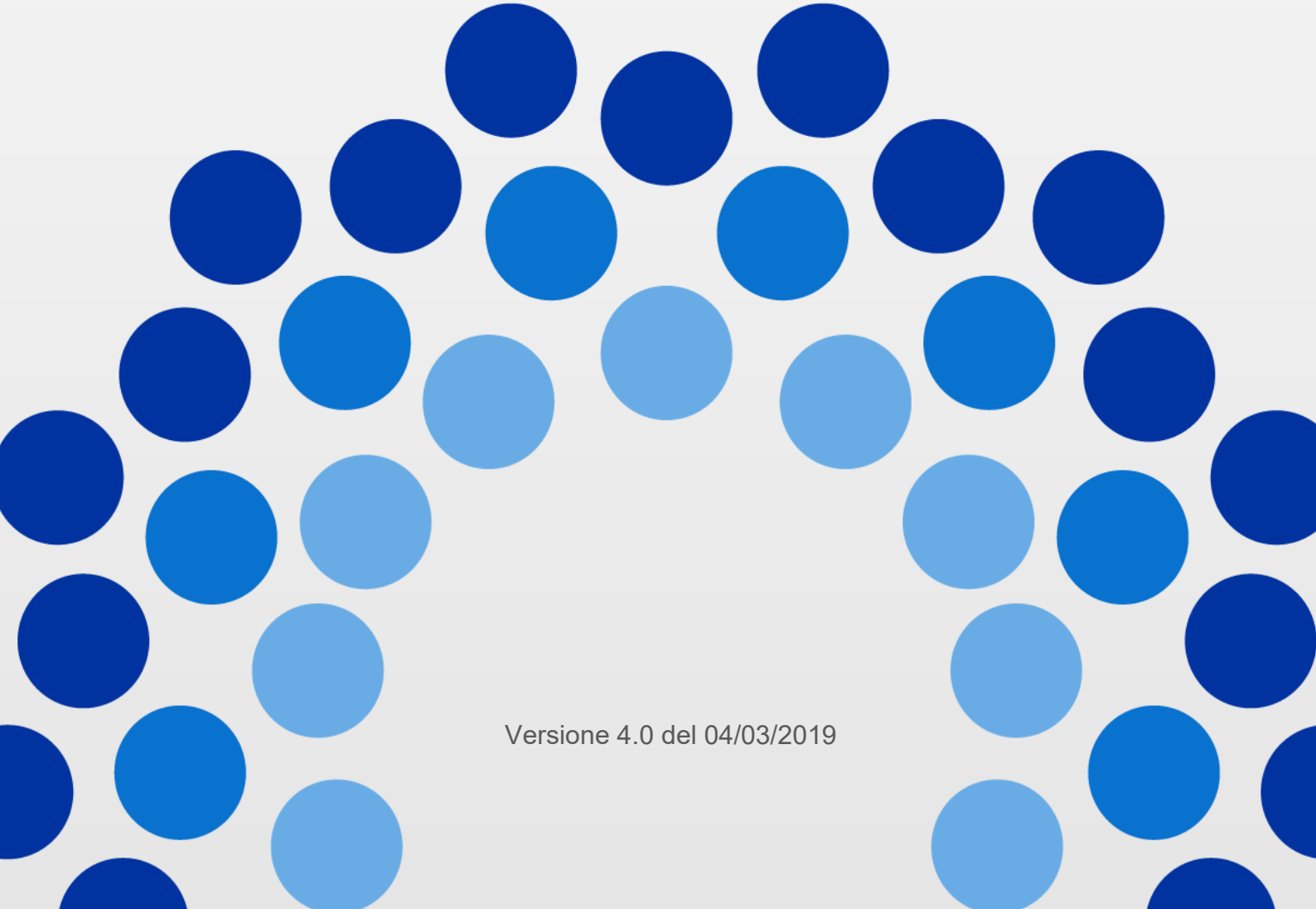
InfoCamere

Manuale di Conservazione



Versione 4.0 del 04/03/2019

EMISSIONE DEL DOCUMENTO

Azione	Data	Nominativo	Funzione
Redazione	04/03/2019	Oscar Berti	Responsabile sviluppo e manutenzione del sistema di conservazione
Verifica	04/03/2019	Beatrice Pugliano Luigi Cantone Grazia Sarto	Responsabile funzione archivistica di conservazione Responsabile Sicurezza dei sistemi per la conservazione Responsabile trattamento dati personali Responsabile sistemi informativi per la conservazione
Approvazione	04/03/2019	Antonio Tonini	Responsabile del servizio di conservazione

REGISTRO DELLE VERSIONI

N°Ver/Rev/Bozza	Data Emissione	Modifiche apportate	Osservazioni
4.0	04/03/2019	Adeguamenti responsabili e organigramma. Evoluzione Archivio CAS	
3.0	22/01/2016	Adeguamenti per requisiti accessibilità documento, modifica MoreInfo VdC, adeguamenti organigramma	
2.0	09/09/2015	Nuova emissione per revisioni	Variazioni al frontespizio e ai paragrafi 6.3, 7.1, 7.2, 7.3, 7.4
1.0	22/06/2015	Prima emissione del documento secondo lo schema del manuale AgID per l'accreditamento	

Indice

1 Scopo e ambito del documento

Il presente documento costituisce il manuale di conservazione di InfoCamere Società Consortile delle Camere di Commercio Italiane per azioni (di seguito InfoCamere) ai sensi dell'art. 8 del DPCM 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 (di seguito Regole Tecniche).

Il presente documento ha lo scopo di descrivere il sistema di conservazione dei documenti informatici adottato dalla azienda, utilizzando lo schema predisposto da AgID che tiene conto di quanto previsto dalla normativa vigente e dal documento "Requisiti di qualità e sicurezza per l'accreditamento e la vigilanza".

Il sistema di conservazione ha come oggetto la realizzazione di un insieme di funzionalità atte a consentire la conservazione dei documenti informatici e a fornire un supporto alle figure coinvolte nel processo di conservazione.

Il software utilizzato per la gestione del processo di conservazione dei documenti informatici è di proprietà di InfoCamere.

Torna al sommario

1.1 Dati identificativi di InfoCamere

L'attività di conservazione di documenti è presente in InfoCamere fin dalla sua nascita nel 1995 e sempre rispondente alla normativa di riferimento.

Per il soddisfacimento dei propri obiettivi InfoCamere si avvale della propria struttura organizzativa certificata ISO 9001: 2008.

Viene di seguito evidenziata una parte del profilo aziendale, che illustra nel dettaglio la mission aziendale; la versione completa si trova sul sito www.infocamere.it.

