Manuale di Conservazione

Sommario

1.1. Scopo del documento

Il presente Manuale della conservazione costituisce uno strumento indispensabile ai fini organizzativi e procedurali per la conservazione dei documenti informatici.

Il documento riporta le informazioni rilevanti sulle entità coinvolte nel processo di conservazione, sul responsabile della conservazione e sui suoi eventuali delegati e descrive nel dettaglio operativo il processo di conservazione implementato e tutti gli adempimenti posti in essere per il rispetto degli obblighi di legge e per l'aderenza agli standard di riferimento.

Il presente Manuale in primo luogo riporta le norme e gli standard di riferimento.

Prende poi in esame il modello generale del processo di conservazione e riporta la descrizione della struttura organizzativa del servizio di conservazione con i ruoli e le responsabilità dei soggetti coinvolti.

Il Manuale descrive successivamente gli oggetti sottoposti a conservazione, identificando le tipologie di documenti trattati e le relative caratteristiche rilevanti ai fini della conservazione.

Viene in seguito trattato il processo di conservazione, evidenziandone le principali fasi e gli aspetti più salienti.

Si descrive poi il sistema a supporto del processo di conservazione, con particolare attenzione alle sue caratteristiche logiche, fisiche e tecnologiche e alle procedure di gestione dell'esercizio e di evoluzione del sistema stesso.

Infine vengono esaminate le procedure di monitoraggio e di controllo dell'integrità del sistema, le misure di sicurezza e le politiche di trattamento dei dati personali.

1.2. Normative e standard di riferimento

1. **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;
2. **Legge 7 agosto 1990, n. 241** - Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi. (G.U. del 18 agosto 1990, n. 192);
3. **DPR 27 giugno 1992, n. 352** - Regolamento per la disciplina delle modalità di esercizio e dei casi di esclusione del diritto di accesso ai documenti amministrativi, in attuazione dell'art. 24, comma 2, della Legge 7 agosto 1990, n. 241, recante nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi. (G.U. 29 luglio 1992, n. 177);
4. **DPR 12 febbraio 1993, n. 39** - Norme in materia di sistemi informativi automatizzati delle amministrazioni pubbliche, a norma dell'art. 2, comma 1, lettera m), della legge 23 ottobre

1992, n. 421. (G.U. 10 febbraio 1993, n. 42);

5. **Legge 15 marzo 1997, n. 59** - Delega al Governo per il conferimento di funzioni e compiti alle regioni ed enti locali, per la riforma della pubblica amministrazione e per la semplificazione amministrativa;
6. **DPCM 28 ottobre 1999** - Gestione informatica dei flussi documentali nelle pubbliche amministrazioni. (G.U. 11 dicembre 1999, n. 290);
7. **Decreto legislativo 29 ottobre 1999, n. 490** - Testo unico delle disposizioni legislative in materia di beni culturali e ambientali, a norma dell'articolo 1 della legge 8 ottobre 1997, n. 352. (G.U. 27 dicembre 1999, n. 302);
8. **DPCM 31 ottobre 2000** - Regole tecniche per il protocollo informatico; valido ai sensi dell'art. 78 del DPR 28 dicembre 2000, n. 445. (G.U. n. 272 del 21 novembre 2000);
9. **Deliberazione AIPA 23 novembre 2000, n. 51**- Regole tecniche in materia di formazione e conservazione di documenti informatici delle pubbliche amministrazioni ai sensi dell'art. 18, comma 3, del DPR 10 novembre 1997, n. 513. (G.U. 14 dicembre 2000, n. 291);
10. **DPR 28 dicembre 2000, n. 445 e s.m.i.**- Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa. (G.U. 20 febbraio 2001, n. 42);
11. **Circolare del 16 febbraio 2001, n. AIPA/CR/27 – Art. 17 del DPR 10 novembre 1997, n. 513** - Utilizzo della firma digitale nelle pubbliche amministrazioni;
12. **Circolare AIPA 7 maggio 2001, n. AIPA/CR/28** - **Articolo 18, comma 2, del DPCM 31 ottobre 2000** recante regole tecniche per il protocollo informatico di cui al DPR 28 dicembre 2000, n. 445 - Standard, modalità di trasmissione, formato e definizioni dei tipi di informazioni minime ed accessorie comunemente scambiate tra le pubbliche amministrazioni e associate ai documenti protocollati. (G.U. 21 novembre 2000, n. 272);
13. **Circolare AIPA 21 giugno 2001, n. AIPA/CR/31** (**Art. 7, comma 6, del DPCM 31 ottobre 2000** recante "Regole tecniche per il protocollo informatico di cui al DPR 20 ottobre 1998, n. 428" - requisiti minimi di sicurezza dei sistemi operativi disponibili);
14. **Direttiva del Ministro per la funzione pubblica del 13 dicembre 2001 –** Formazione del personale. (G.U. del 31 gennaio 2002, n. 26);
15. **Decreto legislativo 23 gennaio 2002, n. 10** - Recepimento della direttiva 1999/93/CE sulla firma elettronica;
16. D**irettiva del Ministro per l'innovazione e le tecnologie, 9 dicembre 2002 –**Trasparenza dell'azione amministrativa e gestione elettronica dei flussi documentali;
17. **Direttiva del Ministro per l'innovazione e le tecnologie, 20 dicembre 2002 –** Linee guida in materia di digitalizzazione dell'amministrazione;
18. **Legge 27 dicembre 2002, n. 289** - Disposizioni per la formazione del bilancio annuale e pluriennale dello Stato;
19. **DPR 7 aprile 2003, n. 137** - Regolamento recante disposizioni di coordinamento in materia di firme elettroniche a norma dell'articolo 13 del decreto legislativo 23 gennaio 2002;
20. **Decreto legislativo 30 giugno 2003, n. 196 e s.m.i.** - Codice in materia di protezione dei dati personali;

21. **Decreto Ministeriale 14 ottobre 2003** - Approvazione delle linee guida per l'adozione del protocollo informatico e per il trattamento informatico dei procedimenti amministrativi. (G.U. del 25 ottobre 2003, n. 249);
22. **Direttiva del Ministro per l'innovazione e le tecnologie 27 novembre 2003** - Impiego della posta elettronica nelle pubbliche amministrazioni. (G.U. 12 gennaio 2004, n. 8);
23. **Direttiva 1999/93/CE del Parlamento europeo e del consiglio del 13 dicembre 2003**;
24. **Direttiva 18 dicembre 2003** - Linee guida in materia di digitalizzazione dell'amministrazione per l'anno 2004. (G.U. 4 aprile 2004, n. 28);
25. **Codice della Privacy (Allegato B del D. Lgs. 196/2003)**;
26. **DPCM 13 gennaio 2004** - Regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici. (G.U. 27 aprile 2004, n. 98);
27. **Decreto legislativo 22 gennaio 2004, n. 42 e s.m.i.** - Codice dei beni culturali e del paesaggio, ai sensi dell'art. 10 della legge 6 luglio 2002, n. 137. (G.U. 24 febbraio 2004, n. 28);
28. **Decreto Legislativo del 7 marzo 2005 n. 82 e s.m.i.** – Codice dell'amministrazione digitale;
29. **Deliberazione CNIPA del 19 febbraio 2004, n. 11** – Regole tecniche per la riproduzione e conservazione di documenti su supporto ottico idoneo a garantire la conformità dei documenti agli originali – Art. 6, commi 1 e 2, del testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa, di cui al decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 e s.m.i.;
30. **DPCM del 30 marzo 2009 (Regole tecniche per la firma digitale)**;
31. **Decreto del Ministero dell'Economia e delle Finanze del 23 gennaio 2004** – Modalità di assolvimento degli obblighi fiscali relativi ai documenti informatici ed alla loro riproduzione in diversi tipi di supporto;
32. **Decreto Legislativo 20 febbraio 2004, n. 52 (Direttiva 2001/115/CE)**;
33. **Circolare dell'Agenzia delle Entrate 45/E del 19 ottobre 2005 – Decreto legislativo 20 febbraio 2004, n. 52** – attuazione della direttiva 2001/115/CE che semplifica ed armonizza le modalità di fatturazione in materia di IVA;
34. **Circolare dell'Agenzia delle Entrate 36/E del 6 dicembre 2006 – Decreto del Ministero dell'Economia e delle Finanze del 23 gennaio 2004** – Modalità di assolvimento degli obblighi fiscali relativi ai documenti informatici ed alla loro riproduzione in diversi tipi di supporto;
35. **Decreto Legislativo del 9 aprile 2008, n. 81** – Attuazione dell'articolo 1 della legge 3 agosto 2007, n. 123, in materia di tutela della salute e della sicurezza nei luoghi di lavoro;
36. **Decreto Legge 185/2008 (art. 2215 bis c.c. e documenti unici**);
37. **Decreto del Presidente del Consiglio dei Ministri del 30 marzo 2009** – Regole tecniche in materia di generazione, apposizione e verifica delle firme digitali e validazione temporale dei documenti informatici;
38. **Risoluzione dell'Agenzia dell'Entrate 158/E del 15 giugno 2009** – Consulenza giuridica Associazione e Ordini Professionali – D.M. 23 gennaio 2004 e fatturazione elettronica –

risposta a quesiti;

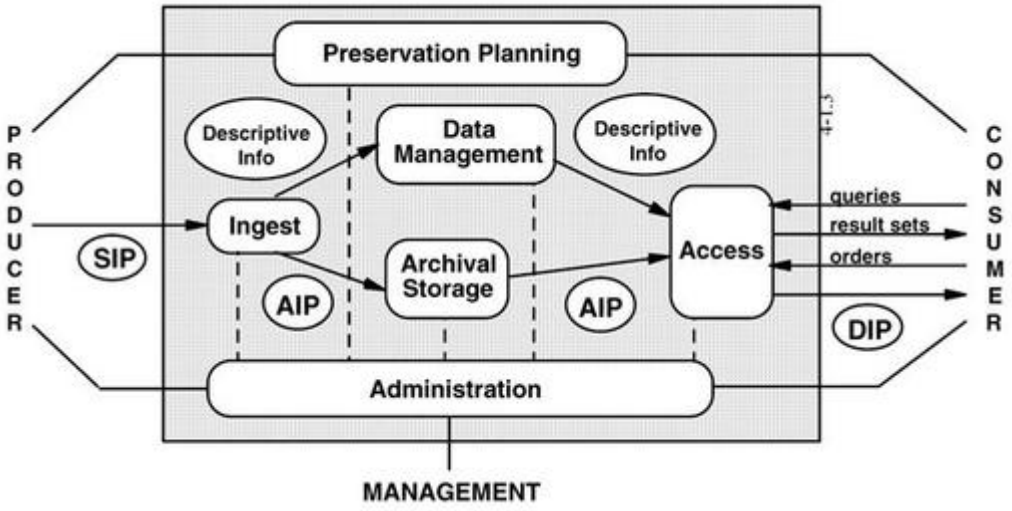
39. **D.Lgs 30 Dicembre 2010 n.235**;
40. **Provvedimento del Direttore dell'Agenzia delle Entrate del 25 ottobre 2010** – Provvedimento attuativo della comunicazione dell'impronta relativa ai documento informatici rilevanti ai fini tributari, ai sensi dell'art. 5 del decreto 23 gennaio 2004;
41. **Circolare dell'Agenzia delle Entrate 5/E del 29 febbraio 2012** – Quesiti riguardanti la comunicazione dell'impronta relativa ai documenti informatici rilevanti ai fini tributari, ai sensi dell'art. 5 del decreto 23 gennaio 2004 e del provvedimento del Direttore dell'Agenzia delle Entrate del 25 ottobre 2010;
42. **DPCM del 22 febbraio 2013** – Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma3, lettera b), 35, comma 2, 36, comma 2, e 71;
43. **DPCM 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;
44. **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;
45. **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;
46. **Standard ISO/IEC 27001:2013**, Information technology - Security techniques - Information security management systems – Requirements, Requisiti di un ISMS (Information Security Management System);
47. **Standard 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;
48. **Standard 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;
49. **Standard ISO 16363:2012** - Space data and information transfer systems - Audit and certification of trustworthy digital repositories (CCSDS 652.0-M-1 OAIS);
50. **Standard ISO 14721:2012** – Open Archival Information System - Recommend Practice (CCSDS 650.0-M-2 OAIS);
51. **Standard UNI 11386:2010 Standard SInCRO** - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali;
52. **Standard ISO 15836:2009 Information and documentation** - The Dublin Core metadata element set, Sistema di metadata del Dublin Core.

