in un registro interno al Sistema denominato "Registro dei formati" in cui ogni *formato* è corredato da informazioni relative a estensioni e ***mimetype***. Inoltre, ogni *formato* è classificato in base alla sua idoneità a essere conservato a lungo termine in riferimento alle indicazioni fornite per la classificazione di formati dal citato Allegato 2 e all'indice di interoperabilità introdotto nel paragrafo 3.2 di detto Allegato. Sulla base di questa suddivisione i *formati* si dividono in:

- **Formati idonei**: sono i *formati* che per le loro caratteristiche di standardizzazione, di apertura, di sicurezza, di portabilità, di *immodificabilità*, di *staticità* e di diffusione sono reputati idonei alla conservazione a lungo termine;
- **Formati gestiti**: sono i *formati* leggibili e accessibili ma potenzialmente soggetti a obsolescenza tecnologica e che, in caso di necessità, possono essere opportunamente migrati in Formati idonei con apposite procedure;

- **Formati deprecati**: sono *formati* ritenuti non idonei per la conservazione a lungo termine e che al contempo non possono essere migrati in Formati idonei, per i quali, quindi, non è possibile assicurare la conservazione a lungo termine.

Con ogni *Produttore* è concordato un elenco di Formati ammessi, che individua i *formati* che il Sistema può accettare dal *Produttore* e che sono previsti per ogni ***tipologia documentaria*** gestita. L'elenco dei Formati ammessi è riportato (e gestito) nelle funzionalità "Amministrazione strutture versanti" del Sistema ed è aggiornato continuamente in base alle esigenze del *Produttore*

Il Sistema identifica i *formati* al momento della ricezione del SIP (vedi paragrafo 7.2) mediante l'analisi dei ***magic number*** o del contenuto del file, in modo tale da consentire l'individuazione dello specifico ***mimetype***.

L'informazione sul *formato* è parte dei *metadati* dei ***Componenti*** dell'***Unità documentaria*** e costituisce elemento dell'Informazione sulla rappresentazione (vedi paragrafo 6.1).

[Torna al Sommario]

6.1.3 Metadati

I *metadati* gestiti dal Sistema sono individuati in coerenza con la normativa italiana e con gli standard e i modelli internazionali di riferimento. Più in dettaglio sono descritti ed analizzati per specifici oggetti da conservare e specifiche ***tipologie documentarie*** tramite i modelli di SIP disponibili per chi ha sottoscritto un accordo. In generale il Sistema gestisce i metadati previsti dalle ***Linee Guida,*** con la definizione di uno specifico profilo in relazione, in particolare, allo schema di metadati indicati nell'allegato 5, in riferimento al documento amministrativo informatico.

I *metadati* gestiti, in base alle funzioni cui assolvono, si dividono nelle seguenti macro classi:

- **Metadati di identificazione:** identificano in modo univoco le ***Unità documentarie*** e archivistiche. Includono i dati identificativi del *Produttore* e i dati di registrazione originari, nonché gli identificativi specifici di ogni elemento dell'***Unità documentaria*** (***Documenti*** e ***Componenti***);
- **Metadati di struttura:** descrivono la struttura dell'***Unità archivistica o documentaria***, indicando nell'ultimo caso il numero e la tipologia di ***Allegati***, ***Annessi*** e ***Annotazioni*** che la compongono, nonché, per ognuno di essi, il numero e la tipologia dei ***Componenti***;
- **Metadati di profilo archivistico:** descrivono il Fascicolo e più in generale la collocazione dell'***Unità documentaria*** nel contesto dell'*archivio* del *Produttore*. Ricomprendono anche i *metadati* che collegano l'***Unità documentaria*** ad altre ***Unità documentarie*** conservate nel sistema (Collegamenti);
- **Metadati di profilo generali**: individuano gli elementi descrittivi essenziali comuni alle diverse tipologie di ***Unità archivistiche***, ***Unità documentarie*** e relativi elementi;
- **Metadati di profilo specifici:** individuano elementi descrittivi ulteriori rispetto a quelli previsti nel profilo generale. Sono definiti per ogni tipologia di ***Unità archivistica e documentaria*** e per ogni *Produttore*;

- **Metadati di conservazione:** sono tipicamente generati dal Sistema nel corso del *processo di conservazione* e attengono tanto all'analisi e alle verifiche effettuate sugli oggetti conservati, che alla descrizione delle attività svolte dal Sistema. Tra i Metadati di conservazione rientrano anche i *metadati* associati alle ***Unità archivistiche*** e ***documentarie*** provenienti da altri *sistemi di conservazione* (Metadati specifici di migrazione) e che contengono le informazioni relative al *processo di conservazione* di cui le ***Unità archivistiche e documentarie*** sono state eventualmente oggetto prima di essere versate nel Sistema.

[Torna al Sommario]

6.2 Pacchetto di versamento (SIP)

I pacchetti di versamento (SIP) sono concordati per struttura e contenuto con il *Produttore* e contengono l'oggetto o gli oggetti da conservare. In base alle specifiche esigenze possono contenere una o più ***Unità archivistiche***, una o più ***Unità documentarie***, un ***Documento*** da aggiungere a un'***Unità documentaria*** già versata o solo informazioni relative a un'***Unità documentaria*** già conservata da aggiornare. Ogni SIP può generare uno o più *Pacchetti di archiviazione* così come più SIP possono costituire un unico *Pacchetto di archiviazione*.

I SIP sono composti dai file dei ***Componenti*** e dall'***Indice del SIP*** (file XML che contiene i *metadati* e la struttura del pacchetto).

Per essere acquisiti e presi in carico dal Sistema, i SIP devono rispettare una determinata struttura dati, nell'ambito della quale viene concordato con il Produttore il contenuto informativo da portare in conservazione. La struttura dati è descritta nelle Specifiche tecniche dei servizi di versamento, mentre le procedure per la trasmissione e l'acquisizione dei SIP sono descritte nel capitolo 7.1.

I modelli di SIP gestiti dal Sistema, descritti in dettaglio nelle Specifiche dei Servizi di Versamento, sono:

- SIP di un'***Unità archivistica*****:** è il SIP utilizzato per versare le *Unità archivistiche* (Fascicoli). Contiene i *metadati* descrittivi dell'***Unità archivistica*** e l'elenco delle ***Unità documentarie*** in esso contenute. Genera un corrispondente *Pacchetto di archiviazione* relativo all'***Unità archivistica***;
- SIP di un'***Unità documentaria***: contiene un'***Unità documentaria*** completa in tutti gli elementi presenti nei sistemi del *Produttore* al momento del versamento. Il versamento di un pacchetto contenente un'***Unità documentaria*** genera un corrispondente *Pacchetto di archiviazione*;
- SIP di un ***Documento*****:** è utilizzato per aggiungere un singolo ***Documento*** e i relativi *metadati* a un'***Unità documentaria*** già presente nel Sistema. Il versamento di tale pacchetto genera l'aggiornamento del *Pacchetto di archiviazione* dell'***Unità documentaria*** cui il ***Documento*** viene aggiunto. La necessità di aggiungere un ***Documento*** a un'***Unità documentaria*** già presente si presenta tipicamente in due casi:
    - quando, per numerosità e dimensioni, è preferibile suddividere il versamento di un'***Unità documentaria*** in più parti;

- qualora uno o più ***Documenti*** appartenenti a un'***Unità documentaria*** siano disponibili sul sistema del *Produttore* solo in un momento successivo a quello in cui l'***Unità documentaria*** di cui fanno parte è stata versata nel Sistema;

- SIP di Aggiornamento metadati: è utilizzato per versare nel Sistema esclusivamente informazioni, tipicamente *metadati*, per integrare, modificare o sostituire quelle già presenti in un'***Unità documentaria*** già conservata nel Sistema. Il versamento di tale pacchetto genera l'aggiornamento del *Pacchetto di archiviazione* dell'***Unità documentaria*** i cui i metadati vengono aggiornati.

Nel caso in cui, per motivi tecnici o organizzativi, il *Produttore* non sia in grado di produrre o versare SIP nella struttura dati richiesta, può trasmettere i documenti sotto forma di generici ***Oggetti*** il cui contenuto e struttura è concordato con l'Ente conservatore. Tali ***Oggetti*** sono sottoposti alla procedura di Preacquisizione (descritta nel paragrafo 7.1.1) per essere trasformati in SIP ed essere così accettati dal Sistema.

[Torna al Sommario]

6.3 Pacchetto di archiviazione (AIP)

Il *Pacchetto di archiviazione* viene generato dal Sistema a conclusione del processo di acquisizione e *presa in carico* dei SIP (vedi paragrafo 7.5). È composto dagli ***Oggetti-dati*** (file), dall'***Indice dell'AIP***, un file XML che contiene tutti gli elementi del *pacchetto informativo*, derivati sia dalle informazioni contenute nel SIP (o nei SIP) trasmessi dal *Produttore*, sia da quelle generate dal Sistema nel corso del *processo di conservazione,* e dai Documenti di conservazione, ovvero i documenti ricevuti o prodotti nel corso del processo di conservazione (Indici dei SIP, Esiti dei versamenti, ecc.).
L'***Indice dell'AIP*** generato dal Sistema è conforme alle specifiche definite dalla norma UNI 11386 - Standard SInCRO - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali, in adesione a quanto previsto dalle **Linee Guida**.

La tabella seguente illustra come i vari elementi del *pacchetto informativo* sono presenti nell'AIP gestito dal Sistema.

Elemento del pacchetto informativo	**Articolazione dell'elemento**	**Descrizione**
Contenuto informativo	***Oggetto-dati***	È la sequenza di bit (tipicamente sotto forma di file) associata al ***Componente***. Può coincidere con quella inviata nel SIP dal *Produttore* o essere stata generata, a partire da questa, dal Sistema nel caso di produzione di copie informatiche.
	Informazioni sulla rappresentazione	Sono contenute a livello di ***Componente*** nell'***Indice dell'AIP*** e sono derivate sia da quelle contenute nel SIP di origine, sia da quelle generate dal Sistema. Includono i *metadati* relativi al *formato*.

Elemento del pacchetto informativo	Articolazione dell'elemento	Descrizione
Informazioni sulla conservazione	**Metadati di provenienza, contesto, identificazione, integrità**	Sono contenuti nell'***Indice dell'AIP*** a livello di ***Unità archivistica***, ***Unità documentaria***, ***Documento*** e ***Componente*** e originano dai SIP ricevuti o dai documenti generati dal *processo di conservazione*.
Informazioni sull'impacchettamento	**-**	A livello di ***Unità archivistica*** sono contenute nell'Indice e includono i riferimenti alle ***Unità documentarie*** che la compongono. A livello di ***Unità documentaria*** sono contenute nei Metadati di struttura e a livello di ***Componente*** negli identificativi utilizzati per associare il ***Componente*** all'***Oggetto-dati***.

Il Sistema è in grado di gestire e produrre tre tipi di AIP, descritti in dettaglio nel documento Modelli di AIP:

- AIP di ***Unità documentaria***: contiene gli ***Oggetti-dati*** e si configura come ***Unità di*** archiviazione (AIU) in quanto oggetto elementare conservato nel Sistema;
- AIP di Unità archivistica: il caso tipico è il Fascicolo e si configura come una collezione di AIP o Raccolta di archiviazione (AIC), il cui contenuto informativo è costituito dagli AIP delle singole unità documentarie appartenenti al fascicolo;
- AIP di Serie: si divide a sua volta in AIP di Serie di Unità documentarie e in AIP di Serie di Unità archivistiche (fascicoli). Si configura anch'esso come una collezione di AIP.

[Torna al Sommario]

6.4 Pacchetto di distribuzione (DIP)

Il *Pacchetto di distribuzione* viene generato dal Sistema a partire dai *Pacchetti di archiviazione* conservati ed è finalizzato a mettere a disposizione degli *Utenti*, in una forma idonea alle specifiche esigenze di utilizzo, gli oggetti sottoposti a conservazione.

Il Sistema mette a disposizione degli *Utenti*, per tutti gli oggetti sottoposti a conservazione, un DIP coincidente con l'AIP, ma può gestire la produzione di DIP specifici in relazione a particolari esigenze. In relazione alle sue caratteristiche e agli utilizzi a cui è destinato, il *Pacchetto di distribuzione* può essere generato al momento della richiesta da parte di un *Utente* e non conservato nel Sistema.

Le modalità di *esibizione* dei DIP sono descritte al paragrafo 7.6.

[Torna al Sommario]

7 PROCESSO DI CONSERVAZIONE

Il *processo di conservazione* si attiva a seguito di sottoscrizione dell'**Accordo** tra il *Produttore* e la Regione Emilia-Romagna con le modalità indicate nell'**Accordo** stesso e dettagliate nel ***Disciplinare tecnico***. L'**Accordo** medesimo disciplina anche la chiusura del servizio in caso di recesso o scadenza dell'**Accordo**, con le modalità operative descritte nel paragrafo 7.9.

7.1 Modalità di acquisizione dei pacchetti di versamento per la loro presa in carico

Il *processo di conservazione* si basa sul ***versamento*** da parte dei *Produttori* degli oggetti da conservare (*Documenti informatici* e *Aggregazioni documentali informatiche*) in due fasi: ***Versamento anticipato*** e ***Versamento in archivio***.

Con ***Versamento anticipato*** si intende il ***versamento*** nel *Sistema di conservazione* di singoli *Documenti informatici* che possono trovarsi ancora nella fase attiva del loro ciclo di vita. Tale versamento avviene in un momento il più possibile prossimo a quello di effettiva produzione del documento ed è definito anticipato perché interviene in un momento antecedente a quello previsto normalmente dalla pratica archivistica, ovvero il versamento del Fascicolo chiuso, o della ***Serie*** completa (o di partizioni di essa) in archivio di deposito.
Il ***Versamento anticipato*** è finalizzato a mettere in sicurezza l'oggetto, prevedendo una serie di controlli tesi a verificarne i metadati, il *formato* e le eventuali firme digitali apposte, al fine di mettere in atto le opportune misure necessarie alla sua conservazione a lungo termine, ovvero:

- la rilevazione dell'eventuale obsolescenza dei formati dei file, in modo da attivare per tempo le misure necessarie a mantenerne la leggibilità;
- l'apposizione di un riferimento temporale certo e opponibile a terzi;
- la rilevazione di eventuali anomalie o errori nella produzione dei documenti, anche al fine di segnalare al *Produttore* le opportune contromisure per la loro risoluzione.

In questa fase è prevista l'acquisizione nel Sistema anche di *Documenti informatici* per i quali la normativa stabilisce tempi precisi di versamento come, ad esempio, il registro giornaliero di protocollo che deve essere "trasmesso entro la giornata lavorativa successiva al *Sistema di conservazione*, garantendo l'*immodificabilità* del contenuto"[9].

Con ***Versamento in archivio*** si intende il ***versamento*** nel Sistema delle *Aggregazioni documentali informatiche* nella loro forma stabile e definitiva, principalmente Fascicoli chiusi e partizioni annuali di ***Serie*** documentarie [10].
Questa fase del *processo di conservazione*, assimilabile al versamento dall'archivio corrente all'archivio di deposito, assolve a un duplice obiettivo: da un lato portare nel Sistema le informazioni necessarie a costruire l'*archivio informatico* dell'ente; dall'altro aggiornare e fissare

[9] Linee Guida AgID, par. 3.1.6.

[10] In ottemperanza a quanto previsto dall'art. 67 del DPR 445/2000, che al comma 1 prevede che "*Almeno una volta ogni anno il responsabile del servizio per la gestione dei flussi documentali e degli archivi provvede a trasferire fascicoli e serie documentarie relativi a procedimenti conclusi in un apposito archivio di deposito costituito presso ciascuna amministrazione".*

definitivamente, qualora si rendesse necessario, le informazioni di corredo relative alle ***Unità documentarie*** versate anticipatamente nel Sistema.

Il versamento in archivio di un'aggregazione documentale informatica avviene dopo che i singoli elementi che compongono l'aggregazione sono stati versati nel Sistema. Nel SIP dell'aggregazione sono elencati tutti gli elementi che la compongono e il versamento avviene solo se nel Sistema questi sono tutti presenti.

A tal fine, prima di procedere con il loro versamento in archivio, è consigliabile effettuare l'aggiornamento dei metadati relativi alle Unità documentarie versate in Versamento anticipato, in modo da assicurare che i metadati conservati nel Sistema siano completi e definitivi.

In altri termini, si può dire che con il ***Versamento in archivio*** viene completato, da parte del *Produttore*, il *processo di conservazione* iniziato con il ***Versamento anticipato***, assicurando che gli oggetti digitali siano correttamente conservati a partire dal momento della loro produzione e resi accessibili per gli usi previsti (esibizione, accesso amministrativo, studio e ricerca). Al tempo stesso, il Sistema è messo in condizioni di acquisire, man mano che sono disponibili, le informazioni di contesto archivistico degli oggetti conservati e di assicurare in questo modo la corretta formazione dell'*archivio* del *Produttore*.

Il Sistema inoltre gestisce altre due modalità di conservazione particolari:

- **Conservazione fiscale**, finalizzata alla conservazione a norma dei documenti rilevanti ai fini tributari, in conformità con quanto previsto dalla normativa di settore vigente (DM del 17 giugno 2014 del Ministero dell'economia e delle finanze);
- ***Migrazione***, che ha per oggetto *Documenti informatici* e/o *Aggregazioni documentali informatiche* provenienti da altri *sistemi di conservazione*. La peculiarità di questa conservazione risiede nella necessità di garantire il mantenimento della catena di custodia e si sostanzia nell'acquisizione, oltre che degli oggetti da sottoporre a conservazione, anche dei documenti e dei *metadati* prodotti dal *Sistema di conservazione* di provenienza; qualora il sistema di provenienza sia un *Sistema di conservazione* conforme alle ***Linee guida*** ai fini dell'*interoperabilità*, il SIP avrà le caratteristiche definite nelle ***Linee Guida*** al paragrafo 4.7 sul processo di conservazione alla lettera h.

I SIP sono prodotti e versati nel Sistema sotto la responsabilità del *Produttore* con le modalità e le procedure descritte nei loro aspetti generali nel presente Manuale e, per gli aspetti operativi e specifici relativi a ogni *Produttore*, nei ***Disciplinari tecnici***, dove sono illustrati i *Documenti informatici* e le *Aggregazioni documentali informatiche* oggetto di conservazione e le procedure operative per il loro ***versamento*** e acquisizione nel Sistema.

Al momento dell'acquisizione i SIP sono oggetto di verifiche automatiche. Nel caso in cui le verifiche abbiano successo, il ***versamento*** viene accettato, il SIP viene acquisito per la sua *presa in carico* e si genera in modo automatico il *Rapporto di versamento,* che viene inviato al sistema che ha effettuato il ***versamento*** in un documento in formato XML denominato "***Esito versamento"***. Qualora il SIP non abbia superato i controlli, l'***Esito versamento*** riporta il dettaglio degli errori che hanno causato il fallimento del ***versamento***.
I SIP presi in carico dal Sistema sono inseriti in ***Elenchi di versamento***, documenti in formato XML, che vengono validati dal Responsabile della funzione archivistica di conservazione o automaticamente dal Sistema. La validazione dell'Elenco innesca la generazione dei *Pacchetti di archiviazione* (AIP) relativi ai SIP in Elenco.

Va ricordato che il Sistema è in grado di acquisire e prendere in carico automaticamente solo SIP che rispettano la struttura dati indicata nei Modelli di SIP e nelle Specifiche tecniche dei servizi di versamento (vedi paragrafo 6.2). Qualora il Produttore non sia in grado di versare i documenti come SIP, può trasmetterli sotto forma di Oggetti (di formato e struttura concordati con l'Ente conservatore) per sottoporli a un'elaborazione preliminare (Preacquisizione), svolta dal Sistema e finalizzata alla loro trasformazione in SIP.

In base a quanto appena illustrato, il processo di acquisizione e *presa in carico* dei SIP prevede le seguenti fasi:

1. Preacquisizione;
2. Acquisizione;
3. Verifica;
4. Rifiuto o accettazione;
5. Presa in carico e generazione del Rapporto di versamento;
6. Generazione del Pacchetto di archiviazione.

Nei paragrafi seguenti sono illustrate nel dettaglio le varie fasi del processo.

[Torna al Sommario]

7.1.1 Preacquisizione

La fase di Preacquisizione ha in input un Oggetto e in output uno o più SIP e ha inizio con la trasmissione dell'Oggetto a cura del *Produttore* o di un Versatore esterno da lui incaricato (vedi paragrafo 4.2). L'Oggetto trasmesso deve essere conforme alle specifiche definite dall'Ente conservatore. Il *Produttore* / *Versatore* trasmette l'Oggetto interfacciando i propri sistemi o utilizzando il client di versamento manuale messo a disposizione dall'Ente conservatore. Non è prevista la trasmissione degli Oggetti su supporti fisici.

Qualora la trasmissione abbia esito positivo al *Produttore* viene attestata la corretta ricezione dell'Oggetto.

L'Oggetto ricevuto è sottoposto a controlli finalizzati a verificarne la conformità con le relative specifiche. Le eventuali non conformità rilevate durante i controlli possono essere bloccanti o non bloccanti. Nel primo caso il processo si interrompe; nel secondo caso, invece, si interviene sull'oggetto ricevuto in modo da eliminare le non conformità rilevate. L'oggetto così modificato, unitamente alla descrizione degli interventi che ha subito, viene versato nuovamente nel Sistema e sottoposto nuovamente ai controlli di cui sopra.

Nel caso in cui i controlli abbiano esito positivo, il Sistema procede alle elaborazioni necessarie a versare il SIP, ovvero:

- trasformazione dell'Oggetto in uno più SIP: ogni SIP generato contiene il riferimento all'Oggetto dal quale è stato generato;
- ***versamento*** dei SIP nel Sistema: i SIP vengono versati nel Sistema con le modalità descritte nel paragrafo 7.1.2.

Il *Produttore* può in ogni momento interrogare il Sistema per ottenere informazioni sullo stato di avanzamento del processo di preacquisizione e sugli esiti del versamento dei SIP così generati.

[Torna al Sommario]

7.1.2 Acquisizione

L'acquisizione avviene con il ***versamento*** di SIP nel Sistema esclusivamente mediante l'utilizzo dei servizi descritti nel paragrafo 8.2 ed in dettaglio nel documento "Specifiche tecniche dei servizi di versamento".

Per effettuare il ***versamento*** dei SIP il *Produttore* può interfacciare i propri sistemi o, in alternativa, utilizzare il client di versamento manuale messo a disposizione da ParER mediante il quale inserire i dati necessari a generare e versare il SIP nel Sistema.

Non è prevista la trasmissione di SIP su supporti fisici.

Al completamento della trasmissione, il Sistema avvia contestualmente il processo di verifica del pacchetto, descritto nel paragrafo seguente.

[Torna al Sommario]

7.2 Verifiche effettuate sui pacchetti di versamento e sugli oggetti in essi contenuti

Il SIP acquisito viene sottoposto a verifiche automatiche da parte del Sistema, finalizzate ad evidenziare eventuali anomalie.

Le verifiche riguardano:

- l'identificazione del Versatore: queste verifiche, effettuate mediante il controllo delle credenziali comunicate dal sistema versante a ogni versamento, sono finalizzate a garantire l'identificazione certa del soggetto che ha formato il documento e dell'amministrazione e/o dell'*area organizzativa omogenea* di riferimento ai sensi del art. 44, comma 1 lettera a) del CAD e a garantire il corretto inserimento nell'*archivio* del *Produttore* nella opportuna ***Struttura*** (vedi paragrafo 6.1.1);
- la conformità dell'***Indice del SIP*** al modello dati stabilito (vedi paragrafo 6.2): queste verifiche sono finalizzate a controllare se l'***Indice del SIP*** è conforme al modello concordato con il *Produttore* e configurato nel sistema;
- l'univocità degli identificativi degli oggetti contenuti nel SIP: il controllo è finalizzato a verificare che gli identificativi assegnati dal *Produttore* e contenuti nel SIP siano effettivamente univoci, verificando che gli stessi non siano già presenti nel Sistema;
- la consistenza dei Metadati di profilo e specifici (vedi paragrafo 6.1.3): questa verifica è finalizzata a controllare che i set di Metadati presenti nel pacchetto siano conformi (in termini di obbligatorietà, valori e formato) a quelli concordati tra il *Produttore* e l'Ente conservatore. Tali set sono configurati nel Sistema mediante le funzionalità di Amministrazione delle Strutture versanti;

- il controllo sulle eventuali firme digitali apposte sugli ***Oggetti-dati*** (file) contenuti nel pacchetto. Le verifiche sono finalizzate a controllare la regolarità della firma digitale apposta in ordine a: formato di firma utilizzato, *integrità* del documento firmato (controllo crittografico), catena trusted, validità del certificato (scadenza e formato), presenza di eventuali revoche. I controlli sono effettuati alla data indicata dal *Produttore* nel SIP (che può essere quella contenuta nella firma, in una marca temporale o un riferimento temporale dichiarato nell'Indice SIP) o, in assenza di questa, alla data del versamento;
- l'ammissibilità dei ***formati*** degli ***Oggetti-dati*** (file) presenti nel pacchetto in base a quanto concordato con il *Produttore*: le verifiche si esplicano nel calcolo del ***mimetype*** dell'***Oggetto-dati*** e nel confronto del valore così ottenuto sia con quello eventualmente dichiarato dal *Produttore* nel SIP, sia con i Formati ammessi, documentati e conservati nel Sistema nelle funzionalità di Amministrazione delle strutture versanti;
- la coerenza e la consistenza delle *Aggregazioni documentali informatiche* versate: si tratta di controlli che vengono svolti in caso di ***Versamento in archivio*** di *Aggregazioni documentali informatiche* e sono finalizzati a verificare la coerenza e la completezza di quanto versato.

La descrizione analitica delle verifiche automatiche e dei controlli a cui sono sottoposti i SIP, nonché le logiche con cui il Sistema opera in quest'attività, sono illustrati nel documento "Specifiche tecniche dei servizi di versamento".

[Torna al Sommario]

7.3 Accettazione e presa in carico dei pacchetti di versamento e generazione del rapporto di versamento

Nel caso in cui tutte le verifiche abbiano avuto esito positivo, il SIP viene acquisito nel Sistema per la sua *presa in carico*, memorizzato nelle sue varie parti (***Indice del SIP*** e ***Oggetti-dati***), associato logicamente all'*archivio* del *Produttore* ed eliminato dall'area di lavoro temporanea.
In particolare, l'***Indice del SIP*** e gli ***Oggetti-dati*** vengono memorizzati nella loro *integrità* e mantenuti nel Sistema anche ai fini del loro successivo inserimento nell'AIP (vedi paragrafo 7.5).
Le operazioni di acquisizione si concludono con la *presa in carico* dei SIP accettati e la generazione automatica del relativo *Rapporto di versamento* che viene memorizzato nel Sistema e associato al SIP cui si riferisce.

Il *Rapporto di versamento* contiene l'Identificativo univoco del Rapporto, il *Riferimento temporale* relativo alla sua creazione (specificato con riferimento al ***tempo UTC***), l'*impronta* dell'***Indice del SIP*** e le *impronte* degli ***Oggetti-dati*** che ne fanno parte, oltre alla descrizione sintetica del contenuto del SIP acquisito. La descrizione analitica del *Rapporto di versamento* e la relativa struttura dati è contenuta nel documento "Specifiche tecniche dei servizi di versamento".

Il *Riferimento temporale* contenuto nel *Rapporto di versamento* è generato dal Sistema con le modalità descritte nel capitolo 8 ed è quindi da considerarsi opponibile ai terzi in base a quanto previsto dal comma 4, lettera b) dell'art. 41 del DPR 22 febbraio 2013.

Il *Rapporto di versamento* è reso disponibile al *Produttore* in varie modalità:

- è trasmesso in risposta al ***versamento*** del SIP nell'***Esito versamento***, un documento in formato XML che contiene, oltre al *Rapporto di versamento*, l'elenco analitico dei controlli eseguiti e dei relativi esiti, i parametri di configurazione del Sistema al momento del versamento e la data di versamento del SIP, descritto in dettaglio nel documento "Specifiche tecniche dei servizi di versamento";
- può essere richiesto utilizzando un apposito servizio, secondo le modalità descritte nel documento "Specifiche tecniche dei servizi di recupero";
- può essere visualizzato e scaricato dall'interfaccia web del Sistema dagli operatori abilitati, utilizzando le apposite funzionalità del Sistema.

[Torna al Sommario]

7.4 Rifiuto dei pacchetti di versamento e modalità di comunicazione delle anomalie

Nel caso in cui almeno una delle verifiche descritte al paragrafo 7.3 non vada a buon fine, il SIP viene rifiutato e il Sistema restituisce al *Produttore* gli errori riscontrati, inviando l'***Esito versamento***, un documento in formato XML, descritto in dettaglio nel documento Specifiche tecniche dei servizi di versamento, in cui sono contenute tutte le informazioni sui controlli effettuati e i relativi esiti, sia sintetici che analitici, nonché l'***Indice del SIP*** rifiutato.

I Pacchetti rifiutati, ovvero l'***Indice dei SIP*** e gli ***Oggetti-dati*** che ne fanno parte, unitamente ai relativi ***Esiti versamento***, sono memorizzati in un'area temporanea del Sistema, logicamente esterna all'*archivio* vero e proprio, a cui sia il *Produttore* che ParER possono accedere utilizzando l'interfaccia web del Sistema, per eventuali ulteriori controlli e verifiche (vedi paragrafo 7.4.1).

I SIP rifiutati restano memorizzati nel Sistema per almeno sei mesi; trascorso questo periodo possono essere cancellati, interamente o per la sola parte di ***Oggetti-dati***. La cancellazione è stabilita ed effettuata sulla base di valutazioni che tengono conto delle ***tipologie documentarie*** trattate, delle caratteristiche del *Produttore* e della quantità e qualità dei versamenti falliti. Eventuali specifiche modalità e tempistiche di cancellazione dei SIP rifiutati sono concordate con il Produttore e configurate nel Sistema.

[Torna al Sommario]

7.4.1 Monitoraggio

Il Sistema mette a disposizione specifiche funzionalità di monitoraggio relative alla gestione dei ***versamenti*** dei SIP e alla generazione e gestione degli AIP, oltre a statistiche e report su quanto presente nel Sistema.

