MANUALE DI CONSERVAZIONE

Codice documento	ManualeConservazione
Versione	1.0

	Data	*Nominativo*	*Funzione*
Redazione	26/11/2020	Giovanni Galazzini	Consulente
		Cristiano Casagni	Responsabile sviluppo e manutenzione del sistema
Verifica	27/11/2020	Gabriele Bezzi	Responsabile funzione archivistica di conservazione
Approvazione	30/11/2020	Marco Calzolari	Responsabile del servizio

REGISTRO DELLE VERSIONI

Versione	Variazioni	Data
1.0	Prima emissione	30/11/2020

SOMMARIO

INDICE DELLE FIGURE

1 SCOPO E AMBITO DEL DOCUMENTO

Il presente documento è il *Manuale di conservazione* (d'ora in poi Manuale) che descrive il sistema di conservazione applicato dalla Regione Emilia-Romagna in quanto Conservatore. E' predisposto dal Servizio Polo archivistico dell'Emilia-Romagna (d'ora in poi ParER), che realizza e gestisce il *processo di conservazione*.

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

Gli elementi illustrati e descritti sono validi e rilevanti per tutti gli enti per i quali Regione Emilia-Romagna svolge la funzione di *conservazione* e realizza e gestisce il *processo di conservazione* ai sensi della normativa nazionale e regionale, secondo il modello organizzativo descritto al paragrafo 4.1. Tali enti sono in primo luogo la Regione Emilia-Romagna stessa, gli enti e gli organismi regionali, quali le agenzie, aziende e istituti e le aziende del Servizio Sanitario Regionale, oltre che gli enti del territorio regionale appositamente convenzionati. Inoltre, il presente Manuale è valido e rilevante anche per gli enti fuori dal territorio regionale, con cui sono stati stipulati appositi accordi.

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

La documentazione di riferimento sia tecnica (p.e. specifiche tecniche di versamento, modelli di *pacchetti informativi*) che amministrativa (p.e. schemi di convenzione o accordo) ed altra eventuale documentazione di analisi di interesse generale sono pubblicate nel sito di ParER: http://parer.ibc.regione.emilia-romagna.it/.

[Torna al Sommario]

2 TERMINOLOGIA (GLOSSARIO, ACRONIMI)

Per i termini utilizzati nel presente Manuale si rimanda al Glossario di cui all'Allegato 1 delle Regole Tecniche e alle definizioni del D.lgs. 82/2005 e del DPR 445/2000 e loro successive modificazioni e integrazioni. In generale la terminologia utilizzata si riferisce alle norme citate o a standard nazionali e internazionali.
Le definizioni riportate in ordine alfabetico in questo capitolo riguardano termini impiegati ripetutamente nel testo non presenti nelle citate fonti 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***.

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

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

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

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

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

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

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

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

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

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

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

Client: componente 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)

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

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

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

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

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

Convenzione: accordo tra il *Produttore* e ParER, che regola i rapporti di servizio, e più precisamente: la natura dei servizi offerti, la responsabilità delle parti e le condizioni economiche, oltre agli strumenti di consultazione e controllo. Con il termine Convenzione si intendono sia le convenzioni propriamente dette, sottoscritte con gli Enti del territorio dell'Emilia-Romagna, sia gli accordi di collaborazione sottoscritti con Enti di altri territori nazionali.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Microservizi: approccio architetturale alla realizzazione di applicazioni caratterizzata dalla suddivisione dell'applicazione nelle sue funzioni di base. Ciascuna funzione, denominata servizio,

può essere compilata e implementata in modo indipendente. Pertanto, i singoli servizi possono funzionare, o meno, senza compromettere gli altri (Fonte: RedHat)

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

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

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

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

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

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

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

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

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

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

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

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

Piano di conservazione: L'art. 68 del DPR 445/2000 (Disposizioni per la conservazione degli archivi), prevede la dotazione da parte dell'ente di un piano di conservazione degli archivi, che deve consentire di selezionare i documenti destinati alla conservazione permanente 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)

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

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***)

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

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

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

SICTR (Servizio ICT - Information and Communication Technology Regionale): struttura organizzativa della Regione Emilia-Romagna deputata, in base a quanto previsto dalle Delibere di Giunta n. 270/2016 e 622/2016, a gestire le infrastrutture informatiche, a fissare gli standard informatici e di rete, a progettare, sviluppare e gestire i sistemi informativi "centrali", a gestire la sicurezza informatica degli strumenti informatici ed apparati di rete utilizzati per le attività della Regione e degli Enti / Agenzie che fruiscono a vario titolo dei servizi informatici e di rete regionali

SIEM (Security Information and Event Management): le soluzioni rientranti in questa categoria di sistemi sono contraddistinte dalla capacità di effettuare analisi 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)

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

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

(Fonte: Wikipedia)

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

Storage: dispositivo per memorizzare i dati in formato digitale; sono considerati storage sia i dispositivi a cassette 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 di archiviazione (AIU): Un Pacchetto di archiviazione (AIP) elementare, il cui contenuto informativo non è ulteriormente decomposto in altri contenuti informativi. Definisce un AIP di Unità documentaria. .[da ***OAIS***]

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

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

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

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

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

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

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

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

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

[Torna al Sommario]

3 NORMATIVA E STANDARD DI RIFERIMENTO

3.1 Normativa di riferimento

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

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

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

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

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

Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 (GDPR) relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).

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

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

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

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

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

Decreto del 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.

Decreto del Presidente del Consiglio dei Ministri 13 novembre 2014 - "Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici nonché di formazione e conservazione dei documenti informatici delle pubbliche amministrazioni ai sensi degli articoli 20, 22, 23-bis, 23-ter, 40, comma 1, 41, e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005".

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

Circolare AGID del 10 aprile 2014, n. 65 - Modalità per l'accreditamento e la vigilanza sui soggetti pubblici e privati che svolgono attività di conservazione dei documenti informatici di cui all'articolo 44-bis, comma 1, del decreto legislativo 7 marzo 2005, n. 82.

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

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

Linee Guida sulla formazione, gestione e conservazione dei documenti informatici, pubblicate da AgID il 9 settembre 2020

[Torna al Sommario]

3.2 Standard di riferimento

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

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

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

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

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

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

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

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

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

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

UNI 11386:2010: - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali (UNI SInCRO): Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali: definisce la struttura dell'insieme di dati a supporto del processo di conservazione; in particolare, precisa e integra alcune disposizioni contenute nella Deliberazione CNIPA 19 febbraio 2004, n. 11, individuando gli elementi informativi necessari alla creazione dell'indice di conservazione e descrivendone sia la semantica sia l'articolazione per mezzo del linguaggio formale XML. L'obiettivo della norma è di consentire agli operatori del settore di utilizzare una struttura-dati condivisa al fine di raggiungere un soddisfacente grado d'interoperabilità nei processi di migrazione, grazie all'adozione dello Schema XML appositamente elaborato.

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

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

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

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

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

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

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

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

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

[Torna al Sommario]

4 RUOLI E RESPONSABILITÀ

4.1 Modello organizzativo

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

I soggetti indicati al citato articolo 19 sono rispettivamente:

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

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

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

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

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

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

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

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

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

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

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

Infatti, la Regione Emilia-Romagna ha dotato il Servizio Polo Archivistico di una specifica struttura tecnologica ed un organico con professionalità qualificate che assommano conoscenze di natura archivistica, informatica, organizzativa e giuridica[4].

---

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

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

[4] Tra le competenze del Servizio, così come ridefinite dalla delibera di Giunta regionale del 5 dicembre 2011, n. 1803, figurano: «la responsabilità dello svolgimento dei processi di conservazione sostitutiva e di riversamento sostitutivo dei Documenti informatici della Regione e degli altri enti convenzionati; la cura delle modalità di trasferimento, accesso e fruizione del patrimonio documentario e informativo conservato in ParER; la promozione dell'adesione degli enti del sistema regionale a ParER; il supporto all'azione dei responsabili del protocollo informatico presso gli Enti produttori per la messa a punto degli strumenti archivistici, organizzativi e software per le esigenze di produzione e conservazione dei documenti digitali, nonché per l'adeguamento al *Sistema di conservazione* digitale di ParER; l'evoluzione tecnologica (hardware, software, formati elettronici, ecc.) e l'aggiornamento o ***migrazione*** dei sistemi di ParER; la gestione ed erogazione di servizi per il trattamento dei Documenti informatici (e dei documenti multimediali) per la Regione e gli enti convenzionati; il coordinamento

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

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

Seguendo quanto indicato dalle ***Regole tecniche*** vigenti e sulla base dello stesso modello ***OAIS*** si possono identificare i seguenti ruoli fondamentali: *Produttore* (o Ente produttore), *Utente*, *Responsabile*.

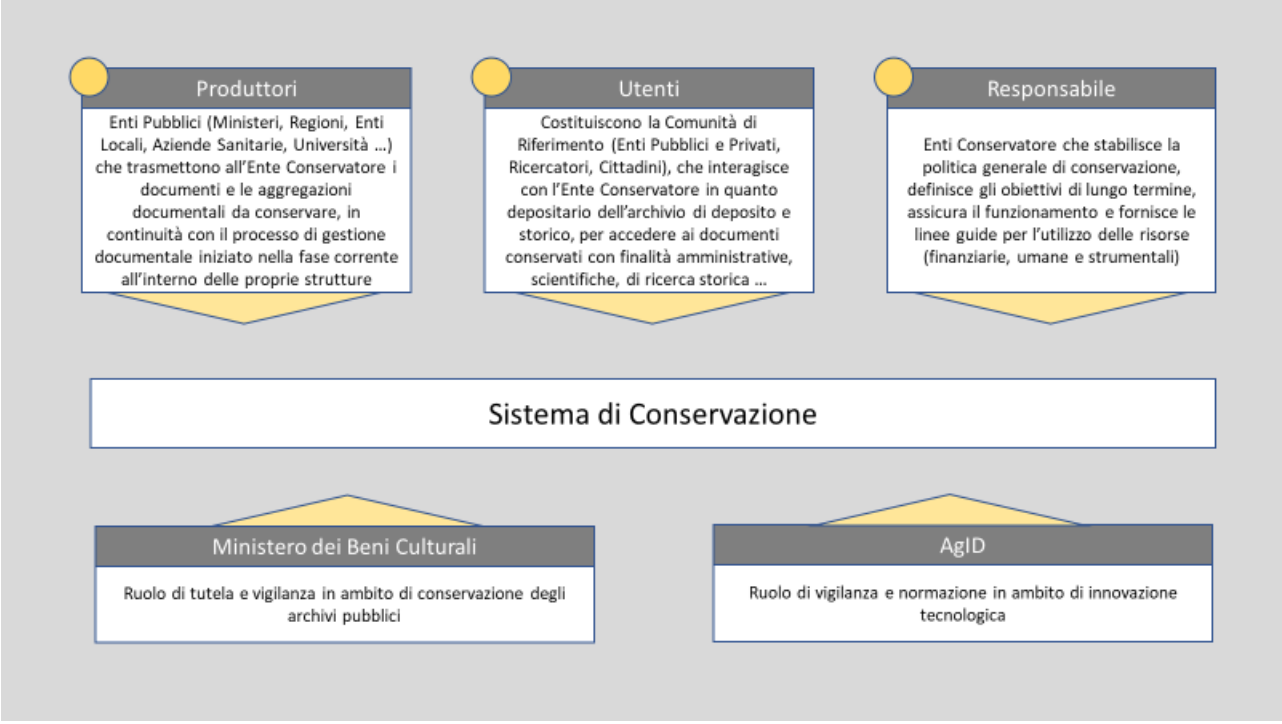

Figura 1 - Sistema e attori

[Torna al Sommario]

4.2 Produttore

dell'attuazione delle linee strategiche per la riorganizzazione e la digitalizzazione delle pubbliche amministrazioni previste dal Codice dell'amministrazione digitale presso l'Istituto, in raccordo con la Direzione generale competente della Giunta regionale».

È il soggetto che affida la conservazione dei propri documenti informatici alla Regione Emilia-Romagna, denominato nella ***Convenzione*** Ente Produttore.

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

I rapporti tra la Regione Emilia-Romagna, tramite ParER, e i *Produttori* vengono formalizzati e regolati per mezzo di due documenti fondamentali: la ***Convenzione*** e il ***Disciplinare tecnico***[5].

La ***Convenzione***, o accordo, regola i rapporti di servizio tra il *Produttore* e ParER, e più precisamente la natura dei servizi offerti, la responsabilità delle parti e le condizioni economiche. Precisa, inoltre, quali sono i servizi offerti da ParER e definisce gli strumenti di consultazione e controllo. Le attuali ***Convenzioni*** prevedono l'erogazione dei servizi di conservazione dei documenti informatici a titolo gratuito per gli enti dell'Emilia-Romagna (enti locali, Aziende sanitarie, Università) e a titolo oneroso per gli enti di altre regioni.

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

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

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

Come indicato dall'art.11 del DPCM 13 novembre 2014 il *Responsabile della gestione documentale* o, se nominato, il *Coordinatore della gestione documentale,* provvede a generare i pacchetti di versamento e stabilisce, per le diverse ***tipologie documentarie***, i tempi di versamento o trasferimento in conservazione, in conformità con le norme vigenti in materia, il sistema di classificazione e il piano di conservazione. Infine, verifica il buon esito della operazione

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

di versamento in particolare tramite la verifica della produzione del *rapporto di versamento* da parte del sistema di conservazione.

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

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

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

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

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

[Torna al Sommario]

4.3 Utente

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 dei *Produttori*, in particolare gli operatori indicati dal *Produttore* che possono accedere esclusivamente ai

documenti versati dal *Produttore* stesso o solo ad alcuni di essi secondo le regole di visibilità e di *accesso* concordate tra ParER e il *Produttore*
L'abilitazione e l'autenticazione di tali operatori avviene in base alle procedure di gestione utenze indicate nel *Piano della sicurezza del sistema di conservazione* e nel rispetto delle misure di sicurezza previste negli articoli da 31 a 36 del D.lgs. 30 giugno 2003, n. 196, in particolare di quelle indicate all'art. 34 comma 1 e dal Disciplinare tecnico in materia di misure minime di sicurezza di cui all'Allegato B del medesimo decreto.
In prospettiva si possono definire *Utenti* potenzialmente tutti coloro che potranno interagire con ParER, quale conservatore e custode di archivi di deposito e storici, per accedere ai documenti conservati per finalità amministrative, scientifiche e di ricerca storica in relazione alle ***tipologie documentarie*** conservate e nel rispetto delle normative vigenti in materia di tutela dei beni culturali e di tutela dei dati personali.

[Torna al Sommario]

4.4 Ente 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 34, comma 1 bis, lettera b) del CAD***,*** prevede che il soggetto produttore affidi la conservazione e il processo di conservazione ad un soggetto conservatore esterno specificamente individuato nella Regione Emilia-Romagna.

La responsabilità del *Sistema di conservazione* e del servizio di conservazione come soggetto che svolge attività di *conservazione* è in capo alla Regione Emilia-Romagna, che individua come Responsabile del servizio di conservazione il Responsabile di ParER.

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

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

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

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

- garantire la conservazione, archiviazione e gestione dei Documenti informatici e degli altri oggetti digitali;
- erogare servizi di accesso basati sui contenuti digitali conservati
- fornire supporto, formazione e consulenza ai Produttori per i processi di dematerializzazione.6

Di fatto, quindi (come definito dal testo della ***Convenzione***, art. 3, comma 1), la Regione Emilia-Romagna, tramite ParER, si impegna alla *conservazione* dei documenti trasferiti e ne assume la funzione di Responsabile del servizio di conservazione ai sensi della normativa vigente, garantendo il rispetto dei requisiti previsti dalle norme in vigore nel tempo per i sistemi di conservazione, e svolge, tramite la struttura organizzativa e di responsabilità di ParER, l'insieme delle attività 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).

I ruoli specificamente individuati sono riportati nella seguente tabella:

RUOLO	NOMINATIVO	ATTIVITÀ DI COMPETENZA	PERIODO NEL RUOLO[7]	DELEGHE
Responsabile del servizio di conservazione	Marco Calzolari	vedi cap. 5	da luglio 2009	-
Responsabile Sicurezza dei sistemi per la conservazione	Marco Calzolari	vedi cap. 5	da luglio 2009	-
Responsabile funzione archivistica di conservazione	Gabriele Bezzi	vedi cap. 5	da novembre 2009	-
Responsabile trattamento dati personali (attuatore)	Marco Calzolari	vedi cap. 10	da dicembre 2019	

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

[7] Si riporta la data da cui il ruolo è stato esercitato presso il precedente conservatore IBACN, che cessa con il subentro di Regione Emilia-Romagna.

RUOLO	NOMINATIVO	ATTIVITÀ DI COMPETENZA	PERIODO NEL RUOLO[7]	DELEGHE
Responsabile protezione dati personali (DPO)	Sergio Duretti	Vedi cap. 10	da gennaio 2020	
Responsabile sistemi informativi per la conservazione	Maurizio Coppari	vedi cap. 5	da dicembre 2019	-
Responsabile sviluppo e manutenzione del sistema di conservazione	Cristiano Casagni	vedi cap.5	da luglio 2009	-

Per la descrizione nel dettaglio della struttura organizzativa e di responsabilità si veda il capitolo 5 e per i dati dei soggetti che nel tempo hanno assunto la responsabilità del *Sistema di conservazione* l'Allegato 2 "Registro dei responsabili".
Nell'Allegato, che verrà mantenuto opportunamente aggiornato, sono riportati i dati delle persone fisiche che, in base ai loro ruoli in Regione Emilia-Romagna, nel tempo hanno esercitato la rappresentanza del conservatore tramite specifiche azioni e/o eventuali sottoscrizioni. In particolare il Dirigente Responsabile del Servizio Polo archivistico regionale dell'Emilia-Romagna (ParER), quale Responsabile del servizio di conservazione e delegato alla firma delle ***Convenzioni;*** il titolare della Posizione organizzativa di presidio della funzione archivistica di conservazione, a cui sono assegnate in particolare le funzioni di sottoscrizione previste nell'ambito del *processo di conservazione* e le funzioni di rappresentanza nei rapporti con il MiBACT e gli altri enti di vigilanza per quanto di competenza.

