|  |  |
| --- | --- |
| + [INSERIRE LOGO ENTE] |  |
|  | |
| MANUALE DI CONSERVAZIONE   |  |  | | --- | --- | | *Codice documento* | Manuale\_Conservazione | | *Versione* | X.X | | |
| |  |  |  |  | | --- | --- | --- | --- | |  | *Data* | *Nominativo* | *Funzione* | | *Redazione* | xx/xx/xxxx | Xxxx Xxxx | Xxxxxxxxx | | *Verifica* | xx/xx/xxxx | Xxxx Xxxx | Responsabile funzione archivistica di conservazione | | *Approvazione* | xx/xx/xxxx | Xxxx Xxxx | Responsabile del servizio | | |
|  | |
| Il presente documento è rilasciato sotto la licenza  **Attribuzione-Non commerciale** delle Creative Commons. | |

SOMMARIO

[REGISTRO DELLE VERSIONI 5](#_Toc521078139)

[CLASSIFICAZIONE DEL DOCUMENTO 5](#_Toc521078140)

[LISTA DI DISTRIBUZIONE 5](#_Toc521078141)

[1 SCOPO E AMBITO DEL DOCUMENTO 6](#_Toc521078142)

[2 TERMINOLOGIA (GLOSSARIO, ACRONIMI) 7](#_Toc521078143)

[3 NORMATIVA E STANDARD DI RIFERIMENTO 16](#_Toc521078144)

[3.1 Normativa di riferimento 16](#_Toc521078145)

[3.2 Standard di riferimento 16](#_Toc521078146)

[4 RUOLI E RESPONSABILITÀ 17](#_Toc521078147)

[4.1 Modello organizzativo 17](#_Toc521078148)

[4.2 Produttore 17](#_Toc521078149)

[4.2.1 Versatore 19](#_Toc521078150)

[4.2.2 Fornitore esterno 19](#_Toc521078151)

[4.3 Utente 20](#_Toc521078152)

[4.4 Conservatore 20](#_Toc521078153)

[4.5 Organismi di tutela e vigilanza 21](#_Toc521078154)

[5 STRUTTURA ORGANIZZATIVA PER IL SERVIZIO DI CONSERVAZIONE 23](#_Toc521078155)

[5.1 Organigramma 23](#_Toc521078156)

[6 OGGETTI SOTTOPOSTI A CONSERVAZIONE 26](#_Toc521078157)

[6.1 Oggetti conservati 26](#_Toc521078158)

[6.1.1 Unità archivistiche e Unità documentarie 30](#_Toc521078159)

[6.1.2 Formati 31](#_Toc521078160)

[6.1.3 Metadati 32](#_Toc521078161)

[6.2 Pacchetto di versamento (SIP) 33](#_Toc521078162)

[6.3 Pacchetto di archiviazione (AIP) 34](#_Toc521078163)

[6.4 Pacchetto di distribuzione (DIP) 35](#_Toc521078164)

[7 PROCESSO DI CONSERVAZIONE 37](#_Toc521078165)

[7.1 Modalità di acquisizione dei pacchetti di versamento per la loro presa in carico 37](#_Toc521078166)

[7.2 Preacquisizione 40](#_Toc521078167)

[7.3 Acquisizione 40](#_Toc521078168)

[7.4 Verifiche effettuate sui pacchetti di versamento e sugli oggetti in essi contenuti 41](#_Toc521078169)

[7.5 Accettazione dei pacchetti di versamento e generazione del rapporto di versamento di presa in carico 42](#_Toc521078170)

[7.6 Rifiuto dei pacchetti di versamento e modalità di comunicazione delle anomalie 43](#_Toc521078171)

[7.6.1 Monitoraggio 44](#_Toc521078172)

[7.6.2 Gestione delle anomalie 45](#_Toc521078173)

[7.7 Preparazione e gestione del Pacchetto di archiviazione 47](#_Toc521078174)

[7.8 Preparazione e gestione del Pacchetto di distribuzione (DIP) ai fini dell’esibizione 50](#_Toc521078175)

[7.9 Produzione di duplicati e copie informatiche e descrizione dell’eventuale intervento del pubblico ufficiale nei casi previsti 51](#_Toc521078176)

[7.10 Scarto dei pacchetti di archiviazione 52](#_Toc521078177)

[7.11 Predisposizione di misure a garanzia dell'interoperabilità e trasferibilità ad altri conservatori 53](#_Toc521078178)

[8 IL SISTEMA DI CONSERVAZIONE 54](#_Toc521078179)

[8.1 Componenti logiche 54](#_Toc521078180)

[8.2 Componenti tecnologiche 56](#_Toc521078181)

[8.2.1 SacER 57](#_Toc521078182)

[8.2.2 VersO 60](#_Toc521078183)

[8.2.3 PING 60](#_Toc521078184)

[8.2.4 XFormer 61](#_Toc521078185)

[8.2.5 DPI 61](#_Toc521078186)

[8.2.6 Interfacce di Acquisizione e di Recupero (Web Service) 62](#_Toc521078187)

[8.2.7 TPI 62](#_Toc521078188)

[8.2.8 DIPS 63](#_Toc521078189)

[8.2.9 SIAM 63](#_Toc521078190)

[8.2.10 Sacerlog 63](#_Toc521078191)

[8.2.11 Componenti di supporto 64](#_Toc521078192)

[8.3 Componenti fisiche 65](#_Toc521078193)

[8.3.1 Schema generale 65](#_Toc521078194)

[8.3.2 Caratteristiche tecniche del Sito primario 67](#_Toc521078195)

[8.4 Procedure di gestione e di evoluzione 70](#_Toc521078196)

[8.4.1 Gestione dell’Esercizio 70](#_Toc521078197)

[8.4.2 Gestione delle Richieste degli Utenti e dei Malfunzionamenti 70](#_Toc521078198)

[8.4.3 Gestione degli Incidenti di Sicurezza 71](#_Toc521078199)

[8.4.4 Evoluzione pianificata 72](#_Toc521078200)

[8.4.5 Richieste di Cambiamento 72](#_Toc521078201)

[8.4.6 Gestione dei Rilasci 73](#_Toc521078202)

[8.4.7 Gestione e conservazione dei Log [da adattare] 74](#_Toc521078203)

[8.4.8 Verifica periodica di conformità a normativa e standard di riferimento [da adattare] 75](#_Toc521078204)

[9 MONITORAGGIO E CONTROLLI 76](#_Toc521078205)

[9.1 Procedure di monitoraggio 76](#_Toc521078206)

[9.2 Funzionalità per la verifica e il mantenimento dell’integrità degli archivi 76](#_Toc521078207)

[9.3 Soluzioni adottate in caso di anomalie 77](#_Toc521078208)

# REGISTRO DELLE VERSIONI

| **Versione** | **Variazioni** | **Data** |
| --- | --- | --- |
| 1.0 | Prima emissione | xx/xx/xx |
| X.X | [INSERIRE LE PRINCIPALI MODIFICHE INTERCORSE RISPETTO ALLA VERSIONE PRECEDENTE] | xx/xx/xx |

# CLASSIFICAZIONE DEL DOCUMENTO

|  |  |
| --- | --- |
| Livello di Riservatezza: | [IN BASE A QUANTO DEFINITO NELLA PROCEDURA DI GESTIONE DOCUMENTALE] |
| Rilevanza: | [IN BASE A QUANTO DEFINITO NELLA PROCEDURA DI GESTIONE DOCUMENTALE] |
| Classificazione: | [IN BASE A QUANTO DEFINITO NELLA PROCEDURA DI GESTIONE DOCUMENTALE] |

# LISTA DI DISTRIBUZIONE

| **Soggetti da Notificare** | |
| --- | --- |
| *Nominativi* | *Ruoli Organizzativi* |
| [INSERIRE I NOMINATIVI, SE IDENTIFICABILI INDIVIDUALMENTE] | [INSERIRE I RUOLI DEI SINGOLI NOMINATIVI, OPPURE I RUOLI IN ASSENZA DI NOMINATIVI] |

# SCOPO E AMBITO DEL DOCUMENTO

Il presente documento è il *Manuale di conservazione* (d’ora in poi Manuale), che descrive il processo di conservazione applicato da [INSERIRE IL NOME DELL’ENTE] in quanto soggetto conservatore ai sensi dell’art. 8 comma 1 del DPCM del 3 dicembre 2013 in materia di sistema di conservazione. In particolare, il presente Manuale descrive il modello organizzativo della conservazione adottato e illustra 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*.

Gli elementi illustrati e descritti sono validi e rilevanti per l’Ente produttore che conserva in house la propria documentazione e realizza e gestisce il *processo di conservazione*, secondo il modello organizzativo descritto al paragrafo 4.1.

Per le tipologie degli oggetti sottoposti a *conservazione* il presente Manuale deve essere integrato con il ***Disciplinare tecnico*** che definisce le specifiche operative e le modalità di descrizione e di versamento dal Sistema di gestione documentale nel *Sistema di conservazione* digitale dei *Documenti informatici* e delle *Aggregazioni documentali informatiche* oggetto di *conservazione*.

La documentazione di riferimento è pubblicata nel sito dell’Ente produttore/conservatore (d’ora in avanti denominato “Ente”: [INSERIRE link relativo alla documentazione]

[[Torna al Sommario](#Sommario)]

# TERMINOLOGIA (GLOSSARIO, ACRONIMI)

Per i termini utilizzati nel presente Manuale si rimanda al Glossario di cui all’Allegato 1 delle Regole Tecniche e alle definizioni del D.lgs. 82/2005 e del DPR 445/2000 e loro successive modifiche 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, ma non presenti nelle citate fonti e 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 Regole tecniche e in ***corsivo grassetto*** i termini contenuti nel presente capitolo.

**Allegato**: ***Documento*** che compone l’***Unità documentaria*** per integrare le informazioni contenute nel ***Documento principale***. È redatto contestualmente o precedentemente al ***Documento principale***. La sua presenza è facoltativa.

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

**Annotazione**: ***Documento*** che compone l’***Unità documentaria,*** riportante elementi identificativi del ***Documento*** e/o 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)

**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 dispostamento 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 da 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)

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

**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*. [da ***OAIS***]

**Contenuto informativo:** l’insieme delle informazioni che costituisce l’obiettivo originario della *conservazion*e. E’ composto dall’***Oggetto-dati*** e dalle ***Informazioni di rappresentazione***.[da ***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 prevede riflessioni anche su persone, siti, risorse e fornitori dell'organizzazione. (Fonte: Wikipedia)

**Control Room:** struttura che si occupa di monitorare in tempo reale il corretto andamento dei servizi IT, individuando i malfunzionamenti, comprendendone l’impatto sui servizi e coordinandone la risoluzione.

**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 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 prodotto dal Sistema a richiesta per ogni *Produttore*, che definisce le specifiche operative del processo 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:** sono i documenti prodotti nel corso del processo di conservazione e normalmente confluiscono nell’AIP.

**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*.

**Esito versamento: *Documento di conservazione*** in formato XML prodotto al termine delle verifiche in fase di ***versamento***, memorizzato nel *Sistema di conservazione* ed 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 una 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)

**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)

**Indice’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 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*. [da ***OAIS***]

**Informazioni sulla rappresentazione:** informazioni che associano un ***Oggetto-dati*** a concetti più significativi. [da ***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***. [da ***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)

**Linee guida sulla conservazione dei documenti informatici:** Documento pubblicato da AgID il 10 dicembre 2015, che illustra le procedure e gli strumenti per l’avvio delle attività di conservazione dei documenti informatici da parte delle Pubbliche Amministrazioni

**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***.

**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. Nel contesto della conservazione digitale si parla di migrazione dei supporti quando i dati sono trasferiti da un supporto di memorizzazione a un altro e di migrazione dei formati, quando gli ***Oggetti-dati*** sono convertiti da un formato a un altro. In entrambi i casi l’obiettivo è contrastare l’obsolescenza tecnologica.

**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)

**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)

**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.

**Oggetto:** insieme di uno o più documenti trasmessi al Sistema per essere sottoposti al processo di Preacquisizione al fine di essere trasformati in SIP ed essere versati in conservazione

**Oggetto-dati o Oggetto digitale:** un oggetto composto da un insieme di sequenze di bit. [da ***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)

**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 oppure 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)

**Regole tecniche:** Decreto del Presidente del Consiglio dei Ministri del 3 dicembre 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.

**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)

**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***;
* a ragione di qualche altra relazione derivante dalle modalità della loro produzione, acquisizione o uso.

(fonte: ***ISAD***)

**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)

**SIEM (Security Information and Event Management):** Le soluzioni rientranti in questa categoria di sistemi sono contraddistinte dalla capacità di effettuare analisi [real-time](https://it.wikipedia.org/wiki/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)

**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***.

**Storage:** dispositivo per memorizzare i dati in formato digitale; sono considerati storage sia i dispositivi a nastro che i dispositivi a disco.