*L'attività della società spazia dunque dalla gestione del patrimonio informativo delle Camere (grazie soprattutto al portale registroimprese.it che è il vero e proprio motore di ricerca nel settore dell'economia nazionale), all'informatizzazione e semplificazione dei servizi che le stesse Camere mettono a disposizione delle imprese soprattutto nel loro rapporto con la Pubblica Amministrazione (ad esempio tramite il software ComUnica, la gestione del portaleimpresainungiorno.gov.it e delle pratiche legate al SUAP), al rilascio di certificati digitali delle Carte Tachigrafiche in qualità di Autorità di Certificazione Nazionale, allo sviluppo di servizi informatici necessari alle attività di back office delle Camere di Commercio**, alla conservazione di documenti informatici***. InfoCamere, dunque, supporta le Camere nella loro missione di curare gli interessi generali delle imprese, promuovendone la competitività.*

Torna al sommario

2 Terminologia (glossario e acronimi)

Glossario dei termini e Acronimi	
AgID	Agenzia per l'Italia Digitale
AIP	Archival Information Package. Definizione dello standard OAIS e sinonimo di Pacchetto di Archiviazione
AIU	Archival Information Unit. Definizione dello standard OAIS – ISO 14721, sottocomponente di un AIP
Circolare AgID	Circolare AgID 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.
Codice della privacy	Decreto Legislativo 30 giugno 2003, n. 196 e s.m.i. – Codice in materia di protezione dei dati personali
GDPR	Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE
Dublin Core	ISO 15836:2009 Information and documentation - The Dublin Core metadata element set, Sistema di metadata del Dublin Core.
Archivio CAS	Archivio basato sul meccanismo di Content Addressable Storage, utilizzato per la memorizzazione di informazioni che possono essere recuperate in base al loro contenuto e non in base alla loro posizione di memorizzazione
DIP	Dissemination Information Package. Definizione dello standard OAIS e sinonimo di Pacchetto di Distribuzione
Funzione hash	una funzione matematica che genera, a partire da una evidenza informatica, una impronta in modo tale che risulti di fatto impossibile, a partire da questa, ricostruire l'evidenza informatica originaria e generare impronte uguali a partire da evidenze informatiche differenti
Impronta	la sequenza di simboli binari (bit) di lunghezza predefinita generata mediante l'applicazione alla prima di una opportuna funzione di hash
IR	Information Representation Definizione dello standard OAIS per rendere comprensibile e leggibile le componenti di una UD. Sinonimo di informazioni sulla rappresentazione

Glossario dei termini e Acronimi	
OAIS	Open Archival Information System è lo standard IS0:14721:2003 e definisce concetti, modelli e funzionalità inerenti agli archivi digitali e gli aspetti di digital preservation.
PDI	Preservation description information Definizione dello standard OAIS per gestire le informazioni sulla conservazione. Sinonimo di informazioni sulla rappresentazione
Piano della sicurezza	documento che, nel contesto del piano generale di sicurezza, descrive e pianifica le attività volte a proteggere il sistema di conservazione dei documenti informatici da possibili rischi nell'ambito dell'organizzazione di appartenenza
Produttore	persona fisica o giuridica, di norma diversa dal soggetto che ha formato il documento, che produce il pacchetto di versamento ed è responsabile del trasferimento del suo contenuto nel sistema di conservazione. Nelle pubbliche amministrazioni, tale figura si identifica con responsabile della gestione documentale.
Regole Tecniche	DPCM 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
Responsabile della conservazione	soggetto responsabile dell'insieme delle attività elencate nell'articolo 8, comma 1 delle Regole Tecniche del sistema di conservazione
SIP	Submission Information Package. Definizione dello standard OAIS e sinonimo di Pacchetto di Distribuzione
TSA	Time Stamping Autorithy Soggetto che eroga la marca temporale
UniSincro	UNI 11386:2010 - Supporto all'Interoperabilità nella conservazione e nel Recupero degli oggetti digitali
UA	Unità archivistica Contenitore di più UD, secondo i concetti archivistici di: Fascicolo, Serie, Aggregazione Documentale
UD	Unità documentaria Unità minima elementare di riferimento di cui è composto un archivio
Utente	persona, ente o sistema che interagisce con i servizi di un sistema di gestione informatica dei documenti e/o di un sistema per la conservazione dei documenti informatici, al fine di fruire delle informazioni di interesse

Torna al sommario

3 Normativa e standard di riferimento

3.1 Normativa di riferimento

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 24 dicembre 2007, n. 244 - Disposizioni per la formazione del bilancio annuale e pluriennale dello Stato;
- Legge 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 Legislativo 7 marzo 2005 n. 82 e s.m.i. – Codice dell'amministrazione digitale (CAD);
- Decreto Legislativo 22 gennaio 2004, n. 42 e s.m.i. – Codice dei Beni Culturali e del Paesaggio;
- Decreto Legislativo 30 giugno 2003, n. 196 e s.m.i. – Codice in materia di protezione dei dati personali;
- Regolamento (UE) 2016/679 - relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati
- Decreto Legislativo 10 agosto 2018, n. 101 - Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati);
- Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 e s.m.i. – Testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa;
- DPCM 13 novembre 2014 Regole tecniche per la formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici nonché di formazione e conservazione dei documenti informatici delle pubbliche amministrazioni;
- Decreto del Presidente del Consiglio dei Ministri 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 3 dicembre 2013 - Regole tecniche per il

protocollo informatico ai sensi degli articoli 40-bis, 41, 47, 57-bis e 71, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005.;

- Decreto del Presidente del Consiglio dei Ministri 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 MEF 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;
- Decreto MEF 3 aprile 2013, n. 55 - Regolamento in materia di emissione, trasmissione e ricevimento della fattura elettronica da applicarsi alle amministrazioni pubbliche ai sensi dell'articolo 1, commi da 209 a 213, della legge 24 dicembre 2007, n. 244;
- Circolare AgID 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;
- Deliberazione Cnipa 21 Maggio 2009, n. 45 – Regole per il riconoscimento e la verifica del documento informatico;
- Linee Guida per disaster recovery delle pubbliche amministrazioni - ai sensi del c. 3, lettera b) dell'art. 50bis del Codice dell'Amministrazione Digitale, Aggiornamento 2013

Torna al sommario

3.2 Standard di riferimento

- ISO 14721:2012 OAIS (Open Archival Information System), Sistema informativo aperto per l'archiviazione;
- ISO/IEC 27001:2013, Information technology - Security techniques - Information security management systems – Requirements, Requisiti di un ISMS (Information Security Management System);
- ISO 9001:2008 sistemi di gestione per la qualità - Requisiti
- ETSI TS 101 533-1 V1.3.1 (2012-04) Technical Specification, Electronic Signatures and Infrastructures (ESI); Information 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 elettronica delle informazioni;