Il monitoraggio consente di avere una vista complessiva, suddivisa per fasce temporali, sull'acquisizione dei SIP, sul rifiuto dei SIP, sui tentativi falliti di versamento e sulle eventuali anomalie, mettendo a disposizione degli operatori tutte le informazioni necessarie a verificare

tanto le anomalie che hanno impedito il ***versamento*** dei SIP nel Sistema, quanto tutti gli elementi relativi ai SIP versati e agli AIP generati o aggiornati a seguito di tali ***versamenti***.

In particolare, sono evidenziati, in tabelle sintetiche complessive o per singola ***Struttura***:

- i ***versamenti*** di SIP svolti con successo, cioè che hanno generato un *Rapporto di versamento*;
- l'inserimento o meno dei SIP in ***Elenchi di versamento***;
- i versamenti rifiutati;
- i tentativi di versamento falliti, che non hanno attivato il processo di acquisizione.

Tali informazioni di monitoraggio sono a disposizione degli *Utenti* degli Enti che dispongono di un profilo adeguato.

Dalle tabelle sintetiche è possibile scendere fino al dettaglio dei singoli versamenti, evidenziando, nel caso dei versamenti rifiutati, opportuni codici d'errore, che consentono agli operatori di individuare le soluzioni necessarie alla risoluzione delle anomalie riscontrate. Le più comuni azioni di risoluzione delle anomalie prevedono:

- Utilizzo di parametri di forzatura dei ***versamenti*****:** nel caso in cui i controlli sulle firme, sui *formati* o sui collegamenti presenti sul SIP non vadano a buon fine e il ***versamento*** del SIP fallisca, i SIP rifiutati possono essere versati nuovamente in conservazione forzando i controlli precedentemente falliti. Tali forzature, che sono operate dal *Produttore* valorizzando appositi parametri presenti nel SIP, consentono di portare in conservazione i SIP anche in presenza delle anomalie, che inizialmente ne avevano pregiudicato l'acquisizione. In questi casi, il Sistema segnala al *Produttore* nell'***Esito versamento*** che il SIP è stato acquisito a seguito di forzatura;
- Modifica di dati non corretti presenti nel SIP: nel caso in cui il SIP non superi i controlli a causa di alcuni dati non corretti nel SIP stesso, il *Produttore* provvede alla correzione dei dati indicati ed effettua nuovamente il ***versamento***;
- Modifica delle configurazioni del Sistema: nel caso in cui il ***versamento*** del SIP non vada a buon fine per la presenza nel SIP stesso di dati non corrispondenti con i valori configurati nel Sistema, ParER può procedere, d'accordo con il *Produttore*, a modificare di conseguenza le configurazioni. Di tale modifica viene data comunicazione al *Produttore,* che provvede a inviare nuovamente in conservazione il SIP;
- Versamenti rifiutati e non risolubili: nel caso in cui un ***versamento*** sia stato rifiutato per la presenza di anomalie che il *Produttore* giudica non risolubili, il ***versamento*** può essere marcato come non risolubile ed escluso, di conseguenza, da futuri controlli;
- Annullamento di versamenti effettuati: nel caso in cui un ***versamento*** andato a buon fine sia stato effettuato per errore o contenga degli errori non correggibili altrimenti, il *Produttore* provvede ad annullarlo, utilizzando apposite funzionalità del Sistema. Il SIP, e il relativo AIP eventualmente generato vengono marcati come Annullati.

Il modulo di Monitoraggio, inoltre, fornisce accesso alle statistiche dei sistemi, del Data Base, dei versamenti, ecc., mettendo a disposizione degli operatori report sia sintetici che analitici.

[Torna al Sommario]

7.4.2 Gestione delle anomalie

Le anomalie che possono riscontrarsi nell'operatività del servizio in fase di ***versamento*** sono gestite in generale secondo lo schema indicato nella tabella seguente.

Tipo anomalia	Descrizione	Modalità di gestione
Mancata risposta al versamento	È il caso in cui l'***Unità documentaria*** viene correttamente versata ma, per vari motivi, la risposta di avvenuta ricezione non perviene al *Produttore*, che pertanto, può ritenerla erroneamente non versata, oltre a non ricevere il rapporto di versamento.	Il *Produttore* trasmette nuovamente l'Unità documentaria e il *Sistema di conservazione* restituisce una risposta di esito negativo che contiene l'indicazione che l'***Unità documentaria*** risulta già versata e il relativo *Rapporto di versamento*. Tale risposta deve essere usata dal *Produttore* come attestazione di avvenuto versamento e l'***Unità documentaria*** deve risultare come versata.
Errori temporanei	È il caso di errori dovuti a problemi temporanei che pregiudicano il ***versamento***, ma si presume non si ripresentino a un successivo tentativo di ***versamento***. Il caso più frequente è l'impossibilità temporanea di accedere alle CRL degli enti certificatori. In questi casi il *Sistema di conservazione* restituisce un messaggio di errore perché non riesce a completare le verifiche previste sulla validità della firma e il ***versamento*** viene quindi rifiutato.	Il *Produttore* deve provvedere a rinviare l'***Unità documentaria*** in un momento successivo. L'operazione potrebbe dover essere ripetuta più volte qualora il problema, seppur temporaneo, dovesse protrarsi nel tempo.
Versamenti non conformi alle regole concordate	È il caso in cui il ***versamento*** non viene accettato perché non conforme alle regole concordate (formato file non previsto, mancanza di *metadati* obbligatori, ecc.).	*Produttore* e ParER concordano una soluzione al problema.
Errori interni o dovuti a casistiche non previste o non gestite	In alcuni casi è possibile che il *Sistema di conservazione* risponda con un messaggio di errore generico che non indica le cause dell'anomalia riscontrata in quanto dovuta a un errore interno o perché legata a una casistica non prevista, non gestita o non gestibile dal *Sistema di conservazione*.	Il *Produttore* segnala il problema a ParER, che si attiverà per la sua risoluzione.

Tipo anomalia	Descrizione	Modalità di gestione
Errori nel contenuto dei dati conservati	È il caso eccezionale in cui per ragioni tecniche il *Sistema di conservazione* abbia effettuato un errore, che non può essere corretto con le procedure standard, oppure siano stati versati dati errati da parte del *Produttore*, che, in accordo con il *Produttore* stesso, si ritiene più semplice correggere per via tecnica, piuttosto che annullare e versare nuovamente	Il *Produttore* richiede formalmente al personale archivistico di ParER di effettuare una correzione tecnica dei dati; il gruppo di sviluppo e manutenzione viene quindi incaricato di intervenire manualmente sul database per effettuare la correzione: l'intervento effettuato viene annotato nell'AIP e l'azione manuale effettuata sul database viene tracciata nel log del database; la richiesta di intervento tecnico e la relativa soluzione rimangono tracciate all'interno del sistema di gestione delle attività di sviluppo e manutenzione.

[Torna al Sommario]

7.5 Preparazione e gestione del Pacchetto di archiviazione

Come elemento ulteriore di controllo dei versamenti effettuati, i SIP accettati e presi in carico sono inseriti in appositi ***Elenchi di versamento***[11] generati secondo criteri, definiti "criteri di raggruppamento", predefiniti per ***tipologia documentaria*** e anno di produzione. Normalmente il criterio standard prevede che l'elenco si chiuda al raggiungimento di un numero massimo di componenti (5000) o dopo 30 giorni dall'apertura, ma tali parametri possono essere variati in base a specifiche esigenze conservative.
L'***Elenco di versamento*** è un documento in formato XML, generato alla chiusura dell'elenco e fornito di un *Riferimento temporale* opponibile ai terzi. Riporta per ogni documento o aggregazione versata l'Identificativo univoco, un set di *metadati* descrittivi, le *impronte* degli ***Oggetti-dati*** che lo compongono e una serie di informazioni sintetiche relative alle verifiche a cui è il SIP è stato sottoposto durante il processo di acquisizione.
L'Elenco è recuperabile dal *Produttore* utilizzando apposite funzionalità dell'interfaccia web del Sistema.
Gli elementi inseriti nell'Elenco possono essere sottoposti a ulteriori controlli, anche a campione, finalizzati a verificare la corrispondenza degli oggetti versati con quanto concordato con il *Produttore* e a evidenziare eventuali anomalie non rilevabili dalle verifiche automatiche al ***versamento***.
Una volta chiuso l'Elenco di versamento e completati i controlli, l'Elenco viene validato, automaticamente o manualmente dal Responsabile della funzione archivistica di conservazione, eventualmente anche con propria firma digitale.
Tale validazione avvia il processo di creazione dei Pacchetti di Archiviazione (AIP) e dei relativi indici in formato conforme allo standard UNI SinCRO.

[11]Tali elementi vengono a sostituire le precedenti azioni di creazione volumi effettuate nel rispetto della Delibera CNIPA 11/2004. Gli ***Elenchi di versamento*** sono prodotti a partire dal 2015 a seguito dell'abbandono definitivo della creazione di volumi precedentemente prevista. Il sistema continua a gestire anche le informazioni relative ai volumi costituiti fino al 2014.

I SIP accettati e presi in carico dal Sistema, dopo la validazione dell'***Elenco di versamento*** in cui sono stati inseriti, sono soggetti a una fase di elaborazione finalizzata alla creazione dell'AIP (o all'aggiornamento di un AIP esistente).
A seguito di queste elaborazioni, nel caso di ***Versamento anticipato***, viene generato (o aggiornato) l'AIP dell'***Unità documentaria***.

L'AIP dell'***Unità documentaria*** è composto da:

- l'***Indice dell'AIP*****:** è un documento in formato XML prodotto in conformità alle specifiche contenute nella norma UNI 11386 - Standard SInCRO - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali e descritto in dettaglio nel documento "Modelli dei pacchetti di archiviazione", che contiene tutti i *metadati* dell'***Unità documentaria*** presenti sul Sistema e i riferimenti agli altri file presenti nel pacchetto. Tra i dati contenuti nell'Indice vi sono:
  - la data di generazione dell'AIP (espressa con un *Riferimento temporale* opponibile ai terzi con le caratteristiche descritte al paragrafo 7.3), che costituisce il *Riferimento temporale* opponibile a terzi di tutti i file elencati nell'Indice stesso;
  - i *metadati* descrittivi dell'***Unità documentaria***;
  - i *metadati* generati dal Sistema nel corso delle verifiche e delle elaborazioni operate sul SIP;
  - le *impronte* dei singoli file (***Oggetti-dati***) dell'AIP stesso;
  - le *impronte* delle eventuali precedenti versioni dell'***Indice dell'AIP*** (in caso di aggiornamento);
  - le *impronte* degli altri documenti generati dal Sistema nel *processo di conservazione*;
  - il riferimento agli ***Elenchi di versamento*** relativi ai SIP da cui è stato generato o aggiornato l'AIP;
- I file **(*Oggetti-dati*)** dell'***Unità documentaria*** ricevuti nel SIP e le eventuali copie informatiche generate dal Sistema;
- I file con le eventuali precedenti versioni dell'***Indice dell'AIP***;
- I file degli ***Indici dei SIP*** da cui è stato generato o aggiornato l'AIP;
- I file degli ***Esiti versamento*** relativi ai SIP da cui è stato generato o aggiornato l'AIP;
- I file dei *Rapporti di versamento* relativi ai SIP da cui è stato generato o aggiornato l'AIP.

La sottoscrizione dell'AIP dell'***Unità documentaria*** può essere effettuata con l'apposizione del sigillo elettronico del conservatore Regione Emilia-Romagna o tramite firma digitale del Responsabile del Servizio di Conservazione o del Responsabile della Funzione Archivistica di Conservazione.

La sottoscrizione degli AIP delle ***Unità documentarie*** può avvenire in due modi, a seconda che il processo di conservazione si svolga in regime di ***versamento anticipato*** o in regime di ***versamento in archivio***.

Nel primo caso, la sottoscrizione viene apposta su un'evidenza informatica, denominata Elenco Indici AIP, prodotta a partire dagli ***Elenchi di versamento*** e contenente gli identificativi e l'impronta degli Indici degli AIP di ogni ***Unità documentarie*** contenuta negli elenchi stessi. Tale evidenza informatica, una volta sottoscritta, è inserita negli AIP delle singole ***Unità documentarie***.

Nel caso di ***Versamento in archivio***, invece, la sottoscrizione degli AIP delle ***Unità documentarie*** avviene attraverso la sottoscrizione degli AIP delle aggregazioni (***Unità archivistiche*** e ***Serie***) in cui le ***Unità documentarie*** sono comprese. Gli Indici di tali AIP contengono, infatti, oltre ai *metadati* descrittivi dell'*Aggregazione documentale informatica*, le *impronte* degli Indici degli AIP delle ***Unità documentarie*** e/o delle ***Unità archivistiche*** che li compongono.

Gli ***Indici dell'AIP*** delle ***Unità archivistiche*** e delle ***Serie*** sono sottoscritti ad attestare il corretto svolgimento del processo di ***Versamento in archivio*** che completa il processo di trasferimento al Sistema dal punto di vista del *Produttore* La sottoscrizione può essere effettuata con l'apposizione del sigillo elettronico del conservatore Regione Emilia-Romagna o tramite firma digitale del Responsabile del Servizio di Conservazione o del Responsabile della Funzione Archivistica di Conservazione.

Con la sottoscrizione dell'AIP dell'*Aggregazione documentale informatica* si determina anche l'accettazione della custodia da parte di ParER dei *Documenti informatici* e delle *Aggregazioni documentali informatiche* versate, cioè la dichiarazione che tutte le ***Unità documentarie*** relative all'*Aggregazione documentale informatica* sono correttamente acquisite e conservate dal Sistema nell'*archivio*.

Contestualmente alla generazione degli AIP, il Sistema memorizza le ***Informazioni descrittive*** sul *Pacchetto di archiviazione*, ovvero un set di *metadati* derivato da quello presente nell'***Indice dell'AIP*** ed eventualmente da altri documenti contenuti nell'AIP stesso, finalizzato a ricercare gli AIP conservati nel Sistema.

Gli AIP sono conservati nel Sistema per il tempo di conservazione previsto dalle norme; allo scadere del tempo di conservazione possono essere scartati con le procedure descritte nel paragrafo 7.8.

Il *Produttore* può accedere agli AIP conservati utilizzando le funzionalità dell'interfaccia web del Sistema o chiamando l'apposito servizio con le modalità descritte nel documento "Specifiche tecniche dei servizi di recupero".

L'aggiornamento degli AIP può essere originato da due eventi: versamento di un SIP da parte del *Produttore* e attivazione di procedure di conservazione da parte del Sistema.

Nel primo caso l'aggiornamento dell'AIP viene innescato dal *Produttore* che può inviare ulteriori SIP per integrare o aggiornare le informazioni e/o altri elementi presenti nell'AIP secondo le modalità descritte nel documento "Specifiche tecniche dei servizi di versamento". Nel secondo caso, invece, gli aggiornamenti derivanti dalle procedure di conservazione sono innescati dal Sistema al verificarsi di determinati eventi e sono finalizzati a mantenere la *leggibilità* e la reperibilità nel tempo degli AIP.

Infine, gli AIP in casi eccezionali possono essere sottoposti a procedure di sequestro e di eventuale annullamento. Le procedure da applicare in questi casi sono descritte operativamente in specifici documenti tecnici.

Le politiche di conservazione dei pacchetti di archiviazione (AIP), per assicurare sia il contenuto dell'informazione all'ente produttore sia l'integrità nel tempo dei pacchetti conservati, sono descritte al capitolo 9.2. Inoltre periodicamente viene verificato che il totale dei componenti

versati con i SIP corrisponda alla somma dei componenti presenti negli AIP, di quelli in lavorazione e di quelli in attesa di lavorazione, al netto dei componenti contenuti in versamenti annullati.

[Torna al Sommario]

7.6 Preparazione e gestione del Pacchetto di distribuzione (DIP) ai fini dell'esibizione

I DIP sono prodotti di norma a partire dagli AIP presenti sul Sistema. Nel caso in cui non sia stato ancora generato l'AIP, è comunque possibile produrre DIP, riferiti agli oggetti versati e ai documenti di conservazione già prodotti.
Esistono varie tipologie di DIP, ognuna corrispondente alle specifiche esigenze di utilizzo da parte degli *Utenti* (***Comunità di riferimento***).

In base alla tipologia di DIP e alle sue specifiche esigenze di utilizzo, il Sistema mette a disposizione funzionalità per la sua produzione e distribuzione, sia automatiche che manuali.
Il Sistema fornisce le seguenti tipologie di DIP:

- DIP coincidente con l'AIP: contiene tutti gli elementi presenti nell'AIP (vedi anche paragrafo 7.9) ed è scaricabile dall'interfaccia web del Sistema o tramite appositi servizi descritti nel documento "Specifiche tecniche dei servizi di recupero";
- DIP coincidente con il SIP: contiene gli Oggetti-dati presenti, l'***Indice del SIP*** e l'***Esito versamento*** ed è scaricabile dall'interfaccia web del Sistema;
- DIP del *Rapporto di versamento*: contiene i *Rapporti di versamento* relativi all'***Unità documentaria*** ed è scaricabile dall'interfaccia web del Sistema o tramite appositi servizi descritti nel documento "Specifiche tecniche dei servizi di recupero";
- DIP dei documenti di conservazione: contiene i documenti di conservazione prodotti nel corso del processo di conservazione (***Indice del SIP***, Informazioni sull'impacchettamento, ***Esito versamento***, *Rapporto di versamento*) ed è scaricabile dall'interfaccia del Sistema;
- DIP dell'***Unità documentaria*****:** contiene esclusivamente gli ***Oggetti-dati*** che la compongono ed è scaricabile dall'interfaccia web del Sistema;
- DIP del ***Documento*****:** contiene esclusivamente gli ***Oggetti-dati*** del ***Documento*** ed è scaricabile dall'interfaccia web del Sistema;
- DIP del **Componente:** contiene il singolo file del ***Componente*** ed è scaricabile dall'interfaccia web del Sistema;
- DIP dell'***Elenco di versamento*****:** contiene l'***Elenco di versamento*** in cui è contenuta l'***Unità documentaria*** ed è scaricabile dell'interfaccia web del Sistema;
- DIP per l'esibizione: contiene i file dell'***Unità documentaria*** e una dichiarazione, sotto forma di file in formato testo, che illustra il contenuto del DIP e fornisce informazioni utili ad agevolarne l'esibizione.

La distribuzione dei pacchetti a fine di *esibizione* avviene utilizzando le funzionalità dell'interfaccia web del Sistema, oppure chiamando l'apposito servizio descritto nel documento "Specifiche tecniche dei sevizi di recupero".

Normalmente i DIP sono trasmessi o resi disponibili al *Produttore,* che poi provvede a consegnarli agli interessati. La consegna o la messa a disposizione dei DIP direttamente agli interessati è possibile solo con specifico accordo tra *Produttore* e ParER.

Il *Produttore* può consultare quanto versato in ParER tramite interfaccia web, collegandosi all'indirizzo comunicato da ParER e autenticandosi tramite username e password preventivamente forniti da ParER.
Gli operatori da abilitare per l'*accesso* tramite interfaccia web al *Sistema di conservazione* sono comunicati formalmente dal *Produttore* a ParER, che provvede a fornire le credenziali di accesso ai diretti interessati.
L'accesso web consente al *Produttore* di ricercare i documenti e le aggregazioni versati, di effettuarne il download e di acquisire le evidenze delle attività di conservazione.

[Torna al Sommario]

7.7 Produzione di duplicati e copie informatiche e descrizione dell'eventuale intervento del pubblico ufficiale nei casi previsti

La produzione di duplicati informatici o copie informatiche dei *Documenti informatici* conservati nel Sistema avviene mediante la messa a disposizione del *Produttore* di DIP comprensivi degli ***Oggetti-dati*** che li compongono.
Tali pacchetti sono acquisibili dagli *Utenti* utilizzando le funzionalità dell'interfaccia web del Sistema o gli appositi servizi descritti nel documento "Specifiche tecniche dei servizi di recupero".

Non è previsto da parte di ParER né il rilascio di copie cartacee conformi agli originali digitali conservati, né l'*accesso* diretto alla documentazione da parte di colui che, dovendo tutelare situazioni giuridicamente rilevanti, abbia presentato istanza di consultazione.
Pertanto, in merito all'esercizio del diritto d'accesso ai documenti conservati da ParER, questo si limita a fornire al *Produttore*, su precisa richiesta di quest'ultimo e senza che su di esso debba gravare alcun particolare onere, il documento informatico conservato, qualora per un qualsiasi motivo il *Produttore* stesso abbia deciso di non acquisirlo direttamente mediante le modalità descritte nel paragrafo 7.6.
Permane in carico al *Produttore* sia la responsabilità di valutare la fondatezza giuridica della domanda di accesso, sia l'onere di far pervenire il documento (o sua eventuale copia cartacea conforme) al soggetto richiedente.
ParER provvederà a consegnare direttamente la documentazione richiesta solo nel caso di visite ispettive presso ParER o provvedimenti di esibizione o sequestro da parte dell'autorità giudiziaria o di altra autorità ispettiva espressamente indirizzati al soggetto conservatore. ParER garantirà all'autorità giudiziaria la massima collaborazione e concorderà insieme ad essa le modalità di accesso e di consegna degli oggetti digitali.

Nei casi previsti dalla normativa, il ruolo di pubblico ufficiale è svolto dal Responsabile del servizio di conservazione in qualità di dirigente dell'ufficio responsabile della conservazione dei documenti, o da altri dallo stesso formalmente designati, quale il Responsabile della Funzione archivistica di conservazione per l'attestazione di conformità all'originale di copie di *Documenti informatici* conservati.

Il ruolo di pubblico ufficiale, per i casi in cui è previsto l'intervento di soggetto diverso della stessa amministrazione, sarà svolto da altro dirigente all'uopo individuato o da altro soggetto da quest'ultimo designato.

[Torna al Sommario]

7.8 Scarto dei pacchetti di archiviazione

Il Produttore ha l'onere di gestire le operazioni di scarto. ParER mette a disposizione dello stesso le funzionalità di supporto per individuare gli oggetti digitali potenzialmente scartabili. Le funzionalità di supporto si basano sui metadati inseriti al versamento, quindi, è importante che i tempi di conservazione risultanti dai propri ***Massimari di scarto*** o ***Piani di conservazione*** vengano correttamente inviati al sistema di conservazione.
In caso di assenza di metadati ParER mette a disposizione dei produttori funzionalità di ricerca che consentono comunque di orientarsi nella selezione.
Il procedimento amministrativo dello scarto è a carico del Produttore, che gestisce in autonomia le modalità di dialogo con l'organo di vigilanza.
Lo scarto degli oggetti digitali può essere effettuato nel sistema di Conservazione solo a valle dell'autorizzazione dell'Organo di Vigilanza.
Parer mette a disposizione le funzionalità per effettuare lo scarto e tiene traccia, secondo il dettato normativo, degli scarti effettuati. In particolare, per procedere con l'eliminazione degli oggetti digitali ParER chiede:

- il numero di protocollo con il quale la richiesta di scarto è stata chiesta all'organo di vigilanza;
- il numero di protocollo della risposta dell'organo;
- gli estremi del provvedimento con il quale il Produttore recepisce le osservazioni dell'Organo di Vigilanza e procede allo scarto.

Il Produttore compila nel sistema di conservazione la richiesta di scarto degli oggetti digitali, ParER effettua controlli e verifiche di consistenza e procede alla cancellazione degli oggetti digitali.
Terminata la cancellazione ParER produce un verbale di avvenuta distruzione che certifica l'avvenuta cancellazione degli oggetti digitali. Il verbale è sottoscritto dal responsabile del servizio di conservazione o della funzione archivistica di conservazione e viene inviato al Produttore.
Quest'ultimo dovrà trasmettere il verbale alla soprintendenza a completamento del processo.
Si ricorda che l'accordo di collaborazione[12] tra ParER e Soprintendenza archivistica e Bibliografica dell'Emilia-Romagna consente a quest'ultima di accedere al sistema al fine di vigilare e tutelare gli archivi degli enti regionali.

[Torna al Sommario]

[12] Cfr. par. 4.6

7.9 Predisposizione di misure a garanzia dell'interoperabilità e trasferibilità ad altri conservatori

L'**Accordo** prevede che, in caso di recesso anticipato o alla scadenza della collaborazione, la Regione Emilia-Romagna, tramite il ParER, è tenuta a restituire i *Documenti informatici* e le *Aggregazioni documentali informatiche* conservate, i *metadati* a essi associati e le *evidenze informatiche* generate nel corso del *processo di conservazione* al *Produttore*, secondo modalità e tempi indicati nel ***Disciplinare Tecnico*** o nella specifica procedura.
ParER garantisce comunque il mantenimento nel proprio *Sistema di conservazione* dei *Documenti informatici* e delle *Aggregazioni documentali informatiche* conservati, con i *metadati* a essi associati e le *evidenze informatiche* generate nel corso del *processo di conservazione* fino alla comunicazione da parte del *Produttore* dell'effettivo recupero del proprio archivio.
ParER provvederà all'eliminazione dal proprio *Sistema di conservazione* di tutti gli oggetti restituiti e di tutti gli elementi riferiti al *Produttore* solo al termine della procedura di restituzione e solo dopo le opportune verifiche - effettuate da entrambe le Parti e svolte di concerto tra le stesse - di corretto svolgimento della stessa.
In tal caso viene garantita la cancellazione e non leggibilità dei dati entro 90 giorni, a partire dal termine della procedura di restituzione e delle relative verifiche, sia dal sistema primario (compresi i backup), sia dal sito di ***business continuity***, sia dal sito di ***Disaster recovery***.
L'intera operazione dovrà comunque avvenire con l'autorizzazione e la vigilanza delle competenti autorità, in particolare delle strutture del MiC.

In caso di chiusura del servizio da parte della Regione Emilia-Romagna, con interventi di modifica alla normativa regionale, si provvederà a trasferire quanto conservato ai *Sistemi di conservazione* individuati per proseguire le attività svolte dalla Regione Emilia-Romagna e a cancellarlo da tutti i sistemi compresi quelli di backup, fornendo evidenze del trasferimento all'Ente Produttore.

Per quanto riguarda gli aspetti operativi per il trasferimento di *archivi* ad altri *sistemi di conservazione*, ParER adotta lo standard Uni Sincro, e provvede a mettere a disposizione l'*archivio* del *Produttore* in un'area a lui dedicata, da cui potrà prelevarlo utilizzando un canale sicuro di trasferimento (***FTPS***). Analogamente il Sistema è predisposto per la ricezione di *archivi* in formato Uni Sincro; qualora il precedente Conservatore non sia in grado di produrre l'*archivio* in formato Uni Sincro, ParER, a seguito di specifici accordi, può mettere a disposizione del *Produttore* consulenza e strumenti per facilitarne il trasferimento.

[Torna al Sommario]

8 IL SISTEMA DI CONSERVAZIONE

8.1 Componenti logiche

Il diagramma in figura, realizzato sul modello della rappresentazione delle entità funzionali di ***OAIS***, schematizza dal punto di vista logico le principali componenti del *Sistema di conservazione* di ParER e le principali relazioni con i soggetti interessati dal *processo di conservazione* descritto nei capitoli precedenti del presente Manuale.

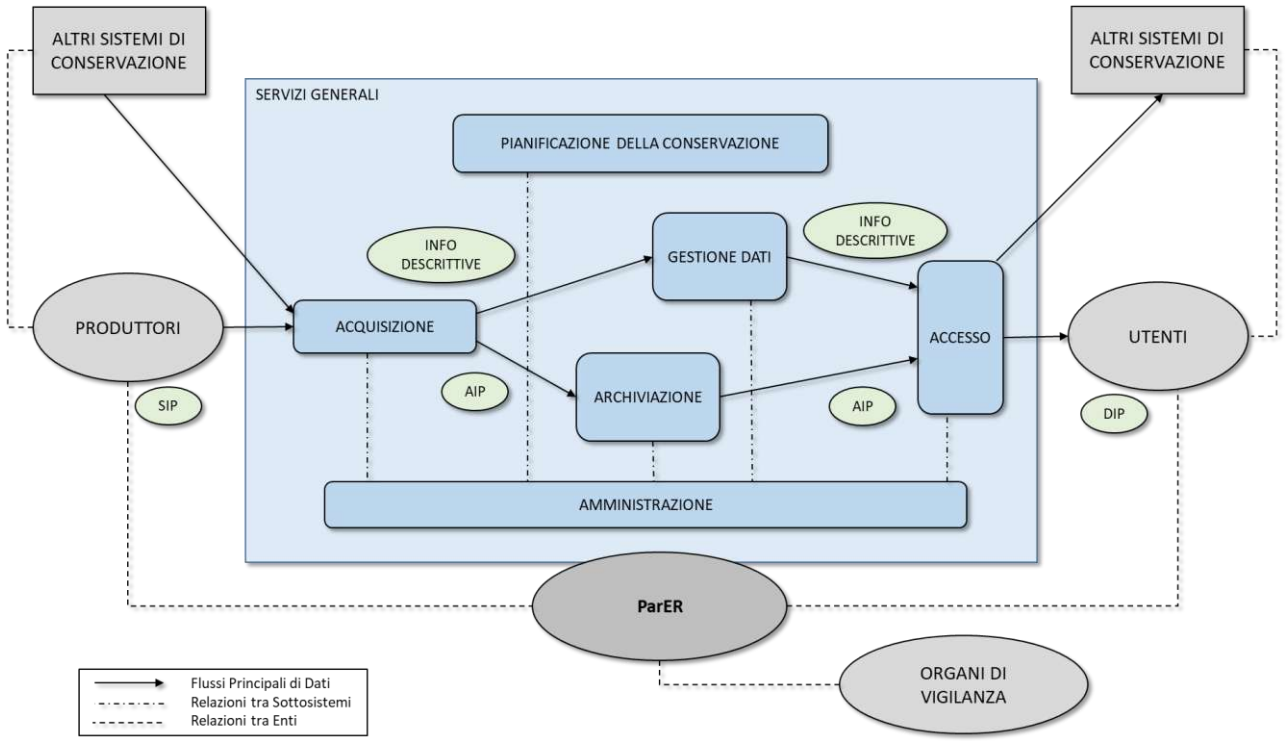


Figura 6 - Schema logico del Sistema di conservazione

Per la descrizione dei ruoli di *Produttori*, *Utenti*, Regione Emilia-Romagna/ParER, come soggetto Conservatore e Amministratore del Sistema, e Organi di vigilanza si rimanda al capitolo 4 del presente Manuale.