**Struttura versante o Struttura:** ripartizione dell’Ente produttore identificativa della specifica area di produzione dei documenti versati, in genere coincidente con l’*area 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 gestisce e registra delle liste di richieste di assistenza o di problemi, organizzato secondo le necessità di chi offre il servizio. […] Un ticket o biglietto, serve per tenere il filo di una richiesta. Ad ogni biglietto corrisponde un identificativo univoco, che ne consente l'archiviazione e la consultazione in qualunque momento, da parte del personale coinvolto nella sua chiusura. I biglietti 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***. [da ***ISAD***]

**Unità documentaria**: aggregato logico costituito da uno più ***Documenti*** che sono considerati come un tutto unico. Costituisce l’unità elementare in cui è composto l’*archivio*.

**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**.**

**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](#Sommario)]

# NORMATIVA E STANDARD DI RIFERIMENTO

## Normativa di riferimento

La principale normativa di riferimento per l’attività di conservazione a livello nazionale, inclusa quella a livello locale (se definita) in vigore nei luoghi dove sono conservati i documenti e quella specifica relativa alle diverse tipologie di documenti conservati è riportata in modo dettagliato e secondo la gerarchia delle fonti nell'Allegato 1 “Normativa e standard di riferimento”, mantenuto aggiornato.

[[Torna al Sommario](#Sommario)]

## Standard di riferimento

I principali standard di riferimento per l’attività di conservazione elencati nell’allegato 3 delle Regole Tecniche in materia di Sistema di conservazione, sono elencati in modo dettagliato nell'Allegato 1 “Normativa e standard di riferimento”, mantenuto costantemente aggiornato.

[[Torna al Sommario](#Sommario)]

# RUOLI E RESPONSABILITÀ

## Modello organizzativo

L’Ente produttore titolare della documentazione provvede anche all’archiviazione e alla conservazione digitale dei propri documenti informatici**,** nel rispetto dei principi di efficacia, efficienza ed economicità.

Il modello organizzativo adottato è previsto dalle vigenti ***Regole tecniche*** alla lettera a) del comma 2 dell'articolo 5 e definito come “in house” al capitolo 6.1 delle **Linee guida sulla conservazione dei documenti informatici**. [inserire eventuali altri riferimenti normativi significativi].

L’Ente ha tutte le caratteristiche istituzionali, giuridiche e tecniche necessarie anche allo svolgimento delle attività legate alla conservazione a norma e a lungo termine della documentazione informatica e alla tenuta dell’archivio. È quindi, per utilizzare le logiche di ***OAIS***, una struttura organizzata di persone e sistemi che conserva documenti informatici e li rende disponibili ad una ***Comunità di riferimento***.

Le logiche organizzative dell’Ente, nei rapporti fra il *Sistema* (o i *Sistemi*) *di gestione informatica dei documenti* e il *Sistema di conservazione*, fanno riferimento al modello Open Archival Information System (***OAIS***), certificato standard ISO 14721 nel 2003 e recentemente aggiornato (ISO 14721:2012).

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

[[Torna al Sommario](#Sommario)]

## Produttore

L’Ente produttore titolare della documentazione provvede anche alla sua conservazione e descrive le modalità di formazione e gestione della documentazione nel sistema corrente in un apposito documento denominato *Manuale di gestione* e negli altri strumenti archivistici di gestione quali il Titolario di classificazione, il Piano di fascicolazione, il Piano di conservazione, il Massimario di selezione e scarto.

Le modalità per la conservazione a norma e a lungo termine della documentazione sono descritte nel presente *Manuale di conservazione*, redatto dall'Ente stesso in quanto conservatore.

L'Ente, inoltre, cura l'interfacciamento del proprio *Sistema di gestione informatica dei documenti* e/o dei propri sistemi versanti con il Sistema di conservazione, redigendo le relative Specifiche tecniche e altri documenti che descrivano le modalità in cui strutturare la documentazione da conservare (ad esempio dei Modelli SIP che descrivano come l'Ente ha deciso di strutturare e descrivere i SIP delle differenti unità documentarie e un ***Disciplinare tecnico*** che descriva le tipologie documentarie da trasferire e le relative modalità di versamento).

L'Ente che conserva la propria documentazione (con o senza il supporto di un fornitore o di più fornitori esterni) prevede necessariamente al suo interno i ruoli richiesti per la gestione della documentazione e per l’attività di conservazione, non necessariamente articolati nelle figure previste dai requisiti per l'accreditamento Agid:

* *Responsabile della gestione documentale o responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi* (può coincidere con il *Responsabile della conservazione*).
* *Responsabile della Conservazione*.
* Responsabile dei sistemi informativi (al quale potrebbe fare capo il Responsabile dello sviluppo e della manutenzione del *Sistema di conservazione* e delle infrastrutture per la conservazione).
* Responsabile dello sviluppo e della manutenzione del *Sistema di conservazione* e delle infrastrutture per la conservazione (può fare capo al Responsabile dei sistemi informativi).
* *Responsabile del trattamento dei dati*.
* *Responsabile della sicurezza* (distinto dal responsabile dei sistemi informativi nel rispetto del concetto di *segregation of duties*).

L'Ente produttore/conservatore ha ottenuto la certificazione 27001 per il perimetro della conservazione documentale [INSERIRE i riferimenti della certificazione, oppure esplicitare che NON ha ottenuto al certificazione], mentre non ha richiesto l’accreditamento Agid, in quanto non agisce come conservatore per conto di altri Enti.

I ruoli sono riportati nella seguente tabella [INSERIRE i responsabili attuali con indicazione dell’inizio del periodo di responsabilità]:

| RUOLI | ATTIVITÀ DI COMPETENZA | NOMINATIVO | PERIODO NEL RUOLO | EVENTUALI DELEGHE |
| --- | --- | --- | --- | --- |
| Responsabile della gestione documentale o responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi | vedi cap. 5 | Xxxx Xxxx | da xx/xx/xx | - |
| Responsabile della Conservazione | vedi cap. 5 | Xxxx Xxxx | da xx/xx/xx | - |
| Responsabile dei sistemi informativi | vedi cap. 5 | Xxxx Xxxx | da xx/xx/xx | - |
| Responsabile dello sviluppo e della manutenzione del sistema di conservazione | vedi cap.5 | Xxxx Xxxx | da xx/xx/xx | - |
| Responsabile del trattamento dei dati | vedi cap. 5 | Xxxx Xxxx | da xx/xx/xx | - |
| Responsabile della sicurezza | vedi cap. 5 | Xxxx Xxxx | da xx/xx/xx | - |

Per la descrizione nel dettaglio delle 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” che verrà mantenuto opportunamente aggiornato e che riporta i dati delle persone fisiche che hanno ricoperto i vari ruoli.

[[Torna al Sommario](#Sommario)]

### Versatore

Il Versatore è il sistema, interno all’Ente, che materialmente versa i SIP dal *Sistema di gestione informatica dei documenti* al *Sistema di conservazione*.

In base alla organizzazione della gestione documentale dell’Ente, i sistemi versanti potrebbero essere anche più di uno o la documentazione potrebbe essere versata al *Sistema di conservazione* direttamente dal *Sistema di gestione informatica dei documenti*.

[[Torna al Sommario](#Sommario)]

### Fornitore esterno

L’Ente, 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 produzione e di conservazione su esplicita autorizzazione dell’Ente.

[[Torna al Sommario](#Sommario)]

## Utente

In base alla definizione del glossario allegato alle vigenti ***Regole tecniche*** si indentifica come *Utente* 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 dell’Ente, in particolare gli operatori indicati in base alle regole di visibilità e di *accesso* stabilite dall’Ente stesso*.*

L'abilitazione e l'autenticazione di tali operatori avviene in base alle procedure di gestione degli accessi al *Sistema di conservazione* indicate [INSERIRE i riferimenti ai documenti appropriati, quali Piano della Sicurezza, Procedura di gestione utenze, Disciplinari dell’Ente, ecc.] e nel rispetto delle misure di sicurezza previste per la conformità con quanto richiesto dalle norme vigenti in materia di privacy.

In prospettiva si possono definire *Utenti* potenzialmente tutti coloro che potranno interagire con il *Sistema di conservazione* 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](#Sommario)]

## Conservatore

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.*

Il modello organizzativo precedentemente descritto, ai sensi dell'articolo 5, comma 2, lettera a) delle vigenti ***Regole tecniche,*** prevede che il soggetto produttore (l’Ente) provveda anche alla conservazione e al processo di conservazione della documentazione di cui è titolare.

Per la descrizione dei ruoli previsti, si veda il capitolo 4.2.

L’Ente svolge in proprio le seguenti attività legate alla conservazione:

* Si occupa del processo di conservazione della documentazione prodotta (documenti informatici e loro aggregazioni con i metadati ad essi associati) e garantisce il mantenimento nel tempo delle caratteristiche di autenticità, integrità, affidabilità, leggibilità, reperibilità, accessibilità, riproducibilità e intellegibilità.
* Cura le modalità di trasferimento, accesso e fruizione del patrimonio documentario e informativo conservato.
* Attua le procedure di selezione e scarto approvate dall'Organismo di vigilanza competente (Soprintendenza Archivistica competente per il territorio dell'Ente).

È lo stesso Ente produttore che, in quanto conservatore della propria documentazione:

* Presenta al suo interno l'infrastruttura tecnologica necessaria alla conservazione, comprensiva di sito primario e sito per il Disaster Recovery (o almeno di Back up) e cura l'evoluzione tecnologica e l'aggiornamento o la migrazione del *Sistema di conservazione*.
* Gestisce i rapporti con gli eventuali fornitori dei propri sistemi, compreso quello di conservazione. L’Ente descrive nel *Manuale di Conservazione* il modello organizzativo della conservazione adottato, i soggetti e i ruoli coinvolti, il processo, le infrastrutture e le architetture utilizzate e le misure di sicurezza adottate.

Di fatto, quindi, l’Ente conserva i propri documenti garantendo il rispetto dei requisiti previsti dalle norme in vigore nel tempo per i sistemi di conservazione, e svolge l’insieme delle attività elencate nell’articolo 7 comma 1 delle ***Regole tecniche***, in particolare quelle indicate alle lettere a), b), c), d), e), f), g), h), i), j), k) e m).

[[Torna al Sommario](#Sommario)]

## Organismi di tutela e vigilanza

Il Ministero per i beni e le attività culturali (MiBAC) 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[[1]](#footnote-2).

La tutela e vigilanza sugli archivi di enti pubblici non statali è esercitata dal MiBAC, tramite le Soprintendenze archivistiche competenti per territorio.

Secondo quanto disposto dall'art. 36, comma 2 lettera a) del recente regolamento di organizzazione del MiBAC (DPCM 29 agosto 2014, n. 171), il Soprintendente archivistico “svolge, sulla base delle indicazione e dei programmi definiti dalla competente Direzione generale, attività di tutela dei beni archivistici 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, e successive modificazioni”, cioè i conservatori accreditati.

La Soprintendenza archivistica 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.

L’Ente consente alla Soprintendenza archivistica 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’art. 19 del D.lgs. n. 42/2004.

Il Dm 27 novembre 2014 ha ridisegnato la distribuzione degli istituti periferici accorpando, in cinque casi, le Soprintendenze di due regioni sotto un'unica direzione: Abruzzo e Molise, Calabria e Campania, Puglia e Basilicata, Umbria e Marche, Veneto e Trentino Alto- Adige, che si sommano alla già esistente Piemonte e Valle d’Aosta.

Bisogna ricordare che, ai sensi del DPR n. 690 del 1 novembre 1973, 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.

In base alle ***Regole tecniche*** i sistemi di conservazione delle pubbliche amministrazioni e i sistemi di conservazione dei conservatori accreditati sono soggetti anche alla vigilanza dell’AgiD. Per tale fine il *Sistema di conservazione* qui descritto prevede la materiale conservazione dei dati e delle Copie di sicurezza sul territorio nazionale e l'accesso ai dati presso la sede dell’Ente.

[[Torna al Sommario](#Sommario)]

# STRUTTURA ORGANIZZATIVA PER IL SERVIZIO DI CONSERVAZIONE

## Organigramma

Di seguito, si espone una descrizione delle responsabilità presenti all’interno dell’Ente.

**Responsabile della gestione documentale o responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi**: in base a quanto indicato nel Glossario delle regole Tecniche, “dirigente o funzionario, comunque in possesso di idonei requisiti professionali o di professionalità tecnico archivistica, preposto al servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi, ai sensi dell’articolo 61 del D.P.R. 28 dicembre 2000, n. 445, che produce il pacchetto di versamento ed effettua il trasferimento del suo contenuto nel sistema di conservazione.”

Può coincidere con il *Responsabile della Conservazione*.

**Responsabile della conservazione:** è il referente per la definizione e attuazione delle politiche complessive del Sistema di conservazione, nonché del governo della gestione del *Sistema di conservazione*. È responsabile della definizione dei requisiti e delle specifiche del *Sistema di conservazione*, sulla base della normativa vigente, e del funzionamento del servizio di conservazione.