- UNI 11386:2010 Standard SInCRO - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali;
- ISO 15836:2009 Information and documentation - The Dublin Core metadata element set, Sistema di metadata del Dublin Core.
- ISO/TS 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 23081-2:2009 - Managing metadata for records – Part 2: Conceptual and implementation issues, Guida pratica per l'implementazione.
- 23081-3:2011 Information and documentation -- Managing metadata for records -- Part 3: Self-assessment method, Guida per un processo di autovalutazione sui metadata.
- ISAD(G) - International Standard Archival description standard adottato dal Comitato per gli standard descrittivi degli archivi
- EAD - Encoded Archival Description, codifica XML dello standard ISAD(G)
- ISAAR - International Standard Archival Authority Records, standard internazionale per I record d'autorità archivistici di enti, persone, famiglie
- EAC - Encoded Archival Context, codifica XML dello standard ISAAR

Torna al sommario

4 Ruoli e responsabilità

Nella tabella successiva vengono indicati le attività svolte e i nominativi delle persone che ricoprono i ruoli indicati nel documento 'Profili professionali' richiamato dalla Circolare AgID.

Ruoli	Nominativo	attività di competenza	periodo nel ruolo	eventuali deleghe
Responsabile del servizio di conservazione	Tonini Antonio	- Definizione e attuazione delle politiche complessive del sistema di conservazione, nonché del governo della gestione del sistema di conservazione; - definizione delle caratteristiche e dei requisiti del sistema di conservazione in conformità alla normativa vigente; - corretta erogazione del servizio di conservazione all'ente produttore; - gestione delle convenzioni, definizione degli aspetti tecnico-operativi e validazione dei disciplinari tecnici che specificano gli aspetti di dettaglio e le modalità operative di erogazione dei servizi di conservazione.	Dal 17/06/2015	
Responsabile Sicurezza dei sistemi per la conservazione	Cantone Luigi	- Rispetto e monitoraggio dei requisiti di sicurezza del sistema di conservazione stabiliti dagli standard, dalle normative e dalle politiche e procedure interne di sicurezza; - segnalazione delle eventuali difformità al Responsabile del servizio di conservazione e individuazione e pianificazione delle necessarie azioni correttive.	Dal 17/06/2015	
Responsabile funzione archivistica di conservazione	Pugliano Beatrice	- Definizione e gestione del processo di conservazione, incluse le modalità di trasferimento da parte dell'ente produttore, di acquisizione, verifica di integrità e descrizione archivistica dei documenti e delle aggregazioni documentali trasferiti, di esibizione, di accesso e fruizione del patrimonio	Dal 17/06/2015	

Ruoli	Nominativo	attività di competenza	periodo nel ruolo	eventuali deleghe
		documentario e informativo conservato; - definizione del set di metadati di conservazione dei documenti e dei fascicoli informatici; - monitoraggio del processo di conservazione e analisi archivistica per lo sviluppo di nuove funzionalità del sistema di conservazione; - collaborazione con l'ente produttore ai fini del trasferimento in conservazione, della selezione e della gestione dei rapporti con il Ministero dei beni e delle attività culturali per quanto di competenza.		
Responsabile trattamento dati personali	Cantone Luigi	- Garanzia del rispetto delle vigenti disposizioni in materia di trattamento dei dati personali; - garanzia che il trattamento dei dati affidati dai Clienti avverrà nel rispetto delle istruzioni impartite dal titolare del trattamento dei dati personali, con garanzia di sicurezza e di riservatezza	Dal 17/06/2015	
Responsabile sistemi informativi per la conservazione	Sarto Grazia	Gestione dell'esercizio delle componenti hardware e software del sistema di conservazione; - monitoraggio del mantenimento dei livelli di servizio (SLA) concordati con l'ente produttore; - segnalazione delle eventuali difformità degli SLA al Responsabile del servizio di conservazione e individuazione e pianificazione delle necessarie azioni correttive; - pianificazione dello sviluppo delle infrastrutture tecnologiche del sistema di conservazione; - controllo e verifica dei livelli di servizio	Dal 17/06/2015	

Ruoli	Nominativo	attività di competenza	periodo nel ruolo	eventuali deleghe
		erogati da terzi con segnalazione delle eventuali difformità al Responsabile del servizio di conservazione.		
Responsabile sviluppo e manutenzione del sistema di conservazione	Oscar Berti	Coordinamento dello sviluppo e manutenzione delle componenti hardware e software del sistema di conservazione; - pianificazione e monitoraggio dei progetti di sviluppo del sistema di conservazione; - monitoraggio degli SLA relativi alla manutenzione del sistema di conservazione; - interfaccia con l'ente 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; - gestione dello sviluppo di siti web e portali connessi al servizio di conservazione.	Dal 04/03/2019	

La nomina è stata firmata per accettazione dai responsabili.

Precedenti Responsabili

Ruoli	Nominativo	attività di competenza	periodo nel ruolo	eventuali deleghe
Responsabile sviluppo e manutenzione del sistema di conservazione	Luigi Pallottini	Coordinamento dello sviluppo e manutenzione delle componenti hardware e software del sistema di conservazione; - pianificazione e monitoraggio dei progetti di sviluppo del sistema di conservazione; - monitoraggio degli SLA relativi alla manutenzione del sistema di conservazione; - interfaccia con l'ente 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; - gestione dello sviluppo di siti web e portali connessi al servizio di conservazione.	Dal 17/06/2015 Al 04/03/2019	

Torna al sommario

5 Struttura organizzativa per il servizio di Conservazione

5.1 Modello OAIS

Le logiche organizzative di InfoCamere fanno riferimento al modello OAIS (Open Archival Information System), che garantisce una distinzione logica del sistema di conservazione dal sistema di gestione documentale, se esistente.

Vengono qui descritti i principali ruoli che si configurano con un contratto di affidamento della conservazione ad un soggetto accreditato come conservatore presso AgID.

Torna al sommario

5.1.1 Produttore / Responsabile della conservazione

Le Regole Tecniche (Glossario, allegato 1) identificano il produttore nel soggetto, titolare dei dati, che produce il pacchetto di versamento ed è responsabile del trasferimento del suo contenuto nel sistema di conservazione.

Affida la conservazione dei propri documenti informatici e dei fascicoli informatici al responsabile della conservazione. I compiti del responsabile della conservazione sono definiti all'art. 7 delle Regole Tecniche.