1.3. Glossario

Per i termini utilizzati nel presente Manuale si rimanda al Glossario di cui all'allegato 1 delle Regole Tecniche.

2. Modello organizzativo della conservazione: ruoli e responsabilità

Seguendo quanto indicato dalle Regole tecniche vigenti, il contesto di riferimento che caratterizza le responsabilità e gli attori che intervengono nel sistema di conservazione dei documenti si articola nell'intervento di Produttore (Producer), Responsabili della conservazione (Management) e Utente (Consumer), che vengono definiti nei paragrafi successivi, in aderenza al modello OAIS riportato nella figura seguente.



2.1. Produttore

Il Produttore (Ente o Soggetto produttore) è l'ente titolare dei documenti da conservare e risponde alle istituzioni competenti sulla corretta conservazione degli stessi. Sottoscrive un contratto per le attività di conservazione assegnando a SIA la gestione in outsourcing del processo di conservazione, **identificando in SIA la figura del Responsabile del servizio di conservazione** in ottemperanza ai requisiti normativi in materia.

Nel ruolo del Produttore possono quindi essere definiti tutti gli enti che versano i documenti e le aggregazioni documentarie da conservare con gli opportuni metadati.

Il Produttore si impegna a depositare i documenti informatici garantendone l'autenticità e l'integrità, 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.

Le tipologie di documenti da trasferire, le modalità di versamento e i metadati sono concordati e specificati negli allegati tecnici ai contratti stipulati con SIA.

Il Produttore resta il responsabile del contenuto del Pacchetto di versamento (SIP) ed è tenuto a trasmetterlo al servizio di conservazione secondo le modalità operative descritte negli allegati tecnici.

2.2. Utente (Consumer)

L'**Utente** è una persona, ente o sistema che ha la possibilità di accedere al sistema di conservazione dei documenti informatici al fine di fruire delle informazioni di interesse conservate al suo interno (recupero dei documenti o di copie di interesse) nei limiti previsti dalle norme vigenti.
Il ruolo dell'Utente si può identificare, al momento, con l'Ente produttore, in relazione a specifici soggetti abilitati indicati dal Produttore stesso, che possono accedere esclusivamente ai documenti da esso stesso versati o solo ad alcuni di essi secondo le regole di visibilità e di accesso concordate negli allegati tecnici al contratto.

2.3. Responsabili della conservazione (Management)

Il Responsabile del servizio di conservazione è un soggetto legato da un rapporto qualificato con il Produttore in quanto **soggetto affidatario** del processo di conservazione per suo conto. La sua attività consiste nell'erogazione del servizio di conservazione dei documenti e nella gestione del relativo sistema informatico di supporto, regolato dal relativo Contratto di servizio col Produttore, in cui vengono evidenziati i compiti specifici del Responsabile della conservazione e le condizioni che regolano lo svolgimento del servizio di conservazione. L'attività di SIA in tale ruolo include la gestione degli strumenti hardware e software di sistema, d'ambiente e di comunicazione necessari per la realizzazione del processo di conservazione, impiegando metodologie aggiornate che ne assicurano precisione, tempestività e sicurezza.

Il Responsabile della conservazione è una persona nominata all'interno del Produttore ed i suoi riferimenti sono indicati nel documento "Specificità del contratto", nel quale sono anche riportate le attività e le responsabilità affidate al Responsabile del servizio di conservazione.

2.4. Organismi di tutela e vigilanza

Il Ministero per i beni e le attività culturali e del turismo (MiBACT) esercita funzioni di tutela e vigilanza sugli archivi degli enti pubblici territoriali e non e di enti privati dichiarati di interesse storico particolarmente importante (ai sensi dell'art. 4 e dell'art. 18 del D.Lgs. 42/2004 e successivi aggiornamenti) e autorizza le operazioni di scarto e trasferimento della documentazione conservata ai sensi del D.Lgs 42/2004.

Le Soprintendenze archivistiche possono, in seguito a preavviso, effettuare ispezioni per accertare lo stato di conservazione e custodia degli archivi e possono emettere prescrizioni per la tutela degli archivi.

3. Organizzazione responsabile della conservazione

3.1. Responsabilità del sistema di conservazione

La responsabilità del servizio di conservazione è in capo a SIA, nella persona del suo Rappresentante Legale.
SIA è leader europeo nella progettazione, realizzazione e gestione di infrastrutture e servizi tecnologici, dedicati alle Istituzioni Finanziarie e Centrali, alle Imprese e alle Pubbliche Amministrazioni, nelle aree dei pagamenti, della monetica, dei servizi di rete e dei mercati dei capitali.
Il Gruppo SIA eroga servizi in circa 40 paesi ed opera anche attraverso controllate in Ungheria e Sud Africa. La società ha sedi a Milano e Bruxelles. Maggiori informazioni sul Gruppo SIA sono disponibili al sito www.sia.eu.

SIA ha istituito al suo interno un servizio di conservazione, gestito da un **Responsabile del servizio di conservazione**, che dispone di una propria struttura organizzativa per le attività specifiche, si avvale di altri servizi già presenti in SIA per le componenti tecnologiche e la gestione della sicurezza e prevede una **figura interna** come proprio **Responsabile della funzione archivistica di conservazione**; tale figura risponde della corretta conservazione dei documenti nei confronti del soggetto che lo ha nominato, conformemente a quanto stabilito nelle Regole tecniche e relativi allegati.
A sua volta il Responsabile della funzione archivistica di conservazione può delegare parte dei compiti e delle responsabilità a lui attribuite, mediante deleghe ad hoc per tipologia di documento e per specifiche attività; tra queste l'attività di firma digitale e marcatura temporale dei lotti di documenti sottoposti a conservazione, che attesta il corretto svolgimento del processo di conservazione.

L'allegato "Soggetti responsabili della conservazione" riporta in ordine cronologico i dettagli dei soggetti coinvolti nel processo di conservazione.

3.2. Gestione del sistema di conservazione

SIA si impegna alla conservazione dei documenti trasferiti dai Produttori, assumendo la funzione di responsabile della conservazione ai sensi della normativa vigente, nel rispetto dei requisiti previsti dalle norme in vigore nel tempo per i sistemi di conservazione.
SIA cura le modalità di trasferimento, accesso e fruizione del patrimonio documentario e informativo conservato, oltre l'evoluzione tecnologica e l'aggiornamento del sistema di conservazione.

I data center utilizzati per la conservazione dei documenti e delle loro copie di sicurezza sono dislocati all'interno del territorio nazionale.

In base a quanto stabilito dall'art. 6 comma 8 delle Regole tecniche, SIA, in veste di conservatore per conto del Produttore, assume anche il ruolo di Responsabile del trattamento dei dati personali previsto dal Codice in materia.

3.3. Struttura organizzativa

SIA, per la gestione del processo di conservazione, nell'ambito della propria struttura organizzativa, ha definito i seguenti ruoli e le relative figure responsabili:

Ruoli	Nominativo	Attività di competenza	Periodo nel ruolo	Eventuali deleghe
Responsabile del servizio di conservazione	Claudio Mauro	Definizione e attuazione delle politiche complessive del sistema di conservazione, della pianificazione annuale delle attività assegnate e dell'organizzazione del lavoro all'interno del servizio, nonché del governo della gestione del sistema di conservazione in conformità alla normativa vigente. È responsabile della definizione delle caratteristiche e dei requisiti del sistema di conservazione, e dell'erogazione del servizio ai Produttori, oltre che della gestione degli aspetti tecnico-operativi degli accordi contrattuali che regolano l'erogazione dei servizi di conservazione e della loro validazione	Dal 2001	
Responsabile Sicurezza dei sistemi per la conservazione	Raffaele Pace	Monitoraggio e controllo del rispetto dei requisiti di sicurezza del sistema di conservazione stabiliti dagli standard, dalle normative e dalle politiche e procedure interne di sicurezza e la segnalazione delle eventuali difformità al Responsabile del servizio di conservazione, oltre all'individuazione e pianificazione delle necessarie azioni correttive	Dal 2010	
Responsabile funzione archivistica di conservazione	Luca Scarfone	Definizione e gestione di tutto il processo conservativo (p.e. modalità di trasferimento da parte dell'ente produttore, descrizione archivistica, esibizione, accesso e fruizione a quanto conservato, esportazione dal sistema di conservazione), di definire e gestire il processo di acquisizione, verifica di integrità e descrizione dei dati, dei documenti e delle aggregazioni documentali trasferiti dal Produttore, della definizione del set di metadati di conservazione dei documenti e dei fascicoli informatici, oltre che del	Da settembre 2008	Delega

		monitoraggio del processo di conservazione e analisi archivistica per lo sviluppo di nuove funzionalità del sistema di conservazione. Tra i compiti del Responsabile della funzione archivistica di conservazione rientrano anche l'analisi e identificazione dell'articolazione strutturale/organizzativa del Produttore e del sistema di gestione documentale da esso adottato, incluse le modalità di registrazione e classificazione della documentazione, oltre la collaborazione con il responsabile della gestione documentale di ciascun Produttore ai fini del trasferimento in conservazione e della selezione		
Responsabile trattamento dati personali	Francesco Orlandini	Garante del rispetto delle vigenti disposizioni in materia di trattamento dei dati personali, assicura che il trattamento dei dati affidati dai Produttori avvenga nel rispetto delle istruzioni impartite dal titolare del trattamento, con garanzia di sicurezza e di riservatezza	Dal 2001	
Responsabile sistemi informativi per la conservazione	Tiziano Paleari	Gestione dell'esercizio delle componenti hardware e software del sistema di conservazione, il monitoraggio del mantenimento dei livelli di servizio concordati con il Produttore, con opportuna segnalazione delle eventuali difformità degli accordi sui livelli di servizio (SLA) al Responsabile del servizio di conservazione e individuazione e pianificazione delle necessarie azioni correttive, la pianificazione dello sviluppo delle infrastrutture tecnologiche del sistema di conservazione ed il controllo e verifica dei livelli di servizio erogati da terzi con segnalazione delle eventuali difformità al Responsabile del servizio di conservazione	Dal 2007	
Responsabile sviluppo e manutenzione del sistema di conservazione	Fabio Giordano	Coordinamento dello sviluppo e manutenzione delle componenti hardware e software del sistema di conservazione, oltre che la pianificazione e il monitoraggio dei progetti di sviluppo del sistema di conservazione e degli SLA relativi alla manutenzione del sistema di conservazione. Funge da interfaccia con il Produttore relativamente alle modalità di trasferimento dei documenti e fascicoli informatici in merito ai formati elettronici da utilizzare, all'evoluzione tecnologica hardware e software, alle eventuali migrazioni verso nuove piattaforme tecnologiche. Si occupa	Da gennaio 2011	

		inoltre della gestione dell'eventuale sviluppo di siti web e portali connessi al servizio di conservazione. L'infrastruttura tecnologica che ospita il sistema di conservazione, nonché tutti i servizi necessari al suo funzionamento, è fornita direttamente da SIA		

Fanno, inoltre, parte della struttura organizzativa a supporto del Servizio di conservazione:

- **gli Operatori di monitoraggio del servizio** sono responsabili di verificare quotidianamente nell'arco del periodo di erogazione del servizio la funzionalità e l'assenza di criticità;
- **gli Operatori a supporto dell'operatività dei clienti** sono responsabili di assistere gli utenti nelle attività di utilizzo del servizio. Verificano inoltre le operazioni automatiche che gestiscono il processo di conservazione (processi di firma, creazione dei pacchetti di archiviazione, archiviazioni sullo storage). In casi specifici svolgono le attività previste dal processo di conservazione, ad esempio creazione manuale dei pacchetti di archiviazione, quando si è in fase di avvio del servizio per un nuovo Produttore e/o tipologia documentale.
- **strutture di Staff** per la gestione delle forniture, l'amministrazione del personale, la gestione delle comunicazioni con l'esterno, la gestione della documentazione utile all'avvio dei contratti con i clienti.