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

[Torna al Sommario]

4.5 Organismi di tutela e vigilanza

Il Ministero per i beni e le attività culturali (MiBACT) 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[8].
La tutela e vigilanza sugli archivi di enti pubblici non statali è esercitata dal MiBACT, tramite le Soprintendenze archivistiche e bibliografiche competenti per territorio.
"Lo spostamento, anche temporaneo dei beni culturali mobili" compresi gli archivi storici e di deposito è soggetto ad autorizzazione della Soprintendenza archivistica (D.lgs 22 gen. 2004, n. 42, art. 21, c. 1, lettera b).
Anche "Il trasferimento ad altre persone giuridiche di complessi organici di documentazione di archivi pubblici, nonché di archivi di privati per i quali sia intervenuta la dichiarazione ai sensi dell'articolo 13", sia che comporti o non comporti uno spostamento, rientra tra gli interventi soggetti ad autorizzazione della Soprintendenza archivistica (D.lgs 22 gen. 2004, n. 42, art.21, c. 1, lettera e).
La disposizione si applica anche:

- all'affidamento a terzi dell'archivio (outsourcing), ai sensi del D.lgs 22 gen. 2004, n. 42, art.21, c. 1, lettera e)
- al trasferimento di archivi informatici ad altri soggetti giuridici, nell'ottica della conservazione permanente sia del documento sia del contesto archivistico.9

La Soprintendenza archivistica e bibliografica può, in seguito a preavviso, effettuare ispezioni per accertare lo stato di conservazione e custodia degli archivi e può emettere prescrizioni per la tutela degli archivi.
Secondo quanto disposto dall'art. 44, comma 2 lettera a) del recente regolamento di organizzazione del Mibact (DPCM 2 dicembre 2019, n. 169, pubblicato sulla GU n. 16 del 21 gennaio 2020), il Soprintendente archivistico e bibliografico "svolge, sulla base delle indicazioni e dei programmi definiti dalla competente Direzione generale, attività di tutela dei beni archivistici e librari presenti nell'ambito del territorio di competenza nei confronti di tutti i soggetti pubblici e privati, ivi inclusi i soggetti di cui all'articolo 44-bis del Codice dell'amministrazione digitale di cui al decreto legislativo 7 marzo 2005, n. 82,", cioè i conservatori esterni accreditati, ora normati dall'art. 34 comma 1 bis lettera b) del CAD.
In aderenza con le funzioni di tutela sopra indicate è stato stipulato un accordo di collaborazione con la Soprintendenza archivistica e Bibliografica dell'Emilia-Romagna, valido fino al 31 dicembre 2033 che prevede tra i punti più qualificanti:

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

[8] Si fa riferimento in particolare agli art. 4, 10, 18 e 21 del citato Decreto legislativo. Il mantenimento delle competenze del MiBAC 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

[9]Dal sito della Soprintendenza archivistica per l'Emilia-Romagna, http://www.sa-ero.archivi.beniculturali.it/index.php?id=21

In particolare, la Soprintendenza archivistica per l'Emilia-Romagna (ora Soprintendenza Archivistica e Bibliografica dell'Emilia-Romagna) svolge un ruolo di vigilanza del *Sistema di conservazione* per verificare che il *processo di conservazione* avvenga in modo conforme alla normativa e ai principi di corretta e ininterrotta custodia, senza però accedere a informazioni personali/sensibili contenute nei documenti o nel sistema.

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

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

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* della Regione Emilia-Romagna prevede la materiale conservazione dei dati e delle Copie di sicurezza sul territorio nazionale e l'accesso ai dati presso la sede del *Produttore*.

AgID vigila inoltre sulla corretta applicazione delle regole del ***Cloud marketplace***, che ParER ha adottato per fornire il servizio di conservazione ai Produttori nella forma di ***SaaS*** (Software as a service).

[Torna al Sommario]

5 STRUTTURA ORGANIZZATIVA PER IL SERVIZIO DI CONSERVAZIONE

5.1 Organigramma della Regione Emilia-Romagna

La Regione Emilia-Romagna è organizzata in Direzioni Generali: all'interno di una di esse, la gestione del *Sistema di conservazione* è in carico a uno dei Servizi in cui si articola. Infatti, la Regione Emilia-Romagna ha attivato il Servizio Polo archivistico regionale dell'Emilia-Romagna (ParER) come struttura dirigenziale a livello di Servizio.

A ParER sono state attribuite diverse competenze, tra le quali in primis la responsabilità dello svolgimento del *processo di conservazione* dei *Documenti informatici* della Regione e degli altri enti convenzionati, e la cura delle modalità di trasferimento, *accesso* e fruizione del patrimonio documentario e informativo conservato.
ParER cura inoltre l'evoluzione tecnologica e l'aggiornamento o la ***migrazione*** del *Sistema di conservazione*.

In una prospettiva di promozione della dematerializzazione e della conservazione digitale, ParER coordina l'attuazione delle linee strategiche per la riorganizzazione e la digitalizzazione delle pubbliche amministrazioni previste dal Codice dell'amministrazione digitale in raccordo con la Direzione generale competente della Giunta regionale; supporta l'azione dei responsabili della gestione documentale presso i *Produttori*, in particolare in vista dell'adeguamento dei sistemi al *Sistema di conservazione*; promuove l'adesione degli enti del sistema regionale; si raccorda con analoghe iniziative a livello nazionale ed europeo.

5.2 Struttura organizzativa del Servizio Polo Archivistico (ParER)

All'interno di ParER, si situano le responsabilità relative al Servizio di Conservazione di seguito dettagliate.

Responsabile del Servizio: dirigente con responsabilità dei procedimenti / processi / progetti di ParER. E' il dirigente responsabile del Servizio Polo archivistico regionale (ParER). È responsabile dei progetti e delle attività di ParER, della definizione e attuazione delle politiche complessive del Sistema di conservazione, nonché del governo della gestione del Sistema di conservazione e della gestione amministrativa del personale assegnato, con responsabilità sulle differenti posizioni organizzative afferenti al servizio e sulla relativa definizione del personale e delle risorse di cui avvalersi per l'attuazione delle attività, sulla pianificazione annuale delle attività assegnate e dell'organizzazione del lavoro all'interno del servizio. Ha l'obbligo di definire i fabbisogni professionali ordinari e straordinari, le proposte di piani di sviluppo del personale e le conseguenti azioni e valutazioni dei risultati. È responsabile della definizione dei requisiti e delle specifiche del Sistema di conservazione, sulla base della normativa vigente, e dell'erogazione del servizio ai *Produttori*, oltre che della gestione delle Convenzioni.

Responsabile della sicurezza dei sistemi per la conservazione: 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. È tenuto a segnalare eventuali difformità al Responsabile del servizio di conservazione e individuazione e pianificazione delle necessarie azioni correttive.

Responsabile della funzione archivistica di conservazione: è il funzionario titolare della Posizione Organizzativa responsabile del presidio della funzione archivistica di conservazione ed opera a stretto contatto con il Responsabile del Servizio. Nella struttura organizzativa del paragrafo successivo va identificato con il Responsabile dell'Area funzione archivistica di conservazione. Rientrano tra le sue mansioni e responsabilità, come da specifica designazione:

- 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 e standard di riferimento e ai loro aggiornamenti;
- la definizione dei requisiti degli accordi e/o Convenzioni dal punto di vista archivistico, con la definizione del set di metadati di conservazione dei documenti e dei fascicoli informatici, anche mediante l'analisi e l'identificazione dell'articolazione strutturale dei Produttori e delle modalità di registrazione e classificazione della documentazione da essi adottate;
- 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 del Produttore ai fini del trasferimento in conservazione e della selezione;
- la gestione dei rapporti con gli enti convenzionati e con la Soprintendenza archivistica per l'Emilia-Romagna (ora Soprintendenza archivistica e bibliografica dell'Emilia-Romagna) e altre articolazioni del MiBACT 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 dei sistemi informativi per la conservazione: individuato nella struttura organizzativa del paragrafo successivo con il Responsabile dell'Area gestione servizi e infrastrutture di ParER. Rientrano tra le sue mansioni:

- 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 del servizio di conservazione, della sicurezza fisica e logica dell'impianto tecnologico di ParER;
- il coordinamento tecnico dei rapporti con i fornitori di data center e supporto tecnologico ai progetti di conservazione digitale;
- la pianificazione, di concerto con i 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 dai 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 di ParER.

Responsabile dello sviluppo e della manutenzione del sistema di conservazione: individuato nella struttura organizzativa del paragrafo successivo con la Posizione Organizzativa di Capo Progetto dell'Area tecnologia e sviluppo sistemi di conservazione. E' responsabile del coordinamento e della gestione dei rapporti con i fornitori per le attività di pianificazione strategica e operativa finalizzate alla progettazione e allo sviluppo del *Sistema di conservazione* di ParER 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, agli standard e alla rispondenza ai criteri di qualità e sicurezza individuati per l'insieme del sistema informativo regionale;
- l'interfaccia con i Produttori, 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 personalizzazione e manutenzione delle soluzioni applicative in relazione alle diverse tipologie di Produttori e 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 e standard di riferimento e ai loro 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.

Il **Responsabile del trattamento dei dati personali** è identificato nel capitolo 10 del presente Manuale.

ParER è organizzato secondo la struttura riportata in figura.

Le aree indicate svolgono le attività di seguito descritte in dettaglio; il Responsabile della Sicurezza coincide attualmente con il Responsabile del servizio e il Responsabile della Qualità coincide con il Responsabile dell'Area funzioni di supporto.

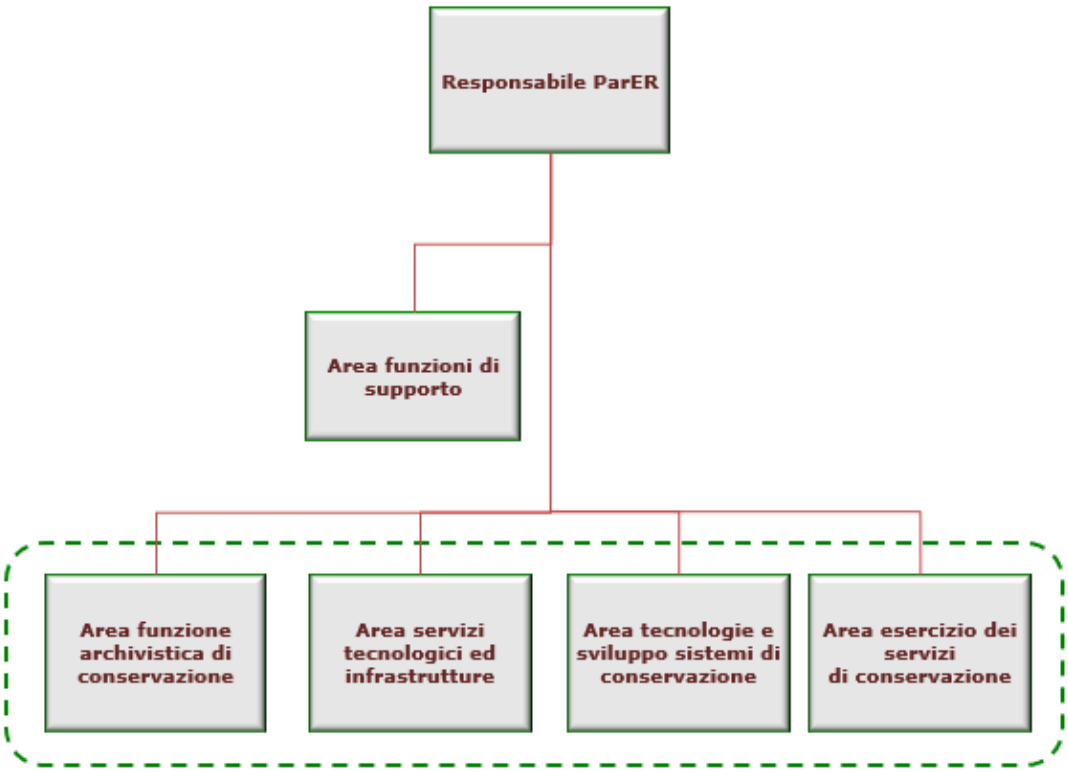

Figura 2 - Struttura organizzativa di ParER

AREA FUNZIONI DI SUPPORTO, per la gestione dei processi amministrativi interni al servizio. In particolare, è in capo a quest'area la responsabilità nella gestione dei rapporti giuridico-amministrativi e nella redazione degli atti di impegno e delle convenzioni con la pubblica amministrazione, degli atti di liquidazione e dei contratti con i fornitori e della gestione delle ***Convenzioni*** con gli enti per l'avvio del rapporto con ParER, l'analisi e gli adempimenti organizzativi relativi all'applicazione della normativa in materia di protezione dei dati personali; la gestione contabile dei capitoli di spesa di competenza di ParER e il relativo monitoraggio; la gestione della procedura amministrativa inerente le ***Convenzioni*** per la funzione di conservazione dei *Documenti informatici* da sottoscrivere con i *Produttori* (enti locali e vari enti pubblici), la gestione dei processi di certificazione e di accreditamento, le gestione della Qualità. Il Responsabile di quest'area è rappresentato dal **Responsabile di Gestione Qualità**, che ha il compito di verificare sia la redazione che l'aggiornamento dei documenti del Sistema di Gestione Integrato (***SGI***) rispettino i requisiti ISO 9001. Una volta definita, è responsabile della distribuzione della documentazione approvata, della definizione dei template e standard documentali, della loro revisione nel caso di cambiamenti e modifiche. Relativamente al suo ambito, è responsabile degli Audit al fine di verificare la corretta applicazione delle procedure e dei requisiti prescritti dalla normativa e analizzare le Non conformità di processo e di sistema in modo da evidenziare eventuali scostamenti, di conseguenza concorda con gli altri Responsabili

l'applicazione di adeguate Azioni Correttive. Rileva gli indici di Qualità ed effettua il riesame per verificare l'adeguatezza e l'efficacia del sistema integrato, focalizzandosi sull'ambito della qualità.

AREA FUNZIONE ARCHIVISTICA DI CONSERVAZIONE, con funzioni di gestione del protocollo, gestione e verifica della conservazione digitale, gestione dell'archivio di deposito e storico analogico della Regione Emilia-Romagna.
Quest'area ha la responsabilità generale del processo di conservazione, e in particolare garantisce l'aderenza del processo alla normativa e standard di riferimento e ai loro aggiornamenti.
Si occupa di fornire le linee guida su tutti gli aspetti archivistici del servizio e ne verifica l'applicazione; ciò si applica in particolare alle ***Convenzioni***, ai ***Disciplinari tecnici***, alla definizione dei modelli di *pacchetti informativi*, Alla definizione degli aspetti non operativi delle procedure, alla gestione della documentazione interna al servizio.
Quest'area si occupa inoltre del monitoraggio complessivo del processo di conservazione e ne garantisce la correttezza, provvedendo alla sottoscrizione digitale dei *pacchetti informativi*.
Dal punto di vista delle nuove applicazioni quest'area contribuisce alla definizione dei requisiti funzionali, garantendone la coerenza con le esigenze del processo di conservazione.
Infine, quest'area mantiene le relazioni con gli enti convenzionati e con gli organismi di sorveglianza e di indirizzo (MiBACT, Soprintendenze archivistiche, AgID), nonché con altri soggetti interessati a sviluppare azioni comuni nell'ambito della conservazione.

AREA SERVIZI TECNOLOGICI E INFRASTRUTTURE, con funzione di presidio della gestione dei servizi di conservazione e dell'infrastruttura informatica di ParER. Il Responsabile di tale area svolge le attività quale Responsabile dei sistemi informativi per la conservazione in base alle mansioni indicate in precedenza.
L'infrastruttura tecnologica che ospita il *Sistema di conservazione*, nonché tutti i servizi necessari al suo funzionamento, è in parte è ospitata presso i ***data center*** della Regione Emilia-Romagna uno contenente il sito primario e l'altro il sito di ***disaster recovery***.
Ambedue i ***data center***, descritti in dettaglio nel capitolo 8, sono situati sul territorio nazionale, per cui deve considerarsi applicabile la normativa nazionale.

AREA TECNOLOGIE E SVILUPPO DEI SISTEMI DI CONSERVAZIONE, con le funzioni di presidio dei sistemi informatici e di gestione dei rapporti con i fornitori dei servizi tecnologici agli enti, per l'interfacciamento di ParER.
In quest'area è prevista la figura di un Responsabile dello sviluppo e della manutenzione del *Sistema di conservazione*, con le mansioni e i compiti indicati in precedenza, per i quali è supportato dalle figure dell'Area.
Sono inoltre previste altre figure: analista informatico (o "analista di sistemi informativi"), analista funzionale (o "Analista di business") e tecnico informatico (o "Analista Programmatore").
L'analista informatico è il gestore delle relazioni con i fornitori degli enti che si vogliono interfacciare con ParER e del supporto tecnico per la definizione delle specifiche tecniche, la progettazione e la validazione delle funzionalità ed evoluzioni del software di conservazione, ivi incluse le problematiche di autenticazione e di sicurezza informatica.
L'analista funzionale è responsabile delle attività di analisi dei requisiti e delle funzionalità che il *Sistema di conservazione* deve garantire nel tempo per poter erogare il servizio richiesto, partecipando alle diverse fasi di progettazione delle funzionalità del *Sistema di conservazione* e delle sue evoluzioni, dallo studio di fattibilità alle fasi di analisi e realizzazione, rilascio e collaudo; la rilevazione e l'analisi critica delle esigenze di evoluzione del sistema; il coinvolgimento nella

reingegnerizzazione dei processi legati alla conservazione e nella scelta dell'evoluzione dell'architettura e delle funzionalità del sistema.
I tecnici informatici sono i soggetti addetti allo sviluppo e all'evoluzione del *Sistema di conservazione*. Tra le loro mansioni figurano la traduzione delle analisi dei requisiti e delle funzioni in specifiche tecniche del *Sistema di conservazione*; lo sviluppo delle evoluzioni software del *Sistema di conservazione*; la realizzazione dei test e della messa in esercizio delle nuove versioni dell'applicativo di conservazione; la realizzazione delle attività di verifica, manutenzione e aggiornamento del *Sistema di conservazione* in uso; lo sviluppo e la manutenzione delle componenti di sicurezza dell'applicativo di conservazione.
Il personale addetto allo sviluppo opera anche nella manutenzione del sistema in esercizio, quando se ne presente la necessità, in base a piani di lavoro che tengono conto sia delle esigenze di nuovi sviluppi che delle esigenze di manutenzione del sistema in esercizio.