Il responsabile della conservazione:

- per le amministrazioni pubbliche deve essere un dirigente o un funzionario se formalmente nominato (art. 7, comma 3, Regole Tecniche) e può coincidere con il responsabile della gestione documentale (art, 7, comma 4, Regole Tecniche)
- per le imprese private è il rappresentante legale o soggetto da lui delegato.

E' possibile affidare il servizio di conservazione ad un soggetto esterno (art. 5, comma 3, Regole Tecniche). Attraverso un contratto di affidamento del servizio di conservazione, sottoscritto tra il soggetto produttore e il soggetto conservatore, vengono definite:

- le attività e le responsabilità che rimangono a carico del produttore nella figura del responsabile della conservazione
- le funzioni e competenze affidate al soggetto conservatore (art. 6, comma 6, delle Regole Tecniche)

Nel seguito del manuale si utilizzerà in genere il termine del Produttore per identificare il soggetto che affida ad InfoCamere il servizio, il quale – nel caso di pubblica amministrazione - avrà al proprio interno nominato una figura di responsabile della conservazione.

Torna al sommario

5.1.2 InfoCamere / Soggetto conservatore

InfoCamere nel contratto di affidamento rappresenta il soggetto conservatore. Secondo il comma 8 dell'art. 6 delle Regole Tecniche assume il ruolo di responsabile del trattamento dei dati come Previsto dal Codice in materia di protezione dei dati personali.
Come soggetto conservatore, si è organizzato:

- nominando le sei figure professionali come indicato nel capitolo 4;
- identificando le strutture organizzative coinvolte dal servizio di conservazione come indicato nel paragrafo 5.1;
- definendo le attività di ciascuna struttura nei contratti di conservazione come indicato nel paragrafo 5.2.

Torna al sommario

5.1.3 Utente

Le Regole Tecniche (Glossario, allegato 1) identificano l'utente come una persona, ente o sistema che interagisce con i servizi di un sistema per la conservazione di documenti informatici.

L'utente richiede al sistema di conservazione l'accesso ai documenti informatici 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.

Per ciascun soggetto produttore sono abilitati ad accedere ai documenti i referenti contrattuali (responsabile della conservazione) e tutti gli altri soggetti da questi delegati, previa comunicazione ad Infocamere nelle modalità stabilite in contratto e nel rispetto della normativa in materia di riservatezza dei dati personali (D. Lgs. n. 196/2003).

Torna al sommario

5.1.4 Organismo di tutela e vigilanza

Il Ministero per i beni e le attività culturali e del turismo (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.

La tutela e vigilanza sugli Archivi di enti pubblici non statali è esercitata dal MiBACT, tramite le Soprintendenze archivistiche 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 alla conservazione informatica dei documenti:

- 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.

La Soprintendenza 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.

In base alle Regole Tecniche i sistemi di Conservazione delle amministrazioni pubbliche e i sistemi di Conservazione dei conservatori accreditati sono soggetti anche alla vigilanza di AgID.

Si precisa che, ai fini della normativa vigente, il sistema di conservazione InfoCamere prevede la materiale conservazione dei dati e delle copie di sicurezza sul territorio nazionale e l'accesso dei dati presso le strutture dedicate allo svolgimento del servizio di conservazione o la sede del produttore.

Torna al sommario

5.2 Organigramma

La seguente figura identifica le principali Strutture Organizzative coinvolte nel sistema di conservazione:

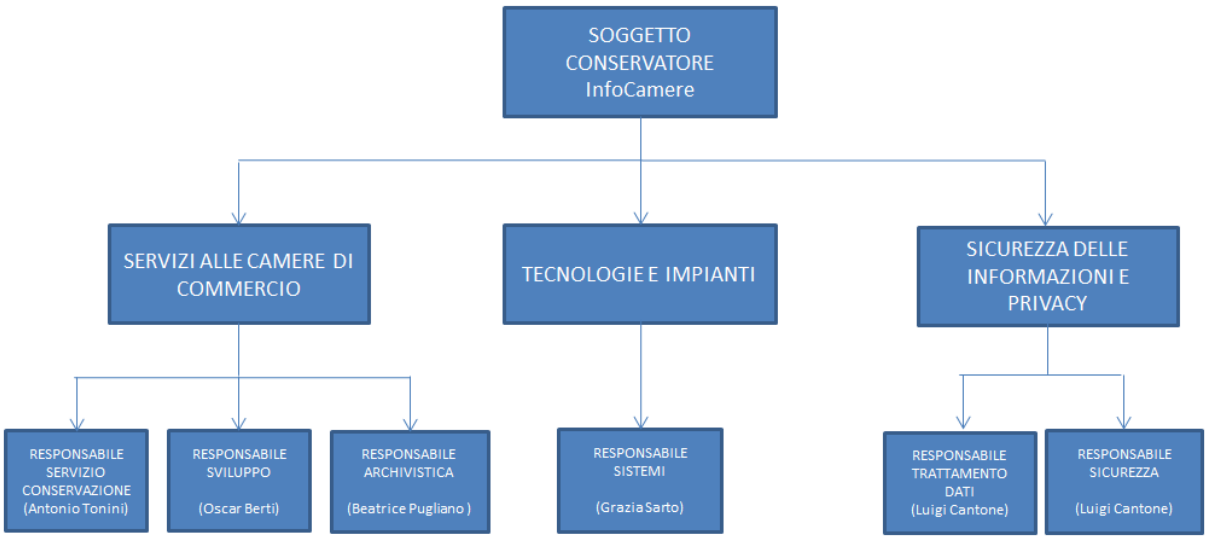


Figura 1 Organizzazione del sistema di conservazione

SERVIZI ALLE CAMERE DI COMMERCIO
Sviluppa e gestisce servizi e applicazioni informatiche, tra cui il sistema di conservazione.

TECNOLOGIE E IMPIANTI
Garantisce il presidio dell'ambiente di produzione di InfoCamere, promuovendo un continuo processo di ottimizzazione delle risorse ed un miglioramento dei servizi offerti. Guida l'evoluzione delle architetture, coerentemente con le esigenze aziendali e l'evoluzione della tecnologia.

SICUREZZA DELLE INFORMAZIONI E PRIVACY
Assicura l'attuazione del Sistema di Gestione della Sicurezza delle Informazioni di InfoCamere e l'attuazione delle disposizioni vigenti in materia di protezione dei dati personali (privacy).

Torna al sommario

5.3 Strutture organizzative

La seguente tabella descrive, per ogni attività, la figura responsabile e la struttura organizzativa di riferimento.