La struttura organizzativa preposta al servizio di conservazione di SIA è subordinata:

- ai processi sottesi dal servizio di conservazione;
- ai requisiti della normativa e degli standard in merito ai principi di separazione dei ruoli e privilegio minimo;
- ai processi aziendali condivisi.

Lo schema che segue illustra attraverso una matrice RAC (A = Accountable o ultimo responsabile del processo; R = Responsible o responsabile operativo del processo; C = Consulted o coinvolto per competenze specifiche) le responsabilità rispetto al ciclo di vita del servizio di conservazione:

	Pianificazione strategica	Progettazione	Sviluppo / acquisizione	Esercizio
Resp. Servizio di Conservazione	**A**	**A**	**A**	**A**
Resp. Sviluppo e Manutenzione del sist. di Conservazione	R	R* [**attività proprie di gestione dei SI** – componente sw]	R* [**attività proprie di gestione dei SI** - componente sw]	R* [**attività proprie di gestione dei SI** - componente sw]
Resp. Sistemi Informativi per la Conservazione	R	R** [**attività proprie di gestione dei SI** - componenti IT]	R** [**attività proprie di gestione dei SI** - componenti IT]	R** [**attività proprie di gestione dei SI** - componenti IT]
Resp. Funzione Archivistica di Conservazione	R	C	C	R [**attività proprie del serv. di conservazione**]
Resp. Sicurezza dei sistemi di Conservazione	R [verifiche rispetto requisiti sicurezza]	R [verifiche rispetto requisiti sicurezza]	R [verifiche rispetto requisiti sicurezza]	R [verifiche rispetto requisiti sicurezza]
Resp. Trattamento dei dati personali	C	C	C	R [verifiche rispetto requisiti normativi]
Operatori di monitoraggio				R [**attività proprie del serv. di conservazione**]
Operatori e strutture di staff				R [**attività proprie del serv. di conservazione**]

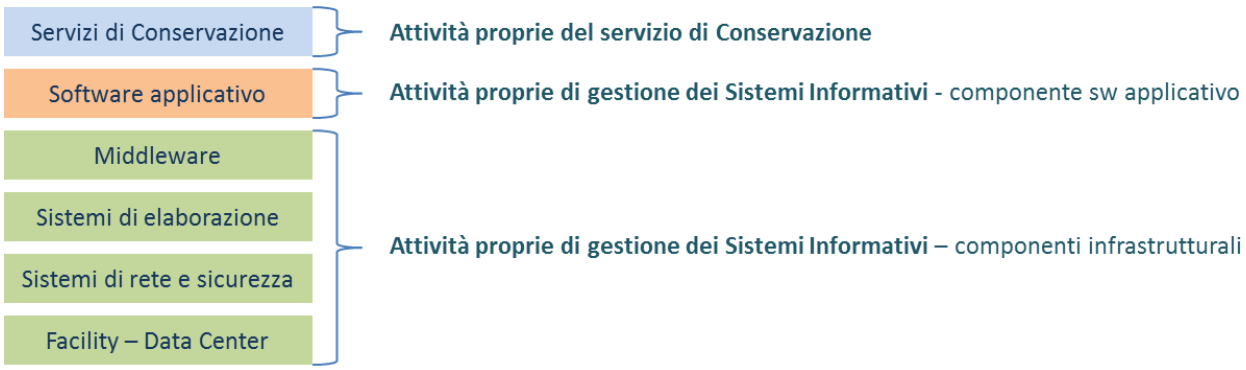
* si avvale delle strutture di sviluppo del Fornitore del software applicativo

** si avvale della struttura IT Management della Direzione Operations di SIA.

Per maggiore chiarezza, lo schema di seguito riportato, illustra la collocazione delle attività richiamate nella matrice RAC:

- **Attività proprie del servizio di conservazione;**
- **Attività proprie di gestione dei Sistemi Informativi** - componente sw applicativo;
- **Attività proprie di gestione dei Sistemi Informativi** - componenti infrastrutturali;

rispetto allo stack rappresentativo di tutti i componenti tecnologici e procedurali del servizio:



Rispetto all'organigramma aziendale di SIA, le figure preposte al servizio di conservazione sono inquadrate come illustrato di seguito:

Direzioni aziendali Ruoli per il Servizio di Conservazione	Dir. Public Sector	Dir. Operations – Service Mgmgt	Dir. Operations – IT Mgmgt	Dir. Risk Governance
Responsabile del servizio di conservazione	**x**			
Responsabile della funzione archivistica di conservazione	**x**			
Responsabile sistemi informativi per la conservazione		**x**		
Responsabile sviluppo e manutenzione del sistema di conservazione	**x**			
Responsabile Sicurezza dei sistemi per la conservazione				**x**
Responsabile trattamento dati personali	**x**			

3.4. Pubblico ufficiale

Il pubblico ufficiale è il notaio, salvo quanto previsto dall'articolo 5, comma 4 della deliberazione CNIPA n° 11 del 2004 e nei casi per i quali possono essere chiamate in causa le altre figure previste dall'articolo 18, comma 2, del Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 e s.m.i.

4. Oggetti sottoposti a conservazione

Gli oggetti sottoposti a conservazione sono documenti informatici, documenti amministrativi informatici e fascicoli informatici, che entrano nel sistema di conservazione sotto forma di pacchetti di versamento, insieme ai metadati che permettono di identificarli all'interno dell'Archivio, di rintracciarne la collocazione e di fornire un riferimento alla struttura di ogni documento, al formato utilizzato e ad altre informazioni utili alla rappresentazione del documento. I metadati permettono inoltre di individuare gli elementi che possono attestare l'integrità e l'autenticità dei documenti versati e vengono rappresentati in coerenza a quanto indicato nell'Allegato 5 alle Regole tecniche.
Ogni documento entrato nel sistema assume un identificativo univoco per tutta la sua permanenza nel sistema.
I pacchetti di versamento vengono elaborati in maniera tale da generare pacchetti di archiviazione aderenti alle specifiche indicate nell'Allegato 4 alle Regole tecniche.
I pacchetti di archiviazione sono conservati in archivi specifici per ogni Produttore e sono suddivisi per gruppi documentali omogenei per natura/modalità di produzione e dal punto di vista giuridico, che vengono definiti Tipologie documentarie.

La gestione delle Tipologie documentarie viene effettuata dal Responsabile della funzione archivistica di conservazione e dai suoi collaboratori, che per ciascuna tipologia documentaria provvedono a definire i metadati standard:

- indici di classificazione della tipologia di documenti;
- parametri di conservazione dei documenti:
    - firma digitale su ciascun documento: i documenti informatici da conservare sono pronti per essere inseriti in pacchetti di archiviazione oppure si necessita di uno step di firma su ciascun documento prima della creazione dei pacchetti di archiviazione;
    - necessità di firma sui pacchetti di archiviazione da parte del responsabile della conservazione o anche di un pubblico ufficiale;
    - periodo di conservazione (Retention Time);
- parametri di servizio per la procedura di trattamento dei documenti:
    - regole per l'estrazione dei documenti dal sistema alimentante per la conservazione;
    - frequenza di estrazione dei documenti dal sistema alimentante;
    - tempistica di conservazione;
    - frequenza delle attività di controllo periodiche;
    - dimensionamento del flusso dei documenti da conservare;
- sistema alimentante e formato dei documenti da conservare:
    - provider del sistema alimentante: esterno o interno;

- formato dei documenti standard (xml, tiff, txt) o proprietario. Nel caso di formato proprietario occorre che vengano compiute le attività di aggiornamento della libreria dei visualizzatori, come descritto in seguito nel paragrafo 5.9 “Misure a garanzia della fruibilità”.

Le principali Tipologie documentarie trattate dal Sistema di conservazione sono descritte nel documento “Tipologie documentarie”, dove per ogni tipologia documentaria vengono indentificati i metadati standard. I metadati specifici relativi ad ogni Produttore sono definiti all’interno del documento ”Specificità del contratto”.

Tutti i formati gestiti sono coerenti con il punto 5 dell’Allegato 2 alle Regole Tecniche e sono elencati e descritti in un registro interno al sistema di conservazione.
I formati gestiti dal sistema d per la conservazione di specifiche tipologie documentarie sono concordati con il Produttore ed esplicitati anch’essi all’interno degli accordi contrattuali, che definiscono anche le eventuali modalità di aggiornamento concordato dei formati gestiti.

I principali formati previsti per i documenti sono:

- XML;
- PDF firmato digitalmente (in base alla tipologia documentaria);
- PDF non firmato digitalmente (in base alla tipologia documentaria);
- TIF firmato digitalmente (documenti che arrivano in formato cartaceo dal Produttore);
- altri formati immagine, come specificato dai singoli accordi contrattuali.

Per tutta la durata della conservazione, i pacchetti di archiviazione possono essere restituiti agli Utenti su loro richiesta, nel formato di pacchetto di distribuzione. Il pacchetto di distribuzione si presenta in una forma idonea alle specifiche esigenze di utilizzo delle tipologie documentarie conservate e delle evidenze informatiche generate dal sistema nel corso del processo di conservazione.

5. Processo di conservazione

Il **processo di conservazione** dei documenti ha come **input** i documenti da conservare, forniti sotto forma di pacchetti di versamento da un sistema alimentante, e produce come **risultato**:

- la conservazione degli stessi documenti all'interno dell'archivio sotto forma di pacchetti di archiviazione;
- i rapporti di versamento dotati di riferimento temporale, che ne attestano la corretta presa in carico da parte del sistema di conservazione.

Gli **attori** coinvolti nel processo sono i seguenti:

- l'operatore dell'Ente Produttore delegato al trattamento dei documenti informatici o gli utenti caricatori e firmatari del Produttore per l'emissione dei documenti;
- un eventuale intermediario quale, per esempio, la banca tesoreria dell'Ente nel caso degli ordinativi di pagamento;
- SIA in quanto responsabile della conservazione per le attività delegate dal Produttore;
- gli utenti dell'Ente abilitati alla consultazione dell'archivio.