AREA ESERCIZIO DEI SERVIZI DI CONSERVAZIONE, con funzioni di gestione operativa dei servizi di conservazione.
Prevede al suo interno la figura di un Responsabile, con mansioni di coordinamento delle attività operative a supporto del processo di conservazione. Il Responsabile si occupa di coordinare le attività delle risorse dell'area, in modo tale da garantire adeguati livelli di servizio agli Enti che conservano presso ParER. Oltre a gestire il ciclo di pianificazione, esecuzione e controllo delle attività, si occupa di definire i processi e le procedure operative del servizio, in coerenza con le linee guida emesse dall'Area Funzione Archivistica di Conservazione; nel caso di nuovo sviluppi applicativi fornisce i requisiti di massima del servizio e verifica i documenti prodotti dall'Area Tecnologia e Sviluppo dei Sistemi di Conservazione.
All'interno dell'area operano diversi archivisti, che si occupano di analizzare le problematiche specifiche delle diverse tipologie documentarie, e in particolare la modellizzazione dei *pacchetti informativi*, di avviare in conservazione nuovi Enti e di estenderne l'uso del servizio a nuove strutture e a nuove tipologie documentarie, di formare gli utenti all'utilizzo del servizio, di verificare l'andamento dei versamenti, di supportare gli utenti nella pratica quotidiana del servizio. A questo scopo parte del personale a turno opera come help desk per gli utenti, sia nelle attività preliminari all'avvio del servizio, che nelle attività di esercizio del servizio stesso; va sottolineato che l'help desk non è una struttura separata, ma un insieme di attività svolte da archivisti a supporto degli utenti, utilizzando procedure e strumenti standardizzati, formalizzati e condivisi con gli altri operatori dell'help desk. Gli archivisti infine contribuiscono allo sviluppo delle nuove applicazioni partecipando quando necessario all'analisi funzionale e ai test preliminari al passaggio in produzione

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

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

Attività	Resp. Servizio	Resp. Sicurezza dei Sistemi	Resp. Funzioni di Supporto e Qualità	Resp. Funzione Archivistica Conservazione	Resp. Esercizio di conservazione	Resp. Servizi Tecnologici Infrastrutture	Resp. Tecnologie e Sviluppo dei Sistemi	Resp. Trattamento Dati Personali
Gestione delle Convenzioni	A		R	C	C			
Attivazione del servizio di conservazione	A			C	R			
Gestione del processo di conservazione				A	R			
Chiusura del servizio di conservazione	A			C	R			
Gestione Infrastruttura	I			I	I	A, R	I	
Sviluppo e manutenzione del sistema	I			I	I	I	A, R	
Monitoraggio del servizio di conservazione	A			R	R	R		
Gestione del Sistema di Qualità	C		A,R	C	C	C	C	C
Verifica di conformità a norme e std di conservazione			I	A, R		I	I	C
Gestione Sicurezza del sistema	I	A,R				I	I	
Gestione degli incidenti di sicurezza	I	A,R		I	I	C	C	I
Gestione del Cambiamento	A	C		C	C	C	R	
Gestione mal-funzionamenti	A			R	R	R	R	
Rapporti con le Autorità di vigilanza	I			A,R				
Amministrazione Processi di Certificazione	I	I	A,R	I	I	I	I	
Trattamento dei dati personali	I	I		R	R			A

[Torna al Sommario]

6 OGGETTI SOTTOPOSTI A CONSERVAZIONE

6.1 Oggetti conservati

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

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

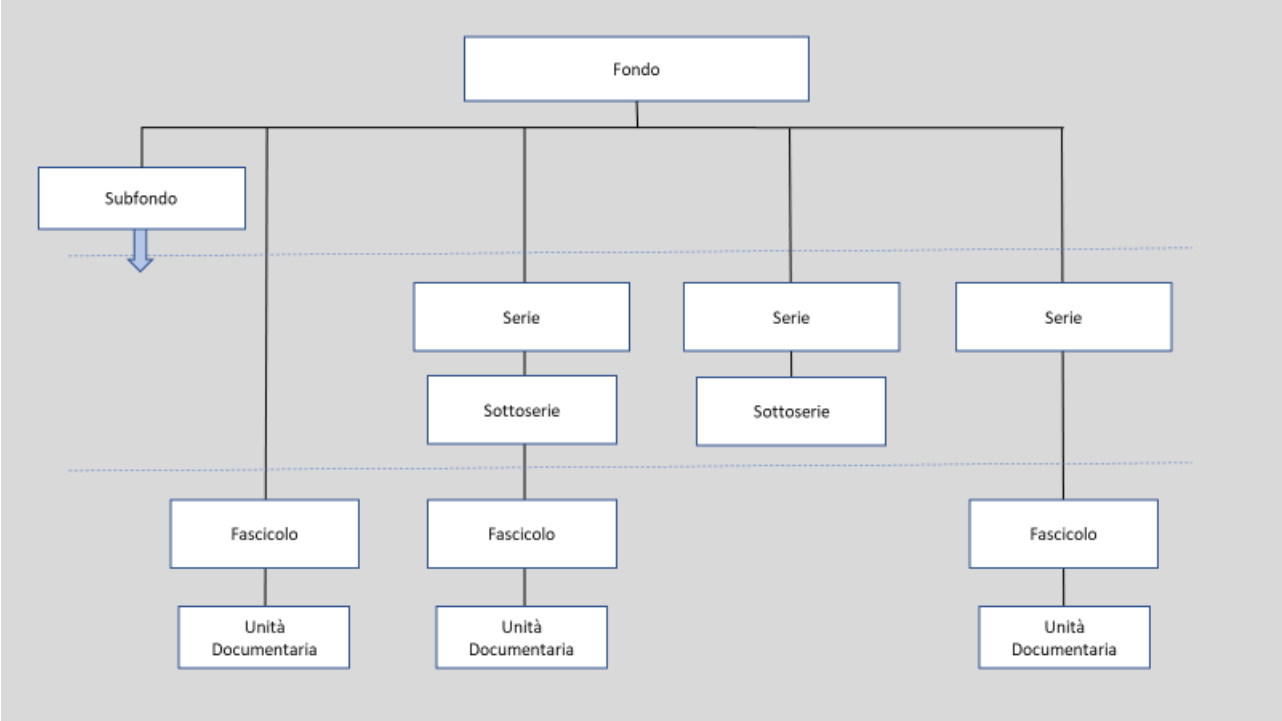

Figura 3 - Modello di ordinamento di archivio derivato da ISAD

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

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

Per mantenere anche nel Sistema le informazioni relative alla struttura dell'*archivio* e dei relativi vincoli archivistici, le ***Unità documentarie*** sono versate corredate di un set di *metadati* di Profilo archivistico che include gli elementi identificativi e descrittivi del Fascicolo, con riferimento alla

voce di *classificazione* e l'eventuale articolazione in sottofascicoli. Inoltre, è gestita la presenza di classificazioni, fascicoli e sotto-fascicoli secondari e collegamenti tra le diverse ***Unità archivistiche*** e documentarie presenti nel sistema.

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

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

- il set dei *metadati* descrittivi che le caratterizzano, ritenuti essenziali per la corretta conservazione dei documenti e delle aggregazioni documentali informatiche (vedi più avanti paragrafo 6.1.3), in coerenza con quanto stabilito nell'Allegato 5 delle ***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 all'attività degli organi consiliari, contratti e accordi, decreti e ordinanze, deliberazioni, determinazioni, documentazione contabile, documenti protocollati, registri, strumenti urbanistici, ecc.;
- **Documentazione sanitaria:** referti e immagini diagnostiche;
- **Documentazione scolastica:** pagelle e registri didattici
- **Documentazione universitaria:** verbali di esame e altri documenti inerenti all'attività didattica;
- **Documenti di conservazione:** Evidenze informatiche prodotte da altri *sistemi di conservazione*.

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

Stante la natura eterogenea degli *archivi* conservati da ParER, diverse sono le attività svolte a garanzia non solo della integrità ma anche della fruibilità degli *archivi* stessi nel lungo periodo per mantenere la loro leggibilità e reperibilità, anche nella prospettiva della futura fruizione come archivi storici.
A tal fine le strategie adottate per la conservazione a cura di ParER prevedono le seguenti azioni:

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

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

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

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

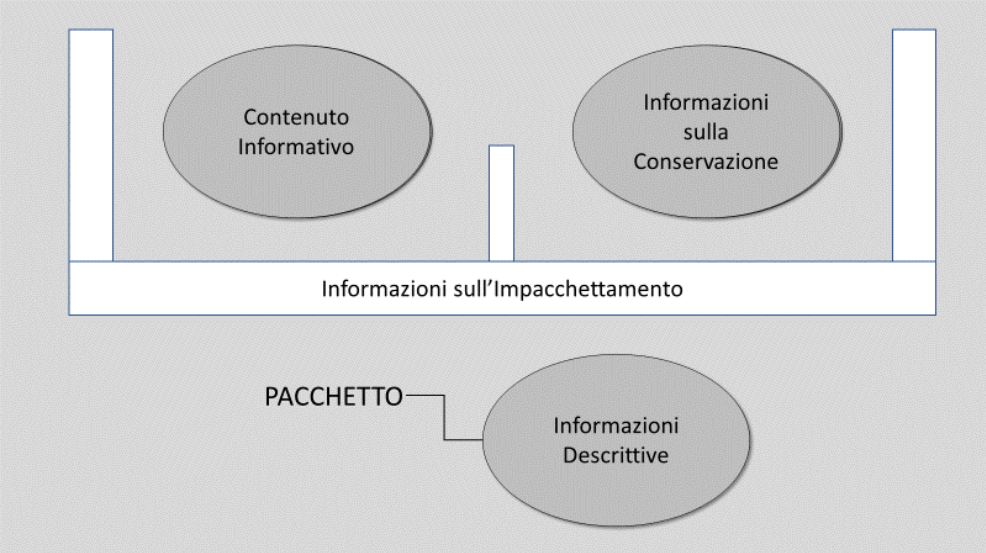

Figura 4 - Pacchetto informativo (da OAIS)

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

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

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

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

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

[Torna al Sommario]

6.1.1 Unità archivistiche e Unità documentarie

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

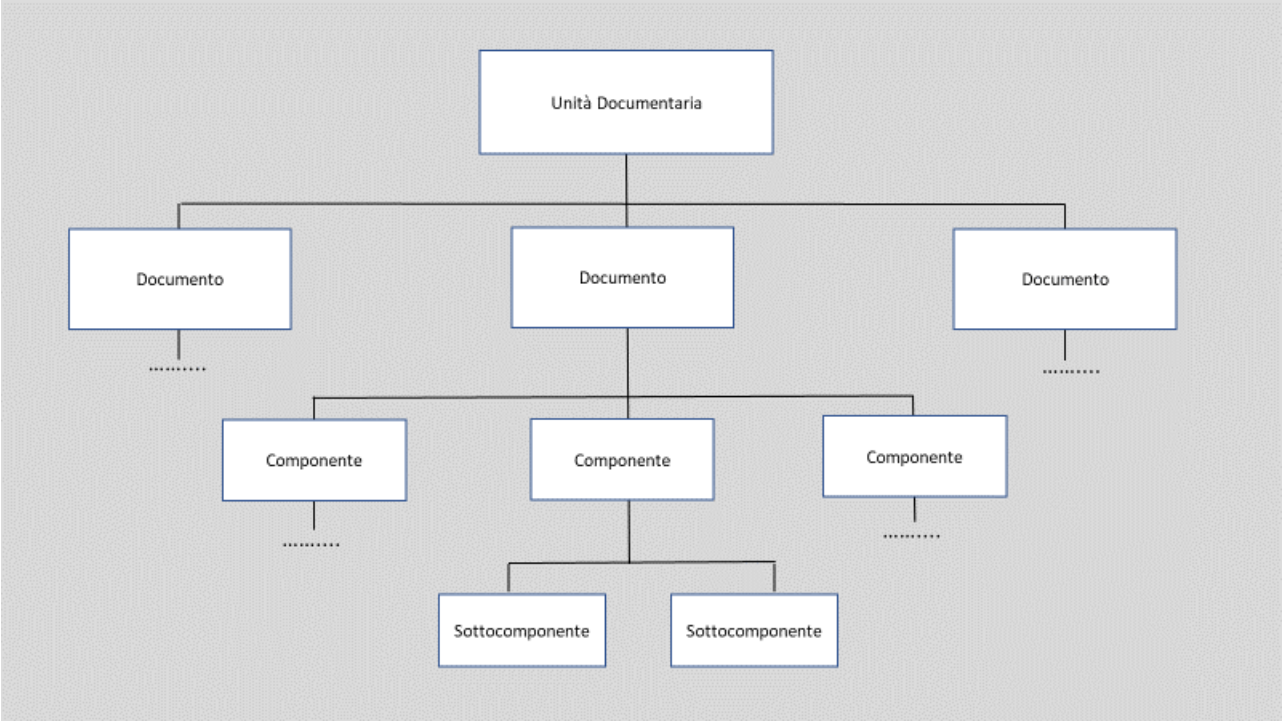

Figura 5 - Struttura dell'Unità documentaria

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

- ***Documento principale***: è il ***Documento*** che definisce il contenuto primario dell'***Unità documentaria***. È obbligatorio e 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 detached*** o ***firma detached***). Il ***Sotto componente*** ha una struttura del tutto simile al ***Componente*** ed è associato logicamente al ***Componente*** cui fa riferimento.

[Torna al Sommario]

6.1.2 Formati

Il *Sistema* utilizza come *formati* di conservazione quelli elencati al punto 5 dell'Allegato 2 alle ***Regole tecniche*** e, inoltre, è in grado di trattare, su richiesta del *Produttore*, anche *formati* non compresi nel suddetto elenco ma che il *Produttore* utilizza nei propri sistemi e che ritiene di dover conservare.

Tutti i Formati 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;
- **Formati gestiti**: sono i *formati* leggibili e accessibili ma potenzialmente soggetti a obsolescenza tecnologica e che, in caso di necessità, possono essere opportunamente migrati in Formati idonei con idonee procedure;
- **Formati deprecati**: sono *formati* ritenuti non idonei per la conservazione a lungo termine e che al contempo non possono essere migrati in Formati idonei, per i quali, quindi, non è possibile assicurare la conservazione a lungo termine.

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

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

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

[Torna al Sommario]

6.1.3 Metadati

I *metadati* gestiti dal Sistema sono individuati in coerenza con la normativa italiana e con gli standard e i modelli internazionali di riferimento. Più in dettaglio sono descritti ed analizzati per specifici oggetti da conservare e specifiche ***tipologie documentarie*** tramite i modelli di SIP pubblicati sul sito del ParER.

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

- **Metadati di identificazione:** identificano in modo univoco le ***Unità documentarie*** e archivistiche. Includono i dati identificativi del *Produttore* e i dati di registrazione originari, nonché gli identificativi specifici di ogni elemento dell'***Unità documentaria*** (***Documenti*** e ***Componenti***);
- **Metadati di struttura:** descrivono la struttura dell'***Unità archivistica o documentaria***, indicando nell'ultimo caso il numero e la tipologia di ***Allegati***, ***Annessi*** e ***Annotazioni*** che la compongono, nonché, per ognuno di essi, il numero e la tipologia dei ***Componenti***;
- **Metadati di profilo archivistico:** descrivono il Fascicolo e più in generale la collocazione dell'***Unità documentaria*** nel contesto dell'*archivio* del *Produttore*. Ricomprendono anche i *metadati* che collegano l'***Unità documentaria*** ad altre ***Unità documentarie*** conservate nel sistema (Collegamenti);
- **Metadati di profilo generali**: individuano gli elementi descrittivi essenziali comuni alle diverse tipologie di ***Unità archivistiche***, ***Unità documentarie*** e relativi elementi;
- **Metadati di profilo specifici:** individuano elementi descrittivi ulteriori rispetto a quelli previsti nel profilo generale. Sono definiti per ogni tipologia di ***Unità archivistica e documentaria*** e per ogni *Produttore*;
- **Metadati di conservazione:** sono tipicamente generati dal Sistema nel corso del *processo di conservazione* e attengono tanto all'analisi e alle verifiche effettuate sugli oggetti conservati, che alla descrizione delle attività svolte dal Sistema. Tra i Metadati di conservazione rientrano anche i *metadati* associati alle ***Unità archivistiche*** e ***documentarie*** provenienti da altri *sistemi di conservazione* (Metadati specifici di migrazione) e che contengono le informazioni relative al *processo di conservazione* di cui le ***Unità archivistiche e documentarie*** sono state eventualmente oggetto prima di essere versate nel Sistema.

[Torna al Sommario]

6.2 Pacchetto di versamento (SIP)

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

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

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

I 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 un'***Unità documentaria***: contiene un'***Unità documentaria*** completa in tutti gli elementi presenti nei sistemi del *Produttore* al momento del versamento. Il versamento di un pacchetto contenente un'***Unità documentaria*** genera un corrispondente *Pacchetto di archiviazione*;
- SIP di un ***Documento*****:** è utilizzato per aggiungere un singolo ***Documento*** e i relativi *metadati* a un'***Unità documentaria*** già presente nel Sistema. Il versamento di tale pacchetto genera l'aggiornamento del *Pacchetto di archiviazione* dell'***Unità documentaria*** cui il ***Documento*** viene aggiunto. La necessità di aggiungere un ***Documento*** a un'***Unità documentaria*** già presente si presenta tipicamente in due casi:
  - quando, per numerosità e dimensioni, è preferibile suddividere il versamento di un'***Unità documentaria*** in più parti;
  - qualora uno o più ***Documenti*** appartenenti a un'***Unità documentaria*** siano disponibili sul sistema del *Produttore* solo in un momento successivo a quello in cui l'***Unità documentaria*** di cui fanno parte è stata versata nel Sistema;
- SIP di Aggiornamento metadati: è utilizzato per versare nel Sistema esclusivamente informazioni, tipicamente *metadati*, per integrare, modificare o sostituire quelle già presenti in un'***Unità documentaria*** già conservata nel Sistema. Il versamento di tale pacchetto genera l'aggiornamento del *Pacchetto di archiviazione* dell'***Unità documentaria*** i cui i metadati vengono aggiornati.