Rientrano tra le sue mansioni e responsabilità:

* + la definizione e gestione del *processo di conservazione*, incluse le modalità di trasferimento, descrizione archivistica, esibizione, accesso e fruizione del patrimonio documentario e informativo conservato;
  + la verifica sistematica dell’aderenza del processo e del *Sistema di conservazione* alla normativa vigente e ai suoi aggiornamenti;
  + il monitoraggio del *processo di conservazione* con la verifica delle modalità di versamento e l’eventuale presenza di errori, la verifica di *integrità* e la descrizione archivistica dei documenti e delle *Aggregazioni documentali informatiche* trasferite;
  + l’analisi archivistica per lo sviluppo di nuove funzionalità del *Sistema di conservazione*;
  + la collaborazione con l’azione del responsabile della gestione documentale (se distinto) ai fini del trasferimento in conservazione e della selezione;
  + la gestione dei rapporti con la Soprintendenza archivistica e le altre articolazioni del MiBAC per quanto di competenza;
  + la sottoscrizione con firma digitale dei *Pacchetti di archiviazione* secondo le modalità descritte nel presente Manuale;
  + l’eventuale sottoscrizione di *Pacchetti di distribuzione* e di attestazioni di conformità di copie cartacee di *Documenti informatici* conservati.

**Responsabile della sicurezza:** è il soggetto al quale compete la definizione delle soluzioni tecniche e organizzative in attuazione delle disposizioni in materia di sicurezza, nonché la verifica del rispetto e il monitoraggio dei requisiti di sicurezza del *Sistema di conservazione* stabiliti dagli standard, dalle normative e dalle politiche e procedure interne di sicurezza.

**Responsabile dei sistemi informativi:** oltre alle mansioni usualmente previste per la gestione dei sistemi informativi dell’Ente, ricopre anche le seguenti mansioni, legate alla responsabilità dei sistemi informativi per la conservazione:

* + la gestione dell’esercizio delle componenti hardware e software del *Sistema di conservazione;*
  + la responsabilità della corretta erogazione dei servizi di conservazione, della verifica e del mantenimento dei relativi livelli di servizi;
  + il monitoraggio, d’intesa con il *Responsabile della Sicurezza*, della sicurezza fisica e logica dell’impianto tecnologico di conservazione;
  + il coordinamento tecnico dei rapporti con eventuali fornitori di data center e supporto tecnologico ai progetti di conservazione digitale;
  + la pianificazione, di concerto con eventuali fornitori, dello sviluppo dell’architettura tecnologica a disposizione per le attività di conservazione e quelle di servizio;
  + il controllo e verifica dei livelli di servizio erogati da eventuali fornitori (SLA), la segnalazione delle eventuali difformità e la pianificazione delle necessarie contromisure;
  + il coordinamento nell’assegnazione, nell’installazione e nella manutenzione delle attrezzature informatiche individuali, nonché nell’assistenza agli operatori, con il supporto dei collaboratori assegnati a tale attività;
  + la collaborazione nelle attività inerenti alla protezione dei dati personali; la predisposizione delle procedure di acquisto di beni e servizi in area informatica;
  + il supporto di rete telematica alle attività dell’Ente.

Potrebbe fare capo al Responsabile dei sistemi informativi anche il Responsabile dello sviluppo e della manutenzione del *Sistema di conservazione*.

**Responsabile dello sviluppo e della manutenzione del sistema di conservazione:** è responsabile del coordinamento e della gestione dei rapporti con eventuali fornitori per le attività di pianificazione strategica e operativa finalizzate alla progettazione e allo sviluppo del *Sistema di conservazione* dell’Ente e per le attività di monitoraggio e di verifica delle operazioni di implementazione del *Sistema di conservazione* e di personalizzazione e implementazione di nuove funzionalità dei sistemi informatici. Tra i suoi compiti rientrano:

* + il monitoraggio dello sviluppo dei progetti informatici e la cura della rispondenza allo standard dei parametri e dei requisiti definiti;
  + il coordinamento delle attività di verifica e di implementazione dei progetti;
  + l’analisi e la progettazione delle nuove procedure informatiche in base alle necessità dell’utenza e agli standard;
  + l’interfaccia con il *Sistema di gestione informatica dei documenti*, in riferimento agli applicativi di gestione, ai formati elettronici da utilizzare, all’evoluzione tecnologica hardware e software, alle eventuali ***migrazioni*** verso nuove piattaforme tecnologiche;
  + l’individuazione di soluzioni di manutenzione delle soluzioni applicative in relazione alle tipologie degli oggetti conservati o da conservare e alle esigenze di evoluzione tecnologica;
  + la definizione delle caratteristiche e dei requisiti del *Sistema di conservazione* (componenti architetturali, applicative, delle risorse e dei servizi);
  + la progettazione e organizzazione del sistema (informativo, informatico, telematico) con riferimento ai diversi processi di sviluppo, di test e rilascio in produzione e di conduzione a regime;
  + la gestione dell'intero ciclo di sviluppo di siti web e portali connessi al servizio di conservazione;
  + il supporto alla verifica dell’aderenza del processo e del sistema di conservazione alla normativa vigente e ai suoi aggiornamenti.

Le figure sopracitate svolgono inoltre le azioni indicate nel *Piano della Sicurezza* in merito alla definizione ed alla attuazione degli indirizzi e delle attività necessarie per assicurare la sicurezza delle informazioni conservate.

**Responsabile del trattamento dei dati**: garantisce il rispetto della normativa vigente in materia del trattamento dei dati personali.

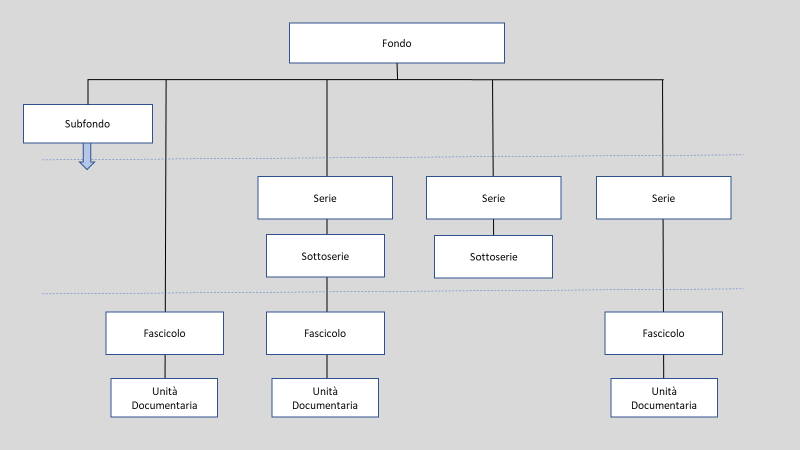
Il *processo di Conservazione* dell’Ente è organizzato secondo la struttura operativa riportata nell’organigramma seguente: [INSERIRE secondo la struttura organizzativa dell’Ente].

# OGGETTI SOTTOPOSTI A CONSERVAZIONE

## Oggetti conservati

Il *Sistema di conservazione* gestito dall’Ente produttore/conservatore conserva *Documenti informatici*, in particolare documenti amministrativi informatici, con i *metadati* ad essi associati e le loro *Aggregazioni documentali informatiche*, (*Fascicoli informatici*). 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, derivato dallo schema dello standard ***ISAD***.



Modello di ordinamento di archivio derivato da ISAD

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, 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 ***Strutture*** (generalmente, ma non necessariamente, corrispondenti alle *Aree Organizzative Omogenee* dell’Ente).

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 sottofascicoli 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 dall’Ente) 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 un determinato 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 dell’Ente.

Per le principali ***tipologie documentarie***, l’Ente elabora e pubblica documenti di studio ed analisi (modelli degli AIP), 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 ***Regole tecniche***;
* 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 l’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 universitaria:** verbali di esame e altri documenti inerenti l’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.

Diverse sono le attività svolte a garanzia non solo della integrità ma anche della fruibilità dell’archivio nel lungo periodo per mantenere la sua leggibilità e reperibilità, anche nella prospettiva della futura fruizione come archivio storico.

A tal fine le strategie adottate per la conservazione prevedono le seguenti azioni:

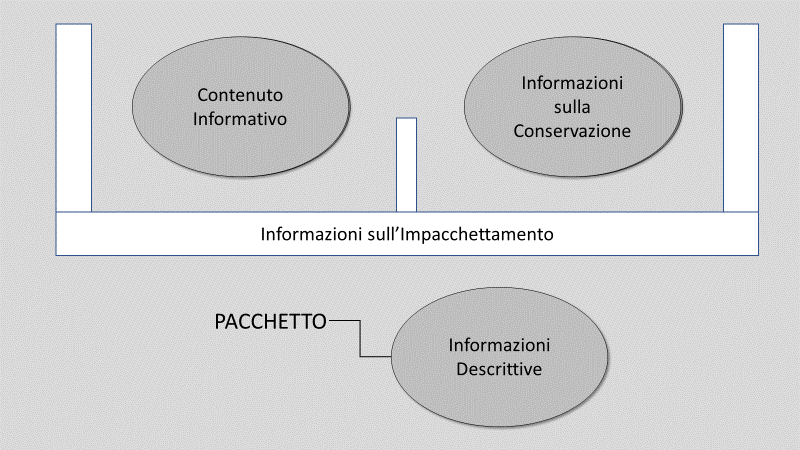
* definire con precisione la ***Comunità di riferimento*** dell’archivio;
* analizzare le caratteristiche archivistiche e tecnologiche dei documenti conservati;
* mantenere attivo un osservatorio tecnologico sulla conservazione ed effettuare sperimentazioni sulle tecnologie disponibili, con particolare 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 dell’archivio nel lungo periodo, l’Ente adotta diverse misure per garantire la reperibilità e la *leggibilità* dei documenti conservati. In particolare per quanto riguarda la reperibilità dei documenti si prevedono appropriate procedure di natura archivistica (creazione di ***Serie***, 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. Quando necessario l’Ente 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, 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.



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](#Sommario)]

### Unità archivistiche e Unità documentarie

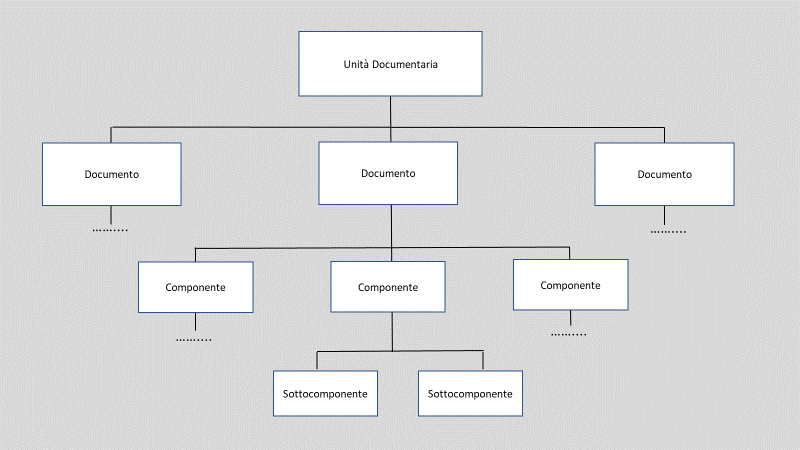
Le ***Unità archivistiche*** contengono una o più ***Unità documentarie***, secondo le logiche di *classificazione* e fascicolazione utilizzate dall’Ente per organizzare i documenti prodotti nel proprio *archivio* (vedi figura successiva).

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***.



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 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***. Normalmente tale contenuto 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*** 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](#Sommario)]

### Formati

Il *Sistema* utilizza come *formati* di conservazione quelli elencati al punto 5 dell’Allegato 5 alle ***Regole tecniche*** e, inoltre, è in grado di gestire anche *formati* non compresi nel suddetto elenco ma che l’Ente utilizza nei propri sistemi e che ritiene di dover conservare.

Tutti i Formati gestiti 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. 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, quali ad esempio quelli elencati al punto 5 dell’Allegato 5 alle ***Regole tecniche***;
* **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 le procedure di cui al comma 1, lettera j, dell’art. 9 delle ***Regole tecniche*** per la produzione delle Copie informatiche di documento informatico;
* **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.

L’Ente individua un elenco di Formati ammessi, che comprende i *formati* che il Sistema può accettare 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 dell’Ente.

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](#Sommario)]

### Metadati

I *metadati* gestiti dal Sistema sono individuati in coerenza a quanto indicato nell’Allegato 5 delle ***Regole tecniche*** e a standard e modelli internazionali di riferimento. Più in dettaglio sono descritti ed analizzati per specifici oggetti da conservare e specifiche ***tipologie documentarie*** tramite i modelli pubblicati.

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* (l’Ente) 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* dell’Ente. 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:** sono contenuti nel SIP e individuano elementi descrittivi ulteriori rispetto a quelli previsti nel profilo generale. Sono definiti per ogni tipologia di ***Unità archivistica*** ***e documentaria***;
* **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](#Sommario)]

## Pacchetto di versamento (SIP)

I pacchetti di versamento (SIP) 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 individuato 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 vari 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 una **Serie:** è il SIP utilizzato per versare le *Serie* (ovvero partizioni annuali – o più generalmente periodiche – delle stesse) e contiene i metadati descrittivi, i dati di consistenza della serie e/o l’elenco delle ***Unità documentarie*** o delle *Unità archivistiche* contenute nella ***Serie*** stessa. Tale SIP genera il corrispondente *Pacchetto di archiviazione* della *Serie*;
* SIP di un’***Unità documentaria***: contiene un’***Unità documentaria*** completa in tutti gli elementi presenti nei sistemi dell’Ente 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, l’Ente 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 precedentemente stabilito. Tali ***Oggetti*** sono sottoposti alla procedura di Preacquisizione (descritta nel paragrafo 7.2) per essere trasformati in SIP ed essere così accettati dal Sistema.