Le principali attività del processo di conservazione sono:

- creare i gruppi di caricamento, ove richiesto, generando le relative distinte;
- caricare i gruppi di caricamento o singoli documenti sul sistema;
- creare i pacchetti di archiviazione e apporre agli stessi firma digitale e marca temporale;
- effettuare le attività di gestione per la conservazione di lungo termine; le attività sono svolte dal sistema di storage in background, che controlla in modo continuo la disponibilità e l'integrità dei pacchetti conservati;
- consultare l'archivio, esibire i documenti e gestire lo scarto.

Le **procedure interne** utilizzate fanno riferimento ai processi e sistemi di gestione descritti nel documento "Company management system SIA – Processi e sistemi di gestione".

5.1. Attività preliminari di configurazione del processo di conservazione

Gestione delle tipologie di documenti

Per permettere le attività di conservazione, **vengono preventivamente gestite le tipologie di documenti**, con l'obiettivo di determinare le regole e i parametri che caratterizzano il processo di conservazione per ciascuna tipologia documentaria. L'attività è eseguita dal responsabile della funzione archivistica di conservazione. Il risultato di tale attività consiste nella definizione di:
indici di classificazione della tipologia di documenti;

- parametri di conservazione dei documenti, quali presenza di firma digitale su ciascun documento, periodo di conservazione (Retention Time), etc.;
- parametri di servizio per la procedura di trattamento dei documenti:
  - tempistica di conservazione;
  - frequenza delle attività di controllo periodiche;
  - dimensionamento dei documenti da conservare;
- sistema alimentante e formato dei documenti da conservare:
  - caricamento singolo tramite funzione on-line;
  - formato dei documenti standard.

Gestione degli attori coinvolti, ruoli e responsabilità

L'attività ha lo scopo di individuare gli attori coinvolti nel processo di conservazione di una determinata tipologia documentaria in relazione al singolo Produttore (associazione Produttore-Tipologia documentaria), al fine di definire i diversi ruoli e responsabilità che li caratterizzano.
Il risultato di tale attività consiste nel definire per ogni tipologia documentaria:

- l'Ente Produttore dei documenti da archiviare;
- gli altri Utenti che devono poter usufruire in consultazione dei documenti conservati;
- gli Operatori del Produttore coinvolti nel processo di caricamento dei documenti o dei gruppi di documenti destinati alla conservazione;
- eventuali soggetti delegati ad apporre la firma digitale sui pacchetti di archiviazione;
- il periodo temporale di validità delle deleghe emanate e di conseguenza il periodo in cui è possibile ai delegati firmare digitalmente i pacchetti di archiviazione. Queste informazioni, gestite dal sistema informatico a supporto della conservazione, permettono di monitorare la validità delle deleghe attive e di impedire l'operatività ad utenti con deleghe scadute, consentendo così una corretta gestione delle responsabilità e dei controlli sul firmatario dei pacchetti di archiviazione;
- l'eventuale pubblico ufficiale da coinvolgere per la conservazione dei documenti analogici originali unici.

L'attività è eseguita dal responsabile della funzione archivistica di conservazione o da suoi delegati.

5.2. Acquisizione del pacchetto di versamento

L'attività di versamento è costituita dalle seguenti operazioni:

- produzione da parte dell'Ente dei documenti nei tempi previsti dalla legge;
- eventuale predisposizione dei gruppi di caricamento composti da file .zip contenenti tutti i documenti da conservare all'interno del range di date che caratterizzano l'estrazione,

avente nome file univoco e identificativo del file stesso e una distinta in formato xml che riporta i metadati caratteristici di ciascun documento;

- caricamento singolo o massivo dei documenti attraverso:
  - apposita funzione on-line nell'applicativo ad opera degli Operatori del Produttore aventi le autorizzazioni per l'accesso e caricamento dei documenti;
  - apposita interfaccia applicativa ad opera del sistema alimentante del Produttore secondo i parametri di servizio concordati nelle attività precedenti.

Per quanto riguarda le modalità di ricezione del pacchetto di versamento da parte del Produttore, sono gestite le seguenti casistiche:

- caricamento del pacchetto di versamento da parte del Produttore mediante upload di file attraverso connessione internet su canale criptato (https);
- caricamento del pacchetto di versamento mediante interfacce applicative di tipo web service attraverso connessione internet su canale criptato (https).

Altre modalità di ricezione dei pacchetti di versamento potranno essere previste e saranno regolamentate nelle specificità del contratto.

5.3. Verifiche sul pacchetto di versamento

Verifiche relative all'Ente Produttore

Ogni versamento da parte del Produttore deve contenere pacchetti omogenei per tipologia documentale ed Ente Produttore.

La verifica relativa all'identificazione dell'Ente Produttore è eseguita mediante il controllo delle credenziali di accesso dell'utente (Postazione, Azienda, Utente), incrociando le stesse con le informazioni relative al codice tipologia documentale e al codice Azienda contenute all'interno del pacchetto di versamento e alla configurazione preventivamente eseguita in sede di avviamento del servizio.

Se tali verifiche portassero a una incongruenza tra questi elementi, allora il pacchetto di versamento verrebbe rifiutato.

In tal modo ci si cautela rispetto a eventuali errori di provenienza dei documenti.

Verifiche in fase di versamento dei formati dei documenti

Il servizio prevede di gestire i formati previsti dalla normativa vigente.

All'atto del caricamento di un pacchetto di versamento viene controllato il formato di ciascun file versato. Tale controllo viene svolto in automatico dal sistema attraverso l'attributo specifico del file che ne indica il formato (*magic number*).

Se il formato del file non dovesse essere contemplato tra quelli previsti dall'allegato 2 del DPCM 3 dicembre 2013, il pacchetto di versamento verrebbe rifiutato.

Verifiche in fase di versamento dei metadati minimi

Il sistema prevede che in fase di acquisizione del pacchetto di versamento venga verificata la

presenza dei metadati obbligatori specifici della tipologia documentale.
In particolare la verifica dei metadati minimi previsti dall'allegato 5 del DPCM 3 dicembre 2013 viene operata combinando i metadati del documento con quelli relativi all'anagrafica dell'Ente Produttore.

Verifiche in fase di versamento della firma del documento

Nel caso in cui il pacchetto di versamento contenga documenti firmati digitalmente dal Produttore si prevede di verificare:

- l'integrità del documento;
- la validità del certificato;
- l'algoritmo di firma utilizzato;
- la lista di revoca;
- l'attendibilità della CA.

Il paragrafo successivo riporta la descrizione delle possibili procedure che possono essere previste in funzione della specificità del contratto in caso di certificato scaduto o non valido. Per tutte le altre verifiche della firma se queste fossero negative, il pacchetto verrebbe rifiutato.

Verifiche in fase di versamento di documenti singoli

Sul singolo documento è verificata la presenza dei metadati obbligatori previsti per la tipologia documentale e la presenza o meno della firma digitale: se la firma è presente, si opera la verifica della firma.

Verifiche in fase di versamento dei gruppi di caricamento

Nel caso di caricamento massivo, per ogni gruppo di caricamento le operazioni di verifica svolte dal sistema di conservazione sono le seguenti:

- controllare la correttezza semantica della distinta, la conformità allo schema definito e la completezza dei documenti rispetto al numero di documenti indicato in distinta;
- verificare la firma dei documenti firmati digitalmente.

5.4. Rifiuto del pacchetto di versamento

Il rifiuto del pacchetto di versamento avviene quando il pacchetto risulta non conforme alle specifiche per:

- elenco file e distinta non coerenti;
- distinta o metadati del documento non corretti;

oppure quando un documento contenuto nel pacchetto non supera una delle verifiche descritte nel paragrafo precedente (verifica dell'Ente produttore, verifica del formato, verifica della firma).
In caso di rifiuto, il Sistema restituisce al Produttore l'elenco degli errori riscontrati e le relative

causali.

La modalità con cui si restituisce al Produttore il messaggio di rifiuto del pacchetto di versamento, dipende dalla modalità di caricamento dello stesso:

- in caso di caricamento del pacchetto di versamento mediante interfaccia utente via browser, il messaggio di rifiuto appare a video contendo tutte le informazioni di cui sopra;
- in caso di caricamento mediante interfaccia applicativa con un sistema informativo alimentante, il messaggio di rifiuto viene trasmesso in risposta alla chiamata di tipo web service che di caricamento documento o di richiesta rapporto di versamento.

Il messaggio di rifiuto non viene sottoposto a conservazione digitale, ma tutte le informazioni di tracciatura dell'operazione sono registrate nei log di sistema, corredati dal riferimento temporale per ciascuna di esse. Il log di sistema viene conservato.

Di seguito, si descrive la procedura in caso di pacchetti di versamento aventi certificato scaduto. Il sistema di default non accetta i documenti che hanno una firma con certificato scaduto al momento del caricamento; pertanto al verificarsi della condizione, il documento viene scartato.
Previo accordo con il Produttore è possibile però procedere all'accettazione del documento secondo due modalità distinte. Se è attiva la gestione dei documenti scaduti, il documento, invece di essere scartato, è caricato e posto in un uno stato particolare, definito "In attesa di seconda firma". Con una apposita utenza (detta "Firmatario documenti scaduti"), che viene rilasciata a chi, lato Produttore, è abilitato per tale compito, è possibile scegliere come il documento proseguirà il suo processo verso la conservazione. Le possibili scelte sono due:

- **apporre una seconda firma:** in questo caso la firma con certificato scaduto viene inglobata in una nuova busta con firma valida. Chi appone la seconda firma garantisce che la firma originaria era stata apposta quando il certificato era valido;
- **accettare che il documento sia conservato ugualmente:** in questo caso il documento prosegue nel suo percorso senza modifiche. Questo è possibile quando ci sono delle condizioni che consentono di validare la firma presente; è il caso ad esempio di un documento protocollato da una Pubblica Amministrazione, per cui la data del protocollo è riconosciuta valida al pari di una marcatura temporale.

5.5. Presa in carico e generazione del rapporto di versamento

Nel caso in cui le verifiche di caricamento singolo o massivo siano andate a buon fine, il sistema provvede a memorizzare ed indicizzare i documenti e a produrre un Rapporto di versamento.

Il Rapporto di versamento è costituito da un identificativo univoco, dalla distinta di versamento e dal riferimento temporale del versamento e contiene le impronte (*hash*) di ciascun documento.

Il Rapporto di versamento resta a disposizione archiviato sul sistema, fino a che tutti i documenti presenti nel rapporto hanno concluso il processo di *ingest* (rif. OAIS). Il Rapporto di versamento

non viene conservato, ma sono mantenuti a norma e per tutto il periodo di conservazione tutti i log delle attività relative al versamento.

La restituzione delle impronte permette la verifica da parte del Produttore della corrispondenza del documento preso in carico con quello inviato.

Il Rapporto di versamento costituisce il documento di controllo e di presa di responsabilità del Responsabile della conservazione verso il Produttore, in quanto viene garantita la conservazione di tutti e soli i documenti per i quali viene emesso il Rapporto di versamento.

In particolare, dal punto di vista organizzativo, laddove sia prevista un'integrazione applicativa tra il sistema documentale alimentante e il sistema di conservazione, la responsabilità di assicurarsi della corretta presa in carico di tutti i documenti da parte del sistema di conservazione è in carico al Produttore, attraverso il sistema documentale, che deve provvedere ad aggiornare sui propri archivi il buon esito del caricamento in conservazione e consentire di individuare eventuali incompletezze o anomalie nel processo di conservazione.