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

[Torna al Sommario]

6.3 Pacchetto di archiviazione (AIP)

Il *Pacchetto di archiviazione* viene generato dal Sistema a conclusione del processo di acquisizione e *presa in carico* dei SIP (vedi paragrafo 7.5). È composto dagli ***Oggetti-dati*** (file), dall'***Indice dell'AIP***, un file XML che contiene tutti gli elementi del *pacchetto informativo*, derivati sia dalle informazioni contenute nel SIP (o nei SIP) trasmessi dal *Produttore*, sia da quelle generate dal Sistema nel corso del *processo di conservazione* e dai Documenti di conservazione, ovvero i documenti ricevuti o prodotti nel corso del processo di conservazione (Indici dei SIP, Esiti 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 dal *Produttore* o essere stata generata, a partire da questa, dal Sistema nel caso di produzione di copie informatiche.
	Informazioni sulla rappresentazione	Sono contenute a livello di ***Componente*** nell'***Indice dell'AIP*** e sono derivate sia da quelle contenute nel SIP di origine, sia da quelle generate dal Sistema. Includono i *metadati* relativi al *formato*.
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*.

Elemento del pacchetto informativo	Articolazione dell'elemento	Descrizione
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 o Raccolta di archiviazione (AIC) il cui contenuto informativo è costituito dagli AIP delle singole unità documentarie appartenenti al fascicolo;
- AIP di Serie: si divide a sua volta in AIP di Serie di Unità documentarie e in AIP di Serie di Unità archivistiche (fascicoli). Si configura anch'essa come una collezione di AIP.

[Torna al Sommario]

6.4 Pacchetto di distribuzione (DIP)

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

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

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

[Torna al Sommario]

7 PROCESSO DI CONSERVAZIONE

Il *processo di conservazione* si attiva a seguito di sottoscrizione della ***Convenzione*** tra il *Produttore* e la Regione Emilia-Romagna con le modalità indicate nella ***Convenzione*** stessa e dettagliate nel ***Disciplinare tecnico***. La ***Convenzione*** medesima disciplina anche la chiusura del servizio in caso di recesso o scadenza della ***Convenzione*** stessa, con le modalità operative descritte nel paragrafo 7.9.

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

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

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

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

In questa fase è prevista l'acquisizione nel Sistema anche di *Documenti informatici* per i quali la normativa stabilisce tempi precisi di versamento come, ad esempio, il registro giornaliero di protocollo che deve essere "trasmesso entro la giornata lavorativa successiva al *Sistema di conservazione*, garantendo l'*immodificabilità* del contenuto"[10].

Con ***Versamento in archivio*** si intende il ***versamento*** nel Sistema delle *Aggregazioni documentali informatiche* nella loro forma stabile e definitiva, principalmente Fascicoli chiusi e partizioni annuali di ***Serie*** documentarie [11].

[10] DPCM 3 dicembre 2013 "Regole tecniche per il protocollo informatico…", art. 7 comma 5.

[11] 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".*

Questa fase del *processo di conservazione*, assimilabile al versamento dall'archivio corrente all'archivio di deposito, assolve a un duplice obiettivo: da un lato portare nel Sistema le informazioni necessarie a costruire l'*archivio informatico* dell'ente; dall'altro aggiornare e fissare definitivamente, qualora si rendesse necessario, le informazioni di corredo relative alle ***Unità documentarie*** versate anticipatamente nel Sistema.

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

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

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

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

Al momento dell'acquisizione i SIP sono oggetto di una serie di verifiche automatiche. Nel caso in cui le verifiche abbiano successo, il ***versamento*** viene accettato, il SIP acquisito per la sua *presa in carico* e 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 funzione archivistica di conservazione o automaticamente dal Sistema. La validazione dell'Elenco innesca la generazione dei *Pacchetti di archiviazione* (AIP) relativi ai SIP in Elenco.

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

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

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

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

[Torna al Sommario]

7.1.1 Preacquisizione

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

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

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

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

- trasformazione dell'Oggetto in uno più SIP: ogni SIP generato contiene il riferimento all'Oggetto dal quale è stato generato;

- ***versamento*** dei SIP nel Sistema: i SIP vengono versati nel Sistema con le modalità descritte nel paragrafo 7.1.2.

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

[Torna al Sommario]

7.1.2 Acquisizione

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

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

Non è prevista la trasmissione di SIP su supporti fisici.

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

[Torna al Sommario]

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

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

Le verifiche riguardano:

- l'identificazione del Versatore: queste verifiche, effettuate mediante il controllo delle credenziali comunicate dal sistema versante a ogni versamento, sono finalizzate a garantire l'identificazione certa del soggetto che ha formato il documento e dell'amministrazione e/o dell'*area organizzativa omogenea* di riferimento ai sensi del art. 44, comma 1 lettera a) del CAD e a garantire il corretto inserimento nell'*archivio* del *Produttore* nella opportuna ***Struttura*** (vedi paragrafo 6.1.1);
- la conformità dell'***Indice del SIP*** al modello dati stabilito (vedi paragrafo 6.2): queste verifiche sono finalizzate a controllare se l'***Indice del SIP*** è conforme al modello concordato con il *Produttore* e configurato nel sistema;
- l'univocità degli identificativi degli oggetti contenuti nel SIP: il controllo è finalizzato a verificare che gli identificativi assegnati dal *Produttore* e contenuti nel SIP siano effettivamente univoci, verificando che gli stessi non siano già presenti nel Sistema;

- la consistenza dei Metadati di profilo e specifici (vedi paragrafo 6.1.3): questa verifica è finalizzata a controllare che i set di Metadati presenti nel pacchetto siano conformi (in termini di obbligatorietà, valori e formato) a quelli concordati tra *Produttore* e l'Ente conservatore. Tali set sono configurati nel Sistema mediante le funzionalità di Amministrazione delle Strutture versanti;
- il controllo sulle eventuali firme digitali apposte sugli ***Oggetti-dati*** (file) contenuti nel pacchetto. Le verifiche sono finalizzate a controllare la regolarità della firma digitale apposta in ordine a: formato di firma utilizzato, *integrità* del documento firmato (controllo crittografico), catena trusted, validità del certificato (scadenza e formato), presenza di eventuali revoche. I controlli sono effettuati alla data indicata dal *Produttore* nel SIP (che può essere quella contenuta nella firma, in una marca temporale o un riferimento temporale dichiarato nell'Indice SIP) o, in assenza di questa, alla data del versamento;
- l'ammissibilità dei ***formati*** degli ***Oggetti-dati*** (file) presenti nel pacchetto in base a quanto concordato con il *Produttore*: le verifiche si esplicano nel calcolo del ***mimetype*** dell'***Oggetto-dati*** e nel confronto del valore così ottenuto sia con quello eventualmente dichiarato dal *Produttore* nel SIP, sia con i Formati ammessi, documentati e conservati nel Sistema nelle funzionalità di Amministrazione delle strutture versanti;
- **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 opera in questo frangente, sono illustrati nel documento "Specifiche tecniche dei servizi di versamento".

[Torna al Sommario]

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

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

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

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

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

[Torna al Sommario]

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

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

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

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

[Torna al Sommario]

7.4.1 Monitoraggio

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

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

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

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

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

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

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

7.4.2 Gestione delle anomalie

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

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

Tipo anomalia	Descrizione	Modalità di gestione
	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*.	
Errori nel contenuto dei dati conservati	È il caso eccezionale in cui per ragioni tecniche il *Sistema di conservazione* abbia effettuato un errore, che non può essere corretto con le procedure standard, oppure siano stati versati dati errati da parte del *Produttore*, che, in accordo con il *Produttore* stesso, si ritiene più semplice correggere per via tecnica, piuttosto che annullare e versare nuovamente	Il *Produttore* richiede formalmente al personale archivistico di ParER di effettuare una correzione tecnica dei dati; il gruppo di sviluppo e manutenzione viene quindi incaricato 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]

7.5 Preparazione e gestione del Pacchetto di archiviazione

Come elemento ulteriore di controllo dei versamenti effettuati, i SIP accettati e presi in carico sono inseriti in appositi ***Elenchi di versamento***[12] generati secondo criteri, definiti "criteri di raggruppamento", predefiniti per ***tipologia documentaria*** e anno di produzione. Normalmente il criterio standard prevede che l'elenco si chiuda al raggiungimento di un numero massimo di componenti (5000) o dopo 30 giorni dall'apertura, ma possono essere variati in base a specifiche esigenze conservative.
L'***Elenco di versamento*** è un documento in formato XML, generato alla chiusura dell'elenco e fornito di un *Riferimento temporale* opponibile ai terzi. Riporta per ogni documento o aggregazione versata l'Identificativo univoco, un set di *metadati* descrittivi, le *impronte* degli ***Oggetti-dati*** che lo compongono e una serie di informazioni sintetiche relative alle verifiche a cui è il SIP è stato sottoposto durante il processo di acquisizione.
L'Elenco è recuperabile dal *Produttore* utilizzando apposite funzionalità dell'interfaccia web del Sistema.
Gli elementi inseriti nell'Elenco possono essere sottoposti a ulteriori controlli, anche a campione, finalizzati a verificare la corrispondenza degli oggetti versati con quanto concordato con il *Produttore* e a evidenziare eventuali anomalie non rilevabili dalle verifiche automatiche al ***versamento***.

[12]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.

Una volta chiuso l'Elenco di versamento e completati i controlli, l'Elenco viene validato, automaticamente o manualmente dal Responsabile della funzione archivistica di conservazione, eventualmente anche con propria firma digitale.
Tale validazione avvia il processo di creazione dei Pacchetti di Archiviazione (AIP) e dei relativi indici in formato conforme allo standard UNI SinCRO.

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

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

- l'***Indice dell'AIP*****:** è un documento in formato XML prodotto in conformità alle specifiche contenute nella struttura dati dell'Allegato 4 delle ***Regole tecniche*** e descritto in dettaglio del documento "Modelli dei pacchetti di archiviazione" che contiene tutti i *metadati* dell'***Unità documentaria*** presenti sul Sistema e i riferimenti agli altri file presenti nel pacchetto. Tra i dati contenuti nell'Indice vi sono:
  - la data di generazione dell'AIP (espressa con un *Riferimento temporale* opponibile ai terzi con le caratteristiche descritte al paragrafo 7.3) che costituisce il *Riferimento temporale* opponibile a terzi di tutti i file elencati nell'Indice stesso;
  - i *metadati* descrittivi dell'***Unità documentaria***;
  - i *metadati* generati dal Sistema nel corso delle verifiche e delle elaborazioni operate sul SIP;
  - le *impronte* dei singoli file (***Oggetti-dati***) dell'AIP stesso;
  - le *impronte* delle eventuali precedenti versioni dell'***Indice dell'AIP*** (in caso di aggiornamento);
  - le *impronte* degli altri documenti generati dal Sistema nel *processo di conservazione*;
  - il riferimento agli ***Elenchi di versamento*** relativi ai SIP da cui è stato generato o aggiornato l'AIP;
- I file **(*Oggetti-dati*)** dell'***Unità documentaria*** ricevuti nel SIP e le eventuali, 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.

L'AIP dell'***Unità documentaria*** prodotto viene firmato dal Responsabile della funzione di archivistica di 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, denominata Elenco Indici AIP, prodotta a partire dagli ***elenchi di versamento*** e contenente gli identificativi e l'impronta degli Indici degli AIP di ogni ***Unità documentarie*** contenuta negli elenchi stessi. Tale evidenza informatica, una volta 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 funzione archivistica di conservazione ad attestare il corretto svolgimento del processo di ***Versamento in archivio*** che completa il processo di trasferimento al Sistema dal punto di vista del *Produttore*.

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

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

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

Il *Produttore* può accedere agli AIP conservati utilizzando le 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 SIP da parte del *Produttore* e attivazione di procedure di conservazione da parte del Sistema.

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

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

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

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

[Torna al Sommario]

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

I DIP sono prodotti di norma a partire dagli AIP presenti sul Sistema. Nel caso in cui non sia stato ancora generato l'AIP è comunque possibile produrre DIP, riferiti agli oggetti versati e ai documenti di conservazione già prodotti.
Esistono varie tipologie di DIP, 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 (vedi anche paragrafo 7.9) ed è scaricabile dall'interfaccia web del Sistema o tramite appositi servizi descritti nel documento Specifiche tecniche dei servizi di recupero;
- DIP coincidente con il SIP: contiene gli Oggetti-dati presenti, l'***Indice del SIP*** e l'***Esito versamento*** ed è scaricabile dall'interfaccia web del Sistema;
- DIP del *Rapporto di versamento*: contiene i *Rapporti di versamento* relativi all'***Unità documentaria*** ed è scaricabile dall'interfaccia web del Sistema o tramite appositi servizi descritti nel documento "Specifiche tecniche dei servizi di recupero";
- DIP dei documenti di conservazione: contiene i documenti di conservazione prodotti nel corso del processo di conservazione (***Indice del SIP***, 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 al *Produttore,* che poi provvede a consegnarli agli interessati. La consegna o la messa a disposizione dei DIP direttamente agli interessati è possibile solo con specifico accordo tra *Produttore* e ParER.

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

[Torna al Sommario]

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

La produzione di duplicati informatici o copie informatiche dei *Documenti informatici* conservati nel Sistema avviene mediante la messa a disposizione del *Produttore* di DIP comprensivi degli ***Oggetti-dati*** che li compongono.
Tali pacchetti sono acquisibili dagli *Utenti* utilizzando 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 di ParER né il rilascio di copie cartacee conformi agli originali digitali conservati, né l'*accesso* diretto alla documentazione da parte di colui che, dovendo tutelare situazioni giuridicamente rilevanti, abbia presentato istanza di consultazione.
Pertanto, in merito all'esercizio del diritto d'accesso ai documenti conservati da ParER, questo si limita a fornire al *Produttore*, su precisa richiesta di quest'ultimo e senza che su di esso debba gravare alcun particolare onere, il documento informatico conservato, qualora per un qualsiasi motivo il *Produttore* stesso abbia deciso di non acquisirlo direttamente mediante le modalità descritte nel paragrafo 7.6.
Permane in carico al *Produttore* sia la responsabilità di valutare la fondatezza giuridica della domanda di accesso, sia l'onere di far pervenire il documento (o sua eventuale copia cartacea conforme) al soggetto richiedente.
ParER provvederà a consegnare direttamente la documentazione richiesta solo nel caso di visite ispettive presso ParER o provvedimenti di esibizione o sequestro da parte dell'autorità giudiziaria o di altra autorità ispettiva espressamente indirizzati al soggetto conservatore.

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

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

[Torna al Sommario]

7.8 Scarto dei pacchetti di archiviazione

Il Produttore, in base ai tempi di conservazione risultanti dai propri ***Massimari di scarto*** invia a Parer un Elenco di scarto, in cui sono indicate le ***Unità archivistiche*** o le ***Unità documentarie*** da sottoporre a procedura di *scarto*.
Tale Elenco di scarto, viene verificato da parte di ParER ed eventualmente adeguato in modo da poter essere utilizzato nel Sistema. L'elenco, se modificato, viene trasmesso al *Produttore* che può rifiutarlo indicandone i motivi (innescando in tal modo una nuova verifica da parte di Parer) o accettato. e trasmesso dal *Produttore* all'Autorità di vigilanza che, in base alle norme vigenti, deve fornire il nulla-osta per lo *scarto*.

Il *Produttore*, 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 alle decisioni dell'Autorità. Una volta che l'*Elenco di scarto* definitivo viene predisposto, il *Produttore* lo valida e trasmette a ParER la richiesta di procedere allo *scarto*.

ParER effettua un ulteriore controllo sulla congruenza dell'*Elenco di scarto* definitivo con quello autorizzato dall'autorità e, in caso riscontrasse anomalie, provvede alla correzione e sottopone nuovamente l'Elenco alla validazione del *Produttore*.

Nel caso in cui il controllo sull'*Elenco di scarto* dia esito positivo, ParER procede alla cancellazione degli AIP contenuti nell'Elenco. Al termine delle operazioni viene data comunicazione al Produttore dell'avvenuto scarto, fornendo nella stessa tutti gli elementi utili a ricostruire l'intero processo.

[Torna al Sommario]

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

La ***Convenzione*** prevede che, in caso di recesso o a scadenza di contratto, la Regione Emilia-Romagna, tramite il ParER, è tenuta a riversare 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* nel sistema indicato dal *Produttore*, secondo modalità e tempi indicati nel ***Disciplinare Tecnico***.
ParER garantisce comunque il mantenimento nel proprio *Sistema di conservazione* dei *Documenti informatici* e delle *Aggregazioni documentali informatiche* conservati, con i *metadati* a essi

associati e le *evidenze informatiche* generate nel corso del *processo di conservazione* fino alla comunicazione da parte del *Produttore* dell'effettiva messa a disposizione del *Sistema di conservazione* in cui effettuare il riversamento.
ParER provvederà all'eliminazione dal proprio *Sistema di conservazione* di tutti gli oggetti riversati e di tutti gli elementi riferiti al *Produttore* solo al termine del riversamento e solo dopo le opportune verifiche - effettuate da entrambe le Parti e svolte di concerto tra le stesse - di corretto svolgimento del riversamento stesso.
In tal caso viene garantita la cancellazione e non leggibilità dei dati entro 90 giorni sia dal sistema primario (compresi i backup), sia dal sito di ***business continuity***, sia dal sito di ***Disaster recovery***.
L'intera operazione dovrà comunque avvenire con l'autorizzazione e la vigilanza delle competenti autorità, in particolare delle strutture del MIBACT.