PRG.	ATTIVITA'	FIGURA PROFESSIONALE	STRUTTURA ORGANIZZATIVA
1	Attivazione del servizio di conservazione (a seguito della sottoscrizione di un contratto di affidamento)	Responsabile servizio conservazione	SERVIZI ALLE CAMERE DI COMMERCIO
2	Setup dell'integrazione tra i sistemi del produttore ed il sistema di conservazione	Responsabile Sviluppo	SERVIZI ALLE CAMERE DI COMMERCIO
3	Definizione metadati dei documenti e informazioni sulla rappresentazione	Responsabile funzione archivistica	SERVIZI ALLE CAMERE DI COMMERCIO
4	Acquisizione, verifica e gestione dei pacchetti di versamento presi in carico e generazione del rapporto di versamento	Responsabile Sviluppo	SERVIZI ALLE CAMERE DI COMMERCIO
5	Preparazione e gestione del pacchetto di archiviazione	Responsabile servizio conservazione	SERVIZI ALLE CAMERE DI COMMERCIO
6	Preparazione e gestione del pacchetto di distribuzione ai fini dell'esibizione	Responsabile funzione archivistica	SERVIZI ALLE CAMERE DI COMMERCIO
7	Produzione di duplicati e copie informatiche su richiesta	Responsabile funzione archivistica	SERVIZI ALLE CAMERE DI COMMERCIO
8	Scarto dei pacchetti di archiviazione	Responsabile funzione archivistica	SERVIZI ALLE CAMERE DI COMMERCIO
9	Chiusura del servizio di conservazione (al termine di un contratto di affidamento)	Responsabile servizio conservazione	SERVIZI ALLE CAMERE DI COMMERCIO
10	Verifica periodica integrità archivi	Responsabile servizio conservazione	SERVIZI ALLE CAMERE DI COMMERCIO
11	Monitoraggio della corretta funzionalità del sistema di conservazione	Responsabile servizio conservazione	SERVIZI ALLE CAMERE DI COMMERCIO
12	Verifica periodica di conformità a normativa e standard di riferimento sulla conservazione	Responsabile servizio conservazione	SERVIZI ALLE CAMERE DI COMMERCIO

PRG.	ATTIVITA'	FIGURA PROFESSIONALE	STRUTTURA ORGANIZZATIVA
13	Definizione e attuazione delle politiche complessive del sistema di conservazione	Responsabile servizio conservazione	SERVIZI ALLE CAMERE DI COMMERCIO
14	Aggiornamento manuale di conservazione	Responsabile funzione archivistica	SERVIZI ALLE CAMERE DI COMMERCIO
15	Conduzione e manutenzione del sistema di conservazione	Responsabile Sistemi	TECNOLOGIE E IMPIANTI
16	Monitoraggio del sistema di conservazione	Responsabile Sistemi	TECNOLOGIE E IMPIANTI
17	Change Management	Responsabile Sistemi	TECNOLOGIE E IMPIANTI
18	Assistenza (produttori e utenti)	Responsabile funzione archivistica	SERVIZI ALLE CAMERE DI COMMERCIO
19	Monitoraggio complessivo del sistema di conservazione	Responsabile servizio conservazione	SERVIZI ALLE CAMERE DI COMMERCIO
20	Correzione di eventuali anomalie applicative che dovessero emergere nel processo di conservazione	Responsabile Sviluppo	SERVIZI ALLE CAMERE DI COMMERCIO
21	Verifica periodica di conformità a normativa e standard di riferimento in materia di sicurezza	Responsabile Sicurezza	SICUREZZA DELLE INFORMAZIONI E PRIVACY
22	Verifica periodica di conformità a normativa e standard di riferimento in materia di trattamento dei dati personali	Responsabile trattamento dati	SICUREZZA DELLE INFORMAZIONI E PRIVACY

Torna al sommario

6 Oggetti sottoposti a conservazione

Il sistema di conservazione gestito da InfoCamere conserva gli oggetti digitali, con i metadati ad essi associati.

In questo capitolo sono illustrate le informazioni principali sugli oggetti trattati e sulla gestione dei pacchetti. Il dettaglio sarà presente nell'ambito delle pattuizioni contrattuali stipulate con i singoli soggetti produttori.

Torna al sommario

6.1 Oggetti conservati

Il modello di riferimento per la gestione degli oggetti da conservare riprende quello gerarchico di un archivio secondo lo standard ISAD(G), come illustrato nella figura seguente.