5.6. Creazione del pacchetto di archiviazione

Conclusa la fase della presa in carico del pacchetto di versamento viene generato il pacchetto di archiviazione. Ogni pacchetto di archiviazione è univocamente identificato all'interno del sistema.

La cadenza con cui vengono creati i pacchetti di archiviazione è stabilita in sede contrattuale con il produttore dei documenti. Il lotto di documenti appartenenti ad un pacchetto di archiviazione è sempre omogeneo per tipologia di documenti contenuti al suo interno.

I pacchetti di archiviazione vengono raggruppati automaticamente in base ai parametri definiti nel sistema, generando l'**indice del pacchetto**, che contiene le impronte di tutti i documenti indicizzati e le altre informazioni definite nell'Allegato 4 alle Regole Tecniche.

L'indice viene firmato digitalmente dal Responsabile della funzione archivistica di conservazione o da suoi delegati. L'indice inoltre viene marcato temporalmente. Ogni indice è univocamente identificato all'interno del sistema.

Per quanto riguarda la descrizione delle procedure di ripristino in caso di corruzione o perdita dei dati si rimanda al paragrafo 6.4.3 "Verifica dell'integrità degli archivi".

In generale il processo di conservazione non prevede l'utilizzo della crittografia degli oggetti conservati, in quanto

- deve assicurare la conservazione a lungo termine del documento digitale e di conseguenza la piena disponibilità nei confronti non solo dell'ente produttore, ma di tutta la comunità di riferimento (previa verifica dell'autorizzazione all'accesso ai documenti);
- non deve in alcun modo alterare il documento inviato in conservazione utilizzando tecniche crittografiche proprie.

Durante la fase di creazione dei pacchetti di archiviazione vengono prodotti i log di sistema registrando tutte le operazioni eseguite (cfr. cap. 6.4.4).

5.7. Gestione dei pacchetti di archiviazione

Per quanto riguarda la gestione dello **scarto**, tale attività viene gestita sul sistema dal Responsabile della funzione archivistica o suoi delegati secondo la seguente procedura:

- con cadenza annuale (o diversamente definito per Tipologia documentale) si procede all'estrazione della lista dei documenti scaduti; per documenti scaduti si intendono quelli per cui la data di conservazione è antecedente di un periodo maggiore del Retention Time del tipo documento a cui appartengono;
- la lista prodotta viene sottoposta all'attenzione del Produttore, che ha il compito di segnalare eventuali documenti aventi procedimenti pendenti e per i quali si rende necessaria la conservazione oltre il periodo di conservazione standard;
- il Responsabile della funzione archivistica di conservazione o suo delegato procede a modificare sul sistema di conservazione il tempo di conservazione prolungandone la durata;
- la lista emendata da tali eccezioni viene firmata dal Responsabile della conservazione e dal Produttore e archiviata come lista di scarto;
- i documenti oggetto della lista di scarto vengono eliminati dal sistema.

Per i documenti che necessitano di un periodo di conservazione superiore ai 20 anni, si prevedono le seguenti attività di mantenimento dell'archivio, sotto la responsabilità del Responsabile della funzione archivistica di conservazione:

- Monitoraggio e **aggiornamento delle scadenze delle Marche temporali**: poiché le Marche temporali apposte dal processo di conservazione hanno validità di 20 anni, occorre monitorare la scadenza delle marche apposte sui pacchetti di archiviazione e apporre nuove marche a quelle in scadenza;
- Monitoraggio e **aggiornamento delle scadenze del Retention Time** (ove si necessiti di conservazione perenne): la scadenza del Retention Time dei documenti con conservazione perenne è fissato a 10 anni dal momento della conservazione e per tali Tipologie documentarie va ampliata prima di tale limite. Il Retention Time è il parametro entro il quale il supporto di memorizzazione rende incancellabili i documenti in esso conservati.

L'attività di **monitoraggio applicativo** sui pacchetti di archiviazione prevede il controllo su di un apposito cruscotto che evidenzia il numero di documenti in attesa di elaborazione. L'evidenza di una coda di documenti non ancora attribuiti a pacchetti di archiviazione innesca la verifica

dell'operatore, che può analizzarli in dettaglio, arrivando ad evidenziare quali documenti, di quale tipologia e Produttore non sono stati correttamente processati. Verificato il problema, l'operatore può intervenire manualmente, sbloccando gli automatismi o ripristinandoli.

La stessa logica di intervento si applica per la firma e la marcatura temporale dei pacchetti di archiviazione.

Il Sistema prevede la possibilità di **modificare il documento già conservato**, in due modalità:

- Modifica del solo documento: i metadati rimangono invariati, il documento viene versionato; il sistema permette attraverso dei link di risalire a tutte le versioni precedenti al documento finale;
- Modifica dei metadati (ed eventualmente anche del documento): il Produttore, oltre a versare il nuovo pacchetto, ha la possibilità di aggiungere in una pagina di annotazione il collegamento tra nuovo e vecchio documento, specificando la motivazione dell'aggiornamento.

5.8. Generazione del pacchetto di distribuzione e modalità di esibizione

I documenti sono ricercabili tramite opportune funzioni di ricerca messe a disposizione dall'applicazione di conservazione che permettono di valorizzare, quale criterio per la ricerca, ciascuno dei metadati caratteristici del documento.

L'accesso al sistema in modalità di consultazione è garantito agli Utenti opportunamente autorizzati, limitatamente agli archivi del Produttore di appartenenza e in base agli accordi contrattuali con esso intercorsi.

È quindi disponibile al conservatore e all'utente la funzionalità di esportazione di pacchetti e relativi indici, attraverso la quale è possibile scaricare un file .zip contenente il file indice dei pacchetti, i documenti conservati e le evidenze della conservazione (firme e marche temporali). Inoltre sono disponibili le interfacce applicative per poter operare l'estrazione dei documenti tramite applicazione esterna.

5.9. Misure a garanzia della fruibilità

Per garantire la fruibilità nel tempo dei documenti conservati, il sistema di conservazione prevede la gestione di una libreria di visualizzatori associata alle tipologie documentarie e ai singoli documenti; in questo modo viene mantenuto un repository comune atto a rendere fruibili, finché possibile, tutti i documenti conservati, senza dover ricorrere a operazioni di riversamento sostitutivo (vedi più avanti al paragrafo 5.11).

Ciò viene realizzato tramite:

- la predisposizione di aree apposite in cui vengono depositati i programmi di installazione dei visualizzatori necessari per poter leggere i file dei documenti informatici conservati con un formato proprietario;
- l'alimentazione dell'anagrafica dei visualizzatori sul sistema di conservazione, qualificando ciascun elemento con il nome e l'indirizzo del programma di installazione depositato, e i requisiti hardware e software necessari per la sua esecuzione;
- l'associazione tra visualizzatore e tipologia documentaria.

5.10. Interoperabilità

Il sistema di conservazione è in grado di accettare il versamento di pacchetti strutturati secondo lo standard UNI 11386:2010, in accordo con quanto definito nell'Allegato 4 delle Regole tecniche. Allo stesso modo, il sistema è in grado di versare ad altri sistemi di conservazione pacchetti e indici secondo la medesima struttura, trasformando i pacchetti di archiviazione in opportuni pacchetti di distribuzione.

5.11. Generazione di copie e duplicati

Riversamento diretto

Per **riversamento diretto** si intende il processo che trasferisce uno o più documenti conservati da un supporto di memorizzazione ad un altro, non alterando la loro rappresentazione informatica. Su richiesta degli utenti è possibile produrre delle estrazioni di documenti dall'archivio dell'Ente di appartenenza da riversare su altro supporto. La memorizzazione su altro supporto è a carico dell'utente che ha estratto i documenti.

Riversamento sostitutivo

Per **riversamento sostitutivo** si intende il processo che trasferisce uno o più documenti conservati da un supporto di memorizzazione ad un altro, modificando la loro rappresentazione informatica. Questa particolare operazione attiene al problema della **leggibilità e** dell' **esibizione dei documenti nel tempo**. In particolare, laddove si voglia cambiare il formato di un documento conservato per far fronte a problematiche di obsolescenza tecnologica delle applicazioni di visualizzazione dei documenti, è possibile ricorrere al riversamento sostitutivo di un documento creando un nuovo documento in altro formato e versandolo nel sistema con le stesse modalità previste per il documento originario. Tale operazione richiede un intervento del Responsabile della funzione archivistica di conservazione, che al termine del riversamento deve apporre la propria firma all'insieme dei documenti riversati (lotto di riversamento) in modo analogo a quanto previsto per la conservazione. Il nuovo documento mantiene i riferimenti al documento originario.

In funzione del grado di omogeneità dei formati della tipologia documentaria, della criticità rappresentata dalla gestione del formato da sostituire, degli strumenti a disposizione per poter trasformare i documenti conservati e della numerosità degli stessi, si decide per quali documenti e verso quale formato occorre procedere al riversamento sostitutivo. Il sistema applicativo mette a disposizione le funzionalità necessarie per operare il riversamento sostitutivo di un documento o di un insieme di documenti.

Possono essere abilitati al riversamento sostitutivo gli utenti già abilitati alla conservazione dei documenti.

In particolare è possibile operare un riversamento singolo, che ha lo scopo di sostituire uno specifico documento, selezionando il documento in oggetto, marcandolo come "da riversare" e caricando un nuovo documento che eredita tutti i metadati del precedente. Il nuovo pacchetto sarà costituito da un solo documento e l'indice sarà attinente solo a quello specifico documento.

In alternativa, è possibile operare un riversamento massivo selezionando sul sistema di conservazione i documenti da riversare e scaricando la distinta contenente i metadati dei documenti selezionati. In tal modo sarà possibile caricare un gruppo di documenti riferito a tale distinta utilizzando le funzioni di caricamento massivo previste dal sistema. Il workflow di riversamento continua analogamente al workflow di conservazione secondo gli step configurati per la specifica tipologia documentaria.

5.12. Cessazione del servizio

In caso di cessazione del servizio verso un Produttore, per naturale scadenza della durata del contratto o nei casi di risoluzione o recesso per qualsivoglia motivo occorso:

- cessa di avere efficacia la nomina di SIA a Responsabile della conservazione;
- SIA provvede a riconsegnare al Produttore i documenti conservati presso i propri archivi, completi dei pacchetti di archiviazione, e a redigere un apposito verbale di consegna che verrà sottoscritto per accettazione dal Produttore;
- SIA si impegna a non comunicare e/o diffondere e/o comunque utilizzare ulteriormente i documenti oggetto del verbale di consegna, ovvero a conservare copia degli stessi, salva la possibilità prevista di produzione e consegna di supporti informatici;
- SIA si impegna a distruggere i documenti oggetto del verbale di consegna dai propri supporti.