In ottica di *interoperabilità* ParER è in grado di ricevere da altri *sistemi di conservazione* documenti già sottoposti a conservazione, e di versarli ad altri Sistemi secondo gli accordi intercorsi con il *Produttore*.

Le funzionalità di Acquisizione gestiscono la fase di Acquisizione e *presa in carico* del *processo di conservazione* (vedi paragrafi 7.1 – 7.4), ovvero, attraverso i ***Web Service*** di versamento esposti dal Sistema, consentono la ricezione dei SIP dei *Produttori*, la loro verifica e la generazione, a partire dai SIP, dei relativi AIP e delle ***Informazioni descrittive*** per la loro ricerca.

Le funzionalità di Gestione Dati gestiscono le ***Informazioni descrittive*** generate al termine della fase di acquisizione e *presa in carico* del *processo di conservazione*. Tali funzionalità garantiscono: *memorizzazione*, manutenzione e aggiornamento all'interno del Sistema sia delle

Informazioni descrittive necessarie a ricercare gli AIP, ricevute dall'Acquisizione, che dei dati necessari per gestire i pacchetti.

Le funzionalità di Archiviazione gestiscono la fase di gestione degli AIP del *processo di conservazione* (vedi paragrafo 7.5): *memorizzazione*, ***migrazione*** dei supporti, backup, ***Disaster recovery*** ed eliminazione (*scarto*) degli AIP conservati nel Sistema.

Le funzionalità di Amministrazione gestiscono il governo dell'intero *processo di conservazione*, permettendo di definire e aggiornare nel Sistema politiche, standard e configurazioni che regolano tutte le altre funzionalità, incluse la gestione degli accordi con i *Produttori*, il monitoraggio del Sistema, la produzione di copie informatiche per la conservazione (***migrazione*** dei *formati*) e la selezione degli AIP per lo *scarto*.

Le funzionalità di Pianificazione della conservazione gestiscono il monitoraggio dell'ambiente in cui il Sistema è inserito e forniscono le indicazioni necessarie per fare in modo che le informazioni conservate restino fruibili nel lungo periodo, tenendo conto dell'evoluzione tecnologica dei sistemi e del cambiamento della ***Comunità di riferimento*** (*Utenti*). Intervengono nella progettazione dei *Pacchetti Informativi* e nella pianificazione dello sviluppo e dei test del software necessario per la ***migrazione*** degli AIP. Tale funzione non è svolta da uno specifico applicativo, né segue procedure meccaniche, ma si configura invece come una serie di attività svolte utilizzando un insieme di strumenti, non solo informatici, finalizzati a raccogliere informazioni, confrontarsi con la ***Comunità di riferimento***, effettuare test e verifiche sugli oggetti conservati, il tutto finalizzato a fornire indicazioni utili a mantenere il *processo di conservazione* aggiornato in relazione sia all'evoluzione tecnologica, che alle esigenze della ***Comunità di riferimento***.
I risultati di questa analisi si concretizzano, tipicamente ma non esclusivamente, in aggiornamenti nei modelli di *pacchetti informativi* gestiti dal Sistema, in implementazione di nuove librerie o altri strumenti software utilizzati dal Sistema, nella definizione e nell'aggiornamento delle politiche di conservazione e nei test su nuovi componenti hardware.
Questi elementi sono inseriti nel Sistema utilizzando principalmente le funzionalità di Amministrazione di SacER e, secondariamente, quelle analoghe presenti negli altri moduli del Sistema, garantendo che il *processo di conservazione* sia sempre in grado tanto di contrastare efficacemente l'obsolescenza tecnologica, quanto di rispondere adeguatamente alle esigenze della ***Comunità di riferimento*** di ParER.

Le funzionalità di *accesso* gestiscono la fase di gestione dei DIP del *processo di conservazione* (vedi paragrafo 7.6), fornendo supporto agli operatori per la ricerca e la restituzione degli oggetti conservati. Le funzioni di *interoperabilità* consentono inoltre la restituzione da parte del Sistema di DIP coincidenti con gli AIP conformi a quanto previsto dalle ***Linee guida***.

Il diagramma in figura schematizza i principali flussi di dati che intercorrono tra le componenti logiche del sistema descritte nei paragrafi precedenti; per completezza nello schema è stata inserita anche la componente '***Disaster recovery***', in quanto, pur non avendo un ruolo rilevante nella gestione ordinaria, riveste un ruolo significativo nello scambio di flussi informativi e svolge funzionalità elaborative autonome, seppur limitate, ai fini della produzione delle copie di salvataggio dei file su cassetta.

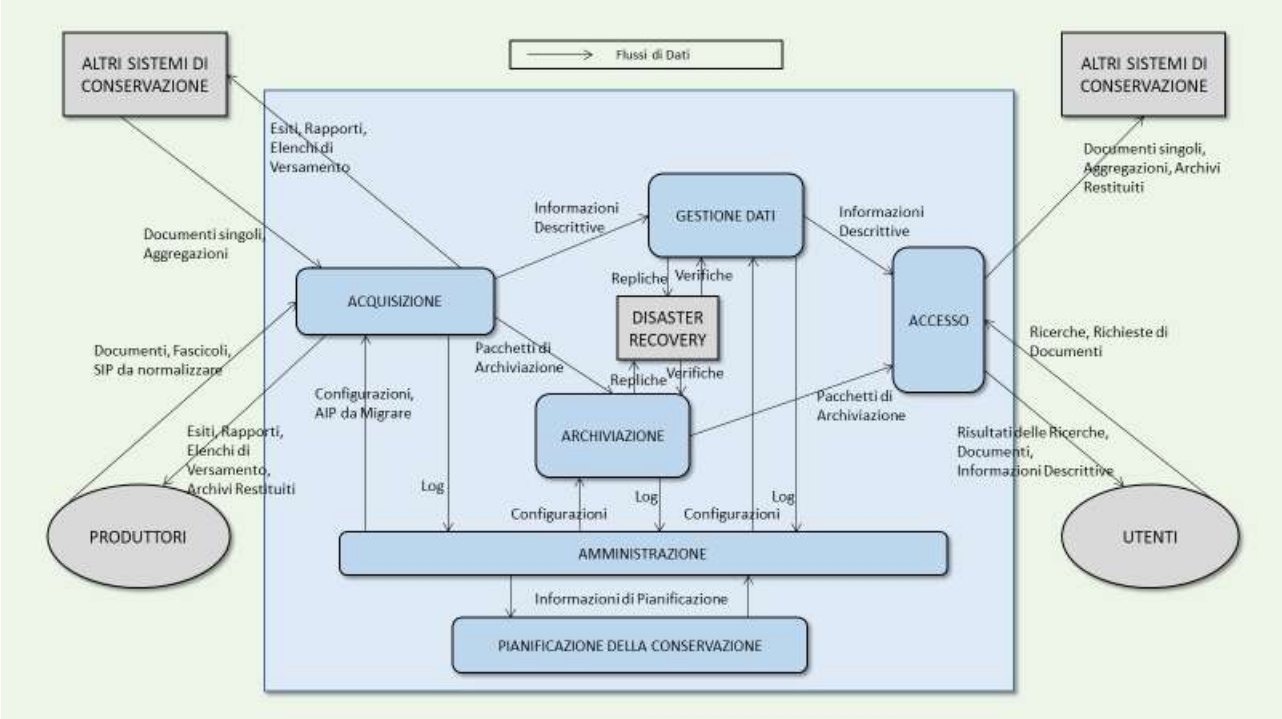


Figura 7 - Flussi di dati nel Sistema di conservazione

Il Servizio di conservazione è supportato da un unico Sistema integrato, suddiviso logicamente in sistemi dedicati agli specifici conservatori (ambienti). Nell'ambito del Sistema gli archivi di ogni Ente *Produttore* sono allocati in aree logicamente separate (strutture). Gli accessi degli utenti sono limitati alle strutture per i quali sono stati profilati in modo tale che gli archivi di ogni Ente risultano adeguatamente protetti.

In aggiunta alle componenti logiche delineate nei paragrafi precedenti, che ne costituiscono il nucleo centrale, il Sistema mette a disposizione diversi Servizi generali a supporto delle altre funzionalità. Oltre ai servizi di gestione e monitoraggio dei sistemi, della rete, e della sicurezza dei sistemi, mette a disposizione in particolare:

- il servizio di **Identity Management**, che, via *IDP,* garantisce i corretti accessi al Sistema da parte dei diversi utilizzatori;
- il servizio di Firma tramite dispositivo ***HSM***, che consente di apporre le firme digitali necessarie nel processo di conservazione senza utilizzare ***applet*** di firma all'interno del browser;
- il servizio di ***Audit*** e **Log**, che mantiene e manda in conservazione la storia degli accessi effettuati al Sistema e ai dati;
- il **Sito Web** di ParER, che fornisce informazioni e documentazioni relative al processo e al *Sistema di conservazione*;
- il Sistema di e-Learning della Regione Emilia-Romagna, che nell'area dedicata a ParER mette a disposizione degli utenti corsi sul processo di Conservazione.

[Torna al Sommario]

8.2 Componenti tecnologiche

Il *Sistema di conservazione* è costituito da diversi moduli software che interagiscono tra loro per la gestione dell'intero *processo di conservazione*. Il Sistema, inoltre, si avvale di ulteriori componenti applicative esterne con funzioni di supporto al processo.
Il diagramma in figura schematizza dal punto di vista tecnologico le principali componenti del *Sistema di conservazione* di ParER e le principali relazioni con altri sistemi interessati dal *processo di conservazione* descritto nei capitoli precedenti del presente Manuale.

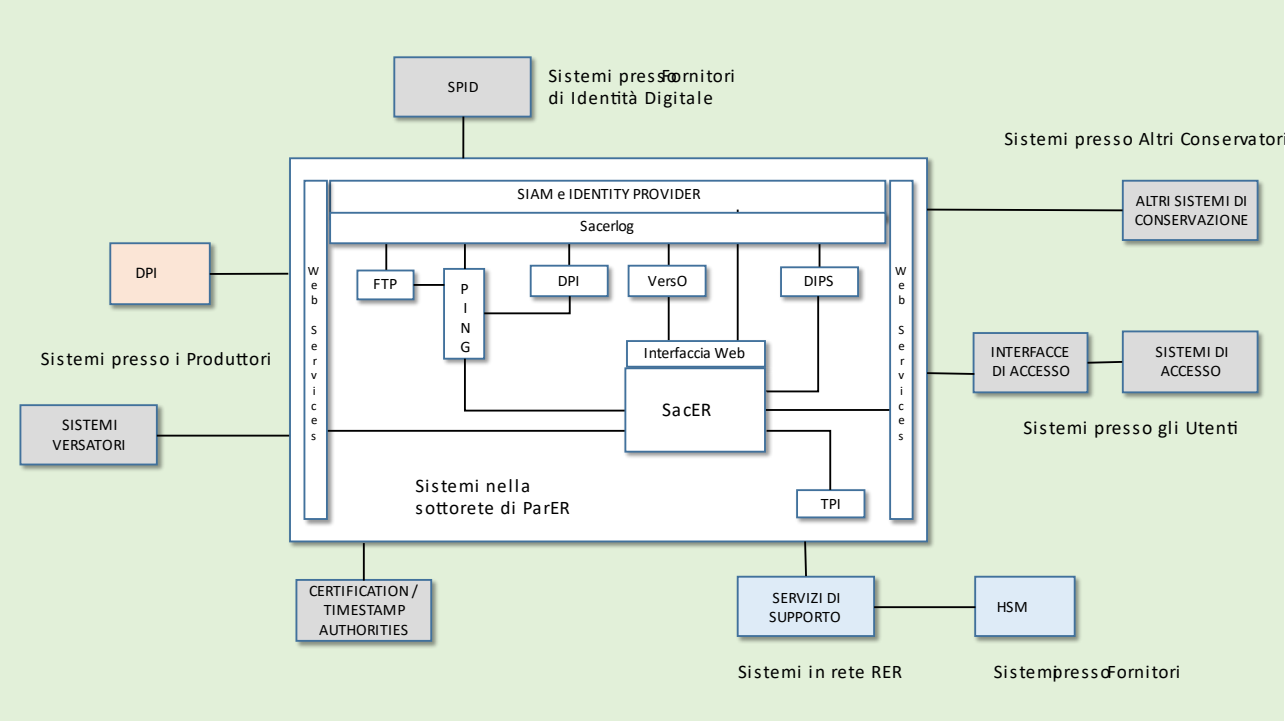


Figura 8 - Schema Tecnologico del Sistema di conservazione

Nella figura sono riportate:

- in bianco le componenti del *Sistema di* conservazione interne al perimetro di sicurezza del data center di ParER;
- in rosa le componenti del *Sistema di* conservazione sviluppate da ParER, ma esterne al perimetro di sicurezza del data center di ParER, in quanto installate nelle reti dei *Produttori*;
- in azzurro le componenti a supporto del Sistema gestite dalla Regione Emilia-Romagna;
- in grigio le componenti che fanno riferimento ai soggetti esterni (*Produttori, Utenti e Authorities*).

Qui di seguito sono illustrati i singoli moduli software del Sistema e le componenti di supporto.

[Torna al Sommario]

8.2.1 SacER

Il modulo software SacER costituisce il nucleo centrale del Sistema e implementa le funzionalità principali del *processo di conservazione*, quali:

- Acquisizione SIP;
- Archiviazione;
- Gestione dati;
- Amministrazione;
- Accesso.

Le funzionalità di Acquisizione SIP di SacER consentono la gestione delle varie fasi del processo di Acquisizione e *presa in carico* (vedi paragrafi 7.1 – 7.4). Operativamente si compongono delle seguenti attività:

- acquisizione del SIP trasmesso attraverso i Servizi di versamento;
- ***memorizzazione*** del SIP in un'area temporanea logicamente distinta dall'*archivio* vero e proprio per effettuare le verifiche previste;
- verifica del SIP in relazione alla struttura dati, ai *metadati* degli oggetti sottoposti a conservazione, alle eventuali firme apposte sui file (***Oggetti-dati***) associati ai ***Componenti***, ai *formati* dei file stessi e generazione del *Rapporto di versamento* in caso di verifica positiva**;**
- restituzione dell'***Esito versamento***, comprensivo, in caso di esito positivo, del *Rapporto di versamento*;
- creazione degli ***Elenchi di versamento*****:** un primo job provvede all'individuazione dei SIP da inserire negli Elenchi secondo i criteri di raggruppamento definiti da ParER; un secondo job genera gli Elenchi e vi appone un *Riferimento temporale* opponibile a terzi; un terzo job esegue i controlli finali e chiude l'Elenco per la sottoscrizione a cura del Responsabile della funzione archivistica di conservazione. Tutti i job sono eseguiti sugli Application server automaticamente ed in modo ricorrente secondo intervalli di tempo stabiliti nel modulo Amministrazione;
- eventuale migrazione di ***formato*** degli ***Oggetti-dati*** contenuti nei SIP sia per contrastarne l'obsolescenza tecnologica, sia per esigenze di miglioramento della fruibilità degli oggetti conservati;
- estrazione dei metadati dal SIP (ed eventuale loro normalizzazione) e dal Sistema da utilizzare per completare le informazioni necessarie a generare l'AIP (***Informazioni sulla rappresentazione***, ***Informazioni sulla conservazione***, ***Informazioni sull'impacchettamento***, ***Informazioni descrittive***);
- generazione dell'***Indice dell'AIP***, utilizzando i metadati estratti dal SIP e quelli generati dal Sistema nel corso del processo di conservazione. SacER produce report di eccezioni a fronte di situazioni anomale nella creazione dell'***Indice dell'AIP***. Tutte le azioni vengono registrate sul sistema in apposite tabelle di log;
- generazione dell'AIP, che avviene impacchettando in un oggetto auto-consistente l'***Indice dell'AIP***, le evidenze informatiche prodotte nel corso del processo di conservazione e gli ***Oggetti-dati***.

Le funzionalità di Archiviazione di SacER gestiscono la parte del processo di Gestione dell'AIP relativa alla *memorizzazione* e verifica degli ***Oggetti-dati*** su Data Base Oracle e ***file system*** (vedi paragrafo 7.5) e comprendono:

- la ***memorizzazione*** degli AIP e l'organizzazione gerarchica dei supporti di memorizzazione. In particolare, gli ***Oggetti-dati*** degli AIP, costituiti dagli ***Indici degli***

AIP e dei SIP, dagli ***Esiti versamento***, dai *Rapporti di versamento* e dai file associati ai ***Componenti***, sono memorizzati su supporti di diverso tipo in ragione della loro dimensione e della frequenza con cui vengono ricercati:

- gli ***Oggetti-dati*** di piccole dimensioni e ad accesso più frequente vengono salvati temporaneamente all'interno del Data Base in opportune tabelle sotto forma di ***BLOb,*** per poi essere memorizzati in modo permanente nell'***object storage***, utilizzando a questo scopo appositi job periodici, descritti più avanti
- gli ***Oggetti-dati*** di grande dimensione e di accesso meno frequente vengono salvati temporaneamente su ***file system*** in cartelle opportunamente strutturate, per poi essere memorizzati in modo permanente su supporti a cassette, utilizzando a questo scopo un apposito componente software chiamato TPI, descritto più avanti;

- il controllo dell'integrità degli oggetti conservati, comprensivo della copia degli archivi, del controllo degli errori e delle procedure di refreshing dei supporti, come descritto nel paragrafo 9.2 e in conformità con il Piano della Sicurezza di ParER;
- la restituzione dei pacchetti alle funzioni di Accesso, mediante opportune funzionalità dell'interfaccia web del Sistema o mediante l'utilizzo di Servizi di recupero;
- la cancellazione degli AIP sottoposti a scarto a seguito della procedura descritta nel paragrafo 7.8.

Le funzionalità di Gestione Dati di SacER sono finalizzate principalmente a gestire le ***Informazioni descrittive*** degli AIP generate durante il processo di acquisizione (vedi paragrafo 7.5) e includono:

- la ***memorizzazione*** dei *metadati* estratti dal SIP o generati dal Sistema nel corso del processo di Acquisizione dei SIP;
- la gestione degli aggiornamenti dei dati generati dalle funzionalità di Amministrazione e nel corso del *processo di conservazione*;
- l'esecuzione delle ricerche e la sua restituzione alle funzionalità di Accesso, che avvengono mediante l'utilizzo di funzionalità da interfaccia web del Sistema o mediante chiamata a Servizi specifici.

Le funzionalità di Amministrazione di SacER consentono di gestire configurazioni e parametrazioni in grado di determinare il funzionamento del Sistema in funzione degli specifici accordi intercorsi con i *Produttori*, definite nel ***Disciplinare tecnico*** e in funzione delle policy stabilite nell'ambito della Pianificazione della conservazione (come descritto più avanti). Inoltre, consentono di monitorare tutta l'attività svolta da SacER, così come descritto nel paragrafo 7.4.1. In particolare, in SacER è possibile configurare tutte le entità significative: Enti, ***Strutture***, operatori e relativi profili, ***tipologie documentarie***, ***formati*** accettati, logiche di controllo dei versamenti, logiche di creazione delle ***Serie***, regole di *accesso* e di esibizione, politiche di monitoraggio del sistema. Anche l'interfaccia web di SacER è configurata automaticamente in ragione del profilo dei singoli operatori che vi accedono.
Le funzionalità di Amministrazione sono costituite da transazioni eseguibili tramite l'interfaccia web del sistema e riservate agli operatori di ParER, ma visibili negli esiti anche agli operatori dei *Produttori*.

Le funzionalità di Accesso di SacER consentono di restituire in forma di DIP gli oggetti conservati. A tal fine SacER mette a disposizione un'interfaccia web per le ricerche e per l'estrazione manuale dei documenti e dei Servizi di recupero per l'estrazione automatica.
Gli AIP forniti sono trasformati in DIP sulla base delle caratteristiche dell'oggetto e degli utilizzi cui è destinato. In molti casi la trasformazione dell'AIP in DIP può richiedere specifici passi

elaborativi e trasformazioni complesse, che, necessitando di elaborazioni onerose, vengono normalmente eseguite da opportuni job batch e mantenute in modo permanente sul Data Base. Secondo la natura dei DIP, l'*esibizione* può avvenire on-line con un download, oppure tramite il trasferimento in un'area di transito, da cui il successivo recupero viene effettuato dal sistema richiedente con chiamata FTP. In molti casi, per comodità di trasferimento e recupero, i vari elementi che costituiscono il DIP vengono compressi in un archivio di tipo ZIP.
Il modulo di Accesso, oltre a verificare tramite i servizi di Autenticazione l'abilitazione dell'*Utente* al recupero del documento, traccia in apposite tabelle di log tutte le richieste prevenute, qualunque ne sia stato l'esito.

[Torna al Sommario]

8.2.2 VersO

Il client di versamento manuale VersO (Versamento Online) è un modulo che ParER mette a disposizione degli Enti produttori per svolgere operazioni routinarie sul sistema. Poiché utilizza un'interfaccia web, non richiede l'installazione di alcun software sulla stazione di lavoro dell'*Utente*.

Il suo utilizzo tipico è il ***versamento*** di ***Unità documentarie*** per le quali non esiste un sistema interfacciato con Sacer. VersO viene richiamato tramite interfaccia web, si autentica sull'***IdP*** di ParER o su ***SPID***, utilizzando in ogni caso logiche di profilazione del Sistema, ed effettua il ***versamento*** dei SIP tramite interazione guidata con l'operatore del *Produttore*.
Tale modulo semplifica le operazioni di ***versamento*** manuale da parte del *Produttore*, automatizzando la generazione dell'***Indice del SIP*** ed effettuando un test completo della correttezza del versamento prima di eseguire il versamento stesso. Inoltre, mantiene il log dei versamenti effettuati e consente di interrompere temporaneamente l'operazione (p.e per raccogliere informazioni necessarie per completarlo), riprendendola successivamente, indipendentemente dalla scadenza della sessione web.

[Torna al Sommario]

8.2.3 PING

Il modulo software PING (PreINGest) gestisce il processo di preacquisizione nel caso di ***versamento*** di Oggetti da trasformare in SIP (vedi paragrafo 7.1.1).

La trasmissione dei pacchetti, solitamente compressi, avviene tramite protocollo ***FTPS***; l'***FTP server*** provvede a memorizzare i file ricevuti sullo ***storage*** dedicato allo spazio FTP di input.
Una volta ricevuti gli Oggetti, un job schedulato provvede alla loro elaborazione per la produzione dei SIP da versare. Un ulteriore job schedulato si occupa di effettuare il ***versamento*** a SacER, che avviene utilizzando un apposito servizio di versamento. Tale servizio accetta in chiamata due file XML, uno con l'***Indice del SIP*** e un altro con le ***Informazioni sull'impacchettamento***, relative alla posizione dei file del SIP memorizzati sullo spazio FTP di input.
SacER utilizza le ***Informazioni sull'impacchettamento*** per recuperare i file dal ***file system*** di PING e depositarli nel proprio per le successive elaborazioni.

Le successive elaborazioni vengono eseguite da PING direttamente, nel caso in cui la normalizzazione possa basarsi su regole precodificate (come p.e. nel caso delle immagini diagnostiche in formato Dicom), oppure utilizzando un motore ETL di esecuzione delle trasformazioni nel caso in cui si debbano applicare regole di trasformazioni specifiche dell'oggetto in questione. In questo caso le regole vengono definite durante la fase di avvio del servizio, tramite uno strumento visuale ed eventuali integrazioni di codice sviluppato ad hoc.

PING traccia e memorizza nel proprio Data Base gli esiti dei versamenti a SacER e può essere interrogato da un operatore tramite interfaccia web o dal sistema versante tramite opportuno ***Web Service,*** per conoscere a quale punto del processo è giunto il SIP.

PING mette inoltre a disposizione del *Produttore* un client di versamento di Oggetti da trasformare, sia on line, sia tramite l'utilizzo di un client ***FTP*** installato sulla postazione di lavoro dell'utente o su un server della rete del *Produttore*.

[Torna al Sommario]

8.2.4 DPI

Il modulo software DPI (Digital Preservation Interface), sviluppato e manutenuto da ParER, consiste in un sistema di interfaccia tra i sistemi dell'Ente produttore e PING; DPI può essere installato all'interno della rete dell'Ente stesso e gestito secondo le politiche di sicurezza dell'Ente, potendo tra l'altro autenticarsi sul suo ***IdP***.

DPI implementa funzionalità di ***versamento*** per specifiche tipologie di SIP. In particolare, qualificandosi come nodo ***DICOM***, DPI riceve dai ***PACS*** studi diagnostici, che poi trasmette a PING per la trasformazione e il ***versamento*** a SacER.
DPI può operare con logiche sia push che pull, ricevendo o estraendo dati e documenti dai sistemi del *Produttore* per poi versarli nel Sistema, richiamando gli opportuni servizi di PING.
Inoltre, DPI fornisce strumenti di monitoraggio dei versamenti effettuati a disposizione dell'Ente produttore.

[Torna al Sommario]

8.2.5 Interfacce di Acquisizione e di Recupero (Web Service)

I sistemi che debbono versare a SacER documenti o aggregazioni e ottenerne l'esibizione colloquiano con SacER tramite opportuni ***Web Service***, che sono definiti nei documenti "Specifiche tecniche dei servizi di versamento" e "Specifiche tecniche dei servizi di recupero". Tali servizi sono invocati anche dai componenti di versamento sviluppati da ParER (DPI, VersO), oltre che dai sistemi di versamento dei *Produttori*.

Nel processo di preacquisizione il client versante (p.e. DPI) utilizza ***Web Service*** per coordinare il processo con il modulo PING, ma trasmette gli oggetti da conservare tramite protocollo ***FTPS***, su un'opportuna area FTP, gestita dal server FTP di ParER. Fa eccezione il client interno a PING, che può versare anche on line, senza appoggiarsi su protocollo ***FTP***.

8.2.6 TPI

Il modulo software TPI (Tivoli Preservation Interface) gestisce la *memorizzazione* degli ***Oggetti-dati*** su supporti a cassette, operata utilizzando come sistema di gestione della ***tape library*** il software Tivoli.

TPI opera nel seguente modo:

- un job schedulato sul file server invia al sistema di gestione della ***tape library*** il comando di archiviazione delle cartelle in cui SacER ha depositato gli oggetti da archiviare, selezionate tramite opportuni criteri definiti in sede di amministrazione di sistema;
- il sistema di gestione della ***tape library*** provvede a leggere i file dalle cartelle e ad archiviarli tramite le sue funzionalità di archiving nella ***tape library***, dove rimangono in situazione ***near-line***, cioè disponibili e raggiungibili nella ***tape library***, senza necessità di reperire cassette da un magazzino;
- una volta che li ha archiviati, TPI provvede a cancellare i file dal ***file system*** su disco;
- l'allineamento tra sito primario e sito di ***Disaster recovery*** viene garantito da un job periodico schedulato sul file server del sito primario, che aggiorna automaticamente il ***file system*** del sito secondario. Il job invia al sito secondario i nuovi file pervenuti nel ***file system***, senza replicare le cancellazioni effettuate in seguito all'archiviazione su cassetta;
- sul sito di ***Disaster recovery***, in maniera indipendente da quanto avviene sul sito primario, ma con politiche analoghe, viene eseguito un job di archiviazione analogo a quello del sito primario, mantenendo così l'indipendenza tra i due siti per quanto riguarda l'archiviazione.

Le funzionalità di Archiviazione di SacER verificano lo stato degli Oggetti-dati nei due siti e lo registrano sul Data Base Oracle.
Presso il sito di ***Disaster recovery*** viene prodotta una seconda copia per ogni cassetta.
Le attività di gestione del sito di ***Disaster recovery*** sono tracciate in uno specifico Data Base del sistema di gestione della ***tape library***.

[Torna al Sommario]

8.2.7 DIPS

Il modulo software DIPS (DIPSpenser), previo controllo dei diritti di accesso alle informazioni, consente di attivare ricerche sul Sistema e di soddisfare richieste relative agli oggetti conservati, anche quando le funzionalità di ricerca messe a disposizione dall'interfaccia web di SacER non riescono a soddisfare le particolari esigenze dell'*Utente*.
DIPS consente ricerche complesse sugli oggetti conservati sulla base delle ***Informazioni descrittive*** memorizzate dalle funzionalità di Gestione dati, e di ottenere l'*esibizione* dei documenti individuati dalla ricerca, sfruttando le funzionalità di Accesso di SacER. DIPS opera ricercando gli AIP da esibire, attraverso le ***Informazioni descrittive*** fornite dalle funzionalità di Gestione dati, e richiedendo gli AIP alle funzionalità di Archiviazione.

Il modulo DIPS consiste di un sistema generalizzato in grado di configurare tramite opportuna parametrazione i criteri da utilizzare nella ricerca e la presentazione dei risultati in ragione delle necessità e delle preferenze dei diversi utenti.

[Torna al Sommario]

8.2.8 SIAM

Il modulo software SIAM (SacER Identity and Access Management) consente di gestire l'autenticazione e la profilatura degli operatori. Tale profilatura viene utilizzata da SacER e dagli altri moduli software del Sistema per valutare a quali viste specifiche di dati e a quali attività ogni operatore abbia accesso, sulla base dei ruoli assegnati.

Per le funzionalità di autenticazione SIAM utilizza sistemi di ***IdP*** (Identity Provider); ParER mette a disposizione un proprio ***IdP***, ma accetta anche l'autenticazione effettuata tramite SPID.

SIAM mantiene il Data Base degli operatori dell'***IdP*** di ParER, nonché il Data Base dei profili di tutti gli operatori abilitati al Sistema, qualunque sia l'***IdP*** su cui si sono autenticati, gestendo quindi in modo centralizzato la profilatura per tutti i moduli del Sistema.
La profilatura si spinge fino al livello delle singole attività previste dal Sistema (p.e. pressione di uno specifico bottone di una specifica videata) ed al livello elementare dei dati gestiti (***Struttura***, ***Unità documentaria***, Registro, ecc.) tramite la definizione e la combinazione di opportuni ruoli.

L'***IdP*** implementato da ParER colloquia con gli altri moduli del Sistema tramite standard SAML (Security Assertion Markup Language); l'utilizzo di SAML consente al *Sistema di conservazione* di accettare operatori autenticati su ***SPID***.