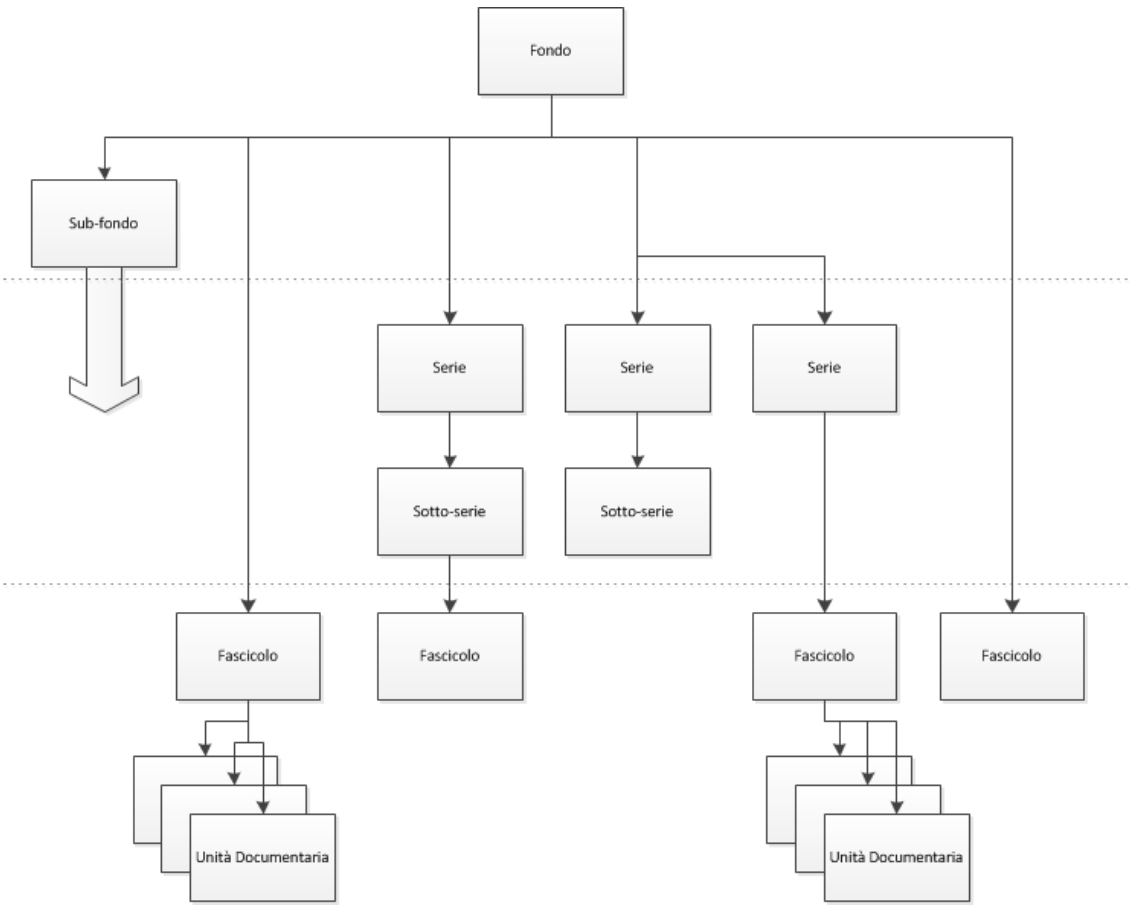


Figura 2 Schema dei livelli di ordinamento di un fondo

I documenti informatici e le aggregazioni informatiche sono trattati nel sistema nella forma di Unità documentarie e Unità archivistiche e sono inviati in conservazione sotto forma di Pacchetti di Versamento (SIP), che contengono sia gli oggetti digitali, sia le informazioni sulla rappresentazione, sia le informazioni sulla conservazione (PDI)

Nel servizio di conservazione InfoCamere, come previsto dall'art. 3 comma 1 delle Regole Tecniche, sono previste:

- **L'Unità Documentaria** (di seguito denominata UD), rappresenta l'unità minima elementare di riferimento di cui è composto un archivio, pertanto rappresenta il riferimento principale per la costruzioni dei pacchetti informativi. Con riferimento a quanto indicato nello standard ISO 23081-2:2009, 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 più

  componenti: la componente principale e gli allegati. All'unità documentaria e ai componenti di cui è costituita sono associati set di metadati che li identificano e li descrivono.

- L'**Unità Archivistica** (di seguito denominata UA), intesa come il contenuto che aggrega fra loro più UD. L'UA aggrega tra loro più UD secondo i concetti archivistici di Fascicolo e Aggregazione Documentale. Contiene solo un set di metadati, tra cui l'elenco delle UD che compongono la UA, secondo le logiche di classificazione e fascicolazione utilizzate dal produttore.

Nella figura seguente viene esemplificato lo schema gerarchico dell'archivio InfoCamere.

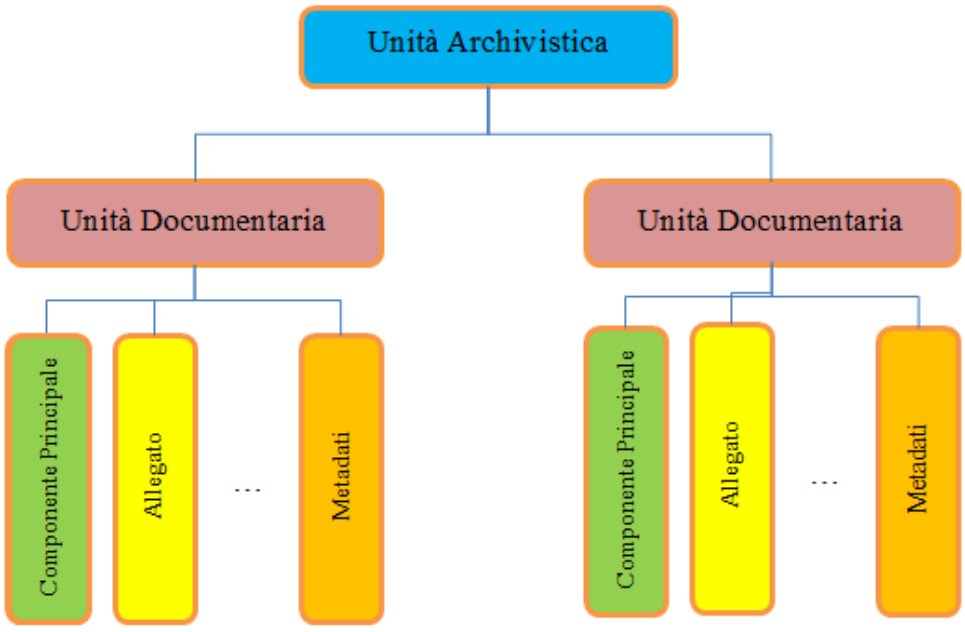


Figura 3 Schema gerarchico dell'archivio InfoCamere

Torna al sommario

6.1.1 Pacchetto informativo

Gli oggetti digitali sottoposti a conservazione sono trasmessi dal Produttore, e memorizzati e conservati nel sistema di conservazione. In seguito ad una precisa richiesta, vengono successivamente distribuiti alla comunità di riferimento sotto forma di pacchetti di distribuzione (DIP). A seconda che siano utilizzati per versare, conservare, o distribuire gli oggetti sottoposti a conservazione, i pacchetti informativi assumono la forma, rispettivamente, di pacchetto di versamento (SIP), pacchetto di archiviazione (AIP) e pacchetto di distribuzione (DIP).

Nella figura seguente viene rappresentato il pacchetto informativo secondo il modello OAIS.