La procedura con cui il Produttore può richiedere la produzione e la consegna dei supporti informatici contenenti tutti i documenti trasmessi a SIA nell'ambito del Servizio ai fini della Conservazione digitale è attuabile esclusivamente durante il periodo in cui il Servizio è regolarmente erogato e di norma con almeno 30 giorni di anticipo rispetto all'eventuale data di

cessazione del Servizio determinata in caso di disdetta o nei casi di Risoluzione o Recesso per qualsivoglia motivo occorso. All'atto della consegna il Produttore rilascia specifica ricevuta, sottoscrivendo la copia dell'elenco dei documenti (verbale di consegna), che rimane a SIA. Entro 15 giorni lavorativi successivi alla consegna del materiale il Produttore deve procedere a verificare la leggibilità del contenuto dei supporti: tutte le contestazioni direttamente/indirettamente connesse alla verificabilità dei contenuti dei supporti che non siano state effettuate formalmente nel termine di 15 giorni dalla consegna non potranno essere più formulate dal Produttore. In ogni caso, decorso il termine di cui sopra senza che il Produttore abbia svolto alcuna attività, tutto il materiale consegnato e di cui all'elenco trasmesso si intende da lui accettato senza riserve. Per tutto il periodo fino allo scadere del termine per le verifiche SIA trattiene una copia di tutto quanto consegnato al Produttore. Soltanto allo scadere del termine dei 15 giorni e nell'eventualità di cessazione del Servizio, avviene l'eliminazione della copia fino a quel momento trattenuta da SIA.

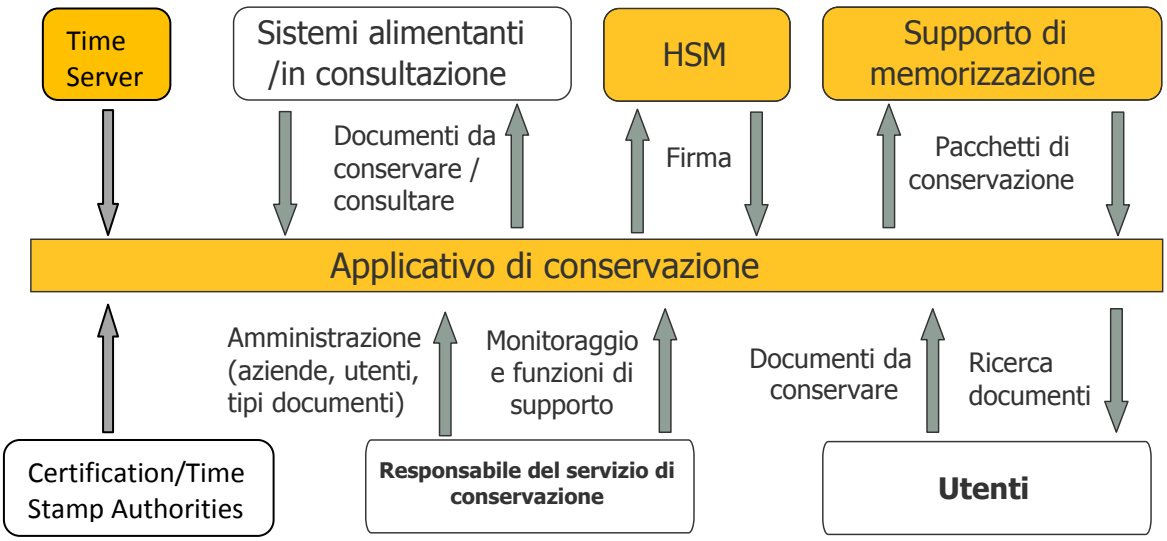
6. Descrizione del Sistema di conservazione

6.1. Componenti Logiche

Il Sistema di conservazione si basa sulle seguenti tre macro componenti:

- la componente applicativa che rende disponibile l'insieme delle componenti funzionali a supporto del processo di conservazione;
- il supporto di memorizzazione, che rappresenta il sistema fisico su cui vengono conservati nel tempo i documenti sottoposti al processo di conservazione;
- il dispositivo HSM per la gestione della procedura di firma dei documenti.

La figura seguente evidenzia le componenti che costituiscono la soluzione.



Nello specifico, l'applicativo di conservazione interagisce con varie tipologie di attori esterni:

- *Sistemi alimentanti/in consultazione* in grado di:
  - alimentare automaticamente il sistema di conservazione con documenti da sottoporre al processo di conservazione;
  - consultare documenti preventivamente sottoposti a conservazione;
- *Dispositivo HSM* per la firma dei documenti;
- *Sistema di memorizzazione*, che rappresenta il sottosistema su cui vengono fisicamente memorizzati tutti i documenti sottoposti a processo di conservazione;
- *Responsabile della conservazione*, per le attività di amministrazione, monitoraggio e altre funzioni di supporto
- *Utenti* che accedono al sistema di conservazione in forza di una credenziale di accesso e di un ruolo e quindi un profilo funzionale a cui sono associati, per effettuare:

  - versamento di singoli documenti;
  - consultazione di documenti conservati.
- Sistemi delle Certification/Time Stamp Authorities per:
  - verifica dei certificati e delle CRL
  - apposizione dei Time Stamp
- Time Server per l'apposizione del riferimento temporale ove non sia necessario un Time Stamp

L'applicazione viene erogata in logica ASP dalle infrastrutture tecnologiche specificatamente predisposte.

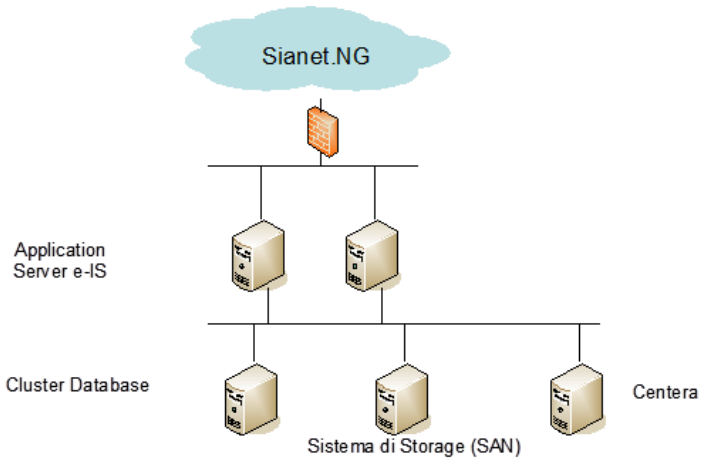
Tutti i componenti del Sistema sono protetti da adeguate misure di sicurezza, descritte all'interno del Piano di Sicurezza.
È mantenuta la separazione degli ambienti di sviluppo, di test e di produzione.

6.2. Componenti Fisiche

L'architettura del Sistema presenta una piattaforma con "no-single-point-of-failure" che è altamente scalabile ed implementa un servizio senza interruzioni, in quanto fondato sull'utilizzo di diversi nodi cooperanti e garantisce performance ottimali utilizzando meccanismi di load balancing tra i diversi nodi. Inoltre la continuità del servizio è garantita dalla presenza di un sito secondario con logiche di disaster recovery.

Il Sistema presenta un'architettura a tre livelli:

1. livello di presentazione (IS-Web Server)
2. livello di logica applicativa (Application Server)
3. livello dati (Database, Storage e Centera)



Schema del sito primario

Le componenti di **Web Server** e **Application Server** sono ospitate su due distinti HP Integrity Superdome (SD 64) che consentono di configurare Cluster di due o più partizioni, all'interno di un singolo Superdome.

La **componente dati** è realizzata su due nodi Superdome in cluster. La gestione dei dati (database RDBMS e dati applicativi) su tutte le componenti previste per l'infrastruttura utilizza una "storage area network"- SAN- che ospita i dischi dove sono memorizzati i dati del servizio con un sistema ridondato in fibra ottica e una SAN consolidata che permette una definizione di concetti di zoning, una connessione dei server di produzione in modalità dual path e un'alta affidabilità in condizioni di path failure. Il Sottosistema di Storage utilizzato è completamente in Fibre Channel e dual controller.

La **componente di gestione documentale,** per mezzo della quale vengono erogate tutte le funzionalità applicative inerenti la gestione dei documenti correlati ai processi di Business della piattaforma, è realizzata da un apposito strato applicativo che si appoggia a una SAN disponibile nell'infrastruttura e alla componente tecnologica Centera di EMC2 per la memorizzazione dei documenti sottoposti a conservazione. Centera viene integrato per mezzo di una specifica interfaccia che fa uso di API proprietarie del Sistema.

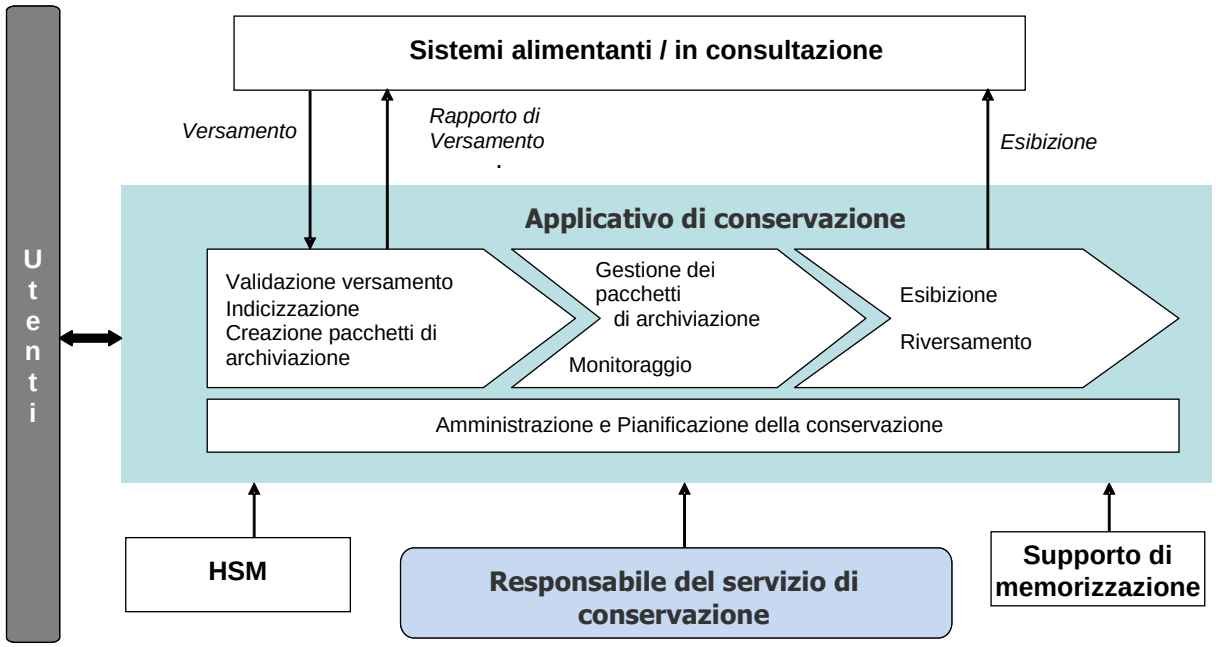
L'**interconnessione adottata tra i sistemi applicativi e il sottosistema di Storage** è realizzata attraverso la SAN con dispositivi di commutazione ottica e mezzo trasmissivo basato interamente su tratte in fibra ottica.

La **connettività** tra i dispositivi di switching ottici, lo Storage e i server è assicurata in alta affidabilità tramite doppio link .

Il **backup** è centralizzato su un'unica libreria di backup attraverso un numero opportuno di switch (dipendente dal numero di server connessi e dal numero di drives della libreria), e può essere effettuato via Fibre channel dai sistemi collegati alla SAN e via rete da tutti gli altri sistemi. L'infrastruttura utilizzata per effettuare i backup si appoggia su apparecchiature centralizzate e ridondate su entrambe le sedi e su un terzo sito distinto per l'archiviazione e la ritenzione storica.