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

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

[Torna al Sommario]

8 IL SISTEMA DI CONSERVAZIONE

8.1 Componenti logiche

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

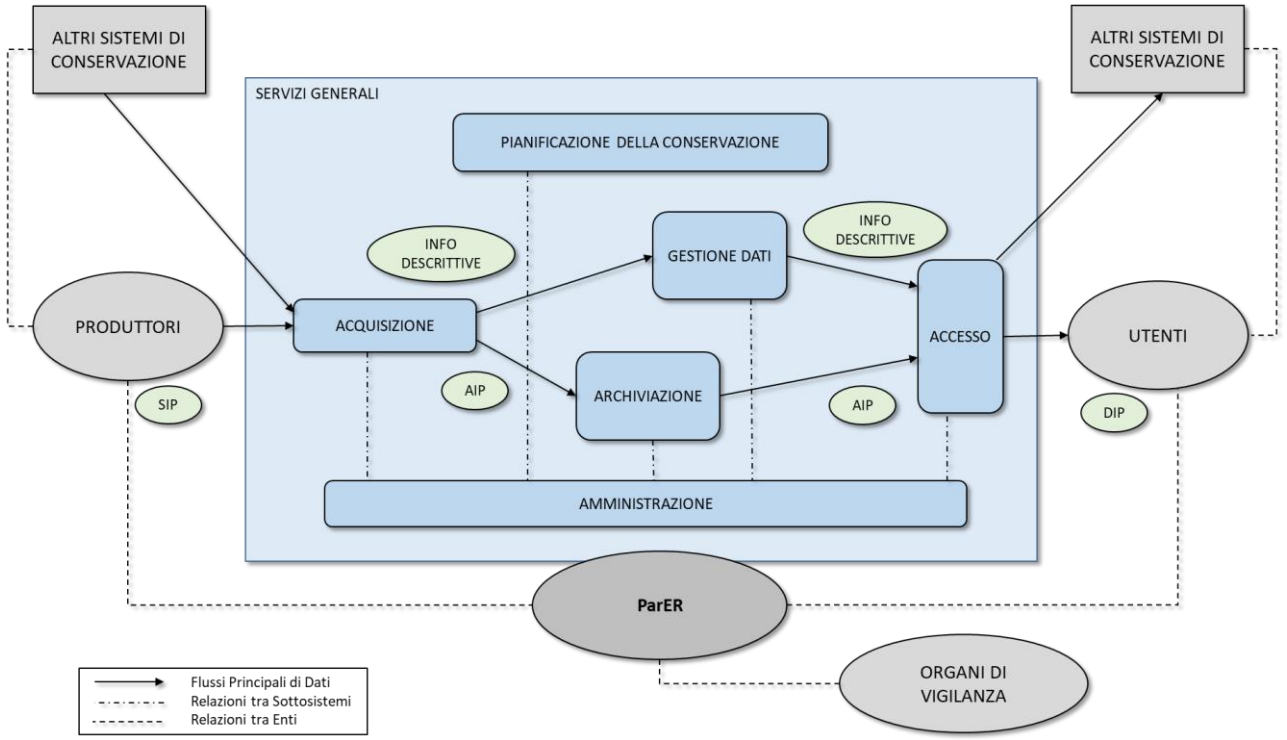

Figura 6 - Schema logico del Sistema di conservazione

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

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

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

Le funzionalità di Gestione Dati gestiscono le ***Informazioni descrittive*** generate al termine della fase di acquisizione e *presa in carico* del *processo di conservazione*. Tali funzionalità

garantiscono: *memorizzazione*, manutenzione e aggiornamento all'interno del Sistema sia delle ***Informazioni descrittive*** necessarie a ricercare gli AIP, ricevute dall'Acquisizione, che dei dati necessari per gestire i pacchetti.

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

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

Le funzionalità di Pianificazione della conservazione gestiscono il monitoraggio dell'ambiente in cui il Sistema è inserito e forniscono le indicazioni necessarie per fare in modo che le informazioni conservate restino fruibili nel lungo periodo tenendo conto dell'evoluzione tecnologica dei sistemi e del cambiamento della ***Comunità di riferimento*** (*Utenti*). Intervengono nella progettazione dei *Pacchetti Informativi* e nella pianificazione dello sviluppo e dei test del software necessario per la ***migrazione*** degli AIP. Tale funzione non è svolta da uno specifico applicativo, né segue procedure meccaniche, 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, 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*** di ParER.

Le funzionalità di *accesso* gestiscono la fase di gestione del DIP del *processo di conservazione* (vedi paragrafo 7.6): 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***.

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

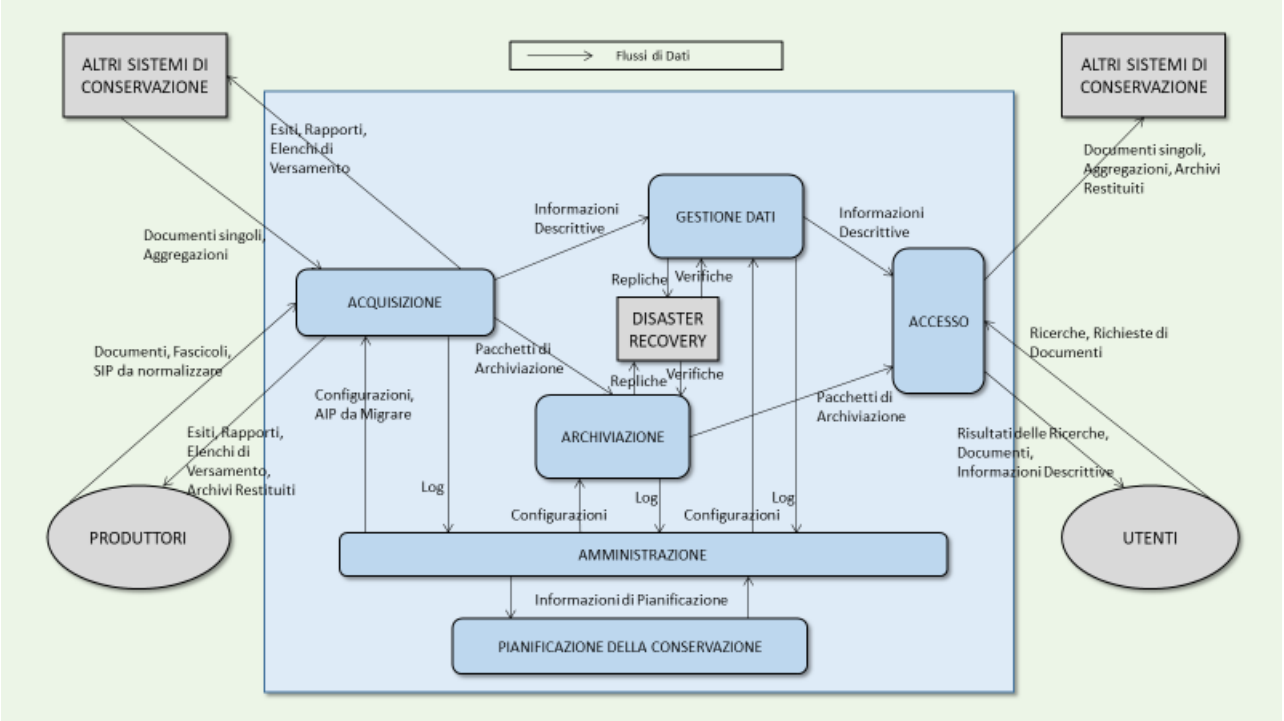

Figura 7 - Flussi di dati nel Sistema di conservazione

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

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

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

[Torna al Sommario]

8.2 Componenti tecnologiche

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

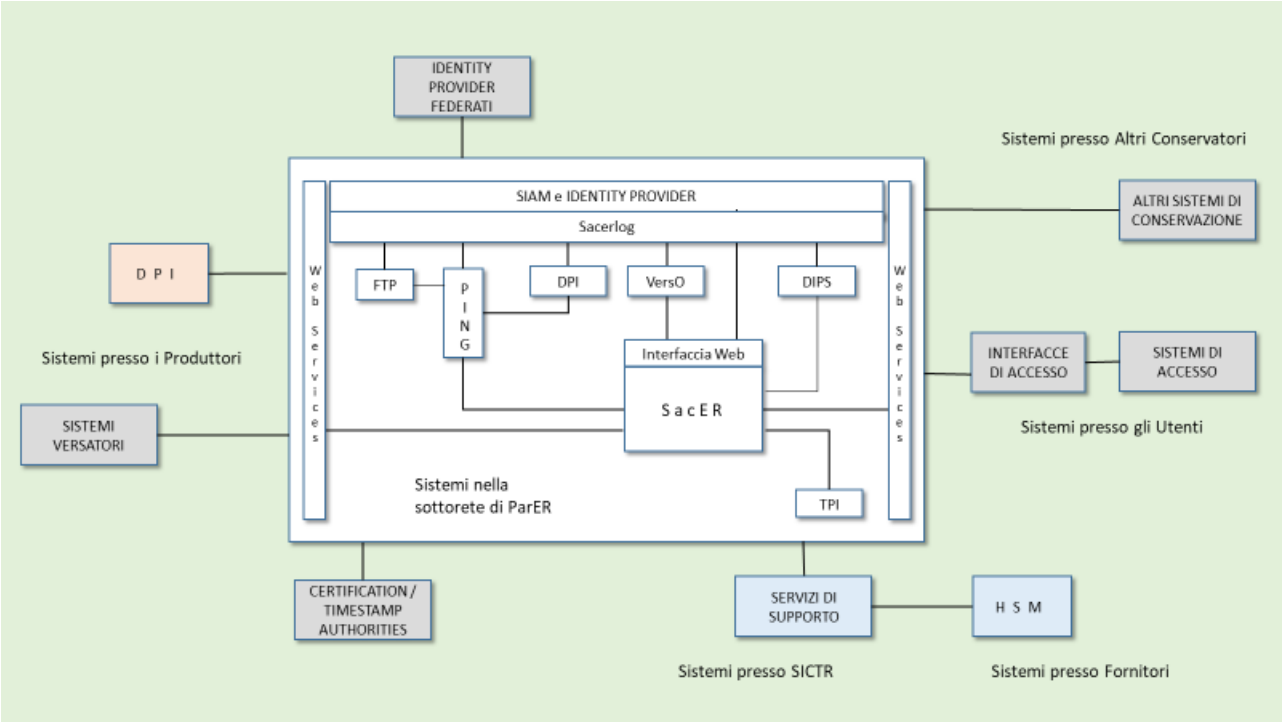

Figura 8 - Schema Tecnologico del Sistema di conservazione

Nella figura sono riportate:

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

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

[Torna al Sommario]

8.2.1 SacER

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

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

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

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

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

- la ***memorizzazione*** degli AIP e l'organizzazione gerarchica dei supporti di memorizzazione. In particolare, gli ***Oggetti-dati*** degli AIP, costituiti dagli Indici degli AIP e dei SIP, dagli ***Esiti versamento***, dai *Rapporti di versamento* e dai file associati ai ***Componenti***, sono memorizzati su supporti di diverso tipo in ragione della loro dimensione e della frequenza con cui vengono ricercati:

  - gli ***Oggetti-dati*** di piccole dimensioni e ad accesso più frequente vengono salvati temporaneamente all'interno del Data Base in opportune tabelle di ***BLOb*** per poi essere memorizzati in modo permanente nell'***object storage***, utilizzando a questo scopo appositi job periodici, descritti più avanti
  - gli ***Oggetti-dati*** di grande dimensione e di accesso meno frequente vengono salvati temporaneamente su ***file system*** in cartelle opportunamente strutturate per poi essere memorizzati in modo permanente su supporti a cassette, utilizzando a questo scopo un apposito componente software chiamato TPI, descritto più avanti;
- il controllo dell'integrità degli oggetti conservati, comprensivo della copia degli archivi, del controllo degli errori e delle procedure di refreshing dei supporti, come descritto nel paragrafo 9.2 e in conformità 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 7.8.

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

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

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

Le funzionalità di Accesso di SacER consentono di restituire in forma di DIP gli oggetti conservati. A tal fine SacER mette a disposizione un'interfaccia web per le ricerche e per l'estrazione manuale dei documenti, e dei Servizi di recupero per l'estrazione automatica.
Gli AIP forniti sono trasformati in DIP sulla base delle caratteristiche dell'oggetto e degli utilizzi cui è destinato. In molti casi la trasformazione dell'AIP in DIP può richiedere specifici passi elaborativi e trasformazioni complesse che, necessitando di elaborazioni onerose, vengono normalmente eseguite da opportuni job batch e mantenute in modo permanente sul Data Base.

Secondo la natura dei DIP, l'*esibizione* può avvenire on-line, 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 molti casi, per comodità di trasferimento e recupero i vari elementi che costituiscono il DIP vengono compressi in un archivio di tipo ZIP.
Il modulo di Accesso, oltre a verificare tramite i servizi di Autenticazione l'abilitazione dell'*Utente* al recupero del documento, traccia in apposite tabelle di log tutte le richieste prevenute, qualunque ne sia stato l'esito.

[Torna al Sommario]

8.2.2 VersO

Il client di versamento manuale VersO (Versamento Online) è un modulo che ParER mette a disposizione degli Enti produttori. Utilizza un'interfaccia web e quindi non richiede l'installazione di alcun software sulla stazione di lavoro del *Produttore*.
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*** di ParER o su un ***IdP*** federato, utilizzando in ogni caso logiche di profilazione del Sistema, ed effettua il ***versamento*** dei SIP tramite interazione guidata con l'operatore del *Produttore*.
Tale modulo semplifica le operazioni di ***versamento*** manuale da parte del *Produttore*, automatizzando la generazione dell'***Indice del SIP*** ed effettuando un test completo della correttezza del versamento prima di eseguire il versamento stesso. Inoltre, mantiene il log dei versamenti effettuati e consente di interrompere temporaneamente l'operazione (p.e per raccogliere informazioni necessarie per completarlo) riprendendola successivamente, indipendentemente dalla scadenza della sessione web.

[Torna al Sommario]

8.2.3 PING

Il modulo software PING (PreINGest) gestisce il processo di preacquisizione nel caso di ***versamento*** di Oggetti da trasformare in SIP (vedi paragrafo 7.1.1).
La trasmissione dei pacchetti, solitamente compressi, avviene tramite protocollo FTPS; l'***FTP server*** provvede a memorizzare i file ricevuti sullo ***storage*** dedicato allo spazio FTP di input.
Una volta ricevuti gli Oggetti, un job schedulato provvede alla loro elaborazione per la produzione dei SIP da versare. Un ulteriore job schedulato si occupa di effettuare il ***versamento*** a SacER, che avviene utilizzando un apposito servizio di versamento. Tale servizio accetta in chiamata due file XML, uno con l'***Indice del SIP*** e un altro con le ***Informazioni sull'impacchettamento***, relative alla posizione dei file del SIP memorizzati sullo spazio FTP di input.
SacER utilizza le ***Informazioni sull'impacchettamento*** per recuperare i file dal ***file system*** di PING e depositarli nel proprio per le successive elaborazioni.
Le successive elaborazioni vengono eseguite da PING direttamente, nel caso in cui la normalizzazione richieda regole precodificate (come p.e. nel caso delle immagini diagnostiche in formato Dicom), oppure utilizzando un motore ETL di esecuzione delle trasformazioni nel caso in cui si debbano applicare regole di trasformazioni specifiche dell'oggetto in questione. In questo

caso le regole sono state definite durante nella fase di avvio del servizio, tramite uno strumento visuale ed eventuali integrazioni di codice sviluppato ad hoc.

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

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

[Torna al Sommario]

8.2.4 DPI

Il modulo software DPI (Digital Preservation Interface), sviluppato e manutenuto da ParER, consiste in un sistema di interfaccia tra i sistemi dell'Ente produttore e PING, installato all'interno della rete dell'Ente stesso e gestito secondo le politiche di sicurezza dell'Ente, potendo tra l'altro autenticarsi sul suo ***IdP***.
DPI implementa funzionalità di ***versamento*** per specifiche tipologie di SIP. In particolare, qualificandosi come nodo ***DICOM***, DPI riceve dai ***PACS*** studi diagnostici, che poi trasmette a PING per la trasformazione e il ***versamento*** a SacER.
DPI può operare con logiche sia push che pull, ricevendo o estraendo dati e documenti dai sistemi del *Produttore* per poi versarli nel Sistema, richiamando gli opportuni servizi di PING.
Inoltre, DPI fornisce strumenti di monitoraggio dei versamenti effettuati a disposizione dell'Ente produttore.

[Torna al Sommario]

8.2.5 Interfacce di Acquisizione e di Recupero (Web Service)

I sistemi che debbono versare a SacER documenti o aggregazioni e ottenerne l'esibizione colloquiano con SacER tramite opportuni ***Web Service***, che sono definiti nei documenti "Specifiche tecniche dei servizi di versamento" e "Specifiche tecniche dei servizi di recupero". Tali servizi sono invocati anche dai componenti di versamento sviluppati da ParER (DPI, VersO), oltre che dai sistemi di versamento dei *Produttori*.
Nel processo di preacquisizione il client versante (p.e. DPI) utilizza ***Web Service*** per coordinare il processo con il modulo PING, ma trasmette gli oggetti da conservare tramite protocollo FTPS, su un'opportuna area FTP, gestita dal server FTP di ParER. Fa eccezione il client interno a PING, che può versare anche on line, senza appoggiarsi su protocollo FTP.

[Torna al Sommario]

8.2.6 TPI

Il modulo software TPI (Tivoli Preservation Interface) gestisce la *memorizzazione* degli ***Oggetti-dati*** su supporti a cassette, operata utilizzando come sistema di gestione della ***tape library*** il software Tivoli.
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 una seconda copia per ogni cassetta.
Le attività di gestione del sito secondario sono tracciate in uno specifico Data Base del sistema di gestione della ***tape library***.

[Torna al Sommario]

8.2.7 DIPS

Il modulo software DIPS (DIPSpenser), previo controllo dei diritti di accesso alle informazioni, consente di attivare ricerche sul Sistema e di soddisfare richieste relative agli oggetti conservati, anche quando le funzionalità di ricerca messe a disposizione dall'interfaccia web di SacER non riescono a soddisfare le particolari esigenze dell'utente.
DIPS consente ricerche complesse sugli oggetti conservati sulla base delle ***Informazioni descrittive*** memorizzate dalle funzionalità di Gestione dati, e di ottenere l'*esibizione* dei documenti individuati dalla ricerca, sfruttando le funzionalità di Accesso di SacER. DIPS opera ricercando gli AIP da esibire, attraverso le ***Informazioni descrittive*** fornite dalle funzionalità di Gestione dati, e richiedendo gli AIP alle funzionalità di Archiviazione.
Il modulo DIPS consiste di un sistema generalizzato in grado di configurare tramite opportuna parametrazione i criteri da utilizzare nella ricerca e la presentazione dei risultati in ragione delle necessità e delle preferenze dei diversi utenti.