[Torna al Sommario]

8.2.9 Sacerlog

Il modulo Sacerlog raccoglie e conserva nel sistema informazioni essenziali sul processo di conservazione in base al paradigma proposto da PREMIS, basato sui concetti di Agente (in generale l'utente collegato al sistema), Evento (p.e. "Inserimento" o "Cancellazione") e Oggetto (p.e. "Parametro di configurazione della ***Struttura***").
In pratica, ogniqualvolta un agente scatena un evento che modifica un oggetto (inclusa la creazione dell'oggetto stesso), il sistema di log registra la fotografia dell'oggetto modificato e le informazioni essenziali sulla modifica (agente, evento, timestamp, ecc.).
Sacerlog è utilizzato anche per registrare nel log eventi di sola consultazione (ad es. "Visualizzazione dettaglio ***Unità documentaria***"), di cui è necessario tenere traccia per ragioni di sicurezza.

Il sistema di log è completamente parametrabile tramite funzioni di amministrazione, che consentono di stabilire quali combinazioni di agenti / eventi / oggetti / debbano essere registrati nel log.

Il log può essere consultato da un utente che possiede le dovute abilitazioni per determinare la storia di quanto accaduto su un oggetto. Il log può essere anche consultato per esporre il contenuto dell'oggetto ad un qualunque istante di riferimento, determinando la fotografia dell'oggetto più recente rispetto all'istante di riferimento.

[Torna al Sommario]

8.2.10 Componenti di supporto

Completano il Sistema i vari moduli di supporto, ovvero le componenti che non implementano specifiche logiche applicative, ma mettono a disposizione funzionalità trasversali agli altri moduli. Più nello specifico:

- il time server della rete regionale tramite protocollo ***NTP*** distribuisce il *Riferimento temporale* all'interno dei ***Data Center*** con fuso orario Europe/Rome (GMT+1) e configurazione della variazione automatica dell'ora solare, allineandolo costantemente con l'orario dell'Istituto Elettrotecnico Nazionale Galileo Ferraris di Torino (ntp.ien.it), che è a disposizione di qualsiasi altro sistema che voglia mantenere l'orario allineato con i sistemi di ParER.
- il modulo di Audit e Log di sistema è costituito da un insieme eterogeneo di componenti che si occupano di raccogliere tutte le informazioni rilevanti sugli eventi accaduti durante la vita del sistema. Si tratta di informazioni sistemistiche (*log di sistema* operativo, del data base e degli application server), di sicurezza (accessi andati a buon fine e rifiutati), che vengono raccolte dai diversi strati tecnologici del Sistema con il supporto di componenti specifici, ivi incluso Sacerlog. Il modulo di Log si basa su un sistema ***SIEM*** (HP ArcSight) opportunamente configurato e alimentato, che si occupa di raccogliere i *log* e memorizzarli in conformità con le politiche definite da ParER sulla base della normativa vigente, con i disciplinari regionali in materia di sicurezza informatica e con la necessità di mantenere nel Sistema tutte le informazioni necessarie a documentare le attività svolte, anche per funzionalità di audit. Le informazioni memorizzate in ArcSight vengono analizzate continuamente in remoto dal Centro Operativo per la Sicurezza (***SOC***), utilizzando opportuni strumenti atti a individuare tempestivamente eventuali minacce per la sicurezza del servizio. Componenti di audit e log sono presenti anche nel sito di ***Disaster recovery;***
- il modulo di Monitoraggio Tecnico è costituito da un insieme eterogeneo di componenti che si occupano di raccogliere in tempo reale le segnalazioni di possibili malfunzionamenti dell'infrastruttura e di segnalarle alla struttura della Regione Emilia-Romagna preposta alla gestione; allo scopo vengono utilizzati diversi software open source tra cui Zabbix, che viene alimentato da opportuni agenti software, e Graylog, che raccoglie temporaneamente i log dei sistemi e li indicizza, per agevolare la diagnostica delle problematiche applicative. Le informazioni di monitoraggio sono raccolte per analisi di periodo nel cruscotto realizzato tramite un'applicazione di ***business intelligence*** costruita con lo strumento open source SpagoBI. Componenti di monitoraggio tecnico sono presenti anche nel sito di ***Disaster recovery;***
- il modulo di Request Tracking viene utilizzato per automatizzare e mantenere traccia dei processi fondamentali del servizio di conservazione: tra questi la gestione delle richieste di rilascio in produzione delle nuove versioni dell'applicativo e le richieste di manutenzione dell'infrastruttura; allo scopo viene utilizzato il software di ***trouble ticket*** della Regione Emilia-Romagna;

- i componenti di supporto allo sviluppo vengono utilizzati per garantire la corretta gestione degli sviluppi del software, per quanto riguarda sia l'evoluzione che la manutenzione correttiva del sistema; in generale si tratta di componenti open source normalmente utilizzati dai gruppi di sviluppo della Regione Emilia-Romagna sulla base di metodologie consolidate; tali componenti, oltre a facilitare lo sviluppo del software e a supportare la gestione dei progetti e delle risorse, consentono di tenere traccia di tutte le attività significative nell'ambito dello sviluppo, dal momento della definizione dei requisiti fino al momento della richiesta di rilascio, e delle relative evidenze documentali. La tracciatura del processo di sviluppo è supportata da un opportuno strumento open source (Redmine), su cui sono definiti diversi workflow in ragione della problematica di sviluppo da affrontare;
- il sito web di ParER espone in modo strutturato informazioni e documentazione utili sia ai *Produttori* che agli *Utenti* (***Comunità di riferimento***). Tali informazioni riguardano, ad esempio, le procedure amministrative di attivazione dei servizi di conservazione e le specifiche per effettuare i ***versamenti*** dei SIP. Inoltre, rende disponibili informazioni aggiornate sulla quantità dei Documenti conservati e sulle tematiche legate agli *archivi*, alla gestione documentale e alla conservazione degli oggetti digitali. Dal sito è possibile, inoltre, iscriversi alla newsletter settimanale con cui ParER tiene aggiornata la ***Comunità di riferimento*** sulle novità in materia di Conservazione;
- nel repository interno di ParER sono registrate e costantemente aggiornate le procedure riferite allo svolgimento della funzione di conservazione;
- SELF, sistema di e-Learning della Regione Emilia-Romagna, è il sistema che la Regione ha adottato per la diffusione dell'e-learning nelle proprie pratiche formative e in quelle di altri enti pubblici, cui SELF offre tecnologie, servizi, risorse didattiche e competenze nella gestione di corsi in e-learning. In particolare, per quanto riguarda ParER, SELF mette a disposizione corsi introduttivi e intermedi sul processo di Conservazione e risorse formative sulla gestione della privacy.

[Torna al Sommario]

8.3 Componenti fisiche

8.3.1 Schema generale

Dal punto di vista tecnico il sistema è progettato e realizzato in maniera da fornire un'elevata continuità di servizio, garantire l'*integrità* degli oggetti conservati, gestire grandi volumi di dati, mantenere performance stabili indipendentemente dai volumi di attività e assicurare la riservatezza degli accessi.
Il Sistema è sviluppato con tecnologie di larga diffusione open source o comunque di libero utilizzo, a parte i sistemi di memorizzazione di dati, per i quali si utilizzano prodotti proprietari, che dispongono però di interfacce standard de facto o de jure; in particolare il Data Base per ragioni di sicurezza e di performance è proprietario (Oracle), ma standard SQL, l'***Object Storage*** (NetApp) è proprietario, ma adotta le specifiche pubbliche ***S3***, mentre il sistema di gestione dello ***storage*** su cassetta (TSM) è fornito da IBM, fornitore della ***tape library***.

Il diagramma in figura schematizza le principali componenti infrastrutturali del *Sistema di conservazione* di ParER e le principali relazioni con altri sistemi interessati dal *processo di conservazione* descritto nei capitoli precedenti del presente Manuale.

Il Sistema è realizzato su due siti che distano circa 100 chilometri l'uno dall'altro: un sito primario con caratteristiche di continuità operativa, installato presso il ***Data Center*** della Regione Emilia-Romagna a Bologna, che svolge funzioni di normale operatività, ed un sito secondario, installato presso il ***Data Center*** di Lepida s.c.p.a. a Parma, ma gestito per i sistemi di conservazione direttamente dalla Regione Emilia-Romagna che ha lo scopo di subentrare come sito di ***Disaster recovery*** nel caso di caduta irreparabile del sito primario.

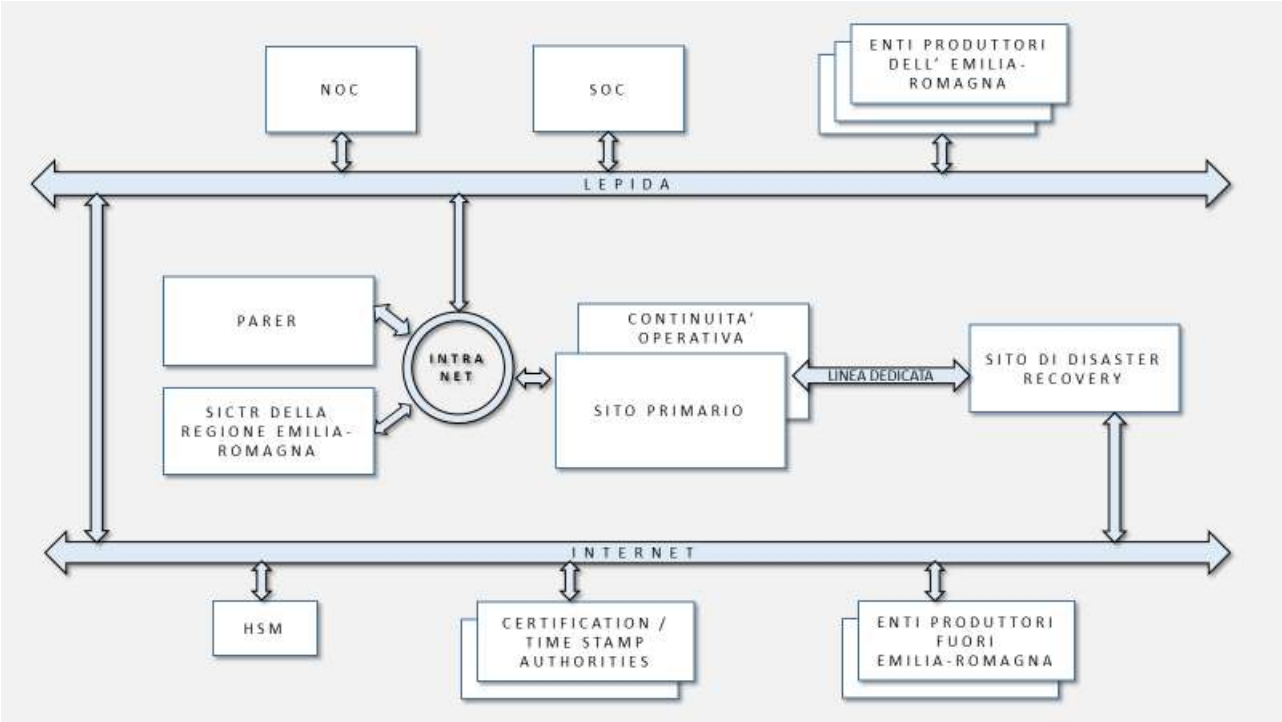


Figura 9 - Schema Infrastrutturale del Sistema di conservazione

Il sito primario e il sito di Parma sono gestiti dalla Regione Emilia-Romagna all'interno di una sottorete dell'Intranet regionale dedicata al *Sistema di conservazione*. Il collegamento tra i due siti è garantito da una linea dedicata in banda larga fornita da Lepida s.c.p.a.. Il sito di ***Disaster recovery*** viene reso accessibile via Internet solo nel momento in cui, a seguito di disastro, dovesse essere promosso a sito primario.
Il Sistema di conservazione, benché sia ospitato in data center di terzi, dispone di sotto reti proprie isolate dalle altre sotto reti.
Alcuni sistemi di supporto sono installati in una sotto rete del ***data center*** della Regione Emilia-Romagna; nello specifico si tratta dei log server, dei time server, dei server di monitoraggio, dei server che ospitano il sito web di ParER e dei ***proxy*** che gestiscono gli scambi con gli ***HSM***. La comunicazione tra la sotto rete del *Sistema di conservazione* e la sotto rete generale della Regione Emilia-Romagna è limitata a protocolli e porte ben specifiche, in modo tale da garantire l'isolamento della porzione di rete del *Sistema di conservazione* dai rimanenti sistemi regionali.
Gli ***HSM*** sono installati presso un fornitore esterno, aggiudicatario di gara per la gestione del servizio per la Regione Emilia-Romagna.
Presso un fornitore esterno aggiudicatario di apposita gara è allocato il Centro di Monitoraggio dell'Infrastruttura (***NOC***), che effettua il controllo continuo delle apparecchiature informatiche e

dei server per tutti i sistemi della Regione Emilia-Romagna, e quindi anche di ParER (escluso il sito di DR).
Presso un altro fornitore esterno aggiudicatario di apposita gara è allocato il Centro Operativo per la Sicurezza (***SOC***), che fornisce i servizi di sicurezza per tutti i sistemi della Regione Emilia-Romagna, e quindi anche di ParER (escluso il sito di DR).

Il sito primario è costituito da due sotto-siti collegati in rete locale in due diversi edifici della Regione, che operano per garantire la ***continuità operativa*** del servizio.
Tutti i componenti del sito primario e del sito di continuità operativa e i componenti esterni sviluppati da ParER, nonché gli ***HSM***, sono ridondati, mentre non lo sono i componenti del sito di ***Disaster recovery***.

Il sistema interagisce con i *Produttori* dell'Emilia-Romagna tramite la rete regionale in banda larga ***Lepida***, che è completamente ridondata; ***Lepida*** è a sua volta attestata su Internet con collegamenti in banda larga. In questo modo viene garantita tramite Internet una connessione ad alta velocità con i sistemi delle Certification / Time Stamp Authorities, con gli ***HSM, con i provider di identità SPID*** e con i *Produttori* che non appartengono all'Emilia-Romagna e che quindi non sono connessi a ***Lepida***.

In situazione di normale funzionamento il Sistema è attivo solo sul sito primario con garanzia di ***continuità operativa*** anche nel caso di caduta di uno dei due sotto-siti; il sito di ***Disaster recovery*** si limita a replicare le informazioni del sito primario in maniera asincrona man mano che vengono generate e a compiere funzioni di ***backup*** gestite autonomamente e di ***archiving*** sotto il controllo del sito primario.
Nel sito primario in situazione di normale funzionamento il carico della maggior parte delle applicazioni è distribuito tra i due sotto-siti; nel caso di caduta di uno dei due sotto-siti, l'altro ancora attivo provvede a garantire la continuità del servizio, sia pure con performance ridotte, fino al ripristino della situazione normale. Nel caso di caduta irreparabile di ambedue i sotto-siti del sito primario non recuperabile nel breve periodo (disastro) il sito di ***Disaster recovery*** viene posto in stato di attività e attivato come destinatario del traffico di rete, con funzionalità ridotte fino al ripristino del sito primario.

Sia nel sito primario che nel sito di ***Disaster recovery*** sono presenti diverse istanze del Sistema:

- un'***istanza*** di Produzione, cui è riservata la maggior parte delle risorse;
- un'***istanza*** di Test, riservata al personale di ParER per il test delle nuove versioni rilasciate dai laboratori di sviluppo;
- un'***istanza*** di Preproduzione, allineata all'***istanza*** di produzione, per i test dei *Produttori*.

I sistemi di sviluppo risiedono presso il ***Data Center*** della Regione Emilia-Romagna.
La separazione delle istanze viene assicurata attraverso l'utilizzo di domini di rete distinti, che non sono visibili l'uno all'altro.

Nell'ambito di ciascuna istanza, il sistema utilizza una logica multi-Ente, assimilabile ad un sistema ***multi-tenant***, intendendo con ciò un insieme di "aree" che, pur condividendo una medesima istanza applicativa, sono logicamente separate tra loro. Tale separazione è realizzata sia per quanto concerne gli accessi, sia per quanto concerne la conservazione dei dati.

[Torna al Sommario]

8.3.2 Caratteristiche tecniche dei Sistemi

Il diagramma in figura schematizza le principali componenti tecniche dei sistemi di ParER. I due sotto-siti del sito primario sono tra loro identici, tranne che per la presenza di una ***tape library*** di dimensioni ridotte in uno dei due siti, che svolge solamente funzioni di ***Backup***; i sistemi del sito di ***Disaster recovery*** sono analoghi a quelli di un sotto-sito del sito primario, a parte la mancata ridondanza dei componenti e l'assenza del ***proxy*** per ***HSM***.

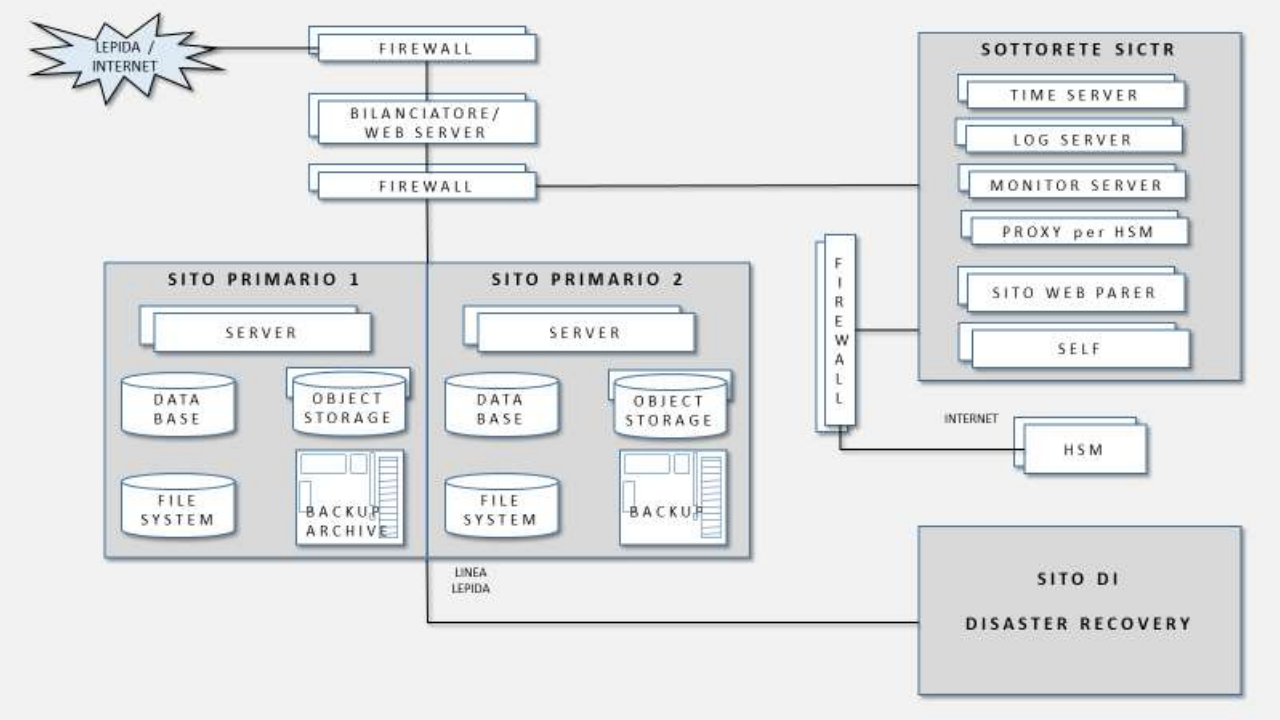


Figura 10 - Schema dei Sistemi di ParER

I servizi ausiliari, in quanto di interesse di tutta l'infrastruttura regionale, sono ospitati su server della sottorete della Regione Emilia-Romagna; tra questi fondamentale per il processo di conservazione è il time server della rete regionale tramite protocollo ***NTP*** distribuisce il *Riferimento temporale* all'interno dei ***Data Center*** con fuso orario Europe/Rome (GMT+1) e configurazione della variazione automatica dell'ora solare, allineandolo costantemente con l'orario dell'Istituto Elettrotecnico Nazionale Galileo Ferraris di Torino (ntp.ien.it).

Nell'ambito del sito primario i sistemi sono aggregati in ***cluster***, mentre nel sito di ***Disaster recovery***, in quanto non ridondato, non sono presenti cluster fisici di sistemi; sono però presenti cluster logici di Application server, in numero ridotto rispetto al sito primario, con lo scopo di distribuire il carico applicativo tra diversi sistemi.

Gli accessi al sistema avvengono esclusivamente passando da ***firewall*** tramite protocolli sicuri (***HTTPS*** e ***FTPS***).

Lo ***storage*** utilizza come supporti di memorizzazione sia dischi che nastri magnetici su cassetta.

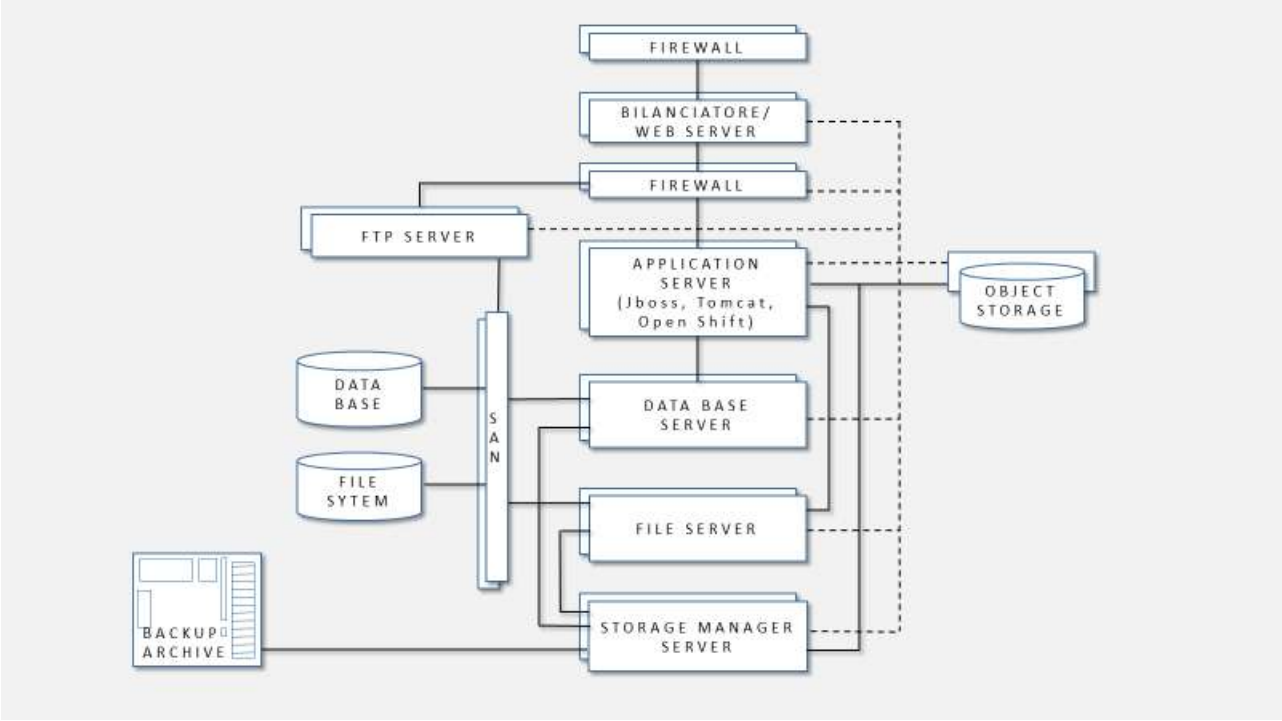


Figura 11 - Schema del Sito Primario

Lo ***storage*** su disco è suddiviso tra:

- **Data Base Oracle** per la *memorizzazione* dei metadati delle informazioni tipiche del processo di conservazione; viene utilizzato anche per memorizzare temporaneamente in forma di ***BLOb*** una parte degli ***Oggetti-dati*** dal momento del loro ingresso nel sistema fino al momento della loro conservazione definitiva nell'***Object storage***;
- ***File system*** per la *memorizzazione* temporanea degli ***Oggetti-dati*** che, in base alle politiche configurate nel sistema, verranno archiviati su cassette; il ***file system*** contiene inoltre tutti i file di servizio (log, configurazioni, ecc.) e un'Area ***FTP*** per il trasferimento ed il recupero asincrono degli ***Oggetti-dati*** da parte dei *Produttori*. Le aree temporanee vengono cancellate normalmente entro una settimana dopo l'utilizzo da opportune procedure applicative. Le aree utilizzate vengono sovrascritte continuamente e quindi i dati temporanei dopo un breve tempo non sono più accessibili.

Lo ***storage*** su disco è ospitato su uno storage array ed è costituito da un'area di storage primario con dischi ad alta velocità e da un'area di storage secondario con dischi a media velocità; in questo modo è possibile ottimizzare la distribuzione dei dati sui dischi in ragione delle necessità applicative.

La maggior parte degli ***Oggetti-dati*** conservati nel sistema risiede permanentemente all'interno di ***appliance*** dedicate alla gestione dell'***Object storage***, su cui vengono trasferite da un processo di elaborazione che li sposta dall'originaria posizione temporanea nel data base.

Lo ***storage*** su nastri magnetici si basa su un sistema a cassette (***tape library***), completamente governato da Tivoli Storage Manager (TSM), che gestisce cassette in standard ***LTO6*** su cui vengono mantenuti:

- in modalità ***archiving***, in situazione ***near-line*** gli ***Oggetti-dati*** che non vengono mantenuti nell'***Object storage*** (tipicamente quelli molto voluminosi e di accesso non frequente);

- in modalità di ***backup***, i backup full ed incrementali e gli archive log del Data Base, immediatamente disponibili per qualsiasi attività di restore che si rendesse necessaria;
- in modalità di ***backup*** i file presenti nel ***File system***.

Il Sistema è sviluppato in ***Java*** su sistemi operativi Linux (Red Hat) utilizzando i seguenti componenti principali:

- ***Bilanciatore di carico*** **LBL** (Oplon), che svolge anche il ruolo di Web server;
- **File Server** GlusterFS per la gestione del file system condiviso tra diversi server e delle aree ***FTP***;
- ***FTP server*** in cluster;
- ***Application server*** JBoss Enterprise (Red Hat) in cluster logico gestito dai componenti di clustering di JBoss;
- ***Servlet container*** Tomcat (Apache) per i componenti che non richiedono l'utilizzo di un application server (p.e. TPI, DPI, Kettle server);
- Open Shift (Red Hat) come orchestratore dei container in cui vengono eseguiti i ***Microservizi***;
- Data Base Oracle con utilizzo delle funzionalità di ***RAC, di Data Guard*** e di ***partitioning***;
- ***Object Storage*** NetApp distribuito in replica su tre siti;
- Tivoli Storage Manager (IBM) con funzionalità di ***Backup*** e ***Archiving*** su ***tape library***.

I moduli applicativi del Sistema, essendo sviluppati in ***Java*** secondo le specifiche **Java Platform Enterprise Edition (*J2EE***), sono raggruppati in diversi contesti applicativi caricati su JBoss. i moduli principali sono ognuno connesso ad un proprio schema di Data Base, in modo da garantire una buona modularità dell'applicativo. I componenti che non dispongono di proprio schema di Data Base utilizzano gli altri schemi, accedendo tramite ***Web Service*** appositamente ottimizzati per l'accesso ai dati, oppure tramite opportuni ***grant***. I componenti applicativi che richiedono un'esecuzione fortemente dinamica sono invece sviluppati tramite ***Microservizi*** caricati in opportuni contenitori la cui gestione viene orchestrata da Open Shift.

Il colloquio tra il Sistema e gli applicativi esterni è effettuato tramite ***Web Service***.
Il trasferimento dei dati sincrono è realizzato in ***HTTPS*** tramite tecnologie ***ReST***, mentre il trasferimento asincrono utilizza tecnologie ***FTPS***.

Il Sistema è Web-based e testato per diversi browser (Firefox, Explorer, Chrome). Non richiede l'installazione di alcun componente sul client.

Il ***framework di sviluppo*** utilizzato è stato derivato dal framework open source Spring, migliorandone gli aspetti di accessibilità; la ***persistenza*** è gestita tramite ***EJB***, generati con la piattaforma Hibernate e solo in pochissimi casi particolari ben identificati e documentati tramite chiamate dirette JDBC, in modo da garantire portabilità verso altri Data Base relazionali e quindi facilitare il riuso dell'applicativo. Il sistema ingloba diverse librerie applicative open source, molte delle quali sviluppate nell'ambito di progetti internazionali, in particolare per la verifica delle firme e dei ***formati***.

La replica dei dati sul sito di ***Disaster recovery*** è garantita da diverse tecnologie:

- il Data Base viene sincronizzato da Oracle tramite Data Guard con modalità di physical standby e maximum availability (il sito primario non attende la fine della scrittura del sito di ***Disaster recovery*** per considerare chiusa la transazione);
- l'***Object storage*** viene replicato nei diversi siti dalle tecnologie intrinseche di NetApp;

- il file system su disco viene allineato tramite ***SCP***;
- l'archivio su cassette viene mantenuto aggiornato da TSM in maniera indipendente tra i due siti tramite opportune politiche di schedulazione; l'applicativo controlla periodicamente la corretta sincronizzazione dei file system e degli archivi su cassette tra i due siti.

Nel caso di dismissione di dispositivi elettronici di memorizzazione dei dati l'Area Infrastrutture e sicurezza regionale si occupa di garantire la cancellazione sicura delle informazioni presenti nel sistema, in base alle politiche e alle procedure di sicurezza della Regione Emilia-Romagna.

[Torna al Sommario]

8.4 Procedure di gestione e di evoluzione

La gestione del *Sistema di conservazione* è affidata a diversi gruppi di operatori, secondo la natura delle attività da svolgere; tali attività includono la gestione operativa del sistema in esercizio, l'avviamento di nuovi enti e di nuovi servizi di conservazione e le eventuali successive modifiche, l'evoluzione dell'infrastruttura e dell'applicativo, e infine la gestione dei malfunzionamenti e degli incidenti di sicurezza.

[Torna al Sommario]

8.4.1 Gestione dell'Esercizio

Per quanto attiene alla gestione operativa del sistema in esercizio, l'Unità Servizi di Conservazione Digitale di ParER presidia le attività descritte nello specifico punto del paragrafo 5.2.