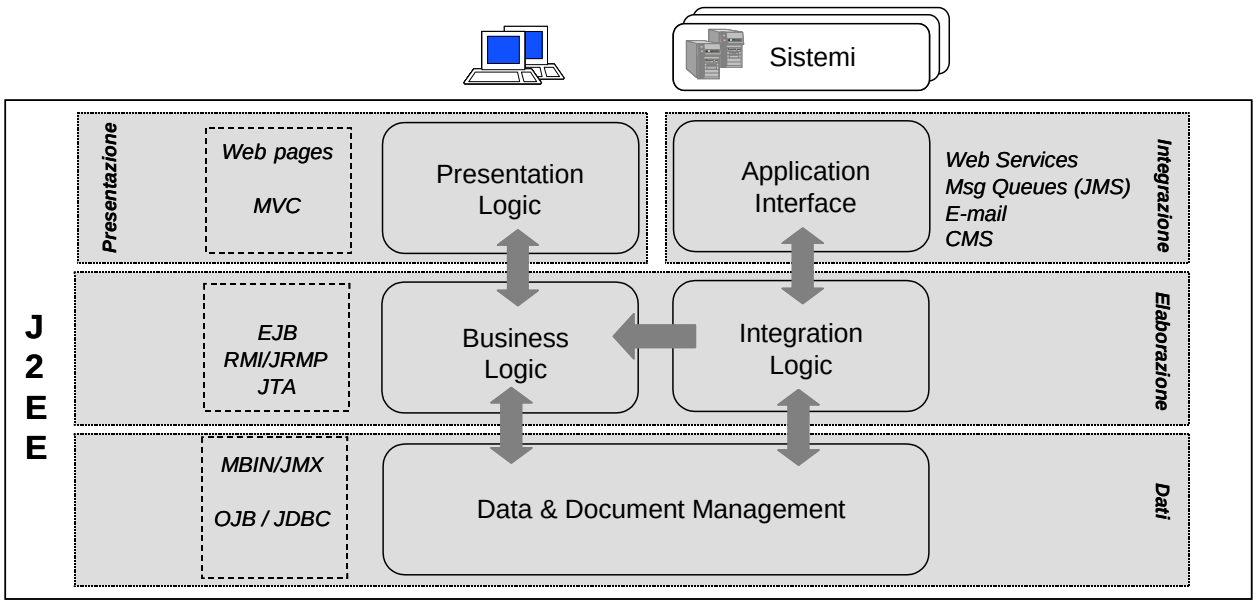
6.3. Componenti Tecnologiche

Lo schema seguente rappresenta il modello tecnologico della soluzione complessiva proposta.



Da un punto di vista applicativo, la soluzione è basata su prodotti software di mercato e open source quali Jboss, Tomcat e Apache. Fa uso di DBMS basato su Oracle e può essere ospitata indifferentemente su sistemi basati su piattaforme Linux, Windows o altre in grado di ospitare i software sopra citati.

L'applicativo di conservazione è sviluppato interamente con **tecnologia J2EE**, secondo lo schema rappresentato nella figura seguente.



Il livello "**presentazione**" segue il paradigma MVC:

- il layer "model", che implementa le logiche di navigazione e validazione dei dati e gestisce l'interfacciamento con la business logic, è realizzato con classi java;

- il layer “view” utilizza il linguaggio di templating Velocity ed è costituito da un insieme di template che consentono di modellare diversi tipi di rappresentazione dei dati in uscita: HTML, XML, PDF;
- il layer “control” è realizzato tramite la servlet Turbine che si incarica della gestione di vari moduli del layer model e della generazione dei flussi di output a partire dai template definiti.

Il livello “**integrazione**” si incarica di esporre le interfaccia della piattaforma verso l’esterno e realizza quindi la “application interface”. Sono previste interfacce basate su web services, su https (streams). Tutte le interfacce della piattaforma sono realizzate seguendo pienamente gli standard WSDL, SOAP e MIME per i web services, e fanno uso di schemi XSD per lo scambio di dati con sistemi esterni.

Il livello di “**elaborazione**” è suddiviso in due componenti logiche: la “business logic”, che sviluppa le funzioni applicative, la “integration logic” che si incarica di realizzare le logiche di l’integrazione della piattaforma con i sistemi esterni.
Il livello di elaborazione è realizzato utilizzando la tecnologia degli EJB. Sono utilizzati due tipologie di EJB:

- “session EJB” per i servizi sincroni;
- “message driver beans” per i servizi asincroni.

La comunicazione tra gli EJBs è realizzata tramite RMI su protocollo JRMP.
L’integrità e la consistenza delle transazioni applicative è garantita attraverso l’impiego dell’architettura JTA “Java Transaction API” che permette di gestire anche transazioni distribuite sui dati e verso applicazioni esterne integrate con il sistema.
La soluzione descritta permette di soddisfare requisiti di **scalabilità** e **affidabilità**:

- la **scalabilità** è garantita dalla possibilità di attivare nuove istanze applicative nell’ambito dello stesso hardware fornito o, se necessario, aggiungendo sistemi HW e le relative nuove istanze applicative;
- l’**affidabilità** e la relativa assenza di punti di failure viene garantita dalla possibilità di configurazione in cluster delle istanze applicative, attuata per mezzo di meccanismi nativi offerti dall’application server Jboss.

L’accesso al data base avviene attraverso il livello denominato “**dati**” e utilizzando un paradigma ad oggetti. La mappatura tra DB relazionale e gli oggetti del sistema è realizzata tramite OJB “Object relational bridge”. Il layer di gestione dei dati espone un’interfaccia JMX, realizzata attraverso oggetti MBeans (Managed Beans), verso il layer di elaborazione.

Il Sistema **memorizza due copie fisiche** (mirroring) di ogni data object su due nodi differenti e indipendenti: in caso di device fault il Sistema è in grado di **rigenerare automaticamente gli oggetti mancanti**. Il Sistema verifica, inoltre, continuamente l’**integrità** dei contenuti e l’**autenticità** dei contenuti per prevenire corruzione di dati. Nel caso di corruzione ricostruisce il

dato attraverso la copia del mirror.

Nel livello dati, la componente di gestione documentale Centera utilizza un nuovo paradigma nell'accesso ai dati conosciuto come "Content Addressing": invece dell'approccio classico basato sulla posizione del dato, presenta al programma di archiviazione uno schema di indirizzamento "flat". Quando un oggetto viene memorizzato per la prima volta, l'applicazione riceve una "ricevuta" (o "claim check") che è derivata univocamente dal contenuto dell'oggetto stesso.

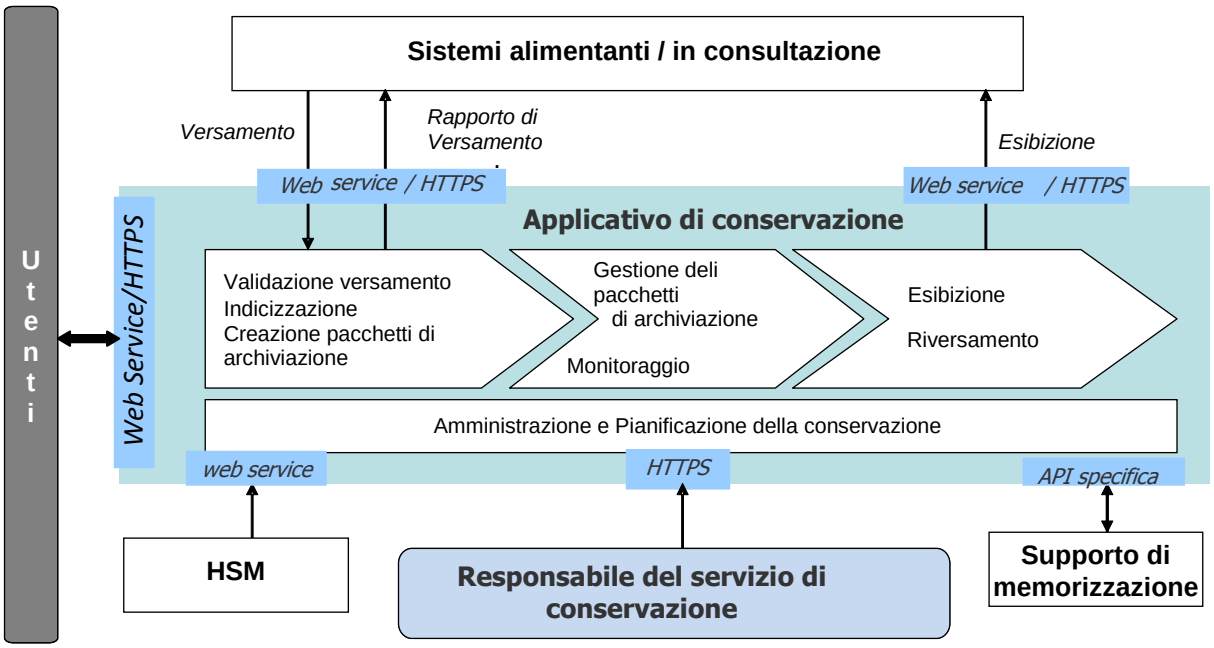
Accessi successivi ai dati vengono compiuti restituendo al repository la "ricevuta", che identifica univocamente l'oggetto.

Tale Sistema di archiviazione consente:

- **Autenticazione del Contenuto**: qualsiasi oggetto presentato al sistema è memorizzato in modo tale da essere immodificabile ed autenticato, cosa che è trasparente all' applicazione utente;
- **Non-cancellazione**: Data objects non possono essere cancellati prima che sia concluso il loro retention period;
- **Replica Efficiente**: usa un indirizzo univoco derivato dal contenuto per assicurare che solo una copia del contenuto è memorizzata. Questo aspetto può ridurre in maniera significativa il quantitativo di informazioni memorizzate;
- **Facilità di gestione**: la tecnologia semplifica enormemente il system planning e la gestione di centinaia di Terabytes di contenuti. Non vi sono tipologie RAID da scegliere, LUN da costruire o file system da creare, le applicazioni cliente sono esenti dalla complessa gestione delle tradizionali topologie di storage;
- **Scalabilità senza riconfigurazione:** il Sistema, basato su tecnologia cosiddetta RAIN (Redundant Arrays of Independent Nodes) è disegnato per essere altamente scalabile (dai terabytes ai petabytes).

Il Sistema consente di **partizionare** il contenuto al suo interno. Questo significa che può essere integrato a più applicazioni e ciascuna applicazione integrata avrà accesso solo ai contenuti presenti nella partizione alla quale è abilitata ad accedere. Tutte le API hanno quindi valore anche solo all'interno di una partizione virtuale.

Come indicato nella figura seguente, la comunicazione con gli attori e i sistemi esterni è realizzata in generale attraverso protocolli standard di interfaccia, ad esclusione del caso di Centera, che fa uso di interfacce proprietarie.



L'utilizzo di API per il sistema di memorizzazione permette una totale indipendenza tra la componente applicativa e il Supporto di memorizzazione, consentendo una migrazione e/o integrazione, nell'ambito della soluzione complessiva, di differenti sistemi fisici di memorizzazione.

6.4. Procedure di gestione ed evoluzione del sistema

Per quanto concerne la **gestione operativa del servizio**, nell'ambito del sistema di qualità aziendale sono definiti i processi di Service Management, che hanno l'obiettivo di gestire tutto il ciclo del servizio, per garantire il raggiungimento degli SLA concordati contrattualmente con i clienti. I processi di gestione coprono tutto il ciclo di vita del servizio e consentono di monitorarne e controllarne tutti gli aspetti.