[Torna al Sommario]

8.2.8 SIAM

Il modulo software SIAM (SacER Identity and Access Management) consente di gestire l'autenticazione e la profilatura degli operatori. Tale profilatura viene utilizzata da SacER e dagli altri moduli software del Sistema per valutare a quali viste specifiche di dati e a quali attività ogni operatore abbia accesso, sulla base dei ruoli assegnati.
Per le funzionalità di autenticazione SIAM utilizza sistemi di ***IdP*** (Identity Provider); ParER mette a disposizione un proprio ***IdP***, ma può accettare anche l'autenticazione effettuata su altri ***IdP*** opportunamente federati nel rispetto delle logiche di sicurezza richieste dalle Politiche della Sicurezza di ParER.
SIAM mantiene il Data Base degli operatori dell'***IdP*** di ParER, nonché il Data Base dei profili di tutti gli operatori abilitati al Sistema, qualunque sia l'***IdP*** su cui si sono autenticati, gestendo quindi in modo centralizzato la profilatura per tutti i moduli del Sistema.
La profilatura si spinge fino al livello delle singole attività previste dal Sistema (p.e. pressione di uno specifico bottone di una specifica videata) ed al livello elementare dei dati gestiti (***Struttura***, ***Unità documentaria***, Registro, ecc.) tramite la definizione e la combinazione di opportuni ruoli.
L'***IdP*** implementato da ParER colloquia con gli altri moduli del Sistema tramite standard SAML (Security Assertion Markup Language); l'utilizzo di SAML consente al *Sistema di conservazione* di accettare operatori autenticati su altri sistemi federati.

[Torna al Sommario]

8.2.9 Sacerlog

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

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

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

[Torna al Sommario]

8.2.10 Componenti di supporto

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

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

su cui sono definiti diversi workflow in ragione della problematica di sviluppo da affrontare;

- il sito web di ParER espone in modo strutturato informazioni e documentazione utile sia ai *Produttori* che agli *Utenti* (***Comunità di riferimento***). Tali informazioni riguardano, ad esempio, le procedure amministrative di attivazione dei servizi di conservazione e le specifiche per effettuare i ***versamenti*** dei SIP. Inoltre, rende disponibili informazioni aggiornate sulla quantità dei Documenti conservati e sulle tematiche legate agli *archivi*, alla gestione documentale e alla conservazione degli oggetti digitali. Dal sito è possibile, inoltre, iscriversi alla newsletter settimanale con cui ParER tiene aggiornata la ***Comunità di riferimento*** sulle novità in materia;
- il sito interno di ParER gestisce in modo strutturato informazioni e documentazione a supporto del Sistema di Gestione Integrato (SGI) della Qualità e della Sicurezza necessario per il conseguimento e il mantenimento delle certificazioni ISO sulla Sicurezza e sulla Qualità del servizio;
- SELF, sistema di e-Learning federato della Regione Emilia-Romagna, è il sistema che la Regione ha adottato per la diffusione dell'e-learning nelle proprie pratiche formative e in quelle di altri enti pubblici, cui SELF offre tecnologie, servizi, risorse didattiche e competenze gestione di corsi in e-learning. In particolare, per quanto riguarda ParER SELF mette a disposizione corsi introduttivi e intermedi sul processo di Conservazione e risorse formative sulla gestione della privacy.

[Torna al Sommario]

8.3 Componenti fisiche

8.3.1 Schema generale

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

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

Il Sistema è realizzato su due siti che distano circa 100 chilometri l'uno dall'altro: un sito primario con caratteristiche di continuità operativa, installato presso il ***Data Center*** della Regione Emilia-Romagna a Bologna, che svolge funzioni di normale operatività, ed un sito secondario, installato

presso il ***Data Center*** di Lepida a Parma, ma gestito per i sistemi di ParER dal SICTR, che ha lo scopo di subentrare come sito di ***Disaster recovery*** nel caso di caduta irreparabile del sito primario.

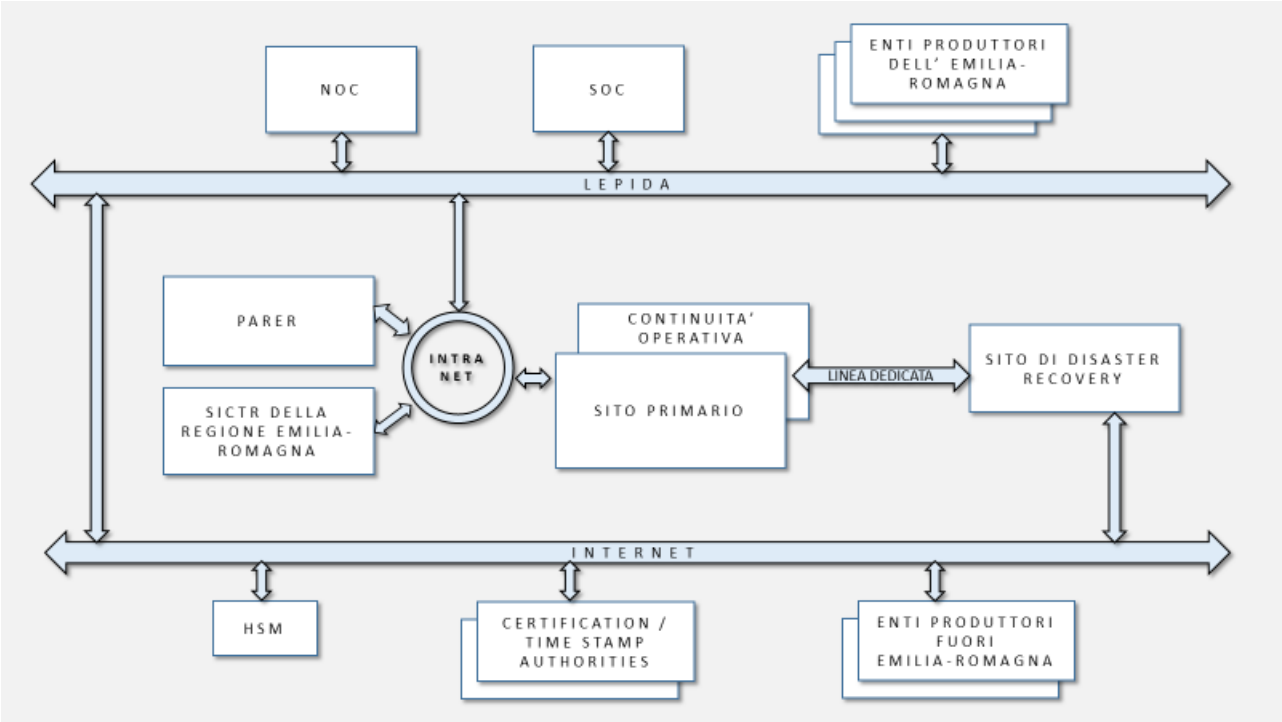

Figura 9 - Schema Infrastrutturale del Sistema di conservazione

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

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

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

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

Sia nel sito primario che nel sito di ***Disaster recovery*** sono presenti diverse istanze del Sistema:
- un'***istanza*** di Produzione, cui è riservata la maggior parte delle risorse;
- un'***istanza*** di Test, riservata al personale di ParER per il test delle nuove versioni rilasciate dai laboratori di sviluppo;
- un'***istanza*** di Preproduzione, allineata all'***istanza*** di produzione, per i test dei *Produttori*.

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

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

[Torna al Sommario]

8.3.2 Caratteristiche tecniche dei Sistemi

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

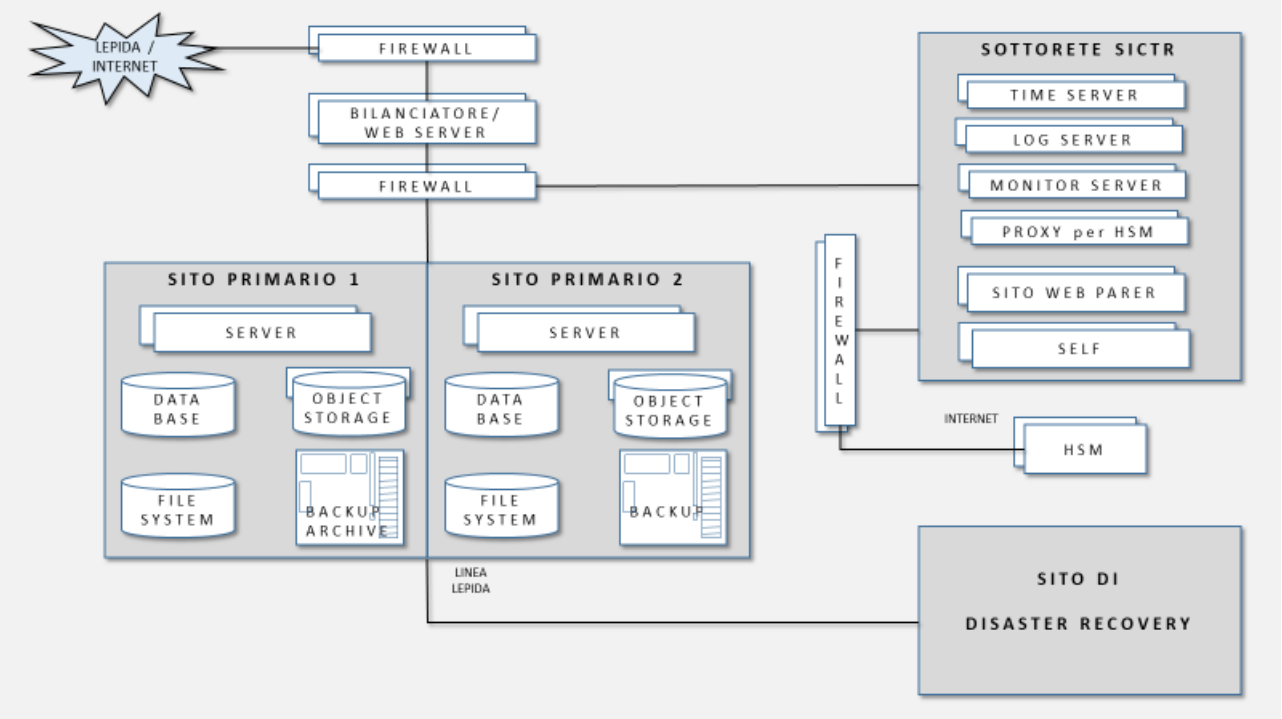

Figura 10 - Schema dei Sistemi di ParER

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

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

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

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

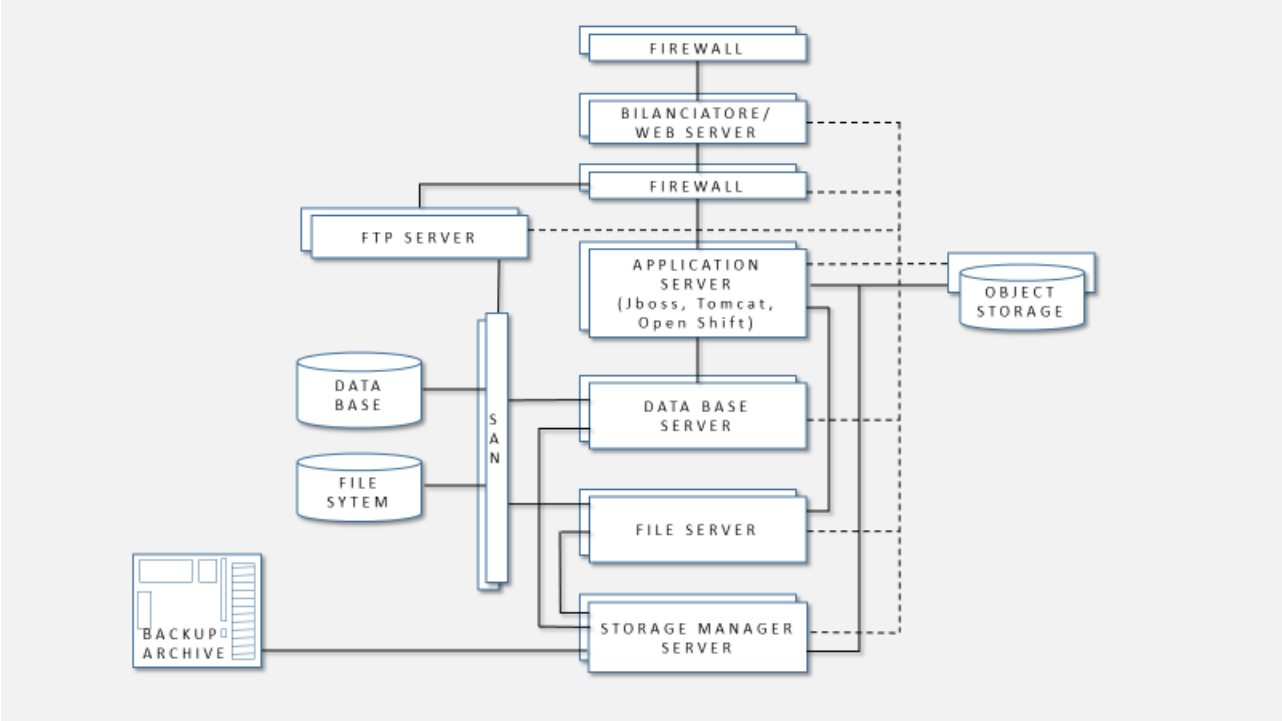

Figura 11 - Schema del Sito Primario

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

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

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

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

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

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

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

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

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

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

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

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

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

La replica dei dati sul sito secondario è garantita da diverse tecnologie:

- il Data Base viene sincronizzato da Oracle tramite Data Guard con modalità di physical standby e maximum availability (il sito primario non attende la fine della scrittura del sito di ***Disaster recovery*** per considerare chiusa la transazione);

- l'***Object storage*** viene replicato nei diversi siti dalle tecnologie intrinseche di NetApp;
- il file system su disco viene allineato tramite ***SCP***;
- l'archivio su cassette viene mantenuto aggiornato da TMS in maniera indipendente tra i due siti tramite opportune politiche di schedulazione; l'applicativo controlla periodicamente la corretta sincronizzazione dei file system e degli archivi su cassette tra i due siti.

Nel caso di dismissione di dispositivi elettronici di memorizzazione dei dati ParER si occupa di garantire la cancellazione sicura delle informazioni presenti nel sistema; a tal fine negli accordi con i gestori dell'infrastruttura ParER richiede esplicitamente l'impegno ad adottare idonei accorgimenti e misure per la distruzione dei supporti di memorizzazione dei dati, una volta dismessi.

[Torna al Sommario]

8.4 Procedure di gestione e di evoluzione

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

[Torna al Sommario]

8.4.1 Gestione dell'Esercizio

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

L'Area di Gestione dei Servizi e delle Infrastrutture di ParER presidia parallelamente l'operatività quotidiana dell'infrastruttura hardware e software sottostante il *Sistema di conservazione*, nonché la pianificazione ed il controllo delle attività straordinarie che possono avere impatto sull'esercizio, come descritto allo specifico punto del paragrafo 5.2, oltre a quelle dettagliate nel paragrafo 9.2; è suo compito indirizzare le attività di gestione che sono svolte dal SICTR della Regione Emilia-Romagna ai fini della gestione del sito primario incluso il sito di ***Continuità Operativa*** e verificarne il buon funzionamento; infine si occupa di verificare il buon funzionamento dell'infrastruttura di ***Disaster Recovery***.

[Torna al Sommario]

8.4.2 Gestione delle utenze

La procedura riportata nel documento "Gestione utenze" e schematizzata in figura descrive le modalità con cui viene garantita la corretta gestione dei soggetti che hanno accesso al sistema

di conservazione, con particolare riguardo alla sicurezza dei dati e delle informazioni conservate, nel rispetto della politica generale di controllo degli accessi di ParER.

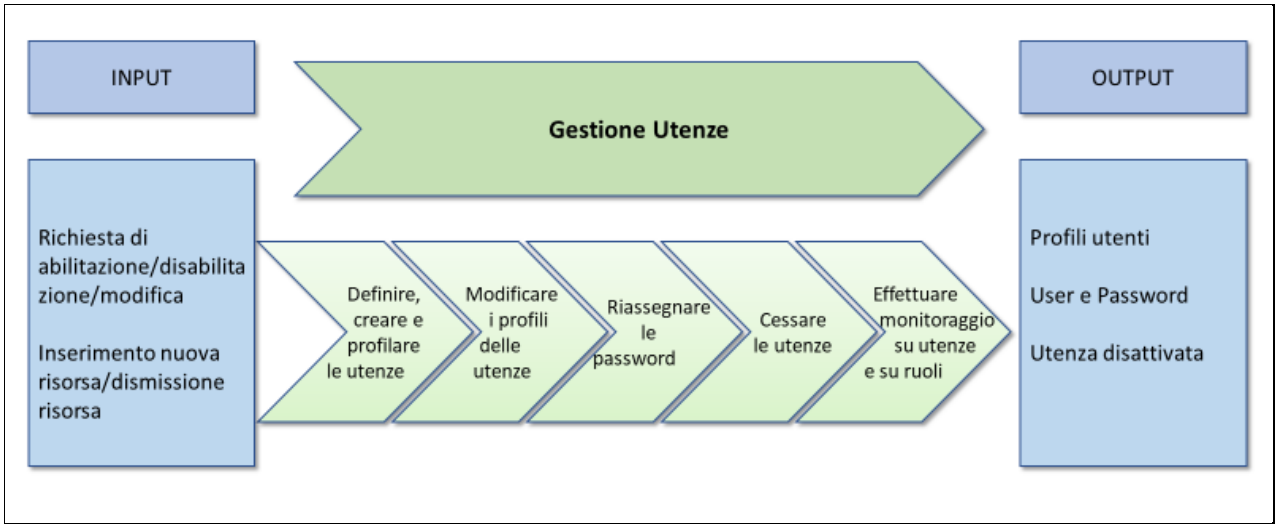

Figura 12 - Procedura di Gestione utenze

La procedura descrive inoltre il metodo seguito per la gestione delle password in coerenza con quanto descritto nella *Politica sulla sicurezza delle informazioni del servizio di Conservazione.*
In particolare, in caso di Creazione di nuovo utente, Riattivazione e Reset di password il sistema genera casualmente le password, le memorizza in forma criptata e le presenta temporaneamente a video in modo che l'operatore possa comunicarle all'utente.
L'operatore di Help Desk di ParER provvede a creare l'utenza nel sistema inviando tramite due e-mail separate lo user-id e la password, che l'utente deve necessariamente cambiare al primo accesso.