L'Area Infrastrutture e sicurezza presidia parallelamente l'operatività quotidiana dell'infrastruttura hardware e software sottostante il *Sistema di conservazione*, nonché la pianificazione ed il controllo delle attività straordinarie che possono avere impatto sull'esercizio, come descritto allo specifico punto del paragrafo 5.2, oltre a quelle dettagliate nel paragrafo 9.2; l'attività dell'Area citata copre sia il sito primario, incluso il sito di ***Continuità Operativa,*** sia l'infrastruttura di ***Disaster Recovery***.

[Torna al Sommario]

8.4.2 Gestione delle utenze

La procedura riportata nel documento "Gestione utenze" descrive le modalità con cui viene garantita la corretta gestione dei soggetti che hanno accesso al sistema di conservazione tramite i suoi moduli applicativi (vedi il paragrafo 8.2), con particolare riguardo alla sicurezza dei dati e delle informazioni conservate, nel rispetto della politica generale di controllo degli accessi di SID.

La procedura descrive inoltre il metodo seguito per la gestione delle password in coerenza con quanto descritto nella *Politica sulla sicurezza SID.*
La richiesta dell'attivazione, della modifica del profilo o della cessazione di un'utenza è effettuata dall'Ente di appartenenza dell'*Utente*.
Se l'autenticazione avviene tramite ***SPID***, la gestione della password è affidata al provider dell'identità SPID; se invece avviene tramite l'***IDP*** di ParER, è affidata a personale di ParER specificamente formato al rispetto delle procedure di sicurezza, in particolare a quelle definite per la gestione delle utenze.
Le password gestite dall'***IDP*** di ParER sono conservate nel Sistema crittografate e non sono accessibili al personale, nemmeno se dotato di privilegi amministrativi.

Periodicamente ParER effettua un controllo delle utenze attive nel *sistema di Conservazione* e delle relative profilature, con il coinvolgimento degli Enti che ne hanno richiesto l'attivazione, al fine di mantenere pulito l'archivio gestito da SIAM (vedi paragrafo 8.2.8).

Il sistema di gestione delle autenticazioni viene costantemente aggiornato in base alle direttive regionali in termini di sicurezza informatica e alle risultanze dei processi di certificazione per la sicurezza e di qualificazione nel Cloud Market Place di AgID.

[Torna al Sommario]

8.4.3 Gestione dei Malfunzionamenti

La procedura riportata nel documento "Gestione delle Richieste di Informazioni, Reclami e Segnalazioni" descrive la maniera in cui ParER tratta le richieste di informazioni, i malfunzionamenti e gli eventuali reclami da parte degli *Utenti* del sistema.

La gestione dei malfunzionamenti può coinvolgere diverse strutture di SID, secondo la natura del malfunzionamento stesso, che può essere rilevato da diverse fonti: malfunzionamenti di natura applicativa possono essere segnalati dagli Enti *Produttori, dagli Enti Conservatori e dagli Enti Gestori*, dall'Unità Servizi di Conservazione Digitale, dalla Funzione Archivistica di Conservazione di ParER o dall'Unità Sistemi di Conservazione, mentre malfunzionamenti di natura tecnica possono essere segnalati dal dall'Area Infrastrutture e sicurezza.

Allo stesso modo diverse possono essere le strutture che intervengono nella soluzione del malfunzionamento: l'Unità Servizi di Conservazione Digitale è normalmente in grado di risolvere i malfunzionamenti che non sono dovuti a problemi tecnici, eventualmente coinvolgendo l'Ente che ha rilevato il malfunzionamento e per suo tramite i suoi fornitori di servizi; i malfunzionamenti di natura infrastrutturale vengono risolti dall'Area Infrastrutture, e sicurezza; l'Unità sistemi di conservazione viene coinvolta nel caso in cui si sia verificato un malfunzionamento del software applicativo; in questo caso si attivano le procedure di manutenzione, che sono descritte nei successivi paragrafi.

[Torna al Sommario]

8.4.4 Gestione degli Incidenti di Sicurezza

Tutte le aree organizzative coinvolte nel sistema di conservazione, con il supporto del ***SOC,*** sono sistematicamente coinvolte nelle attività di prevenzione e di risoluzione degli incidenti di sicurezza, secondo le politiche definite nella *Politica sulla sicurezza SID*.

La procedura riportata nel documento "Gestione incidenti" descrive le modalità con cui vengono gestiti gli eventi che possono avere un impatto sui requisiti di *integrità, disponibilità e riservatezza* dei dati conservati o del Servizio di conservazione.

L'obiettivo della procedura viene raggiunto attraverso le seguenti attività:

- Preparazione;
- Rilevazione e Analisi;
- Contenimento, Rimozione e Ripristino;
- Attività post-incidente.

ParER ha definito le responsabilità nell'ambito della gestione degli incidenti di sicurezza.
In particolare,

- gli Enti che hanno sottoscritto un accordo di collaborazione hanno l'obbligo di notificare tempestivamente a ParER (alla casella helpdeskParER@Regione.Emila-Romagna.it) gli ***Incidenti di sicurezza (compresi i Data Breach)*** di qualsiasi natura, che coinvolgono il Sistema di conservazione, al fine di garantire l'applicazione delle contromisure adeguate. Le notifiche devono essere effettuate sulla base delle regole definite di seguito.
- ParER ha l'obbligo di
    - gestire gli incidenti di sicurezza, garantendone la tracciatura e l'applicazione di soluzioni adeguate alla riduzione degli impatti con il supporto dell'Area Infrastrutture e sicurezza;
    - notificare tempestivamente agli Enti Produttori un'incidente di sicurezza di qualsiasi natura, che coinvolga l'ambito di titolarità dell'Ente. Le notifiche devono essere effettuate sulla base delle regole definite di seguito.

Le notifiche devono essere effettuate via e-mail e contenere almeno le seguenti informazioni:

- data/ora e modalità attraverso le quali si è venuti a conoscenza dell'evento;
- causa, sistemi coinvolti, eventuali disservizi causati, utenti coinvolti, dettagli tecnici rilevanti;
- data/ora e azioni intraprese per contenere i danni causati dall'incidente e per ripristinare i sistemi;
- considerazioni sull'incidente, suggerimenti, adeguamenti da effettuare.

Nel caso in cui tutte le informazioni sopraindicate non siano immediatamente disponibili, queste saranno comunicate nel corso della gestione dell'incidente.

A fronte della richiesta da parte dell'Ente impattato da un eventuale incidente, ParER può condividere eventuali evidenze digitali o altre informazioni dopo la chiusura dell'incidente stesso attraverso opportuni canali di comunicazione.

[Torna al Sommario]

8.4.5 Evoluzione pianificata

L'evoluzione pianificata del Servizio di Conservazione segue le linee guida formulate dal Responsabile del Servizio di Conservazione, che ne stabilisce politiche, priorità e tempistiche; l'evoluzione è inquadrata nell'ambito di un piano annuale, rivisto semestralmente e articolato in progetti, ed è monitorata tramite Stati di Avanzamento Lavori (SAL) periodici, cui partecipano diversi soggetti in ragione dei diversi argomenti trattati. In particolare, si tengono SAL per l'evoluzione degli aspetti operativi del servizio, cui partecipano gli addetti alla Unità Servizi di Conservazione Digitale, SAL per l'evoluzione degli applicativi, cui partecipano, oltre ai responsabili di ParER, i responsabili dei fornitori dello sviluppo. I progetti sono gestiti tramite una pianificazione di dettaglio, che fissa tempi di realizzazione ed impiego delle risorse, con il supporto, ove applicabile, di un opportuno strumento di gestione (Redmine).

L'evoluzione dell'infrastruttura è gestita dall'Area Infrastrutture e sicurezza, in accordo con il Responsabile del Servizio di Conservazione, secondo le politiche e le procedure della Regione Emilia-Romagna.

[Torna al Sommario]

8.4.6 Richieste di Cambiamento

All'evoluzione pianificata si affiancano evoluzioni derivanti dalle necessità di migliorare l'operatività dell'esercizio, e, soprattutto per quanto riguarda il software applicativo, dalla necessità di correggere eventuali errori o imperfezioni del sistema; tali necessità vengono formalizzate come Richieste di Cambiamento, la cui gestione è descritta in dettaglio nel documento "Gestione richieste di cambiamento del Servizio di conservazione".

Le richieste di cambiamento riguardano sia cambiamenti di tipo applicativo che infrastrutturale e di configurazione. Per ogni ambito esiste un responsabile di riferimento, che costituisce il punto di raccolta delle richieste / esigenze che emergono nelle funzioni di competenza. Le richieste di cambiamento vengono valutate prima di essere autorizzate; se autorizzate, ottengono una priorità di realizzazione e vengono pianificate nell'ambito della pianificazione generale dei lavori, qualora non abbiano alta criticità; se invece rivestono carattere d'urgenza, ottengono priorità massima e risorse dedicate, fino alla soluzione; la pianificazione generale riserva normalmente una quota delle risorse per le attività correttive urgenti.

Il monitoraggio della realizzazione dei cambiamenti di una certa entità e la valutazione degli esiti è normalmente discusso nei SAL; i cambiamenti realizzati sono comunicati dai Responsabili al personale del ParER ed eventualmente agli altri soggetti coinvolti nel servizio di conservazione.

Se la richiesta di cambiamento riguarda le componenti applicative del sistema, viene attivato il processo di sviluppo del software, dalla definizione dei requisiti fino al rilascio in produzione, come descritto nei prossimi paragrafi.
La procedura di evoluzione è più snella nel caso di interventi evolutivi di minore rilevanza, quali correzioni di errori e piccole migliorie, che non richiedono la definizione di requisiti e la verifica di compatibilità tecnica; anche il test di accettazione in generale in questi casi risulta notevolmente semplificato.

ParER comunica tempestivamente agli Enti i cambiamenti che hanno impatto sul Servizio.
In particolare:

- modifiche all'infrastruttura di erogazione,
- modifiche dei referenti del Servizio,
- modifiche al processo di conservazione,

sono comunicate tramite pubblicazione sul sito web di ParER e sulla pagina dei conservatori accreditati di AgID, mentre il rilascio di nuove funzionalità viene comunicato tramite la pubblicazione delle informazioni sulle nuove ***release*** sul sistema di conservazione.

[Torna al Sommario]

8.4.7 Progettazione e Realizzazione di Software Applicativo

La procedura riportata nel documento "Progettazione e realizzazione di software applicativo del Servizio di Conservazione" descrive le modalità con cui vengono garantiti lo sviluppo del software e l'esecuzione dei test preliminari al rilascio in produzione, in accordo con tempi, risorse e modalità attuative concordate nel piano delle attività, assicurando l'allineamento con le esigenze espresse e coordinandosi con i fornitori coinvolti.

La procedura inizia con la definizione dei requisiti in accordo con l'Unità Sistemi di Conservazione, e procede poi con il test di integrazione effettuato dagli analisti funzionali e dagli analisti informatici della soluzione realizzata. Il superamento del test di integrazione produce una nuova ***release***, che viene deployata in ambiente di Test.

I test della nuova ***release*** vengono condotti nell'ambiente di Test sulla base del piano di test sotto responsabilità dell'Unità Sistemi di Conservazione con il supporto dell'Unità Servizi di Conservazione Digitale. Questi test analizzano i comportamenti globali del sistema che non è possibile osservare in riferimento al singolo modulo o componente e coprono l'intera gamma delle caratteristiche da testare (test funzionali, test di performance, test di interfaccia, test di affidabilità, test di stress, test di sicurezza).
Le diverse attività prevedono un continuo scambio di informazioni tra le diverse aree e i diversi ambiti di ParER, in particolare tra gli addetti allo sviluppo del sistema di conservazione e il personale dell'Unità Servizi di Conservazione Digitale, coinvolgendo, se necessario, l'Area Infrastrutture e sicurezza, al fine di garantire la coerenza tra i requisiti (funzionali, di sicurezza e di esercibilità) e quanto sviluppato.

Lo sviluppo del software applicativo segue le linee guida fissate dalla Regione Emilia-Romagna per lo sviluppo sicuro e le raccomandazioni degli standard di riferimento internazionali; i dettagli in merito sono riportati nel *Piano della Sicurezza* di ParER.
Lo sviluppo è supportato da strumenti di gestione dello sviluppo e di versioning del codice secondo gli standard definiti dai Sistemi Informativi della Regione Emilia-Romagna.
La tracciatura del processo di sviluppo è supportata da un opportuno strumento (Redmine), su cui sono definiti diversi workflow in ragione della problematica di sviluppo da affrontare.

Al termine del processo di sviluppo il software applicativo viene rilasciato come nuova ***release*** eventualmente deployabile in pre-produzione e produzione; il contenuto della nuova release è documentato all'interno delle Release Notes, in Redmine.

[Torna al Sommario]

8.4.8 Gestione dei Rilasci

Prima di effettuare il rilascio in preproduzione e produzione, l'Unità Sistemi di Conservazione verifica tramite sistemi automatici e controlli manuali l'eventuale obsolescenza delle librerie di componenti utilizzate nella produzione della nuova ***release***; qualora si rilevino criticità nell'ambito della sicurezza o rischi di malfunzionamenti, la nuova release non viene rilasciata, ma rimandata agli sviluppatori per l'aggiornamento dei componenti obsoleti e un nuovo system test. Se non si rilevano problemi bloccanti, l'Unità Sistemi di Conservazione concorda con l'Area Infrastrutture e sicurezza e con l'Unità Servizi di Conservazione Digitale il piano di rilascio della nuova ***release*** nell'ambiente di preproduzione e successivamente nell'ambiente di produzione, e richiede all'Area Infrastrutture e sicurezza di effettuare il rilascio.

La procedura di rilascio di una nuova ***release*** è descritta in dettaglio nel documento "Gestione dei Rilasci del Servizio di conservazione".

L'obiettivo del processo di Gestione dei rilasci viene raggiunto attraverso le seguenti attività:

- pianificare i rilasci relativi a nuove soluzioni nei diversi ambienti precedenti al passaggio in esercizio, in accordo con tempi, finestre temporali predefinite, risorse e modalità attuative concordate;
- definire e pianificare le eventuali attività formative (per utenti, personale interno) che devono accompagnare il rilascio in esercizio;
- verificare che il rilascio non abbia avuto impatti negativi sull'esercizio, e nel caso risolverli;
- coordinare i rilasci in esercizio delle nuove funzionalità, mantenendo il coordinamento e la verifica delle attività in carico all'Area Infrastrutture e sicurezza e garantendo il rispetto dei tempi pianificati.

L' Area Infrastrutture e sicurezza regionale tramite una procedura automatica provvede inoltre a installare nel sito di ***Disaster recovery*** la nuova ***release***, da attivare nel caso di dichiarazione di disastro.

[Torna al Sommario]

8.4.9 Gestione e conservazione dei Log

Tutti i log di sistema, qualunque sia lo strumento che li genera, vengono raccolti nel ***SIEM*** (ArcSight) della Regione Emilia-Romagna, dove possono essere analizzati da personale dotato delle opportune autorizzazioni, secondo quanto definito nei disciplinari regionali in materia; inoltre sono continuamente verificati dal Centro Operativo per la Sicurezza (***SOC***) nell'ambito delle attività di prevenzione e controllo delle minacce informatiche.

In base alle politiche regionali, periodicamente i log più vecchi di un anno vengono cancellati automaticamente dal sistema, sotto controllo del personale dell'Area Infrastrutture e sicurezza, in quanto si ritiene che dopo tale periodo di tempo abbiano esaurito la loro utilità.
I log sono accessibili secondo necessità solo a personale tecnico esplicitamente incaricato a tale scopo dal Responsabile del Servizio di conservazione.

Su richiesta motivata dell'Ente, i Log sono resi disponibili per la consultazione, limitatamente alle informazioni di pertinenza dell'Ente.

[Torna al Sommario]

8.5 Asset

Ai fini dell'erogazione del Servizio di conservazione sono state classificate le seguenti **tipologie di asset:**

Tipo di asset	Descrizione	Responsabile	Tipologia di dati
ASSET INFORMATIVI	pacchetti informativi versati in conservazione (SIP)	Ente produttore proprietari degli Archivi	Dati dei Produttore
	pacchetti informativi generati dal processo di conservazione (AIP e DIP)	Ente Conservatore	Dati Derivati
	evidenze di funzionamento del sistema di conservazione (log)	RER (SID)	Dati Derivati
	dati del SGI, dati di progettazione	RER (SID)	Dati di RER SID
	codice software e dati di configurazione sistemi	RER (SID)	N.A.
ASSET INFRASTRUTTURALI	asset relativi all'infrastruttura principale	RER (SID)	N.A.
	asset relativi al Servizio di DR	RER (SID)	N.A.
PERSONALE	personale archivistico, personale tecnico	RER	Dipendenti di RER /Fornitori esterni

9 MONITORAGGIO E CONTROLLI

9.1 Procedure di monitoraggio

Oltre alle funzionalità di monitoraggio applicativo gestite dal personale di ParER, che sono state illustrate al paragrafo 7.4.1, sono attive procedure di monitoraggio tecnico gestite dal personale dell'Area Infrastrutture e sicurezza, coerentemente con quanto definito nelle politiche e nei disciplinari regionali.

[Torna al Sommario]

9.2 Funzionalità per la verifica e il mantenimento dell'integrità e della consistenza degli archivi

Le procedure di monitoraggio citate nel paragrafo precedente, le politiche di conservazione dei ***backup*** e le caratteristiche delle tecnologie utilizzate garantiscono la completa *integrità* di quanto archiviato in SacER, ovvero di quanto depositato nel Data Base, nell'object storage e negli archivi su cassetta, una volta che sia stato duplicato nel sito di ***Disaster recovery*** e salvato tramite opportuno ***backup*** sia nel sito primario che nel sito di ***Disaster recovery.***

Le funzionalità messe a disposizione per realizzare le componenti logiche di Archiviazione e di Gestione dei dati consentono:

- la manutenzione e l'amministrazione del Data Base, che contiene tutti i metadati trattati nel Sistema. La gestione sistemistica del Data Base è effettuata dall'Area Infrastrutture e sicurezza tramite prodotti certificati da Oracle, ed è tracciata nel *log di sistema*. Il Data Base fornisce periodicamente informazioni statistiche utili a valutarne il dimensionamento e le performance, e quindi a pianificare attività di manutenzione del Data Base stesso e degli applicativi che lo utilizzano;
- il controllo dell'*integrità* del Data Base, che avviene utilizzando funzionalità native del Data Base stesso. Le funzionalità di ***Data Guard*** del Data Base assicurano la replica del Data Base nel sito di ***Continuità operativa*** (in maximum security) e di ***Disaster recovery*** (in maximum availability), mentre le funzionalità di Recovery Management consentono ***backup*** del Data Base completi e incrementali, a caldo e a freddo, secondo le politiche di sicurezza descritte nel Piano della Sicurezza;
- la manutenzione e l'amministrazione dell'***object storage***, che contiene tutti i ***Componenti*** (files) conservati nel Sistema, a parte i file memorizzati temporaneamente nel ***file system*** e definitivamente nello storage a cassette. Tale attività è effettuata dall'Area Infrastrutture e sicurezza tramite prodotti certificati da NetApp, ed è tracciata nel *log di sistema*. L'object storage fornisce periodicamente informazioni statistiche utili a valutarne il dimensionamento e le performance, e quindi a pianificarne le attività di manutenzione del Data Base stesso e degli applicativi che lo utilizzano;
- la congruenza delle copie dei file nei diversi siti in cui è installato l'***object storage***. La congruenza è garantita dalle caratteristiche intrinseche dell'object storage, che vengono opportunamente utilizzate dagli applicativi. Allo stesso modo è garantita dalle specifiche

dell'object storage la possibilità di aggiungere ulteriori nodi anche in altri siti, per aumentare il numero delle copie dei documenti;

- la manutenzione e l'amministrazione ai ***Componenti*** memorizzati su storage a cassette, che è effettuata dall'Area Infrastrutture e sicurezza tramite prodotti certificati da IBM, ed è tracciata nel *log di sistema;*
- l'integrità dei ***Componenti*** memorizzati su storage a cassette. L'integrità nel singolo sito è garantita dalle funzionalità intrinseche del modulo di archiving di TSM per tutti i dati archiviati su cassetta; queste funzionalità includono tra l'altro il controllo ed il riversamento periodico dei dati archiviati su nuove cassette; la congruenza tra il sito primario e il sito di ***Disaster recovery*** è invece garantita dalle logiche applicative implementate nel modulo TPI.

Per quanto riguarda l'integrità del contenuto informativo delle ***Unità Documentarie*** e in particolare dei ***Componenti***, essa è garantita dal mantenimento delle impronte dei file per tutta la vita dei pacchetti informativi.
Esistono nel sistema diversi momenti in cui le impronte vengono verificate dopo il versamento, come ad esempio la creazione dell'AIP e la copia del file dal ***Blob*** del Data Base all'***object storage***.

Inoltre, il Sistema implementa specifica funzionalità per verificare periodicamente la consistenza degli archivi conservati, controllando che tutti gli oggetti trasmessi nel Sistema nei pacchetti di versamento siano correttamente conservati negli AIP o in elaborazione per essere inseriti in nuovi AIP o negli aggiornamenti degli AIP esistenti.

Qualora, nonostante le garanzie fornite dalle tecnologie impiegate, si verificassero anomalie nell'*integrità* degli archivi, sono previste le opportune procedure applicative di ripristino illustrate nel paragrafo seguente; tali procedure sono rese possibili dalle politiche di gestione dei ***backup***, che garantiscono la manutenzione di copie integre degli archivi fino a superamento delle verifiche di *integrità* e ad adozione di procedure di ripristino.

Non sono considerati facenti parte del Sistema, e quindi non fruiscono della stessa garanzia di *integrità*, i dati in ingresso presenti su aree temporanee (spazi FTP, ***file system*** del DPI, ecc.), per i quali le procedure di soluzione di cui al paragrafo seguente prevedono la ritrasmissione nel caso di anomalie.

Il *Piano della Sicurezza* di ParER descrive le modalità con cui ParER assicura gli obiettivi di sicurezza richiesti per la conservazione a lungo termine degli archivi, dettagliando i controlli di sicurezza delle diverse componenti del sistema (organizzazione, accessi, infrastruttura, gestione dell'esercizio, gestione dello sviluppo) e le procedure adottate per garantire i back up degli archivi e il ***Disaster recovery.***

[Torna al Sommario]

9.3 Soluzioni adottate in caso di anomalie

Le anomalie vengono affrontate con diverse metodologie, secondo la natura dell'anomalia stessa e la collocazione dell'evento che le ha generate nel *processo di conservazione*; quindi, oltre alle procedure atte a garantire l'*integrità* e la consistenza degli archivi, nel senso indicato al paragrafo

precedente, esistono anche procedure atte a risolvere anomalie in altre componenti del sistema che registrano dati in SacER. Qui di seguito si trattano esclusivamente le anomalie di origine tecnica, in quanto il trattamento delle anomalie verificatesi nel processo di versamento è già stato descritto precedentemente nel paragrafo 7.4.2.

Le caratteristiche comuni e le specificità delle procedure di risoluzione delle anomalie dipendono da diversi fattori organizzativi e tecnologici, in particolare:

- tutte le funzionalità del sistema che inseriscono o modificano dati nel Data Base e file nell'area FTP o nel ***File System*** operano in modalità transazionale;
- il ***backup*** del Data Base assicura il restore all'ultima transazione completata correttamente;
- la distribuzione delle copie dell'***object storage*** sui diversi nodi ove necessario è verificata per via applicativa;
- del ***File System*** del DPI non viene effettuato backup;
- dell'Area ***FTP*** non viene effettuato backup;
- il ***File System*** di SacER è sottoposto a ***backup*** full a caldo con frequenza settimanale.

Non è quindi possibile far fronte a tutte le possibili anomalie con le stesse procedure, ma sono necessarie procedure specifiche secondo la natura dell'anomalia stessa.

La tabella seguente illustra le misure adottate per risolvere eventuali anomalie, classificate in ragione della collocazione delle informazioni nell'ambito del sistema nel momento in cui si è verificata l'anomalia:

Ambito del sistema	**Misure adottate**
File System del DPI	Si richiede la ritrasmissione dei SIP, sulla base dell'elenco fornito dalla funzione 'Recupero Studi' del DPI
Area FTP	Si eseguono opportune procedure di quadratura sia in DPI che in PING, guidati da informazioni ottenute tramite un'opportuna interrogazione del Data Base di PING; in caso si evidenzino perdite, i file perduti debbono essere ritrasmessi dal *Produttore*
Data Base	Si effettua la restore tramite le funzioni standard di Oracle dal sito primario o dal sito di ***Disaster recovery*** (nel caso di indisponibilità del DB primario)
Object Storage	Si effettua un controllo di congruenza tra Data Base e Object Storage per via applicativa, e si procede poi al recupero dei Componenti ancora presenti nei Blob temporanei del Data Base
File System di SacER	Si effettua la restore tramite le funzioni standard del file server per tutti i file inseriti nel ***file system*** fino all'ultimo back up; per i file inseriti successivamente all'ultimo back up si eseguono opportune procedure di quadratura tra Data Base e ***file system***, che provvedono a riportare il sistema in stato di congruenza. Le procedure di recupero vengono eseguite sia sul sito primario che sul secondario.
Data Base del TSM	Si effettua la restore tramite le funzioni standard di DB2 (Data Base di TSM)

[Torna al Sommario]

9.4 Verifica periodica di conformità a normativa e standard di riferimento

Il Responsabile della Funzione Archivistica di Conservazione partecipa attivamente e regolarmente alle iniziative locali e nazionali sulla conservazione digitale e in particolare ai tavoli promossi in materia da AgID e dal MiC.
Qualora siano emerse problematiche significative, provvede a diffonderle all'interno di ParER e, se lo ritiene necessario, con il supporto dell'Unità Servizi di Conservazione Digitale, anche tra gli altri attori della procedura di conservazione.
Le notizie di maggior interesse vengono anche pubblicate sul sito web di ParER.

[Torna al Sommario]

9.5 Audit e gestione delle Non Conformità

ParER effettua periodicamente audit interni sul suo Sistema di Gestione Integrato (SGI), per verificare l'efficacia di policy, procedure e documenti nel rispetto dei requisiti di:

- ISO 9001
- ISO 27001 con le estensioni ISO 27017 e ISO 27018
- ISO 37001
- Qualificazione nel Cloud Market Place di AgID.

Gli audit interni costituiscono momento fondamentale per il conseguimento e il mantenimento delle certificazioni ISO e della qualificazione.

ParER si impegna a fornire su richiesta dei propri Enti coi quali collabora (Produttori, Conservatori, Gestori) copia aggiornata delle certificazioni conseguite e della relativa documentazione.

Inoltre, ParER garantisce la disponibilità agli audit sia da parte di Organi di vigilanza sia da parte degli Enti coi quali collabora.

La procedura riportata nel documento "Gestione Audit" descrive l'insieme di attività e responsabilità legate alla pianificazione, conduzione e documentazione degli Audit del SGI.

Le eventuali non conformità rilevate nei processi di audit vengono gestite seguendo la procedura descritto nel documento "Gestione delle Non Conformità".

Lo scopo della procedura è fornire indicazioni operative per la gestione delle non conformità effettive o potenziali che, verificandosi, inficiano il buon andamento operativo del Servizio di conservazione e per l'attuazione di azioni volte a eliminare le cause delle non conformità stesse.

[Torna al Sommario]

9.6 Controlli di sicurezza

ParER dedica particolare attenzione alla sicurezza del sistema informativo utilizzato nell'ambito del *servizio di conservazione*. Le politiche e gli strumenti adottati a protezione del sistema in esercizio sono descritte nei documenti "Politica della sicurezza SID" e "Piano della Sicurezza".

La Politica sulla sicurezza è pubblicata e costantemente aggiornata da ParER sul sito web a disposizione di tutti i soggetti interessati e in particolare degli utilizzatori del Sistema di conservazione.

Il rispetto delle regole di sicurezza stabilite da ParER viene periodicamente controllato tramite opportuni test, che vengono svolti da personale esterno specializzato con cadenza periodica prestabilita o anche in maniera estemporanea, qualora il Responsabile della Sicurezza lo richieda.

Le attività relative alle verifiche tecniche e VA/PT (Vulnerability Assessment / Penetration Test) sono descritte all'interno della procedura "Gestione delle vulnerabilità", che viene implementata nell'ambito dei sistemi e degli applicativi in esercizio.

I Vulnerability Assessment sono eseguiti da laboratori (aziende esterne) in possesso di Certificato ISO 17025.

I principali obiettivi della procedura sono:

- verificare l'efficacia dei controlli e delle misure di sicurezza implementate dal ParER;
- valutare l'efficacia delle metodologie e delle soluzioni tecniche/tecnologiche adottate;
- avviare le procedure di soluzione delle vulnerabilità che sono state rilevate durante i test.

[Torna al Sommario]

10 TRATTAMENTO DEI DATI PERSONALI

Il Regolamento europeo sulla protezione dei dati personali (Regolamento (UE) 2016/679 – di seguito GDPR) ha definito le seguenti figure:

- Titolare del Trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento e i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri (art. 4, par. 1, n. 7 GDPR);
- Responsabile del trattamento: la persona fisica, giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento (art. 4, par. 1, n. 8 GDPR);
- Responsabile della Protezione dei Dati (Data Protection Officer o D.P.O.): figura prevista dagli artt. 37 e seguenti del GDPR che ne disciplinano compiti, funzioni e responsabilità.

Al Titolare del Trattamento, ai sensi dell'art. 24 del GDPR, spetta l'adozione di misure tecniche e organizzative adeguate per garantire ed essere in grado di dimostrare che il trattamento effettuato è conforme al Regolamento ed in particolare:
- gli interventi normativi necessari per l'adeguamento al GDPR;
- l'attribuzione di funzioni e compiti ai "soggetti attuatori" per gli adempimenti previsti dal GDPR.

Il Responsabile del Trattamento, ai sensi dell'art. 28 del GDPR, è soggetto esterno, con esperienza, capacità e conoscenza necessarie per mettere in atto misure tecniche e organizzative che soddisfino i requisiti del Regolamento comunitario, anche relativamente al profilo della sicurezza, il quale effettua trattamenti di dati personali per conto del Titolare sulla base di un contratto o da altro atto giuridico che determini la materia del trattamento, la durata, la finalità, le categorie di dati personali trattati, le categorie di interessati, gli obblighi e i diritti del Titolare del trattamento.