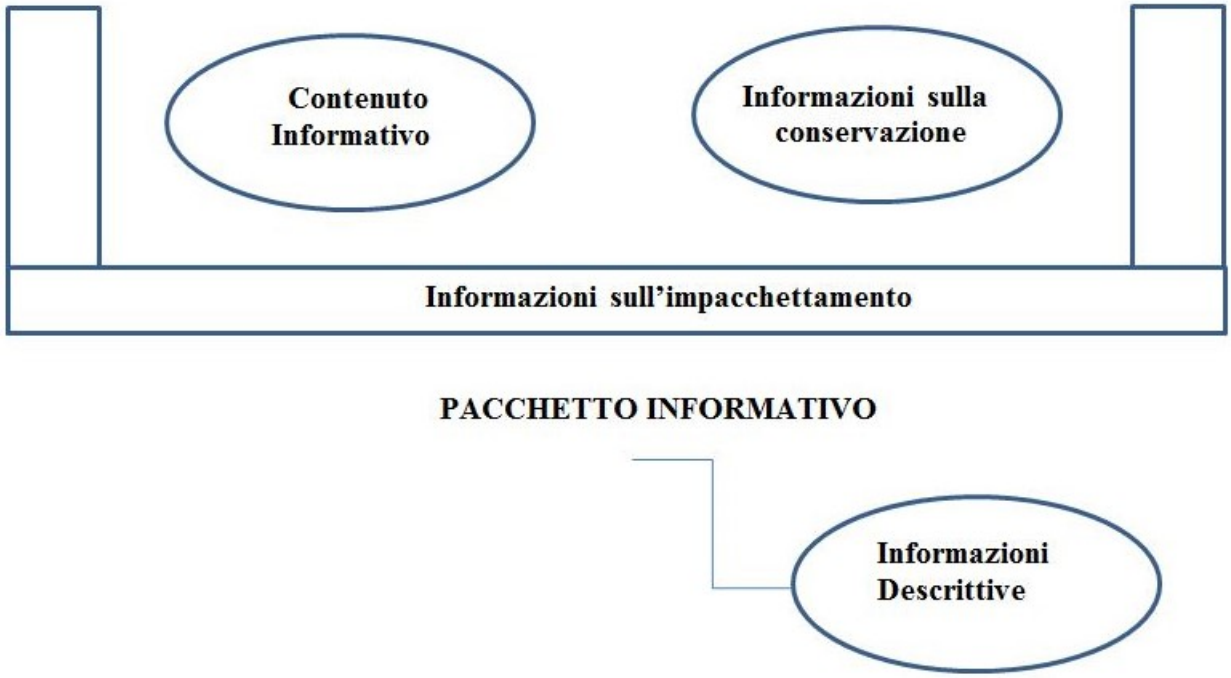


Figura 4 Struttura del pacchetto informativo secondo il modello OAIS

Il pacchetto informativo è un contenitore di due tipi di informazioni: contenuto informativo e informazioni sulla conservazione (PDI) con le seguenti informazioni:

- **Contenuto informativo** composto da:
  - **oggetto dati.** In genere sono i file, cioè la sequenza di bit da conservare
  - **informazioni sulla rappresentazione (IR)**. Le principali informazioni di questa tipologia sono il formato del file e il software visualizzatore, cioè le informazioni necessarie per rendere comprensibile e leggibile nel tempo l'oggetto dati.

- le **Informazioni sulla conservazione (PDI).** Si tratta tipicamente di metadati, cioè di informazioni che servono per conservare il contenuto informativo e garantire che sia sempre identificabile e chiaro il contesto. Definiscono la provenienza, il contesto, l'identificazione e l'integrità del contenuto informativo.

Il contenuto informativo e le informazioni sulla conservazione sono incapsulati e identificabili attraverso le **informazioni sull'impacchettamento**. .

Sono ad esso associate le **informazioni descrittive,** che permettono la ricerca del pacchetto informativo nel sistema, recuperando in genere dallo stesso un sottoinsieme di informazioni.

Relativamente al pacchetto informativo vengono in questo paragrafo definite le caratteristiche principali dei metadati (le informazioni sulla conservazione) e dei formati (Informazioni sulla rappresentazione).

Torna al sommario

6.1.2 Metadati

InfoCamere ha tenuto in considerazione i seguenti standard e modelli di riferimento per la conservazione:

- Dublin Core per la gestione dei documenti
- ISAD(G)/EAD per la descrizione archivistica e dei processi di 'record management'
- ISAAR/EAC per la descrizione dei soggetti produttori, delle attività e processi di lavoro
- UniSincro per la gestione delle informazioni di impacchettamento

Con l'utilizzo integrato degli standard sopracitati sono stati selezionati i metadati necessari al sistema di conservazione, raggruppandoli secondo due macro classificazioni:

- Metadati Semantici
- Metadati di Relazione

Queste informazioni sono in gran parte fornite dal produttore attraverso il SIP e in parte definite dal processo di creazione del pacchetto di archiviazione.

Metadati Semantici

Nella tabella seguente sono riportati alcuni degli attributi più significativi dei pacchetti informativi. La valorizzazione di ciascun attributo permetterà la gestione del pacchetto informativo nel processo di conservazione.

Attributo	**Descrizione**
Tipo di contenuto	Descrizione della tipologia di pacchetto informativo (Unita documentaria o Unita archivistica)
Struttura metadati contenuto	Struttura dei metadati associata ad unità documentarie o archivistiche simili a livello di informazioni/attributi (es. documento amministrativo, documento informatico, fatture, etc)

Attributo	Descrizione
Identificativo contenuto	Identificativo univoco assegnato al contenuto dal produttore
Identificativo contenuto conservato	Identificativo univoco assegnato al contenuto dal sistema di conservazione
Codice produttore	Identificativo del soggetto Produttore
Tipo produttore	Tipologia di soggetto Produttore (Ad esempio: EnteNonTerritoriale, EnteTerritoriale, Azienda, Persona)
Denominazione produttore	Denominazione del soggetto Produttore
Codice sistema versante	Identificativo del prodotto di gestione documentale che ha versato il contenuto
Denominazione sistema versante	Denominazione del prodotto di gestione documentale che ha versato il contenuto
Versione sistema versante	Versione V.R.M. del prodotto di gestione documentale che ha versato il contenuto
Utente	User dell'utente che ha versato il contenuto
Data riferimento conservazione	Data di decorrenza dei tempi di conservazione, da utilizzare per i documenti soggetti a scarto
Tempo di conservazione	Classe temporale di tenuta in conservazione del contenuto. Si rimanda ai mezzi di corredo del produttore nel caso di Pubblica Amministrazione
Data di versamento	Data in cui il contenuto è stato versato
Data limite conservazione	Data massima entro cui il contenuto deve essere conservato. Si tratta di una informazione necessaria per alcune tipologie di contenuti (es. fattura)
Data di archiviazione	Data della marca temporale dell'AIP, cioè la data in cui il contenuto è passato in conservazione
Privacy	Livello di sensibilità, legato al codice della privacy, impostata per il contenuto (Ad esempio: generico, personale, sensibile, giudiziario)
Riservatezza	Livello di conoscibilità del contenuto (Ad esempio: pubblico, interno, riservato)

I metadati di un contenuto variano in funzione della "struttura metadati di contenuto". Per ogni singolo attributo saranno definite le seguenti caratteristiche:

- Tipologia (es. numerico, data, alfanumerico, lista, etc)
- Obbligatorio/Facoltativo
- Ricercabile/Non ricercabile (cioè facente parte o meno delle **informazioni descrittive**)
- Monovalore/Multivalore

Metadati di Relazione

I metadati di Relazione raggruppano tutti quegli attributi la cui valorizzazione conterrà informazioni utili a mantenere le relazioni tra i contenuti: relazioni tra unità documentarie versionate o tra unità documentarie presenti in più unità archivistiche. Sono stati tratti dallo standard Dublin Core.