Nel caso in cui l'utente abbia dimenticato la password il suo Referente può chiederne la riassegnazione (reset) inviando l'opportuna richiesta tramite una comunicazione formale. L'operatore di Help Desk di ParER (o del gestore esterno) provvede a caricare la richiesta in riferimento alla comunicazione, desumendo le informazioni dal testo della comunicazione o dal file allegato.

Il sistema di gestione delle autenticazioni viene costantemente aggiornato in base alle direttive regionali in termini di sicurezza informatica e alle risultanze dei processi di certificazione per la sicurezza e di accreditamento.

[Torna al Sommario]

8.4.3 Gestione dei Malfunzionamenti

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

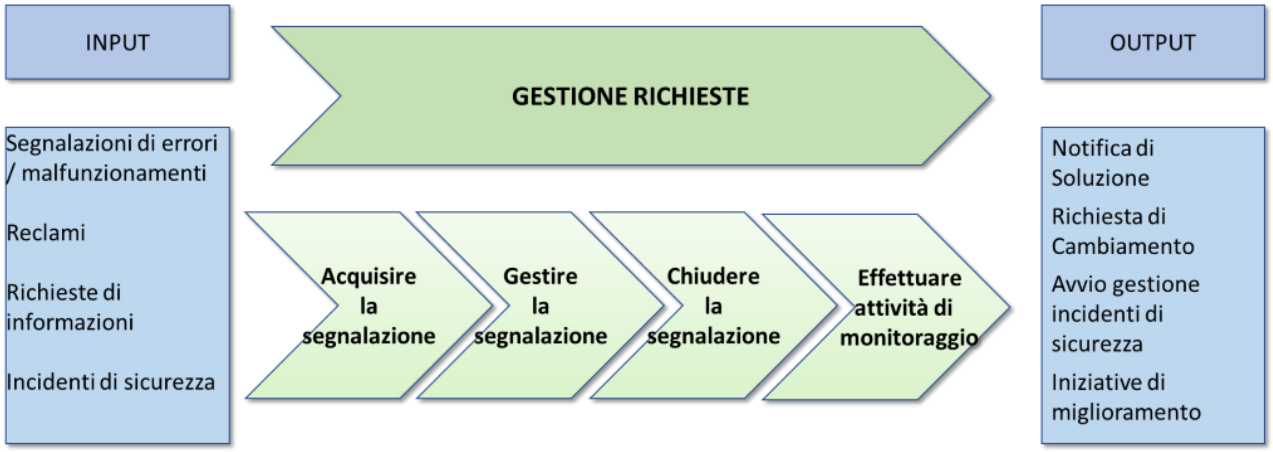

Figura 13 - Procedura di Gestione delle Richieste di Informazioni, Reclami e Segnalazioni

La gestione dei malfunzionamenti può coinvolgere diverse strutture di ParER, secondo la natura del malfunzionamento stesso, che può essere rilevato da diverse fonti: malfunzionamenti di natura applicativa possono essere segnalati dagli Enti *Produttori, dagli Enti Conservatori e dagli Enti Gestori*, dall'Area Esercizio dei Servizi di Conservazione, dall'Area Funzione Archivistica di Conservazione di ParER o dall'Area Tecnologia e Sviluppo Sistemi di Conservazione, mentre malfunzionamenti di natura tecnica possono essere segnalati dall'Area di Gestione dei Servizi e delle Infrastrutture del ParER dal SICTR della Regione Emilia-Romagna.

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

[Torna al Sommario]

8.4.4 Gestione degli Incidenti di Sicurezza

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

La procedura riportata nel documento "Gestione incidenti di sicurezza" e 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 Servizio di conservazione.

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

- gestire gli eventi;

- gestire gli incidenti di sicurezza;
- gestire le attività post-incidente.

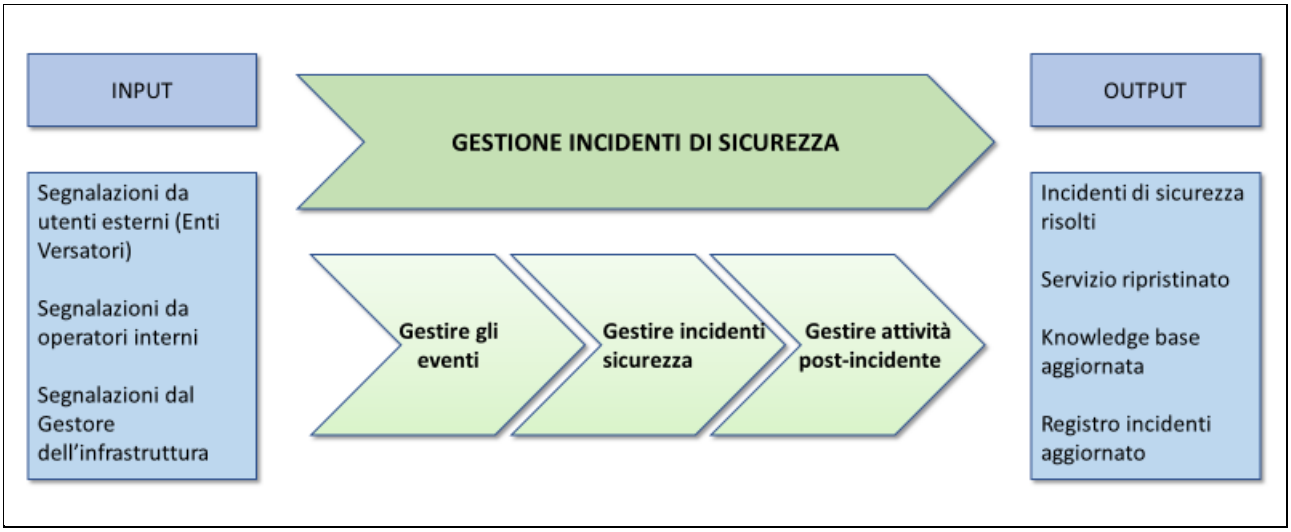

Figura 14 - Procedura di Gestione incidenti di sicurezza

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

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

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

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

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

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

[Torna al Sommario]

8.4.5 Evoluzione pianificata

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

[Torna al Sommario]

8.4.6 Richieste di Cambiamento

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

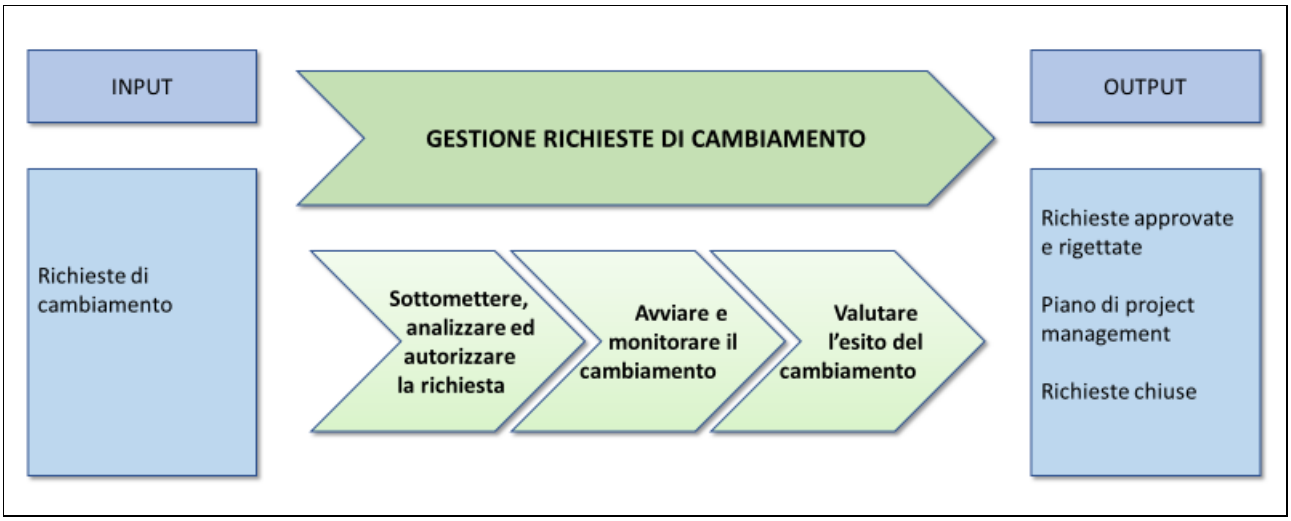

Figura 15 - Procedura di Gestione richieste di cambiamento

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 dai Responsabili delle diverse Aree al personale del ParER ed eventualmente agli altri soggetti coinvolti nel servizio di conservazione.

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

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

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

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

[Torna al Sommario]

8.4.7 Progettazione e Realizzazione di Software Applicativo

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

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

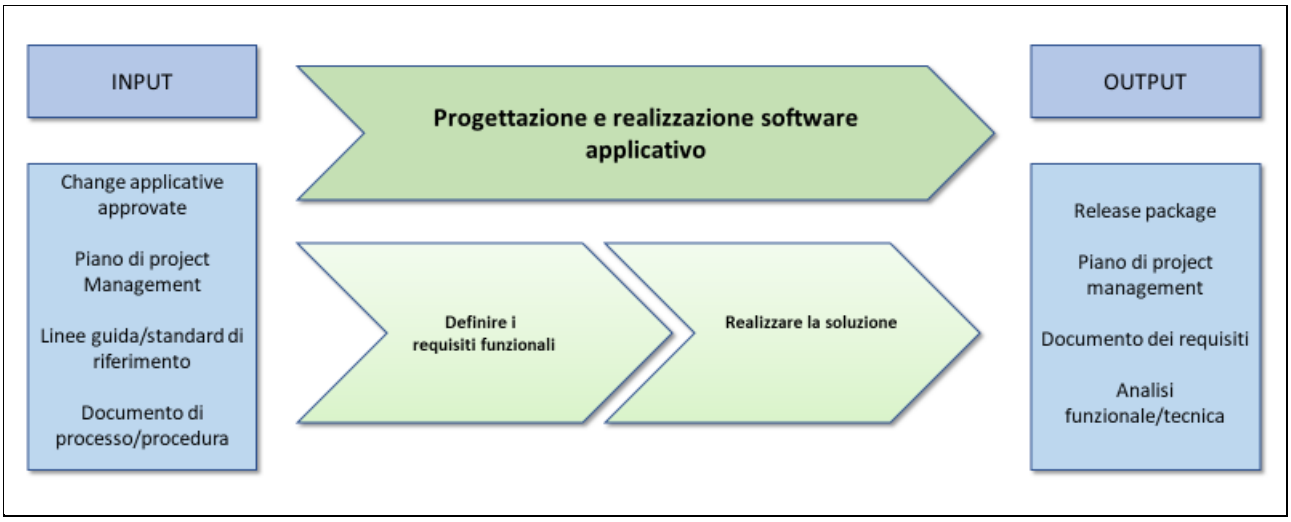

Figura 16 - Procedura di Progettazione e realizzazione di software applicativo

I test della nuova ***release*** vengono condotti nell'ambiente di Test sulla base del piano di test sotto responsabilità dell'Area Tecnologie e Sviluppo con il supporto dell'Area Esercizio dei Servizi Archivistici. Questi test analizzano i comportamenti globali del sistema che non è possibile osservare in riferimento al singolo modulo o componente e coprono l'intera gamma delle caratteristiche da testare (test funzionali, test di performance, test di interfaccia, test di affidabilità, test di stress, test di sicurezza).
Le diverse attività prevedono un continuo scambio di informazioni tra il personale dell'Area Tecnologie e Sviluppo dei Sistemi di Conservazione e il personale dell'Area Esercizio Servizi di Conservazione, al fine di garantire la coerenza tra i requisiti (funzionali, di sicurezza e di esercibilità) e quanto sviluppato.

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

Al termine del processo di sviluppo il software applicativo viene rilasciato come nuova ***release*** eventualmente deployabile in pre-produzione e produzione.

[Torna al Sommario]

8.4.8 Gestione dei Rilasci

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

Gestione dei Servizi e delle Infrastrutture e con l'Area Esercizio dei Servizi di Conservazione il piano di rilascio della nuova ***release*** nell'ambiente di preproduzione e successivamente nell'ambiente di produzione, e richiede al SICTR di effettuare il rilascio.

La procedura di rilascio di una nuova ***release*** è illustrata in figura e descritta in dettaglio nel documento "Gestione dei Rilasci".

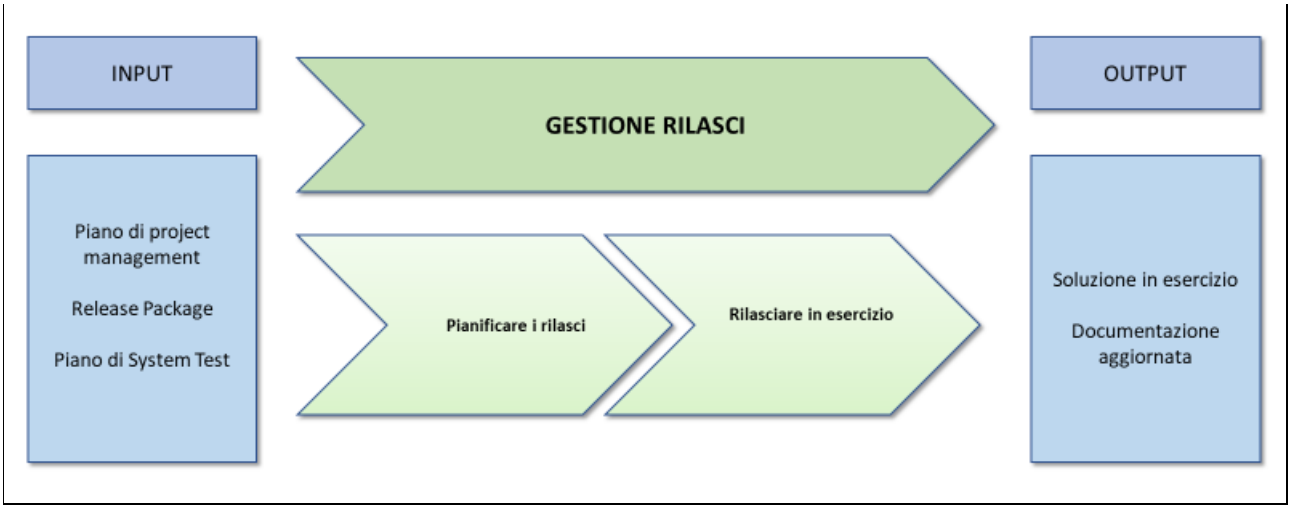

Figura 17 - Procedura di Gestione dei rilasci

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

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

Il SICTR tramite una procedura automatica provvede inoltre a installare nel sito di ***Disaster recovery*** la nuova ***release***, da attivare nel caso di dichiarazione di disastro.

[Torna al Sommario]

8.4.9 Gestione e conservazione dei Log

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

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

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

[Torna al Sommario]

9 MONITORAGGIO E CONTROLLI

9.1 Procedure di monitoraggio

Oltre alle funzionalità di monitoraggio applicativo gestite dal personale di ParER, che sono state illustrate al paragrafo 7.4.1, sono attive procedure di monitoraggio tecnico gestite dal personale del ***SICTR***, che provvede a produrre e rendere disponibili periodicamente all'Area Gestione dei servizi e delle infrastrutture di ParER report di controllo di tutte le aree infrastrutturali (rete, server, ***storage***, database, ***backup***). Si tratta di report tra loro eterogenei, ottenuti per rielaborazione e integrazione delle informazioni prodotte per via automatica dal software di base dei sistemi e dal software di monitoraggio tecnico installato sui medesimi e dai log delle attività svolte dal personale tecnico. Analoghi report vengono prodotti dalla gestione del ***Disaster recovery***.
Periodicamente i report di monitoraggio tecnico vengono esaminati congiuntamente dall'Area Gestione dei servizi e delle infrastrutture di ParER e dall'Area Tecnologie e sviluppo sistemi di conservazione, con lo scopo di individuare eventuali aree di miglioramento negli aspetti tecnici dell'applicativo.

[Torna al Sommario]

9.2 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*** e le caratteristiche delle tecnologie utilizzate garantiscono la completa *integrità* di quanto archiviato in SacER, ovvero di quanto depositato nel Data Base e negli archivi su cassetta, una volta che sia stato duplicato nel sito di ***Disaster recovery*** e salvato tramite opportuno ***backup*** sia nel sito primario che nel sito secondario

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

- la manutenzione e l'amministrazione del Data Base, che si occupa di gestire tutti i metadati trattati nel Sistema. La gestione sistemistica del Data Base è effettuata tramite prodotti certificati da Oracle, ed è tracciata nel *log di sistema*. Il Data Base fornisce periodicamente informazioni statistiche utili a valutarne il dimensionamento e le performance, e quindi a pianificare attività di manutenzione del Data Base stesso e degli applicativi che lo utilizzano;
- il controllo dell'*integrità* del Data Base, che avviene utilizzando funzionalità native del Data Base stesso. Le funzionalità di ***Data Guard*** del Data Base assicurano la replica del Data Base nel sito di ***Continuità operativa*** (in maximum security) e di ***Disaster recovery*** (in maximum availability), mentre le funzionalità di Recovery Management consentono ***backup*** del Data Base completi e incrementali, a caldo e a freddo, secondo le politiche di sicurezza descritte nel Piano della Sicurezza

- la manutenzione e l'amministrazione dell'***object storage***, che si occupa di gestire tutti i ***Componenti*** (files) che transitano nel Sistema, a parte i file memorizzati temporaneamente nel ***file system*** e definitivamente nello storage a cassette, è effettuata tramite prodotti certificati da NetApp, ed è tracciata nel *log di sistema*. L'object storage fornisce periodicamente informazioni statistiche utili a valutarne il dimensionamento e le performance, e quindi a pianificarne le attività di manutenzione del Data Base stesso e degli applicativi che lo utilizzano;
- la congruenza delle copie dei file nei diversi siti in cui è installato l'***object storage*** è garantita dalle caratteristiche intrinseche dell'object storage, che vengono opportunamente utilizzate dagli applicativi. Allo stesso modo è garantita dalle specifiche dell'object storage la possibilità di aggiungere ulteriori nodi anche in altri siti, per aumentare il numero delle copie dei documenti;
- la manutenzione e l'amministrazione ai ***Componenti*** memorizzati su storage a cassette è effettuata tramite prodotti certificati da IBM, ed è tracciata nel *log di sistema;*
- per quanto attiene invece ai ***Componenti*** memorizzati su storage a cassette, l'integrità nel singolo sito 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; la congruenza tra il sito primario e il sito di ***Disaster recovery*** è invece garantita dalle logiche applicative implementate nel modulo TPI.