Il DPO, ai sensi dell'art. 28 del GDPR, ha il compito di sovraintendere alla gestione dei trattamenti di dati personali affinchè siano trattati nel rispetto delle normative privacy europee e nazionali e funge da punto di contatto, tramite la casella e-mail dpo@regione.emilia-romagna.it, per l'autorità di controllo.

Le competenze e le responsabilità in materia di protezione dei dati personali nell'ambito di Regione Emilia-Romagna sono definite con deliberazione della Giunta Regionale, che individua come "Titolare dei trattamenti di dati personali" la Giunta regionale stessa e come "Soggetti attuatori" i Responsabili di Settore ed i Responsabili di Area, in relazione alle attività specificatamente attribuite.

In relazione alla funzione di conservazione dei documenti informatici la tematica del trattamento dei dati personali assume due declinazioni, rispetto alle quali il Responsabile del servizio di conservazione, in quanto responsabile dell'Area sviluppo applicazioni Polo Archivistico e gestione documentale, è soggetto attuatore:

- in relazione ai dati personali degli *Utenti* del *Sistema di conservazione* (*Sacer*), trattati per consentire loro l'accesso al Sistema stesso, Regione Emilia-Romagna è titolare del trattamento;

- in relazione ai dati personali contenuti nei documenti oggetto di conservazione Regione Emilia- Romagna è designata responsabile esterno ai sensi dell'art. 28 del GDPR, con apposito atto giuridico il cui schema è approvato dalla giunta e che costituisce parte integrante e sostanziale di tutti gli accordi sottoscritti con i *Produttori*. Detto atto giuridico dispone, tra il resto, che agli eventuali "sub-responsabili" vengano imposte condizioni vincolanti in materia di trattamento dei dati personali non meno onerose di quelle contenute negli Accordi sottoscritti con i *Produttori*. I contratti con le nomine del responsabile del trattamento degli eventuali sub-responsabili del ParER sono accessibili ai *Produttori* su richiesta, mentre i riferimenti degli atti relativi risultano disponibili nel sito della Regione Emilia-Romagna, nell'area Amministrazione trasparente, nella sezione relativa a Bandi di gara e contratti.

Il Responsabile del servizio di conservazione, in quanto responsabile dell'Area sviluppo applicazioni, Polo Archivistico e gestione documentale, è soggetto attuatore in relazione agli adempimenti previsti dalla normativa in materia di protezione dei dati personali, e svolge, tra gli altri compiti, la verifica della legittimità dei trattamenti, le azioni in collaborazione con il DPO al fine di consentire allo stesso l'esecuzione dei compiti e delle funzioni assegnate, la designazione degli amministratori di sistema e la predisposizione della Valutazione di Impatto sulla Protezione dei Dati (DPIA).
L'articolo 35, paragrafo 1, del GDPR prevede che il processo della Valutazione di Impatto sulla Protezione dei Dati (DPIA) sia obbligatorio quando un trattamento di dati personali "*presenti un rischio elevato per i diritti e le libertà delle persone fisiche*"; il soggetto obbligato ad effettuare una DPIA è il titolare del trattamento (nel processo di conservazione quindi il *Produttore*), con il supporto del Responsabile della protezione dei dati (DPO - *Data Protection Officer*), se nominato, e del Responsabile del trattamento eventualmente coinvolto.
Considerando la dimensione e la criticità dei documenti conservati, ParER, benché non Titolare, ma Responsabile esterno del trattamento, ha comunque ritenuto opportuno effettuare la DPIA sul trattamento "*Gestione dei dati e dei documenti trasmessi dagli Enti produttori al sistema di conservazione del ParER, ai fini del corretto svolgimento del processo di conservazione (trattamento effettuato nel pubblico interesse)",* identificando le misure opportune per la mitigazione del rischio di violazione dei dati personali con il supporto del DPO della Regione Emilia-Romagna.

[Torna al Sommario]

11 DOCUMENTI DI RIFERIMENTO E ALLEGATI

Si riporta l'elenco dei documenti citati nel presente Manuale con indicazione della collocazione in cui sono rintracciabili.

Documento	**Collocazione**
Politica della qualità SID	*pubblicata nel sito di ParER: https://poloarchivistico.regione.emilia-romagna.it, in "Documentazione"*
Modelli dei SIP (Linee guida per la realizzazione dei SIP)	*Repository Regionale*
Modelli dei pacchetti di archiviazione (AIP)	*pubblicata nel sito di ParER: https://poloarchivistico.regione.emilia-romagna.it, in "Documentazione"*
Specifiche tecniche dei servizi di versamento	*pubblicata nel sito di ParER: https://poloarchivistico.regione.emilia-romagna.it, in "Documentazione"*
Specifiche tecniche dei servizi di recupero	*pubblicata nel sito di ParER: https://poloarchivistico.regione.emilia-romagna.it t, in "Documentazione"*
Politica della sicurezza SID	*pubblicata nel sito di ParER: https://poloarchivistico.regione.emilia-romagna.it, in "Documentazione*
Piano della Sicurezza	*Repository Regionale*
Piano di Continuità Operativa del Servizio di conservazione	*Repository Regionale*
DPIA	*Repository Regionale*
Procedura di gestione degli incidenti di sicurezza e Data Breach	*Repository Regionale*
Procedura di gestione richieste di cambiamento del Servizio di conservazione	*Repository Regionale*
Procedura di progettazione e realizzazione di software applicativo del Servizio di conservazione	*Repository Regionale*
Procedura di gestione dei rilasci del Servizio di conservazione	*Repository Regionale*
Procedura di gestione Audit	*Repository Regionale*
Procedura di gestione delle Non Conformità	*Repository Regionale*
Procedura di gestione delle vulnerabilità	*Repository Regionale*
Registro dei formati	*SacER*
Gestione utenze del Sistema Applicativo di conservazione	*Repository Regionale*
Procedura di cessazione del Servizio	*Repository Regionale*

Documento	Collocazione
restituzione dell'archivio	
Gestione di richieste di informazioni, reclami e segnalazioni	*Repository Regionale*

Si riporta l'elenco dei documenti allegati al presente Manuale:

- **Allegato 1 "Normativa e standard di riferimento"**
- **Allegato 2 "Registro dei responsabili"**

[Torna al Sommario]

AGID | Agenzia per l'Italia Digitale

Linee Guida sulla formazione, gestione e conservazione dei documenti informatici

Maggio 2021

AGID | via Liszt, 21 – 00144 Roma | protocollo@pec.agid.gov.it | www.agid.gov.it | tel. 06 85264.1

Presidenza del Consiglio dei Ministri

Sommario

Questo documento raccoglie il testo delle linee guida sulla *Formazione, gestione e conservazione dei documenti informatici*.

CAPITOLO 1 Introduzione, strumenti di lettura e disposizioni comuni

1.1. Scopo del documento

Lo scopo delle presenti linee guida è duplice:

a) aggiornare le attuali regole tecniche in base all'art. 71 del Codice dell'amministrazione digitale[1] (da ora in avanti CAD), concernenti la formazione, protocollazione, gestione e conservazione dei documenti informatici;

b) incorporare in un'unica linea guida le regole tecniche e le circolari in materia, addivenendo ad un "unicum" normativo che disciplini gli ambiti sopracitati, nel rispetto della disciplina in materia di Beni culturali.

1.2. Ambito soggettivo di applicazione

Le presenti Linee Guida sono applicabili ai soggetti indicati nell'art. 2 commi 2 e 3 del CAD[2], fatti salvi gli specifici riferimenti alla Pubblica Amministrazione.

[1] L'art. 71, comma 1, del CAD prevede che "L'AgID, previa consultazione pubblica da svolgersi entro il termine di trenta giorni, sentiti le amministrazioni competenti e il Garante per la protezione dei dati personali nelle materie di competenza, nonché acquisito il parere della Conferenza unificata, adotta Linee guida contenenti le regole tecniche e di indirizzo per l'attuazione del presente Codice".

[2] L'art. 2, comma 2, del CAD prevede che le disposizioni del Codice si applicano:
"a) alle pubbliche amministrazioni di cui all'articolo 1, comma 2, del decreto legislativo 30 marzo 2001, n. 165, nel rispetto del riparto di competenza di cui all'articolo 117 della Costituzione, ivi comprese le autorità di sistema portuale, nonché alle autorità amministrative indipendenti di garanzia, vigilanza e regolazione;
b) ai gestori di servizi pubblici, ivi comprese le società quotate, in relazione ai servizi di pubblico interesse;
c) alle società a controllo pubblico, come definite nel decreto legislativo 19 agosto 2016, n. 175, escluse le società quotate di cui all'articolo 2, comma 1, lettera p), del medesimo decreto che non rientrino nella categoria di cui alla lettera b)".
Il successivo comma 3 prevede che le disposizioni del Codice e le relative Linee guida "concernenti il documento informatico, le firme elettroniche e i servizi fiduciari di cui al Capo II, la riproduzione e conservazione dei documenti di cui agli articoli 43 e 44, il domicilio digitale e le comunicazioni elettroniche di cui all'articolo 3-bis e al Capo IV, l'identità digitale di cui agli articoli 3-bis e 64 si applicano anche ai privati, ove non diversamente previsto".

1.3. Ambito oggettivo di applicazione

Le presenti Linee Guida contengono le regole tecniche sugli ambiti disciplinati dalle seguenti disposizioni del CAD:

- Art. 20, *Validità ed efficacia probatoria dei documenti informatici*, fatte salve le norme in materia di generazione, apposizione e verifica di qualsiasi tipo di firma elettronica
- Art. 21, *Ulteriori disposizioni relative ai documenti informatici, sottoscritti con firma elettronica avanzata, qualificata o digitale*
- Art. 22, commi 2 e 3, *Copie informatiche di documenti analogici*
- Art. 23, *Copie analogiche di documenti informatici*
- Art. 23-bis, *Duplicati e copie informatiche di documenti informatici*
- Art. 23-ter, *Documenti amministrativi informatici*
- Art. 23-quater, *Riproduzioni informatiche*
- Art. 34, *Norme particolari per le Pubbliche Amministrazioni*
- Art. 40, *Formazione di documenti informatici*
- Art. 40-bis, *Protocollo informatico*
- Art. 41, *Procedimento e fascicolo informatico*
- Art. 42, *Dematerializzazione dei documenti delle Pubbliche Amministrazioni*
- Art. 43, *Conservazione ed esibizione dei documenti*
- Art. 44, *Requisiti per la conservazione dei documenti informatici*
- Art. 45, *Valore giuridico della trasmissione*
- Art. 46, *Dati particolari contenuti nei documenti trasmessi*
- Art. 47, *Trasmissione dei documenti tra le Pubbliche Amministrazioni*
- Art. 49, *Segretezza della corrispondenza trasmessa per via telematica*
- Art. 50, *Disponibilità dei dati delle Pubbliche Amministrazioni*
- Art. 51, *Sicurezza e disponibilità dei dati, dei sistemi e delle infrastrutture delle Pubbliche Amministrazioni*
- Art. 64-bis, *Accesso telematico ai servizi della Pubblica Amministrazione*
- Art. 65, *Istanze e dichiarazioni presentate alle Pubbliche Amministrazioni per via telematica*

1.4. Abrogazioni e norme transitorie

Le presenti Linee Guida entrano in vigore il giorno successivo a quello della loro pubblicazione sul sito istituzionale di AGID, di cui si darà notizia sulla Gazzetta Ufficiale.

Esse si applicano a partire dal duecento settantesimo giorno successivo alla loro entrata in vigore.

A partire da questo termine i soggetti di cui all' art. 2 commi 2 e 3 del CAD formano i loro documenti esclusivamente in conformità alle presenti Linee Guida.

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

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

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

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

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

1.5. Principali riferimenti normativi

I principali riferimenti normativi presi in considerazione ai fini della redazione delle presenti Linee Guida sono i seguenti:

a) RD 1163/1911, *Regolamento per gli archivi di Stato*;
b) DPR 1409/1963, *Norme relative all'ordinamento ed al personale degli archivi di Stato*;
c) Legge 241/1990, *Nuove norme sul procedimento amministrativo*;
d) DPR 445/2000, *Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa*;
e) DPR 37/2001, *Regolamento di semplificazione dei procedimenti di costituzione e rinnovo delle Commissioni di sorveglianza sugli archivi e per lo scarto dei documenti degli uffici dello Stato*;
f) D.lgs 196/2003 *recante il Codice in materia di protezione dei dati personali*;
g) D.lgs 42/2004, *Codice dei beni culturali e del paesaggio, ai sensi dell'articolo 10 della legge 6 luglio 2002, n. 137*;
h) Legge 9 gennaio 2004, n. 4 aggiornata dal decreto legislativo 10 agosto 2018, n. 106, *Disposizioni per favorire e semplificare l'accesso degli utenti e, in particolare, delle persone con disabilità agli strumenti informatici;*
i) D.lgs 82/2005 e ss.mm.ii., *Codice dell'amministrazione digitale*;
j) D.lgs 33/2013, *Riordino della disciplina riguardante il diritto di accesso civico e gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni*;
k) DPCM 22 febbraio 2013, *Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali, ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma 3, lettera b), 35, comma 2, 36, comma 2, e 71*;
l) DPCM 21 marzo 2013, *Individuazione di particolari tipologie di documenti analogici originali unici per le quali, in ragione di esigenze di natura pubblicistica, permane l'obbligo della conservazione dell'originale analogico oppure, in caso di conservazione sostitutiva, la loro conformità all'originale deve essere autenticata da un notaio o da altro pubblico ufficiale a ciò autorizzato con dichiarazione da questi firmata digitalmente*

ed allegata al documento informatico, ai sensi dell'art. 22, comma 5, del Codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82 e successive modificazioni;

n) Reg. UE 910/2014, *in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE - Regolamento eIDAS*;
o) Circolare 40 e 41 del 14 dicembre 2015 della Direzione generale degli archivi, *Autorizzazione alla distruzione di originali analogici riprodotti secondo le regole tecniche di cui al DPCM 13.11.2014 e conservati secondo le regole tecniche di cui al DPCM 13.12.2013*;
p) Reg. UE 679/2016 (GDPR), *relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE*;
q) Circolare 18 aprile 2017, n. 2/2017 dell'Agenzia per l'Italia Digitale*, recante le misure minime di sicurezza ICT per le pubbliche amministrazioni*;
r) Circolare n. 2 del 9 aprile 2018, *recante i criteri per la qualificazione dei Cloud Service Provider per la PA;*
s) Circolare n. 3 del 9 aprile 2018, *recante i criteri per la qualificazione di servizi SaaS per il Cloud della PA*;
t) Reg. UE 2018/1807, *relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea;*
u) DPCM 19 giugno 2019, n. 76, *Regolamento di organizzazione del Ministero per i beni e le attività culturali, degli uffici di diretta collaborazione del Ministro e dell'Organismo indipendente di valutazione della performance*.

1.6. Linee guida AGID richiamate

a) Linee guida del 15 aprile 2019 *dell'indice dei domicili digitali delle pubbliche amministrazioni e dei gestori di pubblici servizi*;
b) Linee guida del 6 giugno 2019 *contenenti le Regole Tecniche e Raccomandazioni afferenti la generazione di certificati elettronici qualificati, firme e sigilli elettronici qualificati e validazioni temporali elettroniche qualificate*.
c) Linee guida del 09/01/2020 *sull'Accessibilità degli strumenti informatici*.

1.7. Gruppo di lavoro

Il presente documento è stato redatto dal Tavolo di lavoro dell'Agenzia per l'Italia Digitale, istituito con determinazione del Direttore Generale n. 137 del 2 maggio 2018. Al Tavolo di lavoro, coordinato da Patrizia Gentili, hanno partecipato Alessandra Antolini, Gaetano Bruno, Matteo Carabellese, Antonio Florio, Enrica Massella Ducci Teri, Guido Pera, Vincenzo Travascio, Cristina Valiante. A titolo di esperti hanno partecipato inoltre Walter Arrighetti, Pietro Falletta Giacomo Massi e Luigi Avena, sentito anche il MIC come da art. 23 ter comma 4 del CAD[3].

[3] L'art. 23 ter comma 4 del CAD prevede che "In materia di formazione e conservazione di documenti informatici delle pubbliche amministrazioni, le Linee guida sono definite anche sentito il Ministero dei beni e delle attività culturali e del turismo".

1.8. Allegati

Costituiscono parte integrante delle presenti Linee Guida i seguenti allegati:

1. Glossario dei termini e degli acronimi
2. Formati di file e riversamento
3. Certificazione di processo
4. Standard e specifiche tecniche
5. Metadati
6. Comunicazione tra AOO di Documenti Amministrativi Protocollati, che sostituisce la circolare 60/2013 dell'AgID.

1.9. Premessa metodologica

Le presenti linee guida costituiscono la nuova versione aggiornata delle regole tecniche in materia di formazione, protocollazione, gestione e conservazione del documento, già precedentemente regolate nei DPCM del 2013 e 2014. Obiettivo generale del documento è che la gestione complessiva del documento informatico risulti semplificata attraverso una visione d'insieme che aggrega in un "corpo unico" materie prima disciplinate separatamente.

L'approccio utilizzato è di tipo olistico, ossia diretto a mettere in evidenza e a rappresentare le interdipendenze funzionali tra le varie fasi della gestione documentale dal momento della formazione fino alla selezione per lo scarto o la conservazione permanente.

La tecnica redazionale – stante la natura prescrittiva del testo - ha privilegiato uno stile chiaro e fruibile per il lettore, indipendentemente dalla natura pubblica o privata di quest'ultimo e dalle sue competenze in materia.

Considerata la velocità dell'innovazione, le linee guida devono garantire un adattamento costante ai cambiamenti imposti dall'incessante rivoluzione digitale. Di qui la scelta di prevedere un testo "statico" che contenga la base normativa della materia e una serie di "allegati" i cui contenuti più "flessibili" potranno adeguarsi agevolmente all'evoluzione tecnologica. Tale processo di costante adeguamento degli "allegati" è realizzato in coerenza con il quadro normativo e attuativo in materia di digitalizzazione. Relativamente ai temi della trasmissione di contenuti digitali tra e con le pubbliche amministrazioni si assicura la conformità al Modello di interoperabilità definito da AgID e alle tecnologie introdotte dallo stesso.

1.10. Natura vincolante delle Linee Guida

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

Ne deriva che, nella gerarchia delle fonti, anche le presenti Linee Guida sono inquadrate come un atto di regolamentazione, seppur di natura tecnica, con la conseguenza che esse sono pienamente azionabili davanti al giudice amministrativo in caso di violazione delle prescrizioni ivi contenute. Nelle ipotesi in cui la violazione sia posta in essere da parte dei soggetti di cui all'art. 2, comma 2 del CAD, è altresì possibile presentare apposita segnalazione al difensore civico, ai sensi dell'art. 17 del CAD[4].

1.11. Principi generali della gestione documentale

La gestione documentale è un processo che può essere suddiviso in tre fasi principali: formazione, gestione e conservazione. Nell'ambito di ognuna delle suddette fasi si svolgono una serie di attività che si distinguono per complessità, impatto, natura, finalità e/o effetto, anche giuridico, alle quali corrispondono approcci metodologici e prassi operative distinte.

Il sistema di gestione informatico dei documenti, la cui tenuta può anche essere delegata a terzi, affinché possa essere efficiente e sicuro deve essere necessariamente presidiato da specifiche procedure e strumenti informatici, in grado di governare con efficacia ogni singolo accadimento che coinvolge la vita del documento ed effettuata secondo i principi generali applicabili in materia di trattamento dei dati personali anche mediante un'adeguata analisi del rischio.

Una corretta gestione dei documenti sin dalla loro fase di formazione rappresenta inoltre la migliore garanzia per il corretto adempimento degli obblighi di natura amministrativa, giuridica e archivistica tipici della gestione degli archivi pubblici.

Dal punto di vista archivistico, si distinguono tradizionalmente tre fasi di gestione in ragione delle diverse modalità di organizzazione ed utilizzo dei documenti:

- archivio corrente: riguarda i documenti necessari alle attività correnti;
- archivio di deposito: riguarda i documenti ancora utili per finalità amministrative o giuridiche, ma non più indispensabili per la trattazione delle attività correnti;
- archivio storico: riguarda i documenti storici selezionati per la conservazione permanente.

Nella fase di formazione devono essere perseguiti obiettivi di qualità, efficienza, razionalità, sistematicità, accessibilità e coerenza alle regole tecniche che presidiano la formazione dei documenti

[4] L'art. 17 comma 1-quater del CAD prevede che "È istituito presso l'AgID l'ufficio del difensore civico per il digitale, a cui è preposto un soggetto in possesso di adeguati requisiti di terzietà, autonomia e imparzialità. Chiunque può presentare al difensore civico per il digitale, attraverso apposita area presente sul sito istituzionale dell'AgID, segnalazioni relative a presunte violazioni del presente Codice e di ogni altra norma in materia di digitalizzazione ed innovazione della pubblica amministrazione da parte dei soggetti di cui all'articolo 2, comma 2. Ricevuta la segnalazione, il difensore civico, se la ritiene fondata, invita il soggetto responsabile della violazione a porvi rimedio tempestivamente e comunque non oltre trenta giorni".

informatici, tenendo in debito conto le esigenze e i bisogni pratici del lavoro quotidiano. Al tal fine, risulta decisivo avvalersi di un valido e completo manuale di gestione documentale, di workflow documentali e sistemi di Document & Content Management e di applicativi informatici, per la PA ai sensi degli articoli 68[5] e 69[6] del CAD, che si basino su elevati livelli di automazione ed interoperabilità in grado di operare nel web. In un contesto in continua trasformazione, il manuale di gestione documentale deve essere sottoposto a continuo aggiornamento, in ragione dell'evoluzione tecnologica e dell'obsolescenza degli oggetti e degli strumenti digitali utilizzati. Allo stesso modo, anche i processi e le attività che governano la fase di formazione dei documenti informatici devono essere sottoposti ad un costante lavoro di valutazione, monitoraggio, ri-progettazione e reingegnerizzazione. L'adozione del manuale di gestione documentale e del manuale di conservazione non risponde solo ad esigenze pratico-operative, ma rappresenta un preciso obbligo come specificato ai paragrafi 3.5 e 4.7, al quale per la PA fa seguito l'ulteriore obbligo della loro pubblicazione sul sito istituzionale dell'ente.

La gestione dei documenti informatici prosegue con il suo trasferimento in un sistema di conservazione da realizzarsi in ottemperanza a quanto disposto dal CAD e dalle presenti Linee guida.

La conservazione dei documenti è tipicamente svolta all'interno di un sistema di conservazione dedicato a questa funzione.

Tuttavia, l'attenzione al profilo conservativo deve essere posta fin dal momento della formazione del documento, al fine di garantirne la tenuta all'interno del sistema di gestione informatica dei documenti e di eventuale conservazione a lungo termine all'interno di sistemi dedicati.

Nell'ambito della gestione documentale possono essere necessarie attività di riversamento dei documenti in altro formato diverso da quello originale, come specificato al paragrafo 3.7. Tale riversamento può avvenire più volte nella gestione del documento informatico e in diversi momenti per finalità gestionali o conservative.

In ambito digitale, infine, gli obblighi di pubblicazione di atti e provvedimenti amministrativi aventi effetto di pubblicità legale o comunque derivanti dalla normativa in materia di trasparenza devono essere assolti con la pubblicazione nei rispettivi siti web istituzionali. Affinché il processo di pubblicazione on line possa generare un prodotto atto ad assolvere i predetti obblighi è necessario che esso garantisca la conformità di quanto pubblicato all'originale, l'autorevolezza dell'ente emanatore e del sito web, la validità giuridica dei documenti e quindi la loro veridicità, efficacia e perdurabilità nel tempo.

---

[5] L'art. 68 del CAD prevede che "Le pubbliche amministrazioni acquisiscono programmi informatici o parti di essi nel rispetto dei principi di economicità e di efficienza, tutela degli investimenti, riuso e neutralità tecnologica, a seguito di una valutazione comparativa di tipo tecnico ed economico tra le seguenti soluzioni disponibili sul mercato:
a) software sviluppato per conto della pubblica amministrazione;
b) riutilizzo di software o parti di esso sviluppati per conto della pubblica amministrazione;
c) software libero o a codice sorgente aperto;
d) software fruibile in modalità cloud computing;
e) software di tipo proprietario mediante ricorso a licenza d'uso;
f) software combinazione delle precedenti soluzioni".

[6] L'art. 69 del CAD prevede che "Le pubbliche amministrazioni che siano titolari di soluzioni e programmi informatici realizzati su specifiche indicazioni del committente pubblico, hanno l'obbligo di rendere disponibile il relativo codice sorgente, completo della documentazione e rilasciato in repertorio pubblico sotto licenza aperta, in uso gratuito ad altre pubbliche amministrazioni o ai soggetti giuridici che intendano adattarli alle proprie esigenze, salvo motivate ragioni di ordine e sicurezza pubblica, difesa nazionale e consultazioni elettorali".

CAPITOLO 2 Formazione dei documenti informatici

2.1. Documento informatico

2.1.1. Formazione del documento informatico

Il contenuto del presente capitolo si applica, salvo ove diversamente specificato, ai soggetti di cui all'art. 2 commi 2 e 3 del CAD.

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[7], 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.

[7]Si fa riferimento ai soggetti di cui all'art. 2 comma 2, lettera a) del CAD.

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

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

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

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

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

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

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

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

La disponibilità e la riservatezza delle informazioni contenute nel documento informatico sono garantite attraverso l'adozione di specifiche politiche e procedure predeterminate dall'ente, in

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

2.2. Copie per immagine su supporto informatico di documenti analogici

La copia per immagine su supporto informatico di un documento analogico è prodotta mediante processi e strumenti che assicurino che il documento informatico abbia 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 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".

Fermo restando quanto previsto dall'art. 22 comma 3 del CAD[8] nel caso in cui non vi è 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 1bis, 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[9].

---

[8] L'art. 22 comma 4 del CAD prevede "Le copie per immagine su supporto informatico di documenti originali formati in origine su supporto analogico nel rispetto delle regole tecniche di cui all'articolo 71 hanno la stessa efficacia probatoria degli originali da cui sono tratte se la loro conformità all'originale non è espressamente disconosciuta."

[9] L'art. 22 commi 4 e 5 del CAD prevedono "4. Le copie formate ai sensi dei commi 1, 1 bis, 2 e 3 sostituiscono ad ogni effetto di legge gli originali formati in origine su supporto analogico, e sono idonee ad assolve-re gli obblighi di conservazione previsti dalla legge, salvo quanto stabilito dal comma 5.

5.Con decreto del Presidente del Consiglio dei Ministri possono essere individuate 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."

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

- raffronto dei documenti;
- certificazione di processo.

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

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

Fatto salvo quanto previsto dall'art. 23bis comma 2 del CAD[10] nel caso in cui non vi è l'attestazione di un pubblico ufficiale, la conformità della copia o dell'estratto informatico ad un documento informatico è garantita mediante l'apposizione della firma digitale o firma elettronica qualificata o firma elettronica avanzata, nonché del sigillo elettronico qualificato e avanzato da parte di chi effettua il raffronto.

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

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

2.4. Il documento amministrativo informatico

2.4.1. Formazione del documento amministrativo informatico

Al documento amministrativo informatico si applicano le stesse regole valide per il documento informatico, salvo quanto specificato nel presente paragrafo.

La Pubblica Amministrazione forma gli originali dei propri documenti attraverso gli strumenti informatici riportati nel manuale di gestione documentale oppure acquisendo le istanze, le dichiarazioni e le comunicazioni di cui agli articoli 5 -bis[11], 40 -bis[12] e 65[13] del CAD.

Il documento amministrativo informatico è identificato e trattato nel sistema di gestione informatica dei documenti con le modalità descritte nel manuale di gestione documentale.

Le istanze, le dichiarazioni e le comunicazioni di cui agli articoli 5-bis, 40-bis e 65 del CAD sono identificate e trattate come i documenti amministrativi informatici. Se soggette a norme specifiche che prevedono la sola tenuta di estratti per riassunto sono memorizzate in specifici archivi informatici dettagliatamente descritti nel manuale di gestione documentale.

Il documento amministrativo informatico assume le caratteristiche di immodificabilità e di integrità, oltre che con le modalità di cui al paragrafo 2.1.1, 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 con le modalità descritte nel manuale di gestione documentale.

Al documento amministrativo informatico viene associato l'insieme dei metadati previsti per la registrazione di protocollo ai sensi dell'art 53 del TUDA[14], nonché i metadati relativi alla

[11] L'art. 5-bis, comma 1, del CAD prevede che "La presentazione di istanze, dichiarazioni, dati e lo scambio di informazioni e documenti, anche a fini statistici, tra le imprese e le amministrazioni pubbliche avviene esclusivamente utilizzando le tecnologie dell'informazione e della comunicazione. Con le medesime modalità le amministrazioni pubbliche adottano e comunicano atti e provvedimenti amministrativi nei confronti delle imprese".

[12] L'art. 40-bis del CAD prevede che "Formano comunque oggetto di registrazione di protocollo ai sensi dell'articolo 53 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, le comunicazioni che provengono da o sono inviate a domicili digitali eletti ai sensi di quanto previsto all'articolo 3-bis, nonché le istanze e le dichiarazioni di cui all'articolo 65 in conformità alle regole tecniche di cui all'articolo 71".

[13] L'art. 65 del CAD disciplina "Le istanze e le dichiarazioni presentate per via telematica alle pubbliche amministrazioni e ai gestori dei servizi pubblici".

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

classificazione, ai sensi dell'articolo 56 del TUDA[15], 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 presenti Linee guida.

Sarà cura dell'Amministrazione individuare ulteriori metadati (ad es. metadati relativi al Registro giornaliero di protocollo ecc.) da associare a particolari tipologie di documenti amministrativi informatici. A tal proposito si ricorda che nel manuale di gestione devono essere riportati i metadati definiti per ogni tipologia di documento.

Sono inclusi i documenti soggetti a registrazione particolare, come identificati nel manuale di gestione documentale, 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[16], i documenti amministrativi informatici devono essere accessibili secondo le regole previste dall'art. 11 della legge n. 4/2004.