Attributo	Descrizione
isPartOf	Attributo dell'UD utilizzato per indicare se l'unità documentaria è contenuta in una unità archivistica o meno
hasPart	Attributo della UA utilizzato per elencare le unità documentarie che compongono l'unità archivistica e soggette a vincolo archivistico
requires	Attributo della UA utilizzato per elencare le unità documentarie collegate alla unità archivistica e soggette a sfoltimento
isVersionOf	Attributo dell'UD utilizzato, nel caso di rettifica per errore, per legare la nuova versione dell'unità con la versione precedente dell'unità
isFormatOf	Attributo dell'UD utilizzato, nel caso di rettifica per cambio formato di almeno una componente della unità documentaria, per legare la nuova versione di unità documentaria con la versione precedente

Torna al sommario

6.1.3 Formati

L'unità documentaria si compone di uno o più componenti che si presentano sotto forma di file fisici (sequenza di bit) a cui deve essere associato un formato.

Il sistema gestisce la conservazione di due gruppi di formati:

- **Garantiti**, ovvero i mimetype previsti dalle Regole Tecniche dell'allegato 2 (PDF/A, TIFF, JPG, XML, etc) nella versione vigente al momento della redazione del presente documento;
- **Custom**, ovvero eventuali ulteriori formati specificati negli accordi con i singoli produttori. Il sistema di conservazione non garantisce la conservazione a lungo termine di questi formati in quanto non previsti dall'allegato 2 delle Regole Tecniche.

Per ciascun formato i relativi visualizzatori sono registrati nel sistema con le seguenti informazioni:

- Formato del file
- Versione del formato
- Nome visualizzatore
- Produttore
- Sistema Operativo
- Licenza ed eventuale scadenza

Per ogni produttore sono indicati tutti i formati gestiti. Nel caso di formati Custom è a carico del soggetto produttore fornire i visualizzatori, nel rispetto dei diritti di proprietà intellettuale ed eventuali restrizioni nell'utilizzo del software.

Torna al sommario

6.2 Pacchetto di versamento

I pacchetti di Versamento sono concordati, nell'ambito delle pattuizioni contrattuali stipulate con i singoli soggetti produttori, relativamente alle specifiche operative e alle modalità di descrizione e di versamento nel sistema di conservazione delle unità documentarie e unità archivistiche oggetto di conservazione.

Il servizio è disponibile in modalità web service. Effettua i controlli di validazione del pacchetto e fornisce in modalità sincrona il rapporto di versamento al produttore.

Il processo di conservazione che InfoCamere ha previsto si basa sulla possibilità di gestire il versamento da parte del produttore in due fasi: versamento anticipato e versamento in archivio.

La prima fase riguarda la spedizione in conservazione delle unità documentarie quando, anche se sono nell'archivio corrente nella fase attiva del loro ciclo di vita, queste hanno o si vuole abbiano le caratteristiche di non modificabilità e integrità come indicato dal DPCM 13-11-2014 sulla formazione del documento informatico all'art. 3 comma 4,5,6)

La seconda fase consiste nella spedizione delle unità archivistiche quando queste sono nella loro forma stabile e definitiva (principalmente fascicoli chiusi, aggregazioni documentali chiuse, serie annuali, etc.). Prerequisito per questo versamento è che siano state precedentemente versate le relative unità documentarie.

Per gestire al meglio questa modalità di conservazione i pacchetti di versamento potranno consistere in:

- unità documentaria
  È il pacchetto di versamento principale, composto da tutte le componenti della Unità documentaria, da un file di metadati e dal file indice.

- unità archivistica
  È il pacchetto di versamento utilizzato per gestire i fascicoli e tutte le altre aggregazioni documentali. E' composto da un file di metadati che elenca le unità documentarie che compongono l'unità archivistica e dal file indice.

- rettifica unità documentaria
  E' prevista la funzione di correzione delle informazioni della unità documentaria. Questo servizio permette di adeguare una unità documentaria in cui sono avvenute delle modifiche sui documenti e/o sui metadati; devono essere versate tutte le componenti e i metadati aggiornati della Unità documentaria. L'unità documentaria rettificata viene mantenuta nel sistema di conservazione e verrà gestito il legame tra le versioni.

La struttura dell'indice del Pacchetto di versamento è stata definita considerando lo standard UniSincro. Le informazioni contenute nell'indice sono raggruppate con la stessa logica: Self Description, VDC, Filegroup, Process.

L'indice del pacchetto di versamento e il rapporto di versamento vengono mantenuti anche nel sistema di conservazione.

Una volta che i pacchetti di versamento sono stati acquisiti, questi vanno a comporre i pacchetti di archiviazione (AIP).

Torna al sommario

6.3 Pacchetto di archiviazione

I pacchetti di archiviazione vengono creati utilizzando più pacchetti di versamento con i seguenti criteri:

- pacchetti di versamento dello stesso produttore
- pacchetti di versamento omogenei in termini di informazioni. Tipicamente saranno gli attributi "codice sistema versante", "struttura metadati contenuto" e "tempo di conservazione", illustrati nel paragrafo 6.1, che verranno concordati come criterio di raggruppamento dei pacchetti di versamento al produttore.

Il pacchetto di archiviazione viene generato dal sistema di conservazione a conclusione del processo di acquisizione e presa in carico di più pacchetti di versamento in base a criteri che vengono illustrati nel capitolo 7.

Ciascun livello archivistico, così come previsto dalla modalità descrittiva multi livellare degli standard internazionali riconosciuti dalla comunità scientifica archivistica (v. ISAD(G)/EAD), diverrà esso stesso oggetto di descrizione.

Sempre a livello archivistico, sarà garantito il nesso tra Contenitore (Unità archivistica) e contenuto (Unità documentaria).

Il pacchetto di archiviazione è composto da molteplici pacchetti di versamento e dall'indice del pacchetto di archiviazione.

L'indice del Pacchetto di archiviazione è conforme alle specifiche definite nell'allegato 4 delle Regole Tecniche (standard UniSincro). E' un file xml che contiene, per ciascun pacchetto informativo, le informazioni recuperate dai pacchetti di versamento trasmessi dal produttore e quelle generate nel corso del processo di conservazione.

L'indice del pacchetto di archiviazione permette di gestire le **informazioni sull'impacchettamento**. Di seguito si descrive la collocazione delle altre informazioni dei pacchetti informativi conservati.

Di seguito la rappresentazione grafica del file indice Unisincro, una spiegazione delle sezioni che lo compongono e delle informazioni in esse contenute.