[[Torna al Sommario](#Sommario)]

## 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 7.7). 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, 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 versamenti, ecc.).

L’***Indice dell’AIP*** generato dal Sistema è conforme alle specifiche definite nell’Allegato 4 delle ***Regole tecniche*** e agli specifici Standard individuati dall’Allegato 3.

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 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*. |
| *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 su l’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 (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’essa come una collezione di AIP.

[[Torna al Sommario](#Sommario)]

## 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 e uno coincidente con il SIP, 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 7.8.

[[Torna al Sommario](#Sommario)]

# PROCESSO DI CONSERVAZIONE

Il *processo di conservazione* si attiva con le modalità indicate nel presente *Manuale di conservazione* e dettagliate in un documento quale un ***Disciplinare tecnico***.

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

Il *processo di conservazione* si basa su una logica di conservazione caratterizzata dal ***versamento*** 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 il *formato*, le eventuali firme digitali apposte e a 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 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”[[2]](#footnote-3).

Con ***Versamento in archivio*** si intende il ***versamento*** nel Sistema dei SIP che contengono le *Aggregazioni documentali informatiche* nella loro forma stabile e definitiva, principalmente Fascicoli chiusi e partizioni annuali di ***Serie*** documentarie [[3]](#footnote-4).

Questa fase del *processo di conservazione* è assimilabile al versamento dall’archivio corrente all’archivio di deposito e consente di portare nel Sistema le informazioni necessarie a costruire l’*archivio informatico* dell’ente.

A tal fine, prima di procedere con il loro versamento in archivio, è consigliabile effettuare l’aggiornamento dei metadati dei SIP versati in Versamento anticipato in modo da assicurare che i metadati conservati nel Sistema siano completi e definitivi.

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.

In altri termini si può dire che con il ***Versamento in archivio*** viene completato 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*.

Il Sistema inoltre gestisce 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 ***Regole tecniche*** ai fini dell’*interoperabilità*, il SIP avrà le caratteristiche definite nelle ***Regole tecniche*** all’articolo 9 lettera h.

I SIP sono prodotti e versati nel Sistema con le modalità e le procedure descritte nei loro aspetti generali nel presente Manuale e, per gli aspetti operativi, nel ***Disciplinare tecnico***, 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.

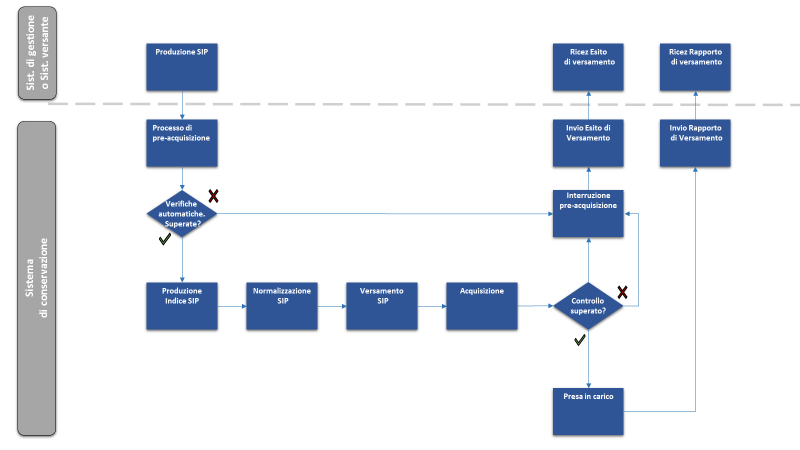
Al momento dell’acquisizione i SIP sono oggetto di una serie di verifiche automatiche. Nel caso in cui le verifiche abbiano avuto successo, il ***versamento*** viene accettato, il SIP viene acquisito per la sua *presa in carico* e viene generato in modo automatico dal Sistema il *Rapporto di versamento,* 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 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 l’Ente non sia in grado di versare i documenti come SIP, può trasmetterli sotto forma di Oggetti (di formato e struttura concordati) 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.



Acquisizione e presa in carico dei SIP

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

[[Torna al Sommario](#Sommario)]

## Preacquisizione

La fase di Preacquisizione ha in input un Oggetto e in output uno o più SIP e si avvia con la trasmissione dell’Oggetto. L’Oggetto trasmesso deve essere conforme alle specifiche definite dall’Ente produttore/conservatore. L’Oggetto viene versato interfacciando un sistema versante o utilizzando il client di versamento manuale messo a disposizione dal *Sistema di conservazione*. Non è prevista la trasmissione degli Oggetti su supporti fisici.

Qualora la trasmissione abbia esito positivo, il *Sistema di conservazione* attesta la corretta ricezione dell’Oggetto.

L’Oggetto ricevuto è sottoposto a una serie di controlli finalizzati a verificarne la conformità con le relative specifiche. Qualora tali verifiche falliscano, il processo si interrompe.

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.

[[Torna al Sommario](#Sommario)]

## Acquisizione

L’acquisizione avviene con il ***versamento*** del SIP normalizzato nel Sistema esclusivamente mediante l’utilizzo dei servizi descritti nel paragrafo 8.2 ed in dettaglio nel documento “Specifiche tecniche dei servizi di versamento”.

Può avvenire mediante l’interfacciamento di sistemi o mediante il client di versamento manuale messo a disposizione dal *Sistema di conservazione*, mediante il quale inserire i dati necessari a generare e versare il SIP normalizzato nel Sistema.

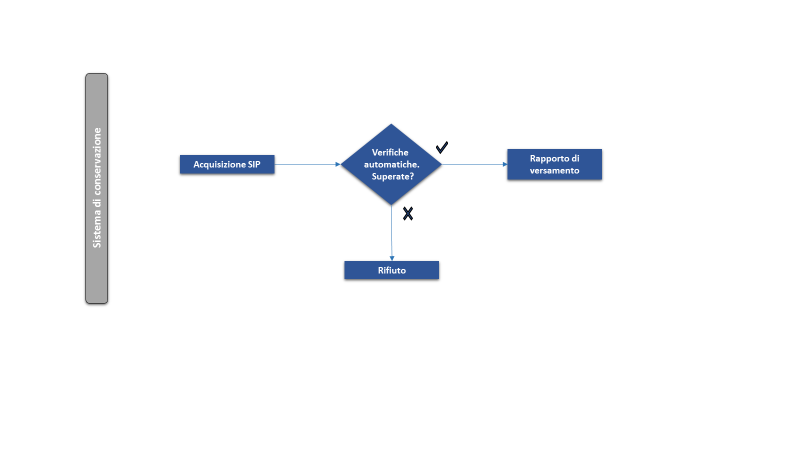
Non è prevista la trasmissione di SIP su supporti fisici.

Al completamento della trasmissione, il SIP è acquisito e memorizzato in un’area di lavoro temporanea del Sistema che avvia contestualmente il processo di verifica del pacchetto, descritto nel paragrafo seguente.

[[Torna al Sommario](#Sommario)]

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

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



Verifiche effettuate sui SIP

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’*area organizzativa omogenea* di riferimento e a garantire il corretto inserimento nell’*archivio* nella opportuna ***Struttura***;
* 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 configurato nel sistema;
* l’univocità degli identificativi degli oggetti contenuti nel SIP: il controllo è finalizzato a verificare che gli identificativi assegnati nel *Sistema di gestione informatica dei documenti* e contenuti nel SIP siano effettivamente univoci, verificando che gli stessi non siano già presenti nel *Sistema di conservazione*;
* 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 precedentemente stabiliti dall’Ente. Tali set sono configurati nel *Sistema di conservazione* 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 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 precedentemente stabilito dall’Ente: le verifiche si esplicano nel calcolo del ***mimetype*** dell’***Oggetto-dati*** e nel confronto del valore così ottenuto sia con quello eventualmente dichiarato nel SIP, sia con i Formati ammessi, documentati e conservati nel *Sistema di conservazione* nelle funzionalità di Amministrazione delle strutture versanti;
* **i controlli di coerenza e 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 di conservazione* opera in questo frangente, sono illustrati nel documento “Specifiche tecniche dei servizi di versamento”.

[[Torna al Sommario](#Sommario)]

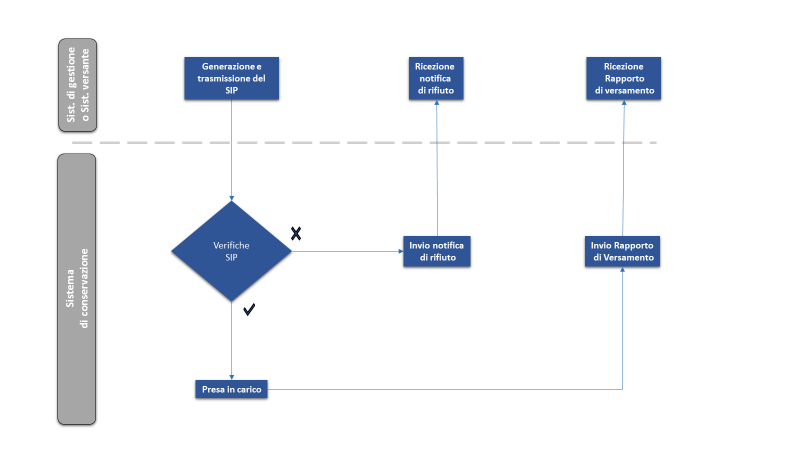
## Accettazione dei pacchetti di versamento e generazione del rapporto di versamento di presa in carico

Nel caso in cui tutte le verifiche abbiano avuto esito positivo, il SIP viene acquisito nel *Sistema di conservazione* per la sua *presa in carico*, memorizzato nelle sue varie parti (***Indice del SIP*** e ***Oggetti-dati***), associato logicamente all’*archivio* 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 7.7).

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 di conservazione* 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”.



Accettazione / Rifiuto dei SIP

Il *Rapporto di versamento* è reso disponibile 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 di conservazione* dagli operatori abilitati utilizzando le apposite funzionalità del Sistema.

[[Torna al Sommario](#Sommario)]

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

Nel caso in cui almeno una delle verifiche elencate al paragrafo 7.4 non vada a buon fine, il SIP viene rifiutato e il *Sistema di conservazione* restituisce gli errori riscontrati, inviando al versatore 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 di conservazione*, logicamente esterna all’*archivio* vero e proprio, a cui gli utenti abilitati possono accedere utilizzando l’interfaccia web del *Sistema di conservazione*, per eventuali ulteriori controlli e verifiche (vedi paragrafo 7.6.1).

I SIP rifiutati restano memorizzati nel *Sistema di conservazione* almeno per un anno, trascorso il quale 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 e della quantità e qualità dei versamenti falliti.

[[Torna al Sommario](#Sommario)]

### Monitoraggio

Il *Sistema di conservazione* 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 normalizzati 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.

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 versatore 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 versatore 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 versatore 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 di conservazione*, si può procedere a modificare di conseguenza le configurazioni (previa decisione dell’Ente). Di tale modifica viene data comunicazione al versatore 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 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 versatore provvede ad annullarlo utilizzando apposite funzionalità del Sistema. 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, e sono richiamabili solo da utenti appositamente abilitati a farlo.

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](#Sommario)]

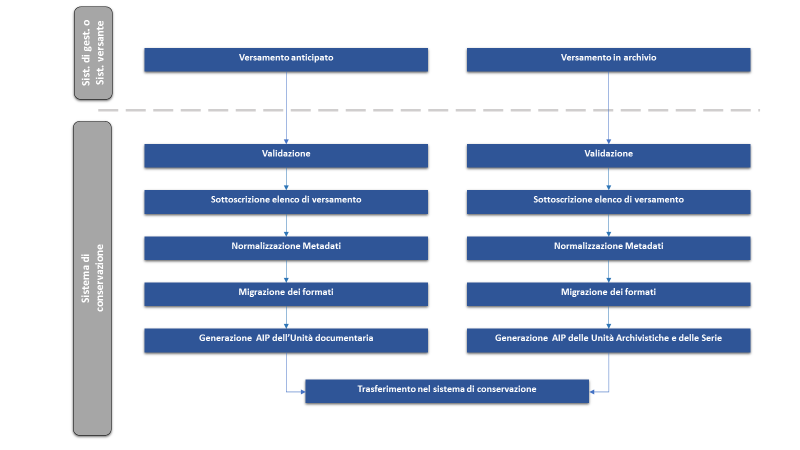
### Gestione delle anomalie

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 sistema versante, che pertanto, erroneamente, lo reputa non versata. | Il sistema versante lo trasmette nuovamente 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 dall’Ente 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 sistema versante 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.). | L’Ente stabilisce 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 sistema versante segnala il problema al *Sistema di conservazione*, che si attiverà per la sua risoluzione. |
| 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 che si ritiene più semplice correggere per via tecnica, piuttosto che annullare e versare nuovamente | L’Ente stabilisce formalmente di effettuare una correzione tecnica dei dati nel *Sistema di conservazione*; il gruppo di sviluppo e manutenzione viene quindi incaricato ad 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 tracciata all’interno del sistema di gestione delle attività di sviluppo e manutenzione. |

[[Torna al Sommario](#Sommario)]

## Preparazione e gestione del Pacchetto di archiviazione



Gestione degli AIP

Come elemento ulteriore di controllo dei versamenti effettuati, i SIP accettati e presi in carico sono inseriti in appositi ***Elenchi di versamento***[[4]](#footnote-5) generati mensilmente per ***tipologia documentaria*** e anno di produzione.