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

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

[Torna al Sommario]

9.3 Soluzioni adottate in caso di anomalie

Le anomalie vengono affrontate con diverse metodologie, secondo la natura dell'anomalia stessa e la collocazione dell'evento che le ha generate nel *processo di conservazione*; quindi oltre alle procedure atte a garantire l'*integrità* degli archivi, nel senso indicato al paragrafo precedente, esistono anche procedure atte a risolvere anomalie in altre componenti del sistema che registrano dati in SacER. Qui di seguito si trattano esclusivamente le anomalie di origine tecnica, in quanto il trattamento delle anomalie verificatesi nel processo di versamento è già stato descritto precedentemente nel paragrafo 7.4.2

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

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

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

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

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

Ambito del sistema	Misure adottate
	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]

9.4 Verifica periodica di conformità a normativa e standard di riferimento

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

[Torna al Sommario]

9.5 Audit e gestione delle Non Conformità

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

- ISO9001
- ISO27001 con le estensioni ISO27017 e ISO27018
- Accreditamento dei Conservatori secondo le modalità definite da AgID con la circolare n.65/2014
- Qualificazione nel Cloud Marketplace di AgID.

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

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

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

Dall'altra parte, ParER in tutte le convenzioni con i fornitori di infrastruttura, si riserva la possibilità di effettuare a sua volta Audit mirati allo scopo di verificare il mantenimento delle condizioni contrattuali stabilite.

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

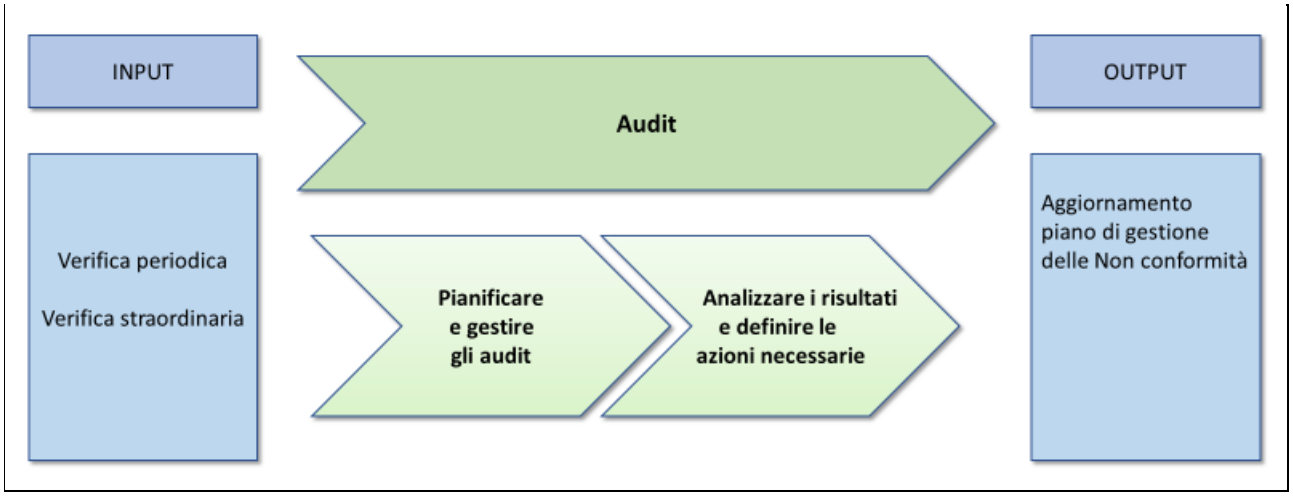

Figura 18 - Procedura di Audit del SGI

Gli Audit vengono eseguiti su base periodica, o in modo straordinario, se i Responsabili lo richiedono, per valutare il grado di applicazione e di efficacia di quanto indicato nella "Politica di sicurezza del sistema di conservazione", nella "Politica per la qualità" e nei documenti ad esso collegati e per orientare la successiva gestione delle Non Conformità riscontrate.
Gli ambiti di verifica sono sia i processi interni che i processi esterni (outsourcing).

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

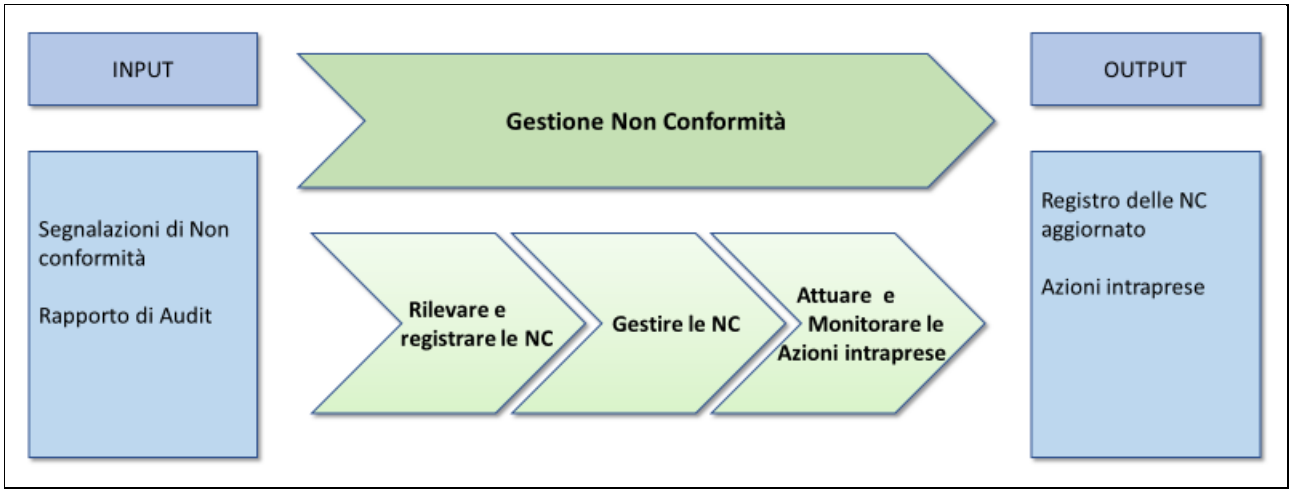

Figura 19 - Gestione delle Non Conformità

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

[Torna al Sommario]

9.6 Controlli di sicurezza

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

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

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

Di seguito in figura viene rappresentato un quadro di sintesi della procedura relativa alle Verifiche Tecniche e VA/PT (Vulnerability Assessment / Penetration Test), che si implementa nell'ambito dei sistemi e degli applicativi in esercizio.

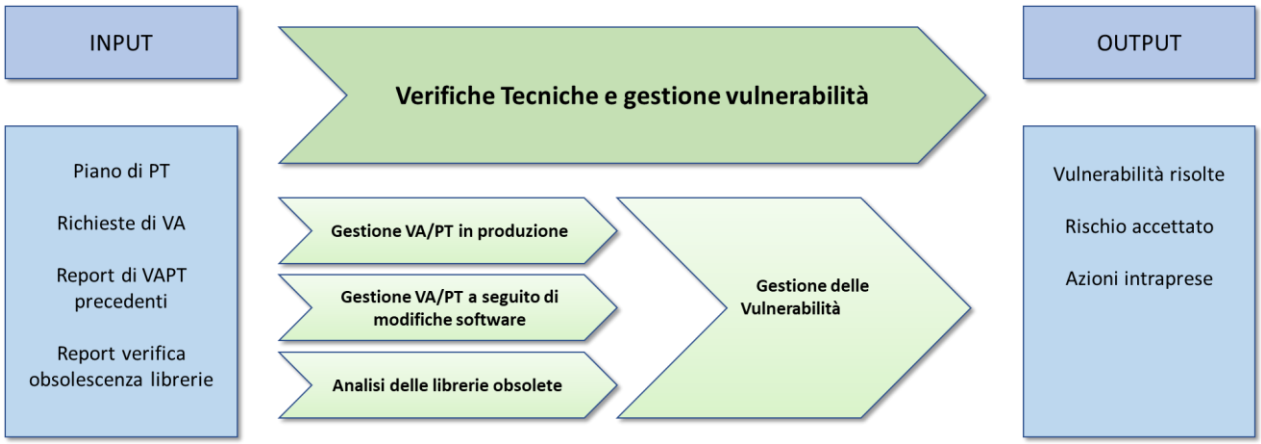

Figura 20 - Procedura di Verifiche Tecniche e VA/PT

I principali obiettivi della procedura sono:

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

.

[Torna al Sommario]

10 TRATTAMENTO DEI DATI PERSONALI

Il nuovo Regolamento europeo sulla protezione dei dati personali (Regolamento (UE) 2016/679 – cd. "GDPR"), ha definito le seguenti figure:

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

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

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

Con deliberazione di Giunta regionale n. 2169 del 20 dicembre 2017, ai sensi dell'art. 37 del GDPR, è stato designato il Responsabile della protezione dei dati (DPO - Data Protection Officer), nella persona del dirigente regionale Dott. Ing. Alessandro Zucchini, specificandone le caratteristiche organizzative e i compiti assegnati. I compiti e le responsabilità del DPO sono stati poi ulteriormente dettagliati nell'allegato A della deliberazione di Giunta regionale n. 1123 del 16 luglio 2018. Tali compiti sono svolti anche per tutte le strutture della Giunta regionale e delle Agenzie e Istituti regionali ai sensi della lettera b), comma 3 bis, art. 1, L.R. 43/2001.
Con successiva deliberazione della Giunta regionale n. 2329 del 22 novembre 2019, a seguito del collocamento a riposo del Dott. Ing. Alessandro Zucchini, dal 1° gennaio 2020 il Responsabile della protezione dei dati (DPO) per le strutture della Giunta e dell'Assemblea Legislativa della Regione Emilia-Romagna e delle Agenzie e Istituti regionali ai sensi della lettera b), comma 3 bis, art. 1, L.R. 43/2001, è stato designato tramite contratto di servizio con la Società LEPIDA S.C.P.A., che lo ha individuato nella persona di Sergio Duretti. Tale designazione esterna del DPO ha durata triennale, salvo mutate condizioni organizzative interne all'Amministrazione che permettano di procedere alla nomina interna del DPO

Il DPO funge da punto di contatto per l'autorità di controllo per questioni connesse al trattamento dei dati personali.

Nel succitato atto deliberativo di Giunta regionale n. 1123 del 16 luglio 2018 sono state individuate, nell'assetto organizzativo dell'Ente, le seguenti figure che intervengono nei trattamenti di dati personali con competenze e responsabilità specifiche:

- "Titolare dei trattamenti di dati personali" è stata individuata la Giunta regionale;
- "Soggetti attuatori" sono stati indicati, tra gli altri, i Direttori Generali della Regione Emilia-Romagna, ciascuno per il proprio ambito di competenza, con attribuzione di funzioni e compiti volti agli adempimenti necessari per la conformità dei trattamenti di dati personali effettuati dall'Ente in esecuzione del regolamento;
- "Responsabili del trattamento" sono designati soggetti esterni dell'Amministrazione che siano tenuti ad effettuare trattamenti di dati personali per conto del Titolare; detta deliberazione n. 1123/2018 dispone che, attesa la natura negoziale della designazione del responsabile del trattamento, questa deve essere effettuata all'interno di contratti o convenzioni e, in ogni caso, in costanza di formazione del rapporto contrattuale, anche in aderenza ai facsimili messi a disposizione dalla struttura della Giunta regionale competente in materia di privacy.

I Direttori Generali possono delegare ai dirigenti Responsabili di Servizio nonché ai dirigenti assegnati alla Direzione relativamente ai trattamenti di diretta responsabilità della stessa, le funzioni e compiti attribuiti in materia di privacy, come specificato al punto 3 dell'allegato A della soprarichiamata deliberazione.

La Regione Emilia-Romagna, in attuazione di quanto previsto dalla legislazione regionale in materia di riordino istituzionale e delle funzioni regionali nel settore del patrimonio culturale, subentra ad IBACN negli atti giuridici (accordi/convenzioni) per la conservazione digitale già sottoscritti dal Responsabile del Servizio Polo Archivistico regionale, comprensivi degli accordi di cui all'art. 28 GDPR, parti integranti e sostanziali, con i quali le parti regolano i trattamenti di dati personali necessari e conseguenti alla sottoscrizione dei medesimi.

Dal quadro organizzativo sopra esposto risulta che il Responsabile del Servizio Polo Archivistico dott. Ing. Marco Calzolari, opportunamente delegato, svolge le funzioni ed i compiti di responsabile del trattamento dati personali previsti in materia di privacy correlati alla conservazione digitale.

Con riferimento alla tematica del trattamento dei dati personali, occorre distinguere preliminarmente la categoria più ampia dei dati personali contenuti nei documenti oggetto di conservazione e la categoria dei dati personali degli *Utenti* del servizio di conservazione, trattati per consentire l'accesso al *Sistema di conservazione*.

L'impostazione adottata negli schemi di convenzione con i *Produttori* consiste pertanto nel riconoscimento della titolarità del trattamento di dati personali contenuti nei documenti oggetto di conservazione in capo allo stesso *Produttore* e nella contestuale designazione della Regione Emilia-Romagna quale "Responsabile del trattamento" dei dati personali necessari all'esecuzione della ***Convenzione/Accordo*** e al compimento degli atti conseguenti.

Di conseguenza, la Regione Emilia-Romagna si impegna, nel trattamento dei suddetti dati, ad attenersi alle istruzioni e a svolgere i compiti indicati dall'Ente Produttore, così come meglio definiti nell'Allegato ex art. 28 del GDPR "Accordo Trattamento dati personali", da considerarsi parte sostanziale e integrante di ogni ***Convenzione/Accordo*** sottoscritta con i *Produttori*.

Coerentemente a quanto espresso, il Responsabile del Servizio Polo Archivistico regionale individuato dagli Enti Produttori, Titolari del trattamento, sulla base di Accordi ex art. 28 del GDPR quale *Responsabile del trattamento*, assume la responsabilità sulla garanzia del rispetto delle vigenti disposizioni in materia di trattamento dei dati personali e sulla garanzia che il trattamento dei dati affidati dai *Produttori* avverrà nel rispetto delle istruzioni impartite dal titolare del trattamento dei dati personali, con garanzia di sicurezza e di riservatezza.

Con precipuo riferimento invece al trattamento dei dati personali degli operatori del servizio di conservazione con livello di abilitazione consultatore, il trattamento dei dati in oggetto ha luogo conformemente a quanto previsto dal GDPR sempre sotto la responsabilità del Responsabile del Servizio Polo Archivistico regionale.
L'archivio logico comprendente i dati degli operatori abilitati alla consultazione di una o più strutture contiene i soli dati obbligatori indispensabili per il rilascio delle credenziali di accesso al sistema e per la corretta gestione del sistema di autorizzazione, nel rispetto di quanto previsto dal sopraindicato GDPR.

L'articolo 35, paragrafo 1, del GDPR prevede che il processo della Valutazione di Impatto sulla Protezione dei Dati (DPIA) sia obbligatorio quando un trattamento di dati personali "*presenti un rischio elevato per i diritti e le libertà delle persone fisiche*"; il soggetto obbligato ad effettuare una DPIA è il titolare del trattamento (nel processo di conservazione quindi il *Produttore*), con il supporto del Responsabile della protezione dei dati (DPO - *Data Protection Officer*), se nominato, e del Responsabile del trattamento eventualmente coinvolto. Considerando la dimensione e la criticità dei documenti conservati, ParER, benché non Titolare, ma Responsabile del trattamento, ha comunque ritenuto opportuno effettuare la DPIA sul trattamento "*Gestione dei dati e dei documenti trasmessi dagli Enti produttori al sistema di conservazione del ParER, ai fini del corretto svolgimento del processo di conservazione (trattamento effettuato nel pubblico interesse)",* identificando le misure opportune per la mitigazione del rischio di violazione dei dati personali, sensibili e giudiziari, con il supporto del DPO della Regione Emilia-Romagna.

[Torna al Sommario]

11 DOCUMENTI DI RIFERIMENTO E ALLEGATI

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

Documento	**Collocazione**
Politica della Qualità del *servizio di Conservazione*	*pubblicata nel sito di ParER: http://parer.ibc.regione.emilia-romagna.it, in "Documentazione"*
Modelli dei SIP (Linee guida per la realizzazione dei SIP)	*pubblicata nel sito di ParER: http://parer.ibc.regione.emilia-romagna.it, in "Documentazione"*
Modelli dei pacchetti di archiviazione (AIP)	*pubblicata nel sito di ParER: http://parer.ibc.regione.emilia-romagna.it, in "Documentazione"*
Specifiche tecniche dei servizi di versamento	*pubblicata nel sito di ParER: http://parer.ibc.regione.emilia-romagna.it, in "Documentazione"*
Specifiche tecniche dei servizi di recupero	*pubblicata nel sito di ParER: http://parer.ibc.regione.emilia-romagna.it, in "Documentazione"*
Politica sulla sicurezza delle informazioni del servizio di Conservazione	*pubblicata nel sito di ParER: http://parer.ibc.regione.emilia-romagna.it, in "Documentazione*
Piano della Sicurezza	*share ParER Doc / Area riservata*
Piano di Continuità Operativa	*share ParER Doc / Policy*
DPIA	*Share regionale / Area riservata*
Gestione incidenti di sicurezza	*share ParER Doc / Procedure / Supporto*
Gestione richieste di cambiamento	*share ParER Doc / Procedure / Supporto*
Progettazione e realizzazione di software applicativo	*share ParER Doc / Procedure / Supporto*
Gestione dei rilasci	*share ParER Doc / Procedure / Supporto*
Audit del SGI	*share ParER Doc / Procedure / Supporto*
Gestione delle Non Conformità	*share ParER Doc / Procedure / Supporto*
Verifiche tecniche e VA/PT	*share ParER Doc / Procedure / Supporto*
Registro dei formati	*SacER*
Gestione utenze	*share ParER Doc / Procedure / Realizzazione del Servizio*
Procedura di restituzione dell'archivio	*share ParER Doc / Procedure / Realizzazione del Servizio*
Gestione di richieste e malfunzionamenti	*share ParER Doc / Procedure / Supporto*

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

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

[Torna al Sommario]