2.5. Copie su supporto informatico di documenti amministrativi analogici

Alle copie su supporto informatico di documenti amministrativi analogici si applicano le disposizioni di cui al paragrafo 2.2.

L'attestazione di conformità della copia informatica di un documento amministrativo analogico, formato dalla Pubblica Amministrazione, ovvero da essa detenuto, può essere inserita nel documento informatico contenente la copia informatica o essere prodotta come documento informatico separato contenente un riferimento temporale e l'impronta di ogni copia per immagine. Il documento informatico contenente l'attestazione è sottoscritto con firma digitale o con firma elettronica qualificata o avanzata del funzionario delegato.

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

[16] L'art. 23-ter comma 5-bis prevede che "I documenti di cui al presente articolo devono essere fruibili indipendentemente dalla condizione di disabilità personale, applicando i criteri di accessibilità definiti dai requisiti tecnici di cui all'articolo 11 della legge 9 gennaio 2004, n. 4".

CAPITOLO 3 Gestione documentale

3.1. Registrazione informatica dei documenti

3.1.1. Ambito di applicazione

Il presente capitolo individua le regole tecniche, i criteri e le specifiche delle informazioni previste nelle operazioni di registrazione e segnatura di protocollo, di cui agli articoli da 50 a 57 e da 61 a 66 del TUDA[17].

Il presente capitolo stabilisce inoltre le regole tecniche, i criteri e le specifiche delle informazioni previste nelle operazioni di registrazione e segnatura di protocollo di cui agli articoli 40-bis, 41 e 47 del CAD[18].

3.1.2. Adeguamento organizzativo e funzionale

Le Pubbliche Amministrazioni, nell'ambito del proprio ordinamento, provvedono a:

A. individuare le aree organizzative omogenee (di seguito AOO) e i relativi uffici di riferimento ai sensi dell'art. 50, comma 4, del TUDA[19];

B. nominare, in ciascuna delle AOO, il responsabile della gestione documentale e un suo vicario, in possesso di idonee competenze giuridiche, informatiche ed archivistiche;

[17] Gli articoli da 50 a 57 e da 61 a 66 del TUDA sono compresi nel Capo IV "Sistemi di gestione informatica del documento".
[18] Gli articoli 40-bis, 41 e 47 del CAD disciplinano, rispettivamente, in materia di protocollo informatico, procedimento e fascicolo informatico, trasmissione dei documenti tra le pubbliche amministrazioni.
[19] L'art. 50, comma 4, del TUDA prevede che "Ciascuna amministrazione individua, nell'ambito del proprio ordinamento, gli uffici da considerare ai fini della gestione unica o coordinata dei documenti per grandi aree organizzative omogenee, assicurando criteri uniformi di classificazione e archiviazione, nonché di comunicazione interna tra le aree stesse".

C. per le amministrazioni con più AOO, nominare il coordinatore della gestione documentale e un suo vicario, in possesso di idonee competenze giuridiche, informatiche ed archivistiche;

D. adottare per ogni AOO il manuale di gestione documentale, su proposta del responsabile della gestione documentale oppure, ove nominato, dal coordinatore della gestione documentale.

Secondo quanto previsto dal CAD e dalle Linee guida AGID del 15 aprile 2019[20], l'Indice dei domicili digitali delle Pubbliche Amministrazioni e dei gestori di pubblici servizi, di seguito indicato con l'acronimo IPA, include, tra gli indirizzi telematici degli Enti ivi iscritti, il domicilio digitale da cui provengono, o sono inviate, comunicazioni, istanze, dichiarazioni e notifiche che formano oggetto di registrazione di protocollo.

3.1.3. Registrazione di protocollo e altre forme di registrazione

La registrazione informatica dei documenti è rappresentata dall'insieme di dati in forma elettronica allegati o connessi al documento informatico al fine dell'identificazione univoca di tutti i documenti prodotti e acquisiti. Per la Pubblica Amministrazione vale quanto disposto ai sensi dell'articolo 53 comma 5 del TUDA[21].

Al termine della registrazione, il documento è identificato da un insieme di dati in forma elettronica che può includere sin da questa fase la classificazione e si integra con il piano di organizzazione delle aggregazioni documentali, definito dal Responsabile della gestione documentale di cui al paragrafo 3.4, nell'ambito del manuale di gestione.

La Pubblica Amministrazione, al fine di dare attuazione alle disposizioni introdotte dal CAD stesso in materia di sistema di gestione informatica dei documenti realizza le funzionalità di gestione dell'archivio corrente, dell'archivio di deposito, dei flussi documentali, automatizzazione dei procedimenti amministrativi sulla base dei propri obiettivi di miglioramento dei servizi e di incremento dell'efficienza operativa, tenuto conto del rapporto costi e benefici, nel rispetto degli articoli 53 e 55 del TUDA[22] e dei requisiti del sistema di gestione informatica dei documenti e dei flussi documentali" definiti negli articoli 52, 65 e 67 del TUDA[23], applicando ove possibile i requisiti fissati per la registrazione di protocollo anche alle altre forme di registrazione informatica dei documenti, fatto salvo quanto disposto per esse da eventuali norme vigenti".

---

[20] Linee Guida dell'Indice dei domicili digitali delle pubbliche amministrazioni e dei gestori di pubblici servizi.

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

[22] Gli articoli 53 e 55 del TUDA disciplinano, rispettivamente, in materia di registrazioni di protocollo e segnatura di protocollo.

[23] Gli articoli 52, 65 e 67 del TUDA disciplinano, rispettivamente, in materia di sistema di gestione informatica dei documenti, requisiti del sistema per la gestione dei flussi documentali e trasferimento dei documenti all'archivio di deposito.

3.1.4. Formato della registrazione e della segnatura di protocollo

La registrazione di protocollo è l'insieme dei metadati che il registro di protocollo deve memorizzare, per tutti i documenti ricevuti o spediti dalla Pubblica Amministrazione e per tutti i documenti informatici che non rientrano tra le tipologie specificate dall'art. 53, comma 5 del TUDA[24] e che non sono oggetto di registrazione particolare da parte dell'amministrazione, al fine di garantirne l'identificazione univoca e certa. In merito, l'articolo 53, comma 1, del TUDA indica le informazioni che caratterizzano il registro di protocollo[25], a cui si aggiungono le informazioni inerenti l'assegnazione interna all'amministrazione e la eventuale classificazione.

La segnatura di protocollo è l'associazione ai documenti amministrativi informatici in forma permanente e non modificabile di informazioni riguardanti i documenti stessi, in ingresso e in uscita al sistema di protocollo, utile alla sua identificazione univoca e certa.

In merito l'articolo 55, comma 1, del TUDA individua le informazioni che caratterizzano la segnatura di protocollo[26].

Le operazioni di segnatura e registrazione di protocollo sono effettuate contemporaneamente.

Gli "standard, le modalità di trasmissione, il formato e le definizioni dei tipi di informazioni minime ed accessorie comunemente scambiate tra le Pubbliche Amministrazioni e associate ai documenti protocollati" sono definiti nell'allegato 6 "Comunicazione tra AOO di Documenti Amministrativi Protocollati".

---

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

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

[26] L'art. 55, comma 1, del TUDA prevede che: "La segnatura di protocollo è l'apposizione o l'associazione all'originale del documento, in forma permanente non modificabile, delle informazioni riguardanti il documento stesso. Essa consente di individuare ciascun documento in modo inequivocabile. Le informazioni minime previste sono:
a) il progressivo di protocollo, secondo il formato disciplinato all'articolo 57;
b) la data di protocollo;
c) l'identificazione in forma sintetica dell'amministrazione o dell'area organizzativa individuata ai sensi dell'articolo 50, comma 4".

3.1.5. Annullamento delle informazioni registrate in forma immodificabile

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

- le informazioni relative all'oggetto, al mittente e al destinatario di una registrazione di protocollo, non possano essere modificate, ma solo annullate con la procedura prevista dall'art. 54 del TUDA[27];
- le uniche informazioni modificabili di una registrazione di protocollo siano l'assegnazione interna all'amministrazione e la classificazione;
- le azioni di annullamento provvedano alla storicizzazione dei dati annullati attraverso le informazioni oggetto della stessa;
- per ognuno di questi eventi, anche nel caso di modifica di una delle informazioni di cui al punto precedente, il sistema storicizzi tutte le informazioni annullate e modificate rendendole entrambe visibili e comparabili, nel rispetto di quanto previsto dall'art. 54, comma 2 del TUDA.

3.1.6. Requisiti minimi di sicurezza dei sistemi di protocollo informatico

Il sistema di protocollo informatico, eventualmente integrato in un sistema di gestione informatica dei documenti, assicura il rispetto delle disposizioni in materia di sicurezza predisposte dall'AgID di cui al paragrafo 3.9 e dagli altri organismi preposti e delle disposizioni in materia di protezione dei dati personali.

In particolare, il sistema di protocollo informatico deve garantire:

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

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

[27] L'art. 54, comma 2, del TUDA prevede che: "La procedura per indicare 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".

3.2. Classificazione dei documenti informatici

La classificazione ha il fine di organizzare logicamente tutti i documenti amministrativi informatici prodotti o ricevuti da un ente nell'esercizio delle sue funzioni. L'attività di classificazione si avvale del piano di classificazione che mappa, su più livelli gerarchici, tutte le funzioni dell'ente.

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, ai sensi degli articoli 56[28] e 64, comma 4[29], del TUDA. 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 o il coordinatore della gestione documentale, ove nominato, verifica periodicamente la rispondenza del piano di classificazione ai procedimenti amministrativi e agli affari in essere e procede al suo aggiornamento.

Nel sistema di gestione informatica dei documenti dell'AOO l'attività di classificazione guida la formazione dell'archivio mediante il piano di organizzazione delle aggregazioni documentali.

3.3. Aggregazioni documentali informatiche

La Pubblica Amministrazione documenta la propria attività tramite funzioni del sistema di gestione informatica dei documenti finalizzate alla produzione, alla gestione e all'uso delle aggregazioni documentali informatiche, corredate da opportuni metadati, così come definiti nell'allegato 5 "Metadati" alle presenti Linee guida.

3.3.1. Fascicoli informatici

Nelle Pubbliche Amministrazioni l'AOO gestisce i flussi documentali mediante fascicoli informatici predisposti secondo il piano di classificazione e relativo piano di organizzazione delle aggregazioni documentali ai sensi dell'art. 64 del TUDA, anche con riferimento a fascicoli non afferenti a procedimenti.

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

[29] L'articolo 64, comma 4, del TUDA prevede che: "Le amministrazioni determinano autonomamente e in modo coordinato per le aree organizzative omogenee, le modalità di attribuzione dei documenti ai fascicoli che li contengono e ai relativi procedimenti, definendo adeguati piani di classificazione d'archivio per tutti i documenti, compresi quelli non soggetti a registrazione di protocollo".

La produzione, il mantenimento e l'uso dei fascicoli informatici sono conformi a quanto stabilito dall'art. 65[30] del TUDA e dell'art 41[31] del CAD.

3.3.2. Altre aggregazioni documentali informatiche

All'interno del sistema di gestione informatica dei documenti la Pubblica Amministrazione forma, gestisce e utilizza tipologie di aggregazioni documentali informatiche diverse dai fascicoli: serie che aggregano documenti e serie che aggregano fascicoli.

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

Le serie di fascicoli sono costituite da fascicoli accorpati per ragioni funzionali in base alla classe di riferimento o alla tipologia di fascicoli.

I fascicoli appartenenti a serie diverse possono essere collegati tra loro.

---

[30]L'articolo 65 del TUDA prevede che: "Oltre a possedere i requisiti indicati all'articolo 52, il sistema per la gestione dei flussi documentali deve:

a) fornire informazioni sul legame esistente tra ciascun documento registrato, il fascicolo ed il singolo procedimento cui esso è associato;
b) consentire il rapido reperimento delle informazioni riguardanti i fascicoli, il procedimento ed il relativo responsabile, nonché la gestione delle fasi del procedimento;
c) fornire informazioni statistiche sull'attività dell'ufficio;
d) consentire lo scambio di informazioni con sistemi per la gestione dei flussi documentali di altre amministrazioni al fine di determinare lo stato e l'iter dei procedimenti complessi".

[31] L'art. 41, comma 2-ter, del CAD prevede che: "Il fascicolo informatico reca l'indicazione:

a) dell'amministrazione titolare del procedimento, che cura la costituzione e la gestione del fascicolo medesimo;
   2. delle altre amministrazioni partecipanti;
   3. del responsabile del procedimento;
   4. dell'oggetto del procedimento;
e) dell'elenco dei documenti contenuti, salvo quanto disposto dal comma 2-quater;
e-bis) dell'identificativo del fascicolo medesimo apposto con modalità idonee a consentirne l'indicizzazione e la ricerca attraverso il sistema di cui all'articolo 40-ter nel rispetto delle Linee guida".

Il successivo comma 2-quater prevede che: "Il fascicolo informatico può contenere aree a cui hanno accesso solo l'amministrazione titolare e gli altri soggetti da essa individuati; esso è formato in modo da garantire la corretta collocazione, la facile reperibilità e la collegabilità, in relazione al contenuto ed alle finalità, dei singoli documenti. Il fascicolo informatico è inoltre costituito in modo da garantire l'esercizio in via telematica dei diritti previsti dalla citata legge n. 241 del 1990 e dall'articolo 5, comma 2, del decreto legislativo 14 marzo 2013, n. 33, nonché l'immediata conoscibilità anche attraverso i servizi di cui agli articoli 40-ter e 64-bis, sempre per via telematica, dello stato di avanzamento del procedimento, del nominativo e del recapito elettronico del responsabile del procedimento. AgID detta, ai sensi dell'articolo 71, Linee guida idonee a garantire l'interoperabilità tra i sistemi di gestione dei fascicoli dei procedimenti e i servizi di cui agli articoli 40-ter e 64-bis".

Il sistema di gestione informatica dei documenti dell'AOO, individuata ai sensi dell'art. 50, comma 4, del TUDA[32], permette la gestione, formazione, utilizzo di serie secondo il piano di classificazione o di fascicolatura, sulla base delle indicazioni contenute nel manuale di gestione.

3.3.3. Registri e repertori informatici

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

3.4. Compiti del responsabile della gestione documentale

Le Pubbliche Amministrazioni definiscono le attribuzioni del responsabile della gestione documentale ovvero, ove nominato, del coordinatore della gestione documentale.

Il responsabile della gestione documentale è preposto al servizio di cui all'articolo 61 del TUDA[33] e, d'intesa con il responsabile della conservazione, il responsabile per la transizione digitale di cui

---

[32] L'art. 50, comma 4, del TUDA, prevede che: "Ciascuna amministrazione individua, nell'ambito del proprio ordinamento, gli uffici da considerare ai fini della gestione unica o coordinata dei documenti per grandi aree organizzative omogenee, assicurando criteri uniformi di classificazione e archiviazione, nonché di comunicazione interna tra le aree stesse".

[33] L'articolo 61 del TUDA prevede che "1. Ciascuna amministrazione istituisce un servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi in ciascuna delle grandi aree organizzative omogenee individuate ai sensi dell'articolo 50. Il servizio è posto alle dirette dipendenze della stessa area organizzativa omogenea.
2. Al servizio è preposto un dirigente ovvero un funzionario, comunque in possesso di idonei requisiti professionali o di professionalità tecnico archivistica acquisita a seguito di processi di formazione definiti secondo le procedure prescritte dalla disciplina vigente. 3. Il servizio svolge i seguenti compiti:
a) attribuisce il livello di autorizzazione per l'accesso alle funzioni della procedura, distinguendo tra abilitazioni alla consultazione e abilitazioni all'inserimento e alla modifica delle informazioni;
b) garantisce che le operazioni di registrazione e di segnatura di protocollo si volgano nel rispetto delle disposizioni del presente testo unico;
c) garantisce la corretta produzione e la conservazione del registro giornaliero di protocollo di cui all'articolo 53;
d) cura che le funzionalità del sistema in caso di guasti o anomalie siano ripristinate entro ventiquattro ore dal blocco delle attività e, comunque, nel più breve tempo possibile;
e) conserva le copie di cui agli articoli 62 e 63, in luoghi sicuri differenti;
f) garantisce il buon funzionamento degli strumenti e dell'organizzazione delle attività di registrazione di protocollo, di gestione dei documenti e dei flussi documentali, incluse le funzionalità di accesso di cui agli articoli 59 e 60 e le attività di gestione degli archivi di cui agli articoli 67, 68 e 69;
g) autorizza le operazioni di annullamento di cui all'articolo 54;
h) vigila sull'osservanza delle disposizioni del presente testo unico da parte del personale autorizzato e degli incaricati.

all'art.17 del CAD[34] e acquisito il parere del responsabile della protezione dei dati personali, di cui agli artt. 37 "Designazione del responsabile della protezione dei dati" e 39 "Compiti del responsabile della protezione dei dati" del Regolamento UE 679/2016, predispone:

- il manuale di gestione documentale relativo alla formazione, alla gestione, alla trasmissione, all'interscambio, all'accesso ai documenti informatici nel rispetto della normativa in materia di trattamenti dei dati personali ed in coerenza con quanto previsto nel manuale di conservazione;

Tale manuale conterrà inoltre, come parte integrante dello stesso, il piano per la sicurezza informatica, per la quota parte di competenza, nel rispetto delle:

- misure di sicurezza predisposte dall'AgID e dagli altri organismi preposti;
- delle disposizioni in materia di protezione dei dati personali in linea con l'analisi del rischio fatta;
- indicazioni in materia di continuità operativa dei sistemi informatici predisposti dall'AGID.

Per l'Amministrazione con più AOO il coordinatore della gestione, sentiti i responsabili della gestione documentale, assicura l'adozione di criteri uniformi per la gestione informatica dei documenti.

Il responsabile della gestione documentale ovvero, ove nominato, il coordinatore della gestione documentale, verifica l'avvenuta eliminazione dei protocolli di settore, dei protocolli multipli e, più in generale, dei protocolli diversi dal protocollo informatico previsto dal TUDA.

3.5. Manuale di gestione documentale

Il manuale di gestione documentale descrive il sistema di gestione informatica dei documenti e fornisce le istruzioni per il corretto funzionamento del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi.

Nel manuale di gestione documentale sono riportati, in particolare:

1. relativamente agli aspetti organizzativi:
   a) le modalità di utilizzo degli strumenti informatici per la formazione dei documenti informatici e per lo scambio degli stessi all'interno ed all'esterno dell'AOO, applicando le modalità di trasmissione indicate nell'allegato 6 "Comunicazione tra AOO di Documenti Amministrativi Protocollati";
   b) l'indicazione delle unità organizzative responsabili (UOR) delle attività di registrazione di protocollo, di archiviazione dei documenti all'interno dell'AOO;
   c) l'indicazione delle regole di assegnazione dei documenti ricevuti con la specifica dei criteri per l'ulteriore eventuale inoltro dei documenti verso aree organizzative omogenee della stessa amministrazione o verso altre amministrazioni;
   d) i criteri e le modalità per il rilascio delle abilitazioni di accesso, interno ed esterno all'Amministrazione, al sistema di gestione informatica dei documenti;

[34] L'art. 17 del CAD prevede che:" …ciascuna pubblica amministrazione affida a un unico ufficio dirigenziale generale, fermo restando il numero complessivo di tali uffici, la transizione alla modalità operativa digitale".

2. relativamente ai formati dei documenti:
   a) l'individuazione dei formati utilizzati per la formazione del documento informatico, come introdotti nel paragrafo 3.6, tra quelli indicati nell'Allegato 2 "Formati di file e riversamento";
   b) la descrizione di eventuali ulteriori formati utilizzati per la formazione di documenti in relazione a specifici contesti operativi che non sono individuati nell'Allegato 2 "Formati di file e riversamento";
   c) le procedure per la valutazione periodica di interoperabilità dei formati e per le procedure di riversamento previste come indicato al paragrafo 3.7 e nell'Allegato 2 "Formati di file e riversamento";

3. relativamente al protocollo informatico e alle registrazioni particolari:
   a) le modalità di registrazione delle informazioni annullate o modificate nell'ambito delle attività di registrazione;
   b) la descrizione completa e puntuale delle modalità di utilizzo della componente «sistema di protocollo informatico» del sistema di gestione informatica dei documenti;
   c) le modalità di utilizzo del registro di emergenza ai sensi dell'art. 63 del TUDA[35], inclusa la funzione di recupero dei dati protocollati manualmente;
   d) l'elenco dei documenti esclusi dalla registrazione di protocollo, per cui è prevista registrazione particolare ai sensi dell'art. 53, comma 5, del TUDA[36];
   e) determinazione dei metadati da associare ai documenti soggetti a registrazione particolare individuati, assicurando almeno quelli obbligatori previsti per il documento informatico dall'Allegato 5 alle presenti Linee Guida;
   f) i registri particolari individuati per la gestione del trattamento delle registrazioni particolari informatiche anche associati ad aree organizzative omogenee definite dall'amministrazione sull'intera struttura organizzativa e gli albi, gli elenchi e ogni raccolta di dati concernente stati, qualità personali e fatti, riconosciuti da una norma;

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

5. relativamente alla formazione delle aggregazioni documentali
   a) le modalità di formazione, gestione e archiviazione dei fascicoli informatici e delle aggregazioni

[35] L'art. 63 del TUDA prevede che: "1. Il responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi autorizza lo svolgimento anche manuale delle operazioni di registrazione di protocollo su uno o più registri di emergenza, ogni qualvolta per cause tecniche non sia possibile utilizzare la normale procedura informatica. Sul registro di emergenza sono riportate la causa, la data e l'ora di inizio dell'interruzione nonché la data e l'ora del ripristino della funzionalità del sistema. 2. Qualora l'impossibilità di utilizzare la procedura informatica si prolunghi oltre ventiquattro ore, per cause di eccezionale gravità, il responsabile per la tenuta del protocollo può autorizzare l'uso del registro di emergenza per periodi successivi di non più di una settimana. Sul registro di emergenza vanno riportati gli estremi del provvedimento di autorizzazione. 3. Per ogni giornata di registrazione di emergenza è riportato sul registro di emergenza il numero totale di operazioni registrate manualmente. 4. La sequenza numerica utilizzata su un registro di emergenza, anche a seguito di successive interruzioni, deve comunque garantire l'identificazione univoca dei documenti registrati nell'ambito del sistema documentario dell'area organizzativa omogenea. 5. Le informazioni relative ai documenti protocollati in emergenza sono inserite nel sistema informatico, utilizzando un'apposita funzione di recupero dei dati, senza ritardo al ripristino delle funzionalità del sistema. Durante la fase di ripristino, a ciascun documento registrato in emergenza viene attribuito un numero di protocollo del sistema informatico ordinario, che provvede a mantenere stabilmente la correlazione con il numero utilizzato in emergenza".

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

documentali informatiche con l'insieme minimo dei metadati ad essi associati;

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

7. relativamente alla organizzazione dei documenti informatici, dei fascicoli informatici e delle serie informatiche:

   a) la definizione della struttura dell'archivio all'interno del sistema di gestione informatica dei documenti. L'archivio informatico - formato ai sensi del capo IV "Sistema di gestione informatica dei documenti" del DPR 445/2000 - deve essere progettato in modo da assicurare certezza e trasparenza all'attività giuridico amministrativa;

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

9. relativamente alla conservazione:
   a) per le Pubbliche Amministrazioni il piano di conservazione è allegato al manuale di gestione documentale, con l'indicazione dei tempi entro i quali le diverse tipologie di oggetti digitali devono essere trasferite in conservazione ed eventualmente scartate;
   b) per i soggetti diversi dalle Pubbliche Amministrazioni che sono sprovvisti di piano di conservazione, qualora si renda necessario redigere un Manuale di gestione per la complessità della struttura organizzativa e della documentazione prodotta, dovrebbero essere definiti i criteri di organizzazione dell'archivio, di selezione periodica e di conservazione dei documenti, ivi compresi i tempi entro i quali le diverse tipologie di oggetti digitali devono essere trasferite in conservazione ed eventualmente scartate.

La Pubblica Amministrazione è tenuta a redigere, adottare con provvedimento formale e pubblicare sul proprio sito istituzionale il Manuale di gestione documentale. La pubblicazione è realizzata in una parte chiaramente identificabile dell'area "Amministrazione trasparente" prevista dall'art. 9 del d.lgs. 33/2013[37].

3.6. Formati di file

I formati da utilizzare nell'ambito delle presenti Linee guida sono quelli previsti dall'Allegato 2 "Formati di file e riversamento". Nello scegliere i formati di file di cui sopra, da utilizzare per i propri documenti informatici, i soggetti di cui all'art. 2 comma 2 e comma 3 del CAD possono effettuare una valutazione di interoperabilità che tenga conto dei seguenti fattori: formati aperti, non proprietari, standard *de iure*, estendibili, parlanti, completamente robusti, indipendenti dal dispositivo.

[37] L'art. 9, comma 1, del d.lgs. 33/2013, prevede che: "Ai fini della piena accessibilità delle informazioni pubblicate, nella home page dei siti istituzionali è collocata un'apposita sezione denominata «Amministrazione trasparente», al cui interno sono contenuti i dati, le informazioni e i documenti pubblicati ai sensi della normativa vigente. Le amministrazioni non possono disporre filtri e altre soluzioni tecniche atte ad impedire ai motori di ricerca web di indicizzare ed effettuare ricerche all'interno della sezione «Amministrazione trasparente»".

Le pubbliche amministrazioni garantiscono sempre la gestione dei formati classificati nell'Allegato 2 "Formati di file e riversamento" come "generici", secondo la distinzione introdotta nell'Allegato 2 tra formati di file generici e specifici.

Qualora l'ordinamento giuridico preveda, per particolari categorie di documenti elettronici, degli obblighi relativamente all'uso di formati di file specifici ovvero di vincoli aggiuntivi su formati generici (quali, ad esempio, l'uso di particolari dialetti o specializzazioni per formati generici), le pubbliche amministrazioni, assolvendo tali obblighi, accettano i suddetti documenti elettronici solo se prodotti nei formati o con i vincoli aggiuntivi obbligatori.

È possibile utilizzare formati diversi da quelli elencati nell'Allegato 2 "Formati di file e riversamento", effettuando una valutazione di interoperabilità.

La valutazione di interoperabilità è effettuata in base alle indicazioni previste nell'Allegato 2 "Formati di file e riversamento". La valutazione di interoperabilità, in quanto parte della gestione informatica dei documenti, viene effettuata periodicamente e, comunque, ogni anno, allo scopo di individuare tempestivamente cambiamenti delle condizioni espresse dai punti sopra elencati.

Il manuale di gestione documentale contiene l'elenco dei formati utilizzati e la valutazione di interoperabilità.

3.7. Riversamento

A seguito della valutazione di interoperabilità, i soggetti di cui all'art. 2 comma 2 e comma 3 del CAD valutano l'esigenza o l'opportunità di effettuare o pianificare il riversamento dei file da un formato di file ad un altro formato, sempre tenendo in considerazione quanto previsto nel punto precedente. Il riversamento è effettuato in base alle indicazioni previste nell'Allegato 2 "Formati di file e riversamento".

3.8. Trasferimento al sistema di conservazione

I termini entro cui i documenti informatici e le aggregazioni documentali informatiche devono essere trasferiti in conservazione sono stabiliti in conformità alla normativa vigente e al piano di conservazione.

Coerentemente con quanto stabilito dal Codice dei beni culturali, il trasferimento a un sistema di conservazione di documenti e aggregazioni documentali informatiche, appartenenti ad archivi pubblici e privati dichiarati di interesse storico particolarmente importante, è assoggettato all'obbligo di cui all'art. 21 del Codice dei Beni Culturali[38] di comunicazione agli organi competenti in materia di tutela dei beni archivistici o, nel caso di affidamento esterno, alla loro autorizzazione.

[38] L'art. 21, comma 1, del Codice dei beni culturali prevede che: "Sono subordinati ad autorizzazione del Ministero: a) la rimozione o la demolizione, anche con successiva ricostituzione, dei beni culturali; b) lo spostamento, anche temporaneo, dei beni culturali mobili, salvo quanto previsto ai commi 2 e 3; c) lo smembramento di collezioni, serie e raccolte; d) lo scarto dei documenti degli archivi pubblici e degli archivi privati per i quali sia intervenuta la dichiarazione ai sensi

I documenti informatici e le aggregazioni documentali informatiche possono essere oggetto di selezione e scarto nel sistema di gestione informatica dei documenti nel rispetto della normativa sui beni culturali.

3.9. Misure di sicurezza

Nell'attuazione delle presenti Linee Guida, le Pubbliche Amministrazioni sono tenute ad ottemperare alle misure minime di sicurezza ICT emanate dall'AgID con circolare del 18 aprile 2017, n. 2/2017. In tale ottica, il responsabile della gestione documentale ovvero, ove nominato, il coordinatore della gestione documentale, in accordo con il responsabile della conservazione di cui al paragrafo 4.6, con il responsabile per la transizione digitale e acquisito il parere del responsabile della protezione dei dati personali, predispone il piano della sicurezza del sistema di gestione informatica dei documenti, prevedendo opportune misure tecniche e organizzative per garantire un livello di sicurezza adeguato al rischio in materia di protezione dei dati personali, ai sensi dell'art. 32 del Regolamento UE 679/2016 (GDPR)[39], anche in funzione delle tipologie di dati trattati, quali quelli riferibili alle categorie particolari di cui agli artt. 9-10 del Regolamento stesso.

L'adozione delle predette misure è in capo al titolare o, in caso di trattamento effettuato per suo conto, al responsabile del trattamento, individuato sulla base dell'art. 28 "Responsabile del trattamento" del Regolamento.

Il piano conterrà altresì la descrizione della proceduta da adottarsi in caso di violazione dei dati personali ai sensi degli artt. 33-34 del Regolamento UE 679/2016[40], e sarà redatto nell'ambito del

dell'articolo 13, nonché lo scarto di materiale bibliografico delle biblioteche pubbliche, con l'eccezione prevista all'articolo 10, comma 2, lettera c), e delle biblioteche private per le quali sia intervenuta la dichiarazione ai sensi dell'articolo 13; e) il trasferimento ad altre persone giuridiche di complessi organici di documentazione di archivi pubblici, nonché di archivi privati per i quali sia intervenuta la dichiarazione ai sensi dell'articolo 13".
Il successivo comma 3 prevede che: "Lo spostamento degli archivi correnti dello Stato e degli enti ed istituti pubblici non è soggetto ad autorizzazione, ma comporta l'obbligo di comunicazione al Ministero per le finalità di cui all'articolo 18".