L’***Elenco di versamento*** è un documento in formato XML che 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.

Gli elementi inseriti nell’Elenco possono essere sottoposti a ulteriori controlli, anche a campione, finalizzati a verificare la corrispondenza degli oggetti versati con quanto precedentemente stabilito e a evidenziare eventuali anomalie non rilevabili dalle verifiche automatiche al ***versamento***.

Una volta completati i controlli, l’Elenco viene chiuso, eventualmente suddiviso in più parti per contenerne la dimensione, gli viene apposto un *Riferimento temporale* opponibile ai terzi e viene firmato digitalmente dal *Responsabile della conservazione* ad attestare la *presa in carico* dei relativi SIP.

Tale Elenco è recuperabile utilizzando apposite funzionalità dell’interfaccia web del Sistema.

I SIP accettati e presi in carico dal Sistema, dopo la validazione e la firma 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) che prevede:

* l’eventuale normalizzazione del set di *metadati* contenuti nel SIP e/o della struttura dell’***Unità documentaria*** per renderli conformi al set di *metadati* e alla struttura dell’AIP così come definiti nel documento “Modelli di pacchetto di archiviazione”;
* l’eventuale ***migrazione*** dei *formati* ritenuti obsoleti (secondo le logiche descritte nel paragrafo 6.1.2) mediante il processo di produzione di copie informatiche con le modalità previste dalla lettera j) comma 1 dell’articolo 9 delle ***Regole tecniche***.

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 struttura dati dell’Allegato 4 delle ***Regole tecniche*** e descritto in dettaglio del documento “Modelli di pacchetto 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 per tutti i file che compongono gli’AIP 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, relative 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.

Una volta prodotto l’AIP dell’***Unità documentaria***, questo viene firmato dal *Responsabile della conservazione*.

La firma 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 firma viene apposta su un’evidenza informatica prodotta a partire dagli ***elenchi di versamento*** e contenente gli identificativi delle ***Unità documentarie*** contenute negli elenchi stessi e l’hash dei relativi Indici AIP. Tale evidenza informatica, una volta firmata, è inserita negli AIP delle singole ***Unità documentarie***.

Nel caso di ***Versamento in archivio***, invece, la firma degli AIP delle ***Unità documentarie*** avviene attraverso la firma 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 firmati dal *Responsabile della conservazione* ad attestare il corretto svolgimento del processo di ***Versamento in archivio*** che completa il processo di trasferimento al *Sistema di conservazione*.

Con la firma dell’AIP dell’*Aggregazione documentale informatica* si determina anche l’Accettazione della custodia da parte del *Sistema di conservazione* 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 7.10.

Gli utenti dell’Ente abilitati possono accedere agli AIP conservati utilizzando le apposite 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 nuovo SIP e attivazione di procedure di conservazione da parte del *Sistema di conservazione*.

Nel primo caso l’aggiornamento dell’AIP viene innescato dall’invio di 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.

[[Torna al Sommario](#Sommario)]

## Preparazione e gestione del Pacchetto di distribuzione (DIP) ai fini dell’esibizione

I DIP sono prodotti di norma 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, ognuno 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 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***, PI SIP, ***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 apposite 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 solo previa autorizzazione da parte dell’Ente.

Gli utenti abilitati dall’Ente possono consultare quanto versato nel *Sistema di conservazione* tramite interfaccia web, collegandosi a un apposito indirizzo e autenticandosi utilizzando username e password preventivamente forniti dall’Ente.

Gli operatori da abilitare per l’*accesso* tramite interfaccia web al *Sistema di conservazione* sono infatti abilitati formalmente dall’Ente.

L’accesso web consente agli utenti di ricercare i documenti e le aggregazioni versati, di effettuarne il download e di acquisire le evidenze delle attività di conservazione.

[[Torna al Sommario](#Sommario)]

## 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 di DIP comprensivi degli ***Oggetti-dati*** che li compongono.

Tali pacchetti sono acquisibili dagli *Utenti* utilizzando specifiche funzionalità dell’interfaccia web del Sistema o utilizzando gli appositi servizi descritti nel documento “Specifiche tecniche dei servizi di recupero”.

Non è previsto da parte del *Sistema di conservazione* 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 nel *Sistema di conservazione*, questo si limita a fornire, su precisa richiesta dell’Ente e senza che su di esso debba gravare alcun particolare onere, il documento informatico conservato, qualora per un qualsiasi motivo l’Ente stesso abbia deciso di non acquisirlo direttamente mediante le modalità descritte nel paragrafo 7.8.

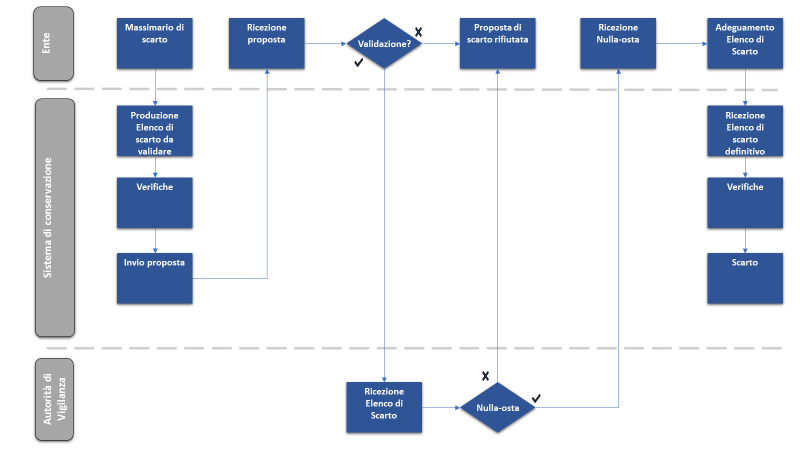
Permane in carico all’Ente sia la responsabilità di valutare la fondatezza giuridica della domanda di accesso, sia l’onere di far pervenire il documento (o sua eventuale copia cartacea conforme) al soggetto richiedente, sia la responsabilità della consegna di documentazione richiesta nel caso di visite ispettive o provvedimenti di esibizione o sequestro da parte dell’autorità giudiziaria o di altra autorità ispettiva.

Nei casi previsti dalla normativa, il ruolo di pubblico ufficiale è svolto dal Responsabile della 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 un dirigente all’uopo individuato o da altro soggetto da quest’ultimo designato.

[[Torna al Sommario](#Sommario)]

## Scarto dei pacchetti di archiviazione



Scarto degli AIP

Il *Sistema di conservazione* mette a disposizione funzionalità dedicate a gestire la selezione e lo *scarto* delle *Aggregazioni documentali informatiche* (***Unità archivistiche*** e ***Serie***) e dei *Documenti informatici* che ne fanno parte, in conformità alle norme vigenti.

In base ai tempi di conservazione risultanti dal ***Massimario di scarto*** dell’Ente produttore/conservatore, definito a livello di ***Piano di Conservazione*** di ***Unità archivistica*** o di ***Unità documentaria*** in appositi *metadati*, il *Sistema di conservazione* produce annualmente, o su richiesta, un Elenco di scarto, cioè un elenco delle ***Unità archivistiche*** o ***Unità documentarie*** che hanno superato il tempo minimo di conservazione e possono essere sottoposte a procedure di *scarto*. Possono essere soggetti a *scarto* solo le *Aggregazioni documentali informatiche* e i *Documenti informatici* che sono stati oggetto di ***Versamento in archivio***.

Tale Elenco di scarto può essere rifiutato dall’Ente (perché non intende procedere allo *scarto*) o validato (eventualmente dopo averlo opportunamente modificato).

L’Elenco di scarto così validato viene trasmesso dall’Ente all’Autorità di vigilanza (Soprintendenza archivistica) che, in base alle norme vigenti, deve fornire il nulla-osta per lo *scarto*.

L’Ente, una volta ricevuto il nulla-osta (che può essere concesso anche solo su una parte dell’Elenco proposto), provvede ad adeguare, se necessario, l’*Elenco di scarto* presente sul *Sistema di conservazione* alle decisioni dell’Autorità. Una volta che l’*Elenco di scarto* definitivo viene predisposto, l’Ente lo valida e viene trasmessa al *Sistema di conservazione* la richiesta di procedere allo *scarto*.

Il *Sistema di conservazione* effettua un ulteriore controllo sulla congruenza dell’*Elenco di scarto* definitivo con quello autorizzato dall’autorità e, in caso siano riscontrate anomalie, l’Elenco viene corretto e sottoposto nuovamente alla validazione da parte dell’Ente.

Nel caso il controllo sull’*Elenco di scarto* dia esito positivo, il *Sistema di conservazione* procede alla cancellazione degli AIP contenuti nell’Elenco. L’operazione di *scarto* viene tracciata sul Sistema mediante la produzione di *metadati* che descrivono le informazioni essenziali sullo *scarto*, inclusi gli estremi della richiesta di nulla osta allo *scarto* e al conseguente provvedimento autorizzatorio e la traccia del passaggio dell’AIP scartato nell’*archivio*.

[[Torna al Sommario](#Sommario)]

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

Nel caso l’Ente decida di passare a un S*istema di Conservazione* in outsourcing, provvede a riversare dal proprio *Sistema di conservazione* 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 nuovo sistema, secondo modalità e tempi concordati con il nuovo conservatore.

Vengono comunque mantenuti nel Sistema di conservazione i *Documenti informatici* e le *Aggregazioni documentali informatiche* conservati, con i *metadati* a essi associati e le *evidenze informatiche* generate nel corso del *processo di conservazione* fino alla ufficializzazione dell’effettiva messa a disposizione del *Sistema di conservazione* in cui effettuare il riversamento.

L’Ente provvederà all’eliminazione dal proprio *Sistema di conservazione* di tutti gli oggetti riversati solo al termine del riversamento e solo dopo le opportune verifiche di corretto svolgimento del riversamento stesso.

L’intera operazione dovrà comunque avvenire con l’autorizzazione e la vigilanza delle competenti autorità, in particolare delle strutture del MIBAC.

Per quanto riguarda gli aspetti operativi per il trasferimento di *archivi* ad altri *sistemi di conservazione*, si adotta lo standard Uni Sincro, e si provvederà a trasferire secondo canali sicuri concordati con il nuovo conservatore le informazioni.

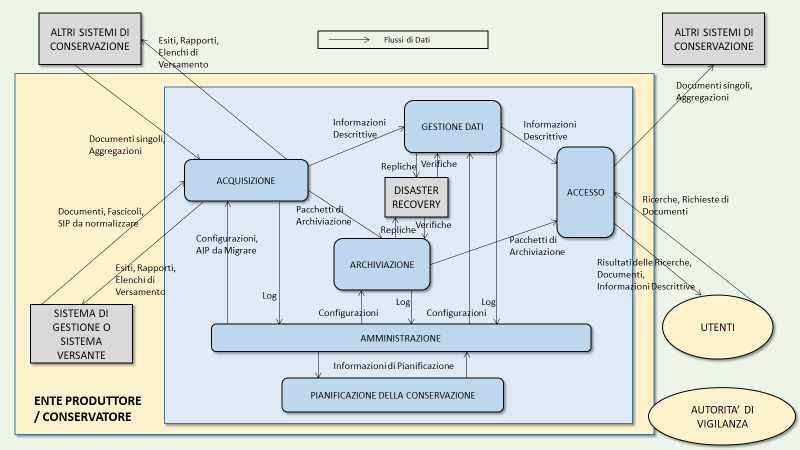
Analogamente il *Sistema di Conservazione* dell’Ente è predisposto per la ricezione di *archivi* in formato Uni Sincro, nel caso l’Ente abbia in precedenza conservato documentazione presso un conservatore in outsourcing.

[[Torna al Sommario](#Sommario)]

# IL SISTEMA DI CONSERVAZIONE

## 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* dell’Ente e le principali relazioni con i soggetti interessati dal *processo di conservazione* descritto nei capitoli precedenti del presente Manuale e i principali flussi di dati tra le componenti del sistema e i relativi attori.



Schema logico del Sistema di conservazione e Flussi dei Dati

In ottica di *interoperabilità* il *Sistema di conservazione* è in grado di ricevere da altri *sistemi di conservazione* documenti già sottoposti a conservazione (nel caso di archivi che l’Ente decide di conservare in proprio, dopo averli affidati per un certo periodo ad un Ente conservatore accreditato), e di versarli ad altri Sistemi (nel caso di archivi che l’Ente decide di affidare ad un Ente conservatore accreditato, dopo averli conservati in proprio per un certo periodo), sulla base di accordi da stabilire di volta in volta con gli altri conservatori (si veda cap. 7.11).