6.4.1. Procedure operative di gestione

Le procedure di gestione operativa del servizio e dei relativi sistemi a supporto, sono referenziate nel documento aziendale interno "Service Management Plan" che include riferimenti a:

- processi di incident e problem management;
- conduzione e manutenzione del sistema di conservazione;
- change & release management;
- capacity management;
- Back-up e Disaster Recovery;

- verifica periodica di conformità a normativa e standard di riferimento.

In particolare il processo di *Incident Management* definisce tutti gli aspetti e le attività necessarie per la gestione di incidenti e/o anomalie (*incident*) rilevate dal personale interno o dai clienti nell'intero ciclo che va dalla segnalazione fino alla chiusura. Nel caso in cui la chiusura di un *incident* non risultasse definitiva ma avesse bisogno di ulteriori indagini, tramite l'apertura di un *problem* viene attivato il processo di *Problem Management.*

Il servizio viene inoltre continuativamente monitorato e controllato al fine di verificare che sia conforme agli SLA definiti (*SLA Management*), ovvero che garantisca gli opportuni livelli di *capacity, continuity ed availability.*

La verifiche periodiche di conformità a normativa e standard di riferimento sono effettuate in conformità al Piano della Sicurezza e al Sistema di gestione della Qualità di SIA.

Il Sistema di Gestione della sicurezza delle informazioni certificato ISO/IEC 27001 di SIA prevede specifici controlli per la **gestione e conservazione dei log**, conformi ai requisiti della normativa sulla Privacy nonché ai requisiti specifici del Servizio di Conservazione dei documenti informatici.

Eventuali modifiche al sistema necessarie per la risoluzione di *incident* o *problem* o per rispondere a richieste di evoluzione da parte dei clienti o per rispondere a modifiche della normativa vigente, vengono gestite nell'ambito del sistema di qualità aziendale secondo quanto definito nel processo di *Change Management,* eventualmente accorpate in release e rilasciate in produzione secondo quanto descritto nel processo di *Release Management*.

Per garantire l'erogazione di servizi a valore aggiunto per i clienti SIA, sono previsti, tra i *processi di business*:

- il *processo di fattibilità,* che viene attivato per analizzare le richieste del Produttore (del mercato di riferimento o interne), per tradurle in requisiti e proporre soluzioni di alto livello che implementino tali requisiti, per analizzare i rischi dell'iniziativa, per effettuare studi di natura tecnica ed economico/finanziaria e per fornire al processo di vendita le informazioni necessarie per la formalizzazione delle richieste dei clienti;
- il *processo di progettazione,* che ha lo scopo di effettuare l'analisi di dettaglio dei requisiti (funzionali e non funzionali) e il disegno delle soluzioni da implementare, e di realizzare quanto progettato in conformità con i requisiti iniziali, nel rispetto dei tempi e dei costi pianificati.

6.4.2. Procedure di monitoraggio

Le procedure di monitoraggio e controllo, effettuate sul funzionamento del software applicativo e di sistema, sono descritte nella procedura "Monitoraggio servizi documentali", che elenca le attività a carico degli Operatori di monitoraggio, suddivise nelle seguenti macro categorie:

- Controllo delle procedure automatiche (job di firma, di caricamento e di controllo del sistema);
- Verifica quantitativa del numero di documenti e pacchetti suddivisi nei vari stati;

- Gestione dei ticket sulle segnalazioni dei clienti;
- Monitoraggio delle mail di segnalazione delle anomalie.

Le procedure delle prime due macro categorie vengono effettuate a cadenze regolari predefinite durante la giornata; quelle delle ultime due, invece, sono effettuate in tempo reale, tramite l'utilizzo di pop-up sui client di posta degli operatori.

6.4.3. Verifica dell'integrità degli archivi

Per quanto riguarda la **verifica dell'integrità dei documenti**, l'attività viene compiuta direttamente dalla componente infrastrutturale di gestione documentale (Centera), attraverso il meccanismo di mirroring e la continua verifica della disponibilità dei nodi e della integrità dei dati.

L'infrastruttura genera automaticamente una copia di sicurezza per ogni documento all'atto della conservazione, che risiede fisicamente su un nodo differente del supporto fisico primario; ambedue le copie sono costantemente monitorate attraverso meccanismi di verifica dell'impronta.

Ogni volta che il Sistema riscontra una non conformità in merito alla leggibilità o all'integrità di un documento memorizzato, traccia in opportuni file di log l'esito negativo della verifica di leggibilità e integrità e procede alla rigenerazione del documento a partire dalla copia ancora integra. Pertanto si ha una evidenza oggettiva di tutti gli interventi di rigenerazione eseguiti dal sistema.

Maggiori dettagli sulla gestione dell'integrità degli archivi sono riportati nel Piano della Sicurezza.

6.4.4. Log di sistema e tracking

Il sistema applicativo genera due file di log:

- log relativi alla tracciatura accessi utente, che registra le connessioni al sistema per i vari utenti
- log di registrazione delle operazioni applicative, che permette di individuare per ogni evento: data, ora, operazione, dati identificativi e esito

Ciascun log è scaricato con frequenza quotidiana. Ai log viene apposta una firma digitale ed un riferimento temporale per poi essere conservati digitalmente.

Il servizio dispone anche di una **gestione applicativa del tracking delle operazioni**. In particolare tale funzioni permettono la registrazione di tutti gli eventi significativi occorsi al singolo

documento o al singolo lotto.

Le informazioni registrate nel file di tracking sono: l'operazione, l'autore, l'ID del documento o del lotto oltre che la data e l'ora, con memorizzazione dei cambi stato e delle modifiche ai metadati. Tali registrazioni sono memorizzate su DB, con pagina di ricerca per utente e/o ID lotto/documento e/o data evento.

Tutte le registrazioni, quindi, sono estratte periodicamente e si provvede a conservare tutti i record di documenti e/o lotti che sono stati conservati.

7. Misure di Sicurezza

Le misure di sicurezza adottate da SIA sono descritte all'interno del Piano della Sicurezza e relativi allegati.

Da sempre SIA considera la Qualità, la Sicurezza delle Informazioni, la Business Continuity, la Compliance e la Gestione dei Rischi un vantaggio competitivo nell'ambito del posizionamento sul mercato.
SIA ha implementato i propri sistemi di gestione con l'obiettivo di aumentare la soddisfazione della propria clientela, di migliorare i processi ed i livelli di qualità e di sicurezza dei servizi, adottando standard internazionali di riferimento riconosciuti a livello mondiale.
La conformità a questi standard è attestata dal conseguimento delle certificazioni:

- ISO 9001:2008 per la Qualità;
- ISO/IEC 27001:2005 per la Sicurezza delle Informazioni;
- ISO 22301:2012 per la Continuità Operativa.

Nell'ambito di una logica di governance di Gruppo, accanto alla propria certificazione aziendale, SIA si è anche dotata di una certificazione ISO 9001:2008 Corporate per poter dare maggior visibilità delle competenze complessive che tutte le aziende del gruppo possono offrire al mercato.
Il Sistema di Gestione della Sicurezza delle Informazioni (SGSI) è definito nel rispetto delle misure di sicurezza previste dagli art. da 31 a 36 del D. lgs. 196/2003 e dal disciplinare tecnico di cui all'allegato B, nonché in coerenza con quanto previsto dalle normative e buone pratiche in tema di Business Continuity; nell'ambito del Sistema SIA:

- definisce la Politica della Sicurezza;
- emana le norme di sicurezza necessarie, affinché l'organizzazione aziendale possa condurre in modo sicuro le proprie attività;
- integra le regole e le soluzioni di sicurezza nel processo di progettazione ed erogazione dei servizi aziendali;
- attua l'analisi dei rischi di sicurezza dei processi e delle infrastrutture volte all'erogazione dei servizi di business aziendali e l'analisi dei rischi inerenti la sicurezza fisica e la sicurezza sul lavoro;
- collabora con il Sistema di Governo della Business Continuity per il raggiungimento degli obiettivi di continuità operativa;
- promuove la cultura relativa alla sicurezza;
- garantisce l'attuazione degli adempimenti alle leggi e normative di sicurezza (tra cui D.Lgs 196/03, PCI-DSS);
- definisce i ruoli e gli incarichi di sicurezza;
- gestisce un Comitato per l'indirizzo e il coordinamento delle tematiche di sicurezza;

- controlla i propri sistemi tramite specifici piani di Vulnerability Assessment;
- esegue il monitoraggio e i controlli interni in ambito sicurezza;
- opera e amministra gli aspetti operativi di sicurezza in una logica di split knowledge e dual control.

SIA per lo sviluppo del proprio SGSI ha scelto di adottare lo standard ISO/IEC 27001.
Gli elementi su cui si basa il sistema di gestione della sicurezza delle informazioni e della continuità operativa di SIA e che compongono il **Piano della Sicurezza** dei servizi dell'organizzazione, incluso il **sistema di conservazione**, sono:

- Politica della sicurezza delle Informazioni;
- Linee guida di sicurezza delle informazioni;
- Monitoraggio e riesame del Sistema;
- Sistema di governo dei rischi;
- Sistema di governo della compliance;
- Sistema di governo della Business Continuity (BCMS).

Oltre all'insieme di controlli specifici per ciascuna delle aree di controllo previste dalla norma ISO/IEC 27001 e attestate dal documento SoA (Statement of Applicability); il sistema dei controlli è progettato, attuato eregolarmente aggiornato sulla base dell'analisi dei rischi.

8. Trattamento dei dati personali

Al fine del corretto adempimento della normativa privacy SIA ha messo a punto un apposito sistema di gestione della Privacy.
Le attività di gestione si compongono di tre filoni principali di azione: i ruoli privacy, gli adempimenti e l'organizzazione.
Sono identificati i ruoli aziendali per assicurare una corretta adozione degli adempimenti richiesti:

- i Responsabili del trattamento (interni ed esterni);
- gli Incaricati del trattamento;
- gli Incaricati del trattamento con funzioni di Amministratore di Sistema.

Gli adempimenti sono realizzati da tutte le Direzioni/Divisioni ognuna per quanto di propria competenza. La responsabilità di attuazione e implementazione degli adempimenti è in carico a tutto il personale, in funzione del proprio ruolo e delle proprie competenze, anche per ciò che riguarda l'applicazione da parte dei terzi coinvolti nello svolgimento delle attività; il riferimento primario per le attività è rappresentato dalla normativa interna regolamentata in appositi documenti. Si segnala in particolare la Policy Privacy che descrive le linee di condotta generali per la corretta applicazione in SIA del Codice Privacy.
L'organizzazione della gestione della privacy include le attività più specificatamente interne a SIA e di ufficio, come ad esempio l'aggiornamento dell'archivio dei soggetti con un ruolo Privacy, il monitoraggio della normativa, le relazioni con le Società Controllate, le consulenze e i pareri alle aree aziendali che ne fanno richiesta. Tra le attività svolte assumono particolare rilievo la revisione e l'aggiornamento, tendenzialmente annuale, di tutti i documenti, oltre al controllo costante dell'adeguamento alla normativa. Particolare attenzione è prestata ai rapporti privacy con soggetti esterni a SIA (tipicamente Clienti e Fornitori); la contrattualistica con tali soggetti prevede specifiche clausole contrattuali ed eventuali nomine a responsabili del trattamento che sono gestite dall'Unità Organizzativa privacy, in accordo con la struttura Legale aziendale.