[39] L'art. 32 del Regolamento (UE) 2016/679 prevede che: "1. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:
a) la pseudonimizzazione e la cifratura dei dati personali;
b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.
2. Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati. 3. L'adesione a un codice di condotta approvato di cui all'articolo 40 o a un meccanismo di certificazione approvato di cui all'articolo 42 può essere utilizzata come elemento per dimostrare la conformità ai requisiti di cui al paragrafo 1 del presente articolo. 4. Il titolare del trattamento e il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri".

[40] Gli artt. 33 e 34 del Regolamento (UE) 2016/679 prevedono, rispettivamente, la procedura di notifica di una violazione dei dati personali all'autorità di controllo e quella di comunicazione di una violazione dei dati personali all'interessato.

piano generale della sicurezza, in coerenza con quanto previsto dal Piano Triennale per l'Informatica nella Pubblica Amministrazione vigente.

In conformità all'art. 28 del Regolamento UE 679/2016, i soggetti esterni a cui è eventualmente delegata la tenuta del sistema di gestione informatica dei documenti sono individuati come Responsabili del trattamento dei dati e devono presentare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del Regolamento e garantisca la tutela dei diritti dell'interessato.

I soggetti privati appartenenti ad organizzazioni che applicano particolari regole di settore per la sicurezza dei propri sistemi informatici possono adottare misure di sicurezza per garantire la tenuta del documento informatico. Le citate misure di sicurezza ICT emanate dall'AGID possono costituire, a tal fine, un modello di riferimento, fermo restando gli obblighi previsti dal citato Regolamento Reg. UE 679/2016.

I servizi devono sempre organizzati nel rispetto dei principi e dei requisiti previsti in materia di sicurezza dei dati e dei sistemi dagli artt.32 e 34 del Regolamento, avuto riguardo anche alla notifica delle violazioni dei dati personali di cui all'art.33 del Regolamento stesso.

CAPITOLO 4 Conservazione

4.1. Sistema di conservazione

Nella Pubblica Amministrazione, il sistema di gestione informatica dei documenti trasferisce al sistema di conservazione, ai sensi dell'art. 44, comma 1-bis, del CAD[41],:

a) i fascicoli informatici chiusi e le serie informatiche chiuse, trasferendoli dall'archivio corrente o dall'archivio di deposito;
b) i fascicoli informatici e le serie non ancora chiuse trasferendo i documenti in essi contenuti sulla base di specifiche esigenze dell'ente, con particolare attenzione per i rischi di obsolescenza tecnologica.

Il sistema di conservazione assicura, dalla presa in carico fino all'eventuale scarto, la conservazione dei seguenti oggetti digitali in esso conservati, tramite l'adozione di regole, procedure e tecnologie, garantendone le caratteristiche di autenticità, integrità, affidabilità, leggibilità, reperibilità:

a) i documenti informatici e i documenti amministrativi informatici con i metadati ad essi associati;
b) le aggregazioni documentali informatiche (fascicoli e serie) con i metadati ad esse associati contenenti i riferimenti che univocamente identificano i singoli oggetti documentali che costituiscono le aggregazioni medesime, nel rispetto di quanto indicato per le Pubbliche Amministrazioni nell'articolo 67, comma 2, del DPR 445/2000[42] e art. 44, comma 1-bis, CAD.

Il sistema di conservazione garantisce l'accesso all'oggetto conservato per il periodo previsto dal piano di conservazione del titolare dell'oggetto della conservazione e dalla normativa vigente, o per un tempo superiore eventualmente concordato tra le parti, indipendentemente dall'evoluzione del contesto tecnologico.

Il sistema di conservazione è almeno logicamente distinto dal sistema di gestione informatica dei documenti.

Gli elenchi degli standard, delle specifiche tecniche e dei formati utilizzabili quali riferimento per il

[41] L'art. 44, comma 1-bis, del CAD prevede che: "Il sistema di gestione dei documenti informatici delle pubbliche amministrazioni è gestito da un responsabile che opera d'intesa con il dirigente dell'ufficio di cui all'articolo 17 del presente Codice, il responsabile del trattamento dei dati personali di cui all'articolo 29 del decreto legislativo 30 giugno 2003, n. 196, ove nominato, e con il responsabile del sistema della conservazione dei documenti informatici delle pubbliche amministrazioni, nella definizione e gestione delle attività di rispettiva competenza. Almeno una volta all'anno il responsabile della gestione dei documenti informatici provvede a trasmettere al sistema di conservazione i fascicoli e le serie documentarie anche relative a procedimenti non conclusi".

[42] L'art. 67, comma 2, del TUDA prevede che: "Il trasferimento deve essere attuato rispettando l'organizzazione che i fascicoli e le serie avevano nell'archivio corrente".

sistema di conservazione sono riportati negli allegati 2 "Formati di file e riversamento" e 4 "Standard e specifiche tecniche".

4.2. Pacchetti informativi

Gli oggetti della conservazione sono trattati dal sistema di conservazione in pacchetti informativi che si distinguono in:

a) pacchetti di versamento;
b) pacchetti di archiviazione;
c) pacchetti di distribuzione.

L'interoperabilità tra i sistemi di conservazione dei soggetti che svolgono attività di conservazione è garantita dall'applicazione delle specifiche tecniche del pacchetto di archiviazione definite dalla norma UNI 11386 - Standard SInCRO - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali.

Il Titolare dell'oggetto della conservazione utilizza, già al momento della formazione, le modalità e i formati individuati nel manuale di gestione e nel manuale di conservazione in conformità con le presenti Linee Guida.

4.3. Modelli organizzativi della conservazione

Le Pubbliche Amministrazioni realizzano il processo di conservazione ai sensi dall'art. 34, comma 1-bis, del CAD[43], fatte salve le competenze del Ministero per i beni e le attività culturali e del turismo ai sensi del decreto legislativo 22 gennaio 2004, n. 42.

Il processo di conservazione può essere pertanto svolto all'interno o all'esterno della struttura organizzativa dell'ente.

I requisiti del processo di conservazione, le responsabilità e i compiti del responsabile della conservazione e del responsabile del servizio di conservazione, e le loro modalità di interazione sono formalizzate nel manuale di conservazione del Titolare dell'oggetto della conservazione e nelle specifiche del contratto di servizio o dell'accordo. Tali modalità trovano riscontro anche nel manuale di conservazione del conservatore.

[43] L'art. 34, comma 1-bis, del CAD prevede che: "Le pubbliche amministrazioni possono procedere alla conservazione dei documenti informatici:
a) all'interno della propria struttura organizzativa;
b) affidandola, in modo totale o parziale, nel rispetto della disciplina vigente, ad altri soggetti, pubblici o privati che possiedono i requisiti di qualità, di sicurezza e organizzazione individuati, nel rispetto della disciplina europea, nelle Linee guida di cui all'art 71 relative alla formazione, gestione e conservazione dei documenti informatici nonché in un regolamento sui criteri per la fornitura dei servizi di conservazione dei documenti informatici emanato da AgID, avuto riguardo all'esigenza di assicurare la conformità dei documenti conservati agli originali nonché la qualità e la sicurezza del sistema di conservazione".

Al fine di garantire l'autenticità, l'integrità, l'affidabilità, la leggibilità e la reperibilità dei documenti, i fornitori di servizi di conservazione devono possedere requisiti di elevato livello in termini di qualità e sicurezza in aderenza allo standard ISO/IEC 27001 (*Information security management systems - Requirements*) del sistema di gestione della sicurezza delle informazioni nel dominio logico, fisico e organizzativo nel quale viene realizzato il processo di conservazione e ISO 14721 OAIS (*Open Archival Information System - Sistema informativo aperto per l'archiviazione)*, e alle raccomandazioni ETSI TS 101 533-1 v. 1.2.1, *Requisiti per realizzare e gestire sistemi sicuri e affidabili per la conservazione elettronica delle informazioni*.

4.4. Ruoli e responsabilità

I ruoli individuati nel processo di conservazione sono:

a) titolare dell'oggetto della conservazione;
b) produttore dei PdV;
c) utente abilitato;
d) responsabile della conservazione
e) conservatore.

Nelle Pubbliche Amministrazioni, il ruolo di produttore del PdV è svolto da persona interna alla struttura organizzativa.

L'utente abilitato può richiedere al sistema di conservazione l'accesso ai documenti per acquisire le informazioni di interesse nei limiti previsti dalla legge e nelle modalità previste dal manuale di conservazione.

Nelle Pubbliche Amministrazioni il responsabile della gestione documentale o il coordinatore della gestione documentale, ove nominato, svolge il ruolo di produttore di PdV e assicura la trasmissione del pacchetto di versamento al sistema di conservazione, secondo le modalità operative definite nel manuale di conservazione.

Nel caso di affidamento a terzi, il produttore di PdV provvede a generare e trasmettere al sistema di conservazione i pacchetti di versamento nelle modalità e con i formati concordati con il conservatore e descritti nel manuale di conservazione del sistema di conservazione. Provvede inoltre a verificare il buon esito della operazione di trasferimento al sistema di conservazione tramite la presa visione del rapporto di versamento prodotto dal sistema di conservazione stesso.

4.5. Responsabile della conservazione

Il responsabile della conservazione opera secondo quanto previsto dall'art. 44, comma 1-quater, del CAD[44].

[44] L'art. 44, comma 1-quater, del CAD prevede che: "Il responsabile della conservazione, che opera d'intesa con il responsabile del trattamento dei dati personali, con il responsabile della sicurezza e con il responsabile dei sistemi informativi, può affidare, ai sensi dell'articolo 34, comma 1-bis, lettera b), la conservazione dei documenti informatici ad

Nella Pubblica Amministrazione, il responsabile della conservazione:

a) è un ruolo previsto dall'organigramma del Titolare dell'oggetto di conservazione;
b) è un dirigente o un funzionario interno formalmente designato e in possesso di idonee competenze giuridiche, informatiche ed archivistiche;
c) può essere svolto dal responsabile della gestione documentale o dal coordinatore della gestione documentale, ove nominato.

Per i soggetti diversi dalla Pubblica Amministrazione, il ruolo del responsabile della conservazione può essere svolto da un soggetto esterno all'organizzazione, in possesso di idonee competenze giuridiche, informatiche ed archivistiche, purché terzo rispetto al Conservatore al fine di garantire la funzione del Titolare dell'oggetto di conservazione rispetto al sistema di conservazione.

Il responsabile della conservazione definisce e attua le politiche complessive del sistema di conservazione e ne governa la gestione con piena responsabilità ed autonomia.

Il responsabile della conservazione, sotto la propria responsabilità, può delegare 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 delega, riportata nel manuale di conservazione, deve individuare le specifiche funzioni e competenze delegate.

In particolare, il responsabile della conservazione:

a) definisce le politiche di conservazione e i requisiti funzionali del sistema di conservazione, in conformità alla normativa vigente e tenuto conto degli standard internazionali, in ragione delle specificità degli oggetti digitali da conservare (documenti informatici, aggregazioni informatiche, archivio informatico), della natura delle attività che il Titolare dell'oggetto di conservazione svolge e delle caratteristiche del sistema di gestione informatica dei documenti adottato;
b) gestisce il processo di conservazione e ne garantisce nel tempo la conformità alla normativa vigente;
c) genera e sottoscrive il rapporto di versamento, secondo le modalità previste dal manuale di conservazione;
d) genera e sottoscrive il pacchetto di distribuzione con firma digitale o firma elettronica qualificata, nei casi previsti dal manuale di conservazione;
e) effettua il monitoraggio della corretta funzionalità del sistema di conservazione;
f) effettua la verifica periodica, con cadenza non superiore ai cinque anni, dell'integrità e della leggibilità dei documenti informatici e delle aggregazioni documentarie degli archivi;
g) al fine di garantire la conservazione e l'accesso ai documenti informatici, adotta misure per rilevare tempestivamente l'eventuale degrado dei sistemi di memorizzazione e delle registrazioni e, ove necessario, per ripristinare la corretta funzionalità; adotta analoghe misure con riguardo all'obsolescenza dei formati;
h) provvede alla duplicazione o copia dei documenti informatici in relazione all'evolversi del contesto tecnologico, secondo quanto previsto dal manuale di conservazione;
i) predispone le misure necessarie per la sicurezza fisica e logica del sistema di conservazione come previsto dal par. 4.11;
j) assicura la presenza di un pubblico ufficiale, nei casi in cui sia richiesto il suo intervento, garantendo allo stesso l'assistenza e le risorse necessarie per l'espletamento delle attività al medesimo attribuite;
k) assicura agli organismi competenti previsti dalle norme vigenti l'assistenza e le risorse necessarie per l'espletamento delle attività di verifica e di vigilanza;
l) provvede per le amministrazioni statali centrali e periferiche a versare i documenti

altri soggetti, pubblici o privati, che offrono idonee garanzie organizzative, e tecnologiche e di protezione dei dati personali. Il responsabile della conservazione della pubblica amministrazione, che opera d'intesa, oltre che con i responsabili di cui al comma 1-bis, anche con il responsabile della gestione documentale, effettua la conservazione dei documenti informatici secondo quanto previsto all'articolo 34, comma 1-bis".

informatici, le aggregazioni informatiche e gli archivi informatici, nonché gli strumenti che ne garantiscono la consultazione, rispettivamente all'Archivio centrale dello Stato e agli archivi di Stato territorialmente competenti, secondo le tempistiche fissate dall'art. 41, comma 1, del Codice dei beni culturali[45];

m) predispone il manuale di conservazione di cui al par. 4.7 e ne cura l'aggiornamento periodico in presenza di cambiamenti normativi, organizzativi, procedurali o tecnologici rilevanti.

Nel caso in cui il servizio di conservazione venga affidato ad un conservatore, le attività suddette o alcune di esse, ad esclusione della lettera m), potranno essere affidate 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 altresì a svolgere le necessarie attività di verifica e controllo in ossequio alle norme vigenti sul servizi affidati in outsourcing dalle PA.

Si precisa che il nominativo ed i riferimenti del responsabile della conservazione devono essere indicati nelle specifiche del contratto o della convenzione di servizio con il Conservatore nel quale sono anche riportate le attività affidate al responsabile del servizio di conservazione.

4.6. Manuale di conservazione

Il manuale di conservazione è un documento informatico che deve illustrare 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 utilizzate, le misure di sicurezza adottate e ogni altra informazione utile alla gestione e alla verifica del funzionamento, nel tempo, del sistema di conservazione.

Il manuale di conservazione, inoltre, deve riportare:

a) i dati dei soggetti che nel tempo hanno assunto la responsabilità del sistema di conservazione, descrivendo in modo puntuale, in caso di delega, i soggetti, le funzioni e gli ambiti oggetto della delega stessa;
b) la struttura organizzativa comprensiva delle funzioni, delle responsabilità e degli obblighi dei diversi soggetti che intervengono nel processo di conservazione;
c) la descrizione delle tipologie degli oggetti digitali sottoposti a conservazione, comprensiva dell'indicazione dei formati gestiti, dei metadati da associare alle diverse tipologie di oggetti e delle eventuali eccezioni;
d) la descrizione delle modalità di presa in carico di uno o più pacchetti di versamento, comprensiva della predisposizione del rapporto di versamento;
e) la descrizione del processo di conservazione e del trattamento dei pacchetti di archiviazione;
f) la modalità di svolgimento del processo di esibizione e di esportazione dal sistema di conservazione con la produzione del pacchetto di distribuzione;
g) la descrizione del sistema di conservazione, comprensivo di tutte le componenti tecnologiche, fisiche e logiche, opportunamente documentate e delle procedure di gestione

[45] L'art. 41, comma 1, del Codice dei beni culturali prevede che: "Gli organi giudiziari e amministrativi dello Stato versano all'archivio centrale dello Stato e agli archivi di Stato i documenti relativi agli affari esauriti da oltre trent'anni, unitamente agli strumenti che ne garantiscono la consultazione. Le liste di leva e di estrazione sono versate settant'anni dopo l'anno di nascita della classe cui si riferiscono. Gli archivi notarili versano gli atti notarili ricevuti dai notai che cessarono l'esercizio professionale anteriormente all'ultimo centennio".

e di evoluzione delle medesime;
h) la descrizione delle procedure di monitoraggio della funzionalità del sistema di conservazione e delle verifiche sull'integrità degli archivi con l'evidenza delle soluzioni adottate in caso di anomalie;
i) la descrizione delle procedure per la produzione di duplicati o copie;
j) i tempi entro i quali le diverse tipologie di oggetti digitali devono essere trasferite in conservazione ed eventualmente scartate, qualora, nel caso delle Pubbliche Amministrazioni, non siano già indicati nel piano di conservazione allegato al manuale di gestione documentale;
k) le modalità con cui viene richiesta la presenza di un pubblico ufficiale, indicando anche quali sono i casi per i quali è previsto il suo intervento;
l) le normative in vigore nei luoghi dove sono conservati gli oggetti digitali.

Le Pubbliche Amministrazioni sono tenute a redigere, adottare con provvedimento formale e pubblicare sul proprio sito istituzionale il Manuale di conservazione.

La pubblicazione è realizzata in una parte chiaramente identificabile dell'area "Amministrazione trasparente" prevista dall'art. 9 del d.lgs. 33/2013.

In caso di affidamento del servizio di conservazione ad un conservatore esterno, le Pubbliche Amministrazioni possono descrivere nel proprio manuale anche le attività del processo di conservazione affidate al conservatore, in conformità con il contenuto del manuale di conservazione predisposto da quest'ultimo, o rinviare, per le parti di competenza, al manuale del conservatore esterno.

Resta fermo l'obbligo in carico alla Pubblica Amministrazione di individuare e pubblicare i tempi di versamento, le tipologie documentali trattate, i metadati, le modalità di trasmissione dei PdV e le tempistiche di selezione e scarto dei propri documenti informatici.

Resta ferma inoltre la competenza del Ministero dei beni e delle attività culturali e del Turismo in materia di tutela dei sistemi di conservazione sugli archivi pubblici e privati che rivestono interesse storico particolarmente importante, così come disciplinato dalla normativa sui beni culturali.

4.7. Processo di conservazione

Il trasferimento dell'oggetto di conservazione nel sistema di conservazione avviene generando un PdV nelle modalità e con il formato previsti dal manuale di conservazione di cui al paragrafo 4.6.

Il processo di conservazione prevede:
a) l'acquisizione da parte del sistema di conservazione del PdV per la sua presa in carico;
b) la verifica che il PdV e gli oggetti digitali contenuti siano coerenti con le modalità previste dal manuale di conservazione e con quanto indicato nell' allegato 2 "Formati di file e riversamento" relativo ai formati;
c) il rifiuto del PdV, nel caso in cui le verifiche di cui alla lettera b) abbiano evidenziato delle anomalie. Il numero massimo di rifiuti è stabilito nell'ambito di un contratto o convenzione;
d) la generazione, anche in modo automatico, del rapporto di versamento relativo ad uno o più pacchetti di versamento, univocamente identificato dal sistema di conservazione e contenente un riferimento temporale, specificato con riferimento al Tempo universale coordinato (UTC), e una o più impronte, calcolate sull'intero contenuto del pacchetto di versamento, secondo le modalità descritte nel manuale di conservazione;
e) la sottoscrizione del rapporto di versamento con la firma digitale o firma elettronica

qualificata o avanzata apposta dal responsabile della conservazione o dal responsabile del servizio di conservazione, ove prevista nel manuale di conservazione;

f) la preparazione, la sottoscrizione con firma digitale o firma elettronica - qualificata o avanzata - del responsabile della conservazione o del responsabile del servizio di conservazione o con il sigillo elettronico - qualificato o avanzato – apposto dal conservatore esterno, nonché la gestione del pacchetto di archiviazione sulla base delle specifiche della struttura dati indicate dallo standard UNI 11386 e secondo le modalità riportate nel manuale di conservazione;
g) ai fini dell'esibizione richiesta dall'utente la preparazione e la sottoscrizione con firma digitale o firma elettronica qualificata o avanzata del responsabile della conservazione o del responsabile del servizio di conservazione, oppure l'apposizione del sigillo elettronico qualificato o avanzato, secondo le modalità indicate nel manuale di conservazione, di pacchetti di distribuzione che possono contenere parte, uno o più pacchetti di archiviazione;
h) ai soli fini della interoperabilità tra sistemi di conservazione, la produzione di pacchetti di distribuzione coincidenti con i pacchetti di archiviazione o comunque contenenti pacchetti di archiviazione generati sulla base delle specifiche della struttura dati indicate dallo standard UNI 11386 e secondo le modalità riportate nel manuale di conservazione;
i) la produzione di duplicati informatici o di copie informatiche effettuati su richiesta degli utenti in conformità a quanto previsto dalle presenti linee guida;
j) la produzione di copie informatiche tramite attività di riversamento al fine di adeguare il formato alle esigenze conservative di leggibilità nel tempo in base alle indicazioni previste dall'allegato 2 "Formati di file e riversamento";
k) l'eventuale scarto del pacchetto di archiviazione dal sistema di conservazione alla scadenza dei termini di conservazione previsti dalla norma o secondo quanto indicato dal piano di conservazione del Titolare dell'oggetto di conservazione e le procedure descritte nel successivo paragrafo 4.12;
l) nel caso degli archivi pubblici o privati, che rivestono interesse storico particolarmente importante, l'eventuale scarto del pacchetto di archiviazione avviene previa autorizzazione del MIC rilasciata al Titolare dell'oggetto della conservazione secondo quanto previsto dalla normativa vigente in materia e al successivo paragrafo 4.12.

Nel caso di affidamento a terzi del servizio di conservazione le modalità sono indicate nei manuali del Titolare dell'oggetto di conservazione e del conservatore e concordate tra le parti.

4.8. Infrastrutture

Fatto salvo quanto previsto dal Codice dei beni culturali, nel rispetto del principio di libera circolazione dei dati all'interno dell'Unione europea[46], si sottolinea l'obbligo, in capo al fornitore del servizio di conservazione, di conservare e rendere disponibili le descrizioni del sistema di conservazione all'interno del territorio nazionale. I conservatori devono altresì garantire alle amministrazioni l'accesso elettronico effettivo e tempestivo ai dati conservati, indipendentemente dallo Stato membro nel cui territorio i dati sono conservati.

Le componenti tecnologiche hardware e software utilizzate dai sistemi di conservazione delle Pubbliche Amministrazioni e dei conservatori sono segregate logicamente. Qualora i servizi di conservazione siano erogati in modalità cloud, il servizio deve essere qualificato come previsto dalla Circolare Agid n. 3 del 9 aprile 2018 e, conseguentemente, essere presente nel "Catalogo dei servizi

[46] Reg. (UE) 2018/1807 all'articolo 4, paragrafo 1 recita:" Gli obblighi di localizzazione di dati sono vietati a meno che siano giustificati da motivi di sicurezza pubblica nel rispetto del principio di proporzionalità."

Cloud per la PA qualificati" pubblicato sul sito di Agid.

I sistemi di conservazione devono essere realizzati nel rispetto del principio di integrità e riservatezza, nonché dei principi di protezione fin dalla progettazione e per impostazione predefinita, e dei conseguenti adempimenti previsti dagli artt. 25[47] e 32 del citato Regolamento UE 679/2016.

4.9. Modalità di esibizione

Fermi restando gli obblighi previsti in materia di esibizione dei documenti dalla normativa vigente, il sistema di conservazione permette ai soggetti autorizzati l'accesso diretto, anche da remoto, agli oggetti digitali conservati, attraverso la produzione di pacchetti di distribuzione secondo le modalità descritte nel manuale di conservazione, prevedendo opportune misure tecniche e organizzative per garantire un livello di sicurezza adeguato al rischio e modalità di accesso diverse, in funzione delle tipologie di dati personali trattati, nonché delle operazioni di trattamento consentite.

Nel caso di affidamento esterno del servizio di conservazione tali modalità sono concordate tra le parti e indicate nei rispettivi manuali.

4.10. Misure di sicurezza

Nell'attuazione delle presenti Linee Guida, le Pubbliche Amministrazioni sono tenute ad ottemperare alle misure minime di sicurezza ICT emanate dall'AgID con circolare del 18 aprile 2017, n. 2/2017. In tale ottica, il responsabile della conservazione, di concerto con il responsabile per la transizione digitale, con il responsabile della gestione documentale e acquisito il parere del responsabile della protezione dei dati personali, predispone il piano della sicurezza del sistema di gestione informatica dei documenti, prevedendo opportune misure tecniche e organizzative per garantire un livello di sicurezza adeguato al rischio in materia di protezione dei dati personali, ai sensi dell'art. 32 del Regolamento UE 679/2016[48], anche in funzione delle tipologie di dati trattati, quali quelli riferibili alle categorie particolari di cui agli artt. 9-10 del Regolamento stesso.

---

[47] L'art. 25 del Regolamento "Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita**"**

[48] L'art. 32 del Regolamento (UE) 2016/679 prevede che: "1. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:
a) la pseudonimizzazione e la cifratura dei dati personali;
b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.
2. Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati. 3. L'adesione a un codice di condotta approvato di cui all'articolo 40 o a un meccanismo di certificazione approvato di cui all'articolo 42 può essere

L'adozione delle predette misure è in capo al titolare o, in caso di trattamento effettuato per suo conto, al responsabile del trattamento, individuato sulla base dell'art.28 del Regolamento.

Il piano conterrà altresì la descrizione della proceduta da adottarsi in caso di violazione dei dati personali ai sensi degli artt. 33-34 del Regolamento UE 679/2016[49], e sarà redatto nell'ambito del piano generale della sicurezza, in coerenza con quanto previsto dal Piano Triennale per l'Informatica nella Pubblica Amministrazione vigente.
Le misure di sicurezza sono descritte nel manuale di conservazione di cui al par. 4.7.

Nel caso di affidamento esterno del servizio di conservazione le misure di sicurezza sono concordate tra le parti e indicate nei rispettivi manuali. In conformità all'art. 28 del Regolamento UE 679/2016, i soggetti esterni a cui è delegata la tenuta del sistema di conservazione sono individuati come Responsabili del trattamento dei dati e devono presentare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del Regolamento e garantisca la tutela dei diritti dell'interessato.

I soggetti privati appartenenti ad organizzazioni che applicano particolari regole di settore per la sicurezza dei propri sistemi informatici adeguano il sistema di conservazione a tali regole. Le citate misure di sicurezza ICT emanate dall'AGID possono costituire, a tal fine, un modello di riferimento, fermo restando gli obblighi previsti dal citato Regolamento UE 679/2016.

I servizi devono sempre organizzati nel rispetto dei principi e dei requisiti previsti in materia di sicurezza dei dati e dei sistemi dagli artt.32 e 34 del Regolamento, avuto riguardo anche alla notifica delle violazioni dei dati personali di cui all'art.33 del Regolamento stesso.

4.11. Selezione e scarto dei documenti informatici

I documenti informatici e le aggregazioni documentali informatiche possono essere oggetto di selezione e scarto nel sistema di conservazione nel rispetto della normativa sui beni culturali.

Nel sistema di conservazione, la selezione e lo scarto dei pacchetti di archiviazione sono definiti dal Titolare dell'oggetto di conservazione e, nel caso delle Pubbliche Amministrazioni, secondo quanto indicato dal piano di conservazione. Nel caso di affidamento esterno del servizio di conservazione le modalità operative sono concordate dal Titolare dell'oggetto di conservazione e dal Conservatore.

Il responsabile della conservazione genera l'elenco dei pacchetti di archiviazione contenenti i documenti destinati allo scarto e, dopo aver verificato il rispetto dei termini temporali stabiliti dal piano di conservazione, lo comunica al responsabile della gestione documentale o del coordinatore della gestione documentale, ove nominato. In caso di affidamento esterno del servizio di conservazione l'elenco dei pacchetti di archiviazione contenenti i documenti destinati allo scarto è generato dal responsabile del servizio di conservazione e trasmesso al responsabile della conservazione che a sua volta, verificato il rispetto dei termini temporali stabiliti dal piano di

utilizzata come elemento per dimostrare la conformità ai requisiti di cui al paragrafo 1 del presente articolo. 4. Il titolare del trattamento e il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri".

[49] Gli artt. 33 e 34 del Regolamento (UE) 2016/679 prevedono, rispettivamente, la procedura di notifica di una violazione dei dati personali all'autorità di controllo e quella di comunicazione di una violazione dei dati personali all'interessato.

conservazione, lo comunica al responsabile della gestione documentale o al coordinatore della gestione documentale.

Nel caso degli archivi pubblici e degli archivi privati con il solo riferimento a quelli dichiarati di interesse storico particolarmente importante l'autorizzazione è rilasciata ai sensi della normativa vigente in materia di beni culturali.

Il Titolare dell'oggetto di conservazione, una volta ricevuta l'autorizzazione, che può essere concessa anche solo su una parte dell'elenco proposto, procede alla distruzione dei pacchetti di archiviazione.

Nel caso di affidamento esterno del servizio di conservazione, il Titolare dell'oggetto di conservazione, una volta ricevuta l'autorizzazione, che può essere concessa anche solo su una parte dell'elenco proposto, provvede a trasmetterlo al conservatore affinché provveda alla distruzione dei pacchetti di archiviazione.

L'operazione di scarto viene tracciata sul sistema mediante la produzione delle informazioni essenziali sullo scarto, inclusi gli estremi della richiesta di nulla osta allo scarto e il conseguente provvedimento autorizzatorio.

Al termine delle operazioni di distruzione dal sistema di conservazione dei pacchetti di archiviazione scartati, il Titolare dell'oggetto di conservazione notifica l'esito della procedura di scarto agli organi preposti alla tutela come già indicato in precedenza. Analoga comunicazione è inviata al Ministero dell'interno in caso di eliminazione di pacchetti di archiviazione contenenti documenti e/o dati di carattere riservato.

Tale operazione avrà completa efficacia solo al momento del completo aggiornamento delle copie di sicurezza del sistema.

I documenti e le aggregazioni documentali informatiche sottoposti a scarto nel sistema di conservazione devono essere distrutti anche in tutti i sistemi gestiti dal Titolare dell'oggetto di conservazione.