Le funzionalità di Acquisizione gestiscono la fase di Acquisizione e *presa in carico* del *processo di conservazione* (vedi paragrafi 7.3-7.6), ovvero, attraverso i ***Web Service*** di versamento esposti dal Sistema, consentono la ricezione dei SIP, 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 7.7): *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, inclusi 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 di conservazione* 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. Tali funzioni non sono svolte da uno specifico applicativo, né seguono procedure meccaniche, configurandosi 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 di conservazione*, in implementazione di nuove librerie o altri strumenti software utilizzati dal Sistema, nella definizione e nell’aggiornamento delle politiche di conservazione, nei test su nuovi componenti hardware, e in altro ancora.

Normalmente 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*** dell’Ente.

Le funzionalità di *accesso* gestiscono la fase di gestione del DIP del *processo di conservazione* (vedi paragrafo 7.8): 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 dagli allegati 3 e 4 delle ***Regole tecniche***.

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 [ELIMINARE O ADATTARE questa frase se non si gestiscono file su cassetta, quali le immagini DICOM].

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 dei sistemi operativi, di rete e di sicurezza dei sistemi, mette a disposizione in particolare:

* il servizio di **Identity Management**, via *IDP,* che garantisce i corretti accessi al Sistema da parte dei diversi utilizzatori;
* il servizio di Firma remota tramite dispositivo ***HSM*** [OPPURE INDICARE il proprio sistema di Firma], che consente al *Responsabile della conservazione* o a un suo delegato di apporre la firma digitale agli ***Elenchi di versamento*** e agli AIP senza utilizzare ***applet*** di firma all’interno del browser;
* il servizio di **Log**, che mantiene e manda in conservazione la storia degli accessi effettuati al Sistema, sia in scrittura che in lettura, e i registri dei nodi hardware e software del Sistema, ivi compresi i registri dello sviluppo e della manutenzione del software;
* il servizio di **Audit**, che consente di analizzare gli eventi accaduti, accedendo ai registri di log ad alle altre informazioni registrate dal Sistema, ed organizzandole ai fini della fruizione dell’Auditor;
* il servizio di **Monitoraggio Tecnico**, [ADATTARE in base alla propria infrastruttura] che consente alla struttura sistemistica di gestione di mantenere sotto controllo l’intera infrastruttura, mettendo a disposizione meccanismi specifici di controllo, di allerta e di prevenzione dei problemi;
* il servizio di ***Trouble Ticket*** [SE E’ PRESENTE], che mantiene traccia delle segnalazioni di problemi e malfunzionamenti e delle richieste di supporto da parte degli utenti [INDICARE eventuali altri utilizzi];
* il **Sito Web** dell’Ente, che fornisce informazioni e documentazioni relative al processo e al *Sistema di conservazione*.

[[Torna al Sommario](#Sommario)]

## 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.

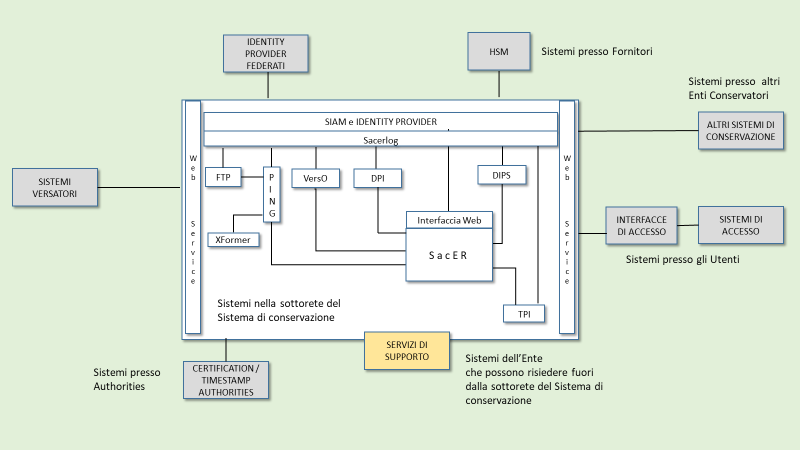
Il diagramma schematizza dal punto di vista tecnologico le principali componenti del *Sistema di conservazione* dell’Ente e le principali relazioni con altri sistemi interessati dal *processo di conservazione* descritto nei capitoli precedenti del presente Manuale.

Il *Sistema di conservazione* utilizzato è quello fornito in riuso dall’IBACN (Istituto dei Beni Artistici Culturali e Naturali della regione Emilia-Romagna) sotto il nome del suo componente principale (SacER - Sistema per l’archivio di conservazione dell’Emilia-Romagna) e originariamente implementato e successivamente manutenuto e sviluppato presso il ParER (Polo archivistico dell’Emilia-Romagna).

Il diagramma in figura rappresenta il *Sistema di conservazione* nel suo complesso, ivi inclusi i principali sistemi esterni, che interagiscono sistematicamente con il sistema stesso al fine di realizzare il processo di conservazione.

Nella figura [DA MODIFICARE in base all’infrastruttura tecnologica di riferimento e alla presenza dei moduli facoltativi, quali PING, XFormer, DPI, TPI] sono riportate

* in bianco le componenti del *Sistema di* conservazione interne al perimetro di sicurezza del *Sistema di conservazione*;
* in arancione le componenti a supporto del *Sistema di conservazione* gestite dall’Ente, ma esterne al perimetro di sicurezza del *Sistema di conservazione*;
* in grigio le componenti gestite da soggetti esterni al *Sistema di conservazione* (*Sistema di gestione informatica dei documenti, Sistema versante,* *Utenti, Authorities, Fornitori di servizi*).



Schema Tecnologico del Sistema di conservazione

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

[[Torna al Sommario](#Sommario)]

### 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 SacERconsentono la gestione delle varie fasi del processo di Acquisizione e *presa in carico* (vedi paragrafi 7.3-7.6). Operativamente si compongono delle seguenti attività:

* acquisizione del SIP normalizzato 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 dall’Ente; 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 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 Sistemada 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 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 7.7) 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 [ADATTARE il testo, in ragione dell’utilizzo che si fa del file system] 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 mantenuti all’interno del Data Base in opportune tabelle di ***BLOb***
  + 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’integritàdegli 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 al Piano di Sicurezza;
* 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 7.10, gli oggetti dati degli AIP sono cancellati dal Sistema. Tale cancellazione può essere fisica o logica, a seconda dei supporti di memorizzazione utilizzati e delle tipologie degli AIP.

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 7.7) e includono:

* la ***memorizzazione*** dei *metadati* estratti dal SIP o generati dal Sistema nel corso del processo di Acquisizione 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 delle decisioni dell’Ente, definite nel ***Disciplinare tecnico*** e in funzione delle policy determinate 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 7.6.1. In particolare, in SacER è possibile configurare tutte le entità significative: Ente, ***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 del *Sistema di conservazione*, ma visibili negli esiti anche agli altri operatori dell’Ente abilitati.

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. Nel caso in cui la trasformazione dell’AIP in DIP richieda specifici passi elaborativi e trasformazioni complesse che necessitano di elaborazioni onerose, tali elaborazioni vengono eseguite da opportuni job batch e mantenute in modo permanente sul Data Base.

Secondo la natura dei DIP, l’*esibizione* può avvenire on-line, tramite download, oppure tramite il trasferimento in un’area di transito, da cui il successivo recupero viene effettuato dal sistema richiedente con chiamata FTP. In generale, 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](#Sommario)]

### VersO

Il client di versamento manualeVersO (Versamento Online) è un modulo che utilizza un’interfaccia web e quindi non richiede l’installazione di alcun software sulla stazione di lavoro dell’operatore.

Il suo utilizzo tipico è per 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*** dell’Ente, utilizzando in ogni caso logiche di profilazione del Sistema, ed effettua il ***versamento*** dei SIP tramite interazione guidata con l’operatore.

Tale modulo semplifica le operazioni di ***versamento*** manuale da parte dell’operatore, 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](#Sommario)]

### PING

[ELIMINARE SE NON PRESENTE] Il modulo software PING (PreINGest) gestisce il processo di preacquisizione nel caso di ***versamento*** di Oggetti da trasformare in SIP (vedi paragrafo 7.2).

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 di 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*** (normalizzato) 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 richieda regole precodificate (come p.e. nel caso delle immagini diagnostiche in formato Dicom), oppure tramite il modulo XFormer.

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

PING mette inoltre a disposizione un client di versamento di Oggetti da normalizzare, sia on line (utilizzabile nel caso di Oggetti di dimensioni contenute), sia tramite l’utilizzo di un client ***FTP*** installato sulla postazione di lavoro dell’utente o su un server della rete dell’Ente.

[[Torna al Sommario](#Sommario)]

### XFormer

[ELIMINARE SE NON PRESENTE] Il modulo software XFormer viene utilizzato da PING per normalizzare i pacchetti di versamento durante il processo di preacquisizione, in tutti i casi in cui le regole precodificate non siano applicabili.

In questo caso vengono applicate regole di trasformazione ad hoc in base alla tipologia documentaria da conservare e al formato dello specifico Oggetto trasmesso; XFormer si occupa di trasformare l’Oggetto ricevuto, producendo i SIP normalizzati da versare, che restituisce a PING per l’effettivo versamento.

Le regole di trasformazione vengono sviluppate tramite uno strumento visuale ad hoc, e integrate all’interno di XFormer.

[[Torna al Sommario](#Sommario)]

### DPI

[ELIMINARE SE NON PRESENTE] Il modulo software DPI (Digital Preservation Interface) consiste in un sistema di interfaccia tra i sistemi di produzione e PING, che può essere installato all’interno della rete dell’Ente, venendo gestito secondo le politiche di sicurezza dell’Ente.

DPI implementa funzionalità di ***versamento*** per specifiche tipologie di Oggetti. In particolare, qualificandosi come nodo ***DICOM***, DPI riceve dai ***PACS*** studi diagnostici, che poi trasmette a PING per la normalizzazione e il ***versamento*** a SacER.

DPI può operare con logiche sia push che pull, ricevendo o estraendo dati e documenti dai sistemi di produzione per poi versarli nel Sistema, richiamando gli opportuni servizi di PING.

Inoltre DPI fornisce strumenti di monitoraggio dei versamenti effettuati.

[[Torna al Sommario](#Sommario)]

### 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 sevizi di recupero”. Tali servizi sono invocati anche dai componenti di versamento del Sistema di conservazione (DPI, VersO), oltre che dai sistemi di versamento.

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 dell’Ente. Fa eccezione il client interno a PING, che può versare anche on line, senza appoggiarsi su protocollo FTP.

[[Torna al Sommario](#Sommario)]

### TPI

[ELIMINARE SE NON PRESENTE O ADATTARE SE SI UTILIZZANO ALTRI SISTEMI DI GESTIONE DEL FILE SYSTEM] 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.

In particolare, 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 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 anche una seconda copia per ogni cassetta; le copie vengono trasportate in camera di sicurezza, dove vengono immagazzinate al sicuro da eventi catastrofici, assieme alle copie dei backup del Data Base Oracle.

Le attività di gestione del sito secondario sono tracciate in uno specifico Data Base del sistema di gestione della ***tape library***.

[[Torna al Sommario](#Sommario)]

### 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](#Sommario)]

### 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), ma mantiene il Data Base dei profili di tutti gli operatori abilitati al Sistema, gestendo 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*** colloquia con i moduli del Sistema tramite standard SAML (Security Assertion Markup Language).

[[Torna al Sommario](#Sommario)]

### 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.). E’ completamente parametrabile tramite funzioni di amministrazione quali combinazioni di agenti / eventi / oggetti / debbano essere registrati nel log.

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 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](#Sommario)]

### Componenti di supporto

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

* il time server della rete 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).
* 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. [ADATTARE in base alle specifiche tecnologie utilizzate] Il modulo di Log si basa su un sistema ***SIEM*** opportunamente configurato e alimentato, che si occupa di raccogliere i *log* e memorizzarli in conformità con le politiche definite dall’Ente sulla base della normativa vigente, in conformità con i disciplinari dell’Ente e con la necessità di mantenere nel Sistema tutte le informazioni necessarie a documentare le attività svolte, anche per funzionalità di audit; componenti di audit e log sono inoltre presenti sul sito di ***Disaster recovery***
* [ADATTARE in base alle specifiche tecnologie utilizzate]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 preposta alla gestione. Analoghe componenti di monitoraggio tecnico sono presenti sul sito di ***Disaster recovery;***
* ELIMINARE se non è presente] il modulo di trouble ticketing viene utilizzato per automatizzare e mantenere traccia dei processi fondamentali del servizio di conservazione: tra questi la gestione dei malfunzionamenti, la gestione delle richieste di rilascio in produzione delle nuove versioni dell’applicativo e le richieste di manutenzione dell’infrastruttura. Analoga situazione è presente per il sito di ***Disaster recovery;***
* [ELIMINARE se non si effettuano sviluppi integrativi al sistema in riuso] i componenti di supporto allo sviluppo vengono utilizzati per garantire la corretta gestione degli sviluppi a integrazione del software in riuso, per quanto riguarda sia l’evoluzione che la manutenzione correttiva; in generale si tratta di componenti open source normalmente utilizzati dai gruppi di sviluppo 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 opportuni strumenti;
* [ADATTARE] il sito web e/o l’intranet dell’Ente espone in modo strutturato informazioni e documentazione utile agli *Utenti* (***Comunità di riferimento***). Dal sito è possibile inoltre [AGGIUNGERE eventuali altri utilizzi del sito];
* [ELIMINARE se non si dispone di un sistema di e-learning, oppure citare quello di ParER, se utilizzato] sistema di e-Learning per la diffusione delle pratiche di conservazione.

[[Torna al Sommario](#Sommario)]

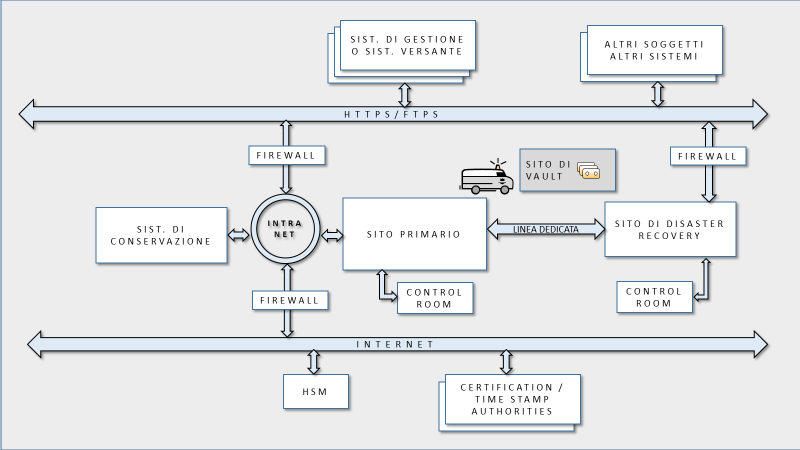
## Componenti fisiche

### 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 ed assicurare la riservatezza degli accessi.

Il Sistema è sviluppato con tecnologie di larga diffusione open source o comunque di libero utilizzo, a parte il Data Base, che, per ragioni di sicurezza e di performance, è proprietario ma standard SQL,[ELIMINARE O ADATTARE p.e. nel caso di memorizzazione su file system] e il sistema di gestione dello ***storage*** su cassetta, che è legato alla tecnologia della ***tape library***.

Il diagramma in figura [DA MODIFICARE in base all’infrastruttura tecnologica utilizzata, alla presenza di un sito di Vault, ecc] schematizza le principali componenti infrastrutturali del *Sistema di conservazione* dell’Ente e le principali relazioni con altri sistemi interessati dal *processo di conservazione* descritto nei capitoli precedenti del presente Manuale.



Schema Infrastrutturale del Sistema di conservazione

[ADATTARE in base alla propria infrastruttura] Il Sistema è realizzato su due siti: un sito primario, installato presso il ***Data Center*** xxxxx a xxxxx, che svolge funzioni di normale operatività, ed un sito secondario, installato presso il ***Data Center*** di xxxxx a xxxxx, che ha lo scopo di subentrare come sito di ***Disaster recovery*** nel caso di caduta irreparabile del sito primario. Il sito primario è gestito all’interno di una sottorete dell’Intranet dell’Ente dedicata al *Sistema di conservazione*, e controllato dal personale della Control Room di xxxxx, mentre il sito di ***Disaster recovery*** è gestito dalla ***Control Room*** di xxxx. Il collegamento tra i due siti è garantito da una linea dedicata in banda larga a x Gb/s, fornita da xxxx. 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.

Una copia di back up del sistema viene effettuata su un sito di vault, che dista xxxxx km dal sito primario e xxxxx km dal sito secondario.

Alcuni sistemi di supporto sono installati in una sottorete separata del ***data center***, ad esempio i log server, i time server, i server di monitoraggio, i server che ospitano il sito web dell’Ente e i ***proxy*** che gestiscono gli scambi con gli ***HSM***. La comunicazione tra la sottorete del *Sistema di conservazione* e la sottorete 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 xxxxx.

Tutti i componenti del sito primario, inclusi quelli installati nella sottorete, e i componenti esterni sviluppati dall’Ente conservatore, nonché gli ***HSM***, sono ridondati, mentre non lo sono i componenti del sito di ***Disaster recovery***.

Il *Sistema di conservazione* interagisce con il *Sistema di gestione informatica dei documenti* tramite protocollo https/ftps.

In situazione di funzionamento normale il Sistema è attivo solo sul sito primario; il sito secondario 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 [SOLO con TPI attivo] di archiving sotto il controllo del sito primario.

In caso di caduta irreparabile del sito primario (disastro) il sito secondario viene posto in stato di attività e attivato come destinatario del traffico di rete tramite rotazione del ***DNS***.

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 del *Sistema di conservazione* per il test delle nuove versioni rilasciate dai laboratori di sviluppo;
* [SE NON ESISTE, rivedere la descrizione del sistema di Test] un’***istanza*** di Pre-produzione, allineata all’***istanza*** di produzione, per i test effettuati dai Sistemi versanti.

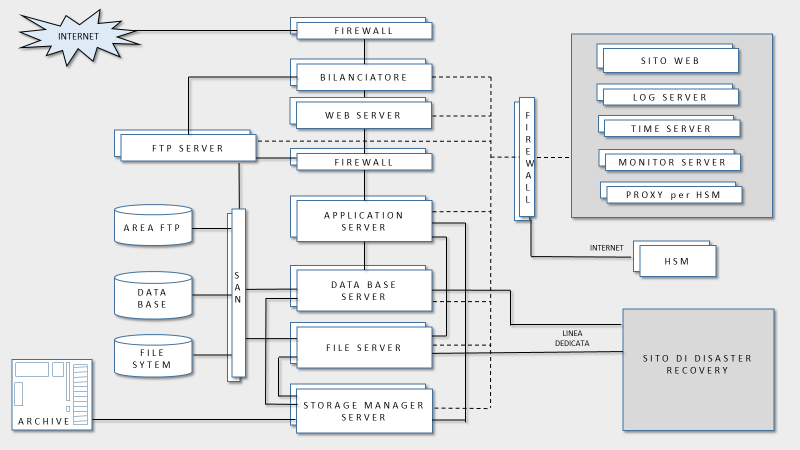
[[Torna al Sommario](#Sommario)]

### Caratteristiche tecniche del Sito primario

[ADATTARE – quella indicata è un’infrastruttura “ideale”] Il Sistema è sviluppato in ***Java*** su sistemi operativi Linux utilizzando i seguenti componenti principali:

* ***Bilanciatore di carico*** [INDICARE il tipo di bilanciatore] in cluster;
* Web server [INDICARE il tipo di web server] in cluster;
* ***FTP server*** [INDICARE il tipo di FPT server] in cluster;
* ***Application server*** JBoss Enterprise (Red Hat) [TEORICAMENTE possibile anche la versione non licenziata da Red Hat, ma autocompilata] in cluster logico gestito dai componenti di clustering di JBoss;
* ***Servlet container*** Tomcat (Apache)in cluster per i componenti che non richiedono l’utilizzo di un application server (p.e. TPI e DPI);
* Data Base Oracle in cluster con utilizzo delle funzionalità di ***RAC*** [CONSIGLIATO, MA NON INDISPENSABILE]***, di*** ***Data Guard*** e di ***partitioning***;
* Storage Manager Tivoli (IBM) con funzionalità di ***Backup*** e ***Archiving*** [SOLO SE ATTIVO IL TPI].

Il diagramma in figura [ADATTARE] schematizza le principali componenti tecniche del sito primario (quelle del sito secondario sono analoghe, a parte [INDICARE le principali differenze; p.e. la mancata ridondanza del sito di DR]).

**Principali Componenti Fisiche del Sito Primario**

[ADATTARE se si è adottao un altro modello] Nell’ambito del sito primario i ***cluster*** sono tutti di tipo active / active, ovvero un server o un’applicazione interviene automaticamente a rilevare l’attività di un altro server o applicazione nel caso in cui quest’ultimo abbia smesso di funzionare correttamente, mentre nel sito secondario, 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 il solo scopo di distribuire il carico applicativo tra diversi sistemi.

Gli accessi al sistema avvengono esclusivamente passando da ***firewall*** tramite protocolli sicuri (***HTTPS*** e ***FTPS***). Il nucleo centrale del Sistema di conservazione, e in particolare i dati conservati, sono protetti da diversi livelli di firewall, sia verso l’esterno che verso altre sottoreti interne, che contengono servizi di supporto.

[ELIMINARE O ADATTARE] Lo ***storage*** utilizza come supporti di memorizzazione sia dischi che cassette di nastri magnetici.

Lo ***storage*** su disco è suddiviso in tre categorie:

* **Data Base Oracle** per la *memorizzazione* delle informazioni e di parte degli ***Oggetti-dati*** conservati in forma di ***BLOb***;
* [ADATTARE O ELIMINARE] ***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.);
* [ELIMINARE se non si utilizza PING] Area ***FTP*** per il trasferimento ed il recupero asincrono degli ***Oggetti-dati***.

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.

[ADATTARE O ELIMINARE sia per il back up che per l’archiving del TPI] Lo ***storage*** su nastri magnetici si basa su un sistema a cassette (***tape library***), completamente governato da Tivoli, che gestisce cassette in standard ***LTO6*** su cui vengono mantenuti:

* in modalità ***archiving***, in situazione ***near-line*** gli ***Oggetti-dati*** che non vengono mantenuti nei ***BLOb*** del Data Base (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.

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 tarmite opportune grant.

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 per i componenti di SacER è stato derivato dal framework open source Spring, migliorandone gli aspetti di accessibilità; la ***persistenza*** è gestita tramite ***EJB***, generati con il framework JPA. 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***. []ELIMINARE se non si sono sviluppati componenti aggiuntivi a SacER Il ***framework di sviluppo*** utilizzato per i componenti è [DESCRIVERE].

La replica dei dati sul sito secondario è garantita da diverse tecnologie: il Data Base viene sincronizzato da Oracle tramite ***Data Guard*** con modalità di [ADATTARE] physical standby e maximum availability (il sito primario non attende la fine della scrittura del sito di **Di*saster recovery*** per considerare chiusa la transazione), [ELIMINARE se non si utilizza il TPI] il ***file system*** temporaneo su disco viene allineato tramite ***SCP***, mentre l’archivio su cassette viene mantenuto aggiornato da Tivoli in maniera indipendente tra i sue siti tramite opportune politiche di schedulazione; l’area ***FTP*** non viene replicata. L’applicativo controlla periodicamente la corretta sincronizzazione dei ***file system*** e degli archivi su cassette tra i due siti.

[[Torna al Sommario](#Sommario)]

## Procedure di gestione e di evoluzione

La gestione del *Sistema di conservazione* è affidata a diversi gruppi di operatori dell’Ente conservatore, 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, ed infine la gestione delle richieste degli utenti e dei malfunzionamenti.

Le procedure di evoluzione del sistema tengono conto sia delle necessità di evoluzione pianificate, che di quelle estemporanee, che possono sorgere al di fuori della pianificazione; in ogni caso qualsiasi modifica evolutiva del sistema è testata adeguatamente prima del rilascio in produzione.

Particolare attenzione viene dedicata alla gestione della sicurezza del sistema ed in particolare alla prevenzione e alla soluzione degli incidenti di sicurezza; gli eventi più significativi ai fini della sicurezza del sistema sono gestiti tramite sistemi e procedure di tracciatura (log).

[[Torna al Sommario](#Sommario)]

### Gestione dell’Esercizio

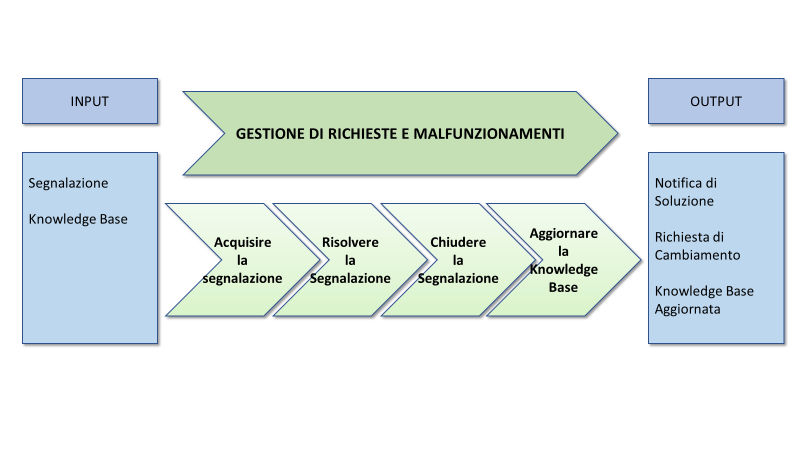
Per quanto attiene alla gestione operativa del sistema in esercizio, le relative attività sono presidiate dal Responsabile della conservazione dell’Ente.

Il Responsabile dei Sistemi informativi dell’Ente 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, oltre a quelle dettagliate nel paragrafo 9.2; infine si occupa di verificare il buon funzionamento dell’infrastruttura di ***Disaster Recovery***.

[[Torna al Sommario](#Sommario)]

### Gestione delle Richieste degli Utenti e dei Malfunzionamenti

La gestione delle richieste e dei malfunzionamenti può coinvolgere diverse strutture dell’Ente, secondo la natura della problematica.

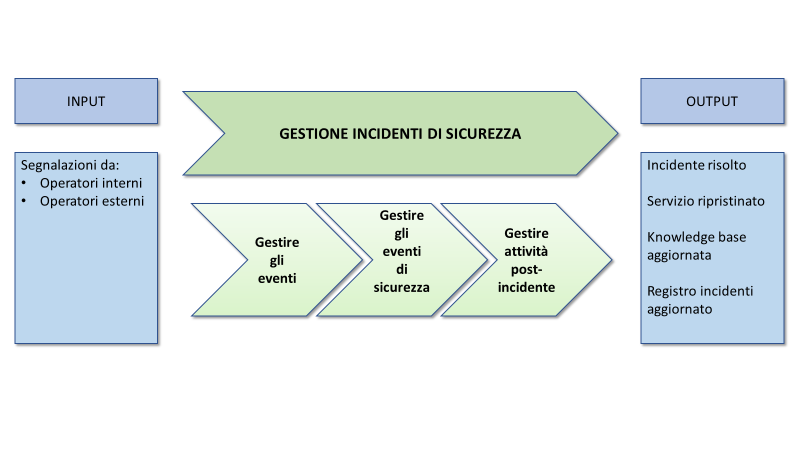


Diversi possono essere i soggetti che intervengono nella soluzione delle problematiche segnalate: il *Responsabile della conservazione* è normalmente in grado di risolvere qualsiasi problematica che non sia dovuta a problemi tecnici, eventualmente coinvolgendo il Responsabile della gestione documentale e eventuali fornitori di servizi; le problematiche di natura infrastrutturale vengono risolte dal Responsabile dei Sistemi informativi.

[[Torna al Sommario](#Sommario)]

### Gestione degli Incidenti di Sicurezza

La procedura di Gestione degli incidenti di sicurezza, schematizzata in figura, 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 *Sistema di conservazione*.



L’obiettivo del processo viene raggiunto attraverso le seguenti attività:

* gestire gli eventi;
* gestire gli incidenti di sicurezza;
* gestire attività post-incidente.

Tutte le aree organizzative dell’Ente e la struttura di gestione del ***Disaster recovery*** sono sistematicamente coinvolte nelle attività di prevenzione e di risoluzione degli incidenti di sicurezza, [INDICARE eventuale altro documento] come descritto in maggior dettaglio nel *Piano della Sicurezza* dell’Ente.

[[Torna al Sommario](#Sommario)]

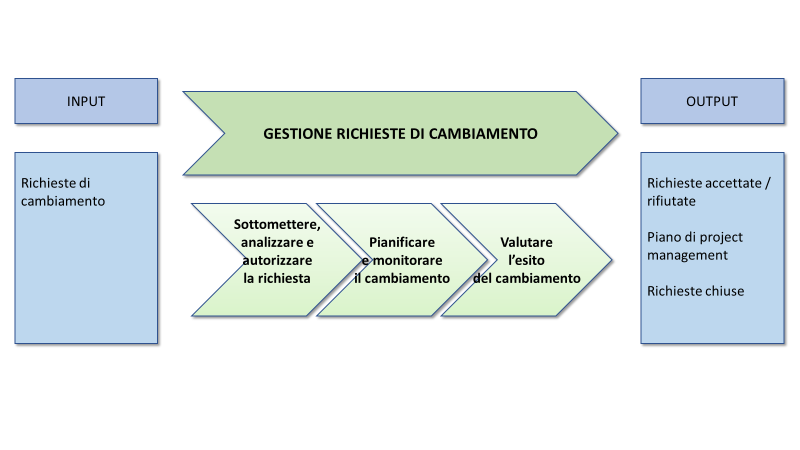
### Evoluzione pianificata

L’evoluzione pianificata del *Sistema di Conservazione* segue le linee guida formulate dal *Responsabile della 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, SAL per l’evoluzione degli applicativi e, quando necessario, SAL per l’evoluzione dell’infrastruttura. 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.

[[Torna al Sommario](#Sommario)]

### 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 nella procedura di Gestione delle richieste di cambiamento, schematizzata in figura.



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 nell’area 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.

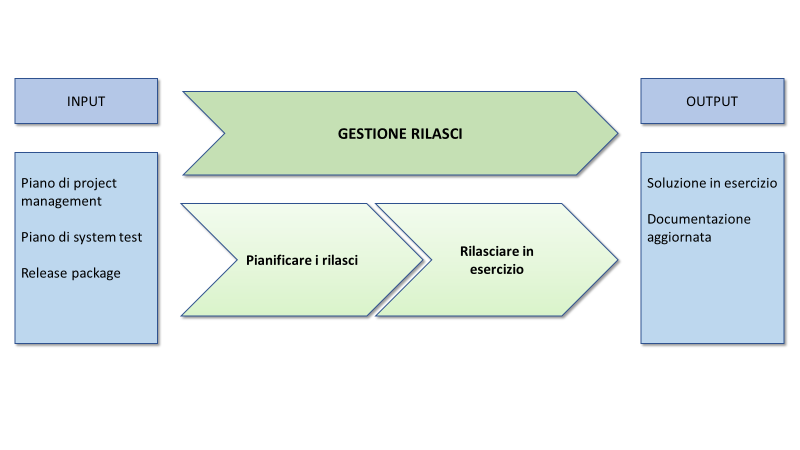
Il monitoraggio della realizzazione dei cambiamenti di una certa entità e la valutazione degli esiti è normalmente discusso nei SAL; i cambiamenti realizzati sono comunicati al personale dell’Ente ed eventualmente agli altri soggetti coinvolti nel servizio di conservazione.

Se la richiesta di cambiamento riguarda le componenti applicative sviluppate a integrazione del software in riuso, si procede secondo le metodiche previste dalle procedure di sviluppo [INSERIRE riferimenti alle proprie procedure di sviluppo del software]; se invece la richiesta di cambiamento riguarda le componenti applicative del software in riuso, viene contattato il ParER per illustrare i requisiti e valutare congiuntamente come possano essere recepiti nello standard di SacER [INSERIRE il riferimento a eventuali accordi specifici con ParER].

[[Torna al Sommario](#Sommario)]

### Gestione dei Rilasci

Il processo di rilascio di una nuova ***release***è illustrato in figura e prevede che ogni nuova release sia pianificata attentamente, al fine di ridurre al minimo i disservizi per il versatore e per gli *Utenti*.



Processo di Gestione dei rilasci

Per quanto riguarda le componenti applicative sviluppate a integrazione del software in riuso, si procede secondo le metodiche previste dalle procedure di sviluppo [INSERIRE riferimenti alle proprie procedure di sviluppo del software]. Per quanto riguarda il software in riuso, una volta che ParER ha inviato la nuova release, in forma sorgente e oggetto, viene rilasciata la nuova versione in ambiente di ***Test***, e su tale ambiente vengono condotti i test sulla base del piano di test predisposto in ragione delle release notes fornite da ParER, da parte sia del *Responsabile della conservazione*, sia del *Responsabile dei Sistemi informativi* (test funzionali, test di performance, test di interfaccia, test di affidabilità, test di stress, test di sicurezza).

Qualora i test non fossero soddisfacenti per problemi imputabili al software, viene aperta una segnalazione a ParER. Qualora invece i test risultino soddisfacenti, il software applicativo viene qualificato come nuova ***release*** eventualmente rilasciabile in pre-produzione [SE ESISTE] e produzione.

Il *Responsabile della conservazione* concorda con il *Responsabile dei Sistemi informativi* il piano di rilascio della nuova ***release*** nell’ambiente di pre-produzione e successivamente nell’ambiente di produzione e richiede di effettuare il rilascio. Il *Responsabile dei Sistemi informativi* provvede a inviare alla struttura di gestione del ***Disaster recovery*** la nuova ***release***, da caricare nel caso di dichiarazione di disastro.

[[Torna al Sommario](#Sommario)]

### Gestione e conservazione dei Log [da adattare]

I log di sistema e applicativi vengono conservati come indicato nei capitoli 8.2.10 e 8.2.11.

Periodicamente i log più vecchi di un anno vengono cancellati automaticamente dal sistema, sotto controllo del personale che si occupa dell’infrastruttura, in quanto si ritiene dopo tale periodo di tempo abbiano esaurito la loro utilità.

[[Torna al Sommario](#Sommario)]

### Verifica periodica di conformità a normativa e standard di riferimento [da adattare]

Il *Responsabile della 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 MIBAC.

Qualora siano emerse problematiche significative, provvede a diffonderle all’interno dell’Ente e, se lo ritiene necessario, anche tra gli altri attori del processo di conservazione.

Le notizie di maggior interesse vengono anche pubblicate sul sito web dell’Ente.

[[Torna al Sommario](#Sommario)]

# MONITORAGGIO E CONTROLLI

## Procedure di monitoraggio

[ADATTARE] Oltre alle funzionalità di monitoraggio applicativo gestite dal personale del *Sistema di conservazione* che sono state illustrate al paragrafo 7.6.1, sono attive procedure di monitoraggio tecnico gestite dal personale preposto, che provvede a produrre e rendere disponibili periodicamente report di controllo di tutte le aree infrastrutturali (rete, server, ***storage***, database, ***backup***). Si tratta di report tra loro eterogenei, prodotti in prevalenza per via automatica dal software di base dei sistemi e dal software di monitoraggio tecnico installato sui medesimi. Analoghi report vengono prodotti dalla gestione del ***Disaster recovery***.

Periodicamente i report di monitoraggio tecnico vengono esaminati dal Responsabile dello sviluppo e della manutenzione del Sistema di conservazione, con lo scopo di individuare eventuali aree di miglioramento negli aspetti tecnici dell’applicativo.

[[Torna al Sommario](#Sommario)]

## Funzionalità per la verifica e il mantenimento dell’integrità degli archivi

Le procedure di monitoraggio illustrate nel paragrafo precedente, le politiche di conservazione dei ***backup*** illustrate nel [O ALTRO DOCUMENTO da indicare] *Piano della Sicurezza* e le caratteristiche delle tecnologie utilizzate garantiscono la completa *integrità* di quanto archiviato nel *Sistema di conservazione*, ovvero di quanto depositato nel Data Base e negli archivi su cassetta [SOLO per TPI], una volta che sia stato duplicato nel sito di ***Disaster recovery*** e salvato tramite opportuno backup sia nel sito primario che nel sito secondario

Le funzionalità di Archiviazione consentono:

* l’amministrazione del Data Base, che si basa sulle funzionalità del Data Base e si occupa di gestire tutti i dati che transitano nel Sistema, a parte i file memorizzati nel ***file system***. Gli accessi al Data Base sono effettuati tramite opportuni moduli applicativi, che garantiscono l’indipendenza dell’applicativo dallo specifico Data Base (purché SQL) e dalla sua specifica release;
* la manutenzione del Data Base. Le funzionalità di ***Data Guard*** del Data Base assicurano la replica del Data Base nel sito di ***Disaster recovery***, 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 [O ALTRO DOCUMENTO da indicare] *Piano della Sicurezza*. La gestione sistemistica del Data Base è effettuata tramite prodotti certificati, 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 sfruttando funzionalità native del Data Base.

Per quanto attiene alla componente di Data Base degli archivi, l’*integrità* è garantita dalle funzionalità intrinseche di Oracle per tutti i *metadati* di classificazione e di pianificazione e per tutti i documenti archiviati nei BLOb, in particolare dalle funzionalità di replica remota e di backup del Data Base.

[SOLO se attivo TPI] Per quanto attiene invece alla componente di ***file system*** degli archivi, l’*integrità* è garantita da funzionalità intrinseche del modulo di archiving di TMS per tutti i dati archiviati su cassetta; queste ultime includono tra l’altro il controllo ed il riversamento periodico dei dati archiviati su nuove cassette.

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* a 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 [O ALTRO DOCUMENTO da indicare] *Piano della Sicurezza* dell’Ente descrive anche le modalità con cui l’Ente 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, il ***Disaster recovery*** e la ***continuità operativa***. [O ALTRO DOCUMENTO da indicare] Maggiori dettagli sull’approccio dell’Ente alla ***continuità operativa*** sono contenuti nel documento “Piano di Continuità Operativa”.

[[Torna al Sommario](#Sommario)]

## 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* 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 7.6.2.

[ADATTARE in funzione dell’esistenza di PING, DPI, TPI e delle proprie procedure] 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;
* 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 versatore |
| Data Base | Si effettua la restore tramite le funzioni standard di Oracle dal sito primario o dal sito secondario (nel caso di indisponibilità del DB primario) |
| 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 debbono essere 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 TMS) |

[[Torna al Sommario](#Sommario)]

1. Si fa riferimento in particolare agli art. 4, 10, 18 e 21 del citato Decreto legislativo. Il mantenimento delle competenze del MiBACT in materia di tutela dei sistemi di conservazione degli archivi pubblici è ribadito dall’art. 6 comma 9 e dall’art. 9 comma 2 delle Regole Tecniche [↑](#footnote-ref-2)
2. DPCM 3 dicembre 2013 “Regole tecniche per il protocollo informatico…”, art. 7 comma 5. [↑](#footnote-ref-3)
3. 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”.* [↑](#footnote-ref-4)
4. 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. [↑](#footnote-ref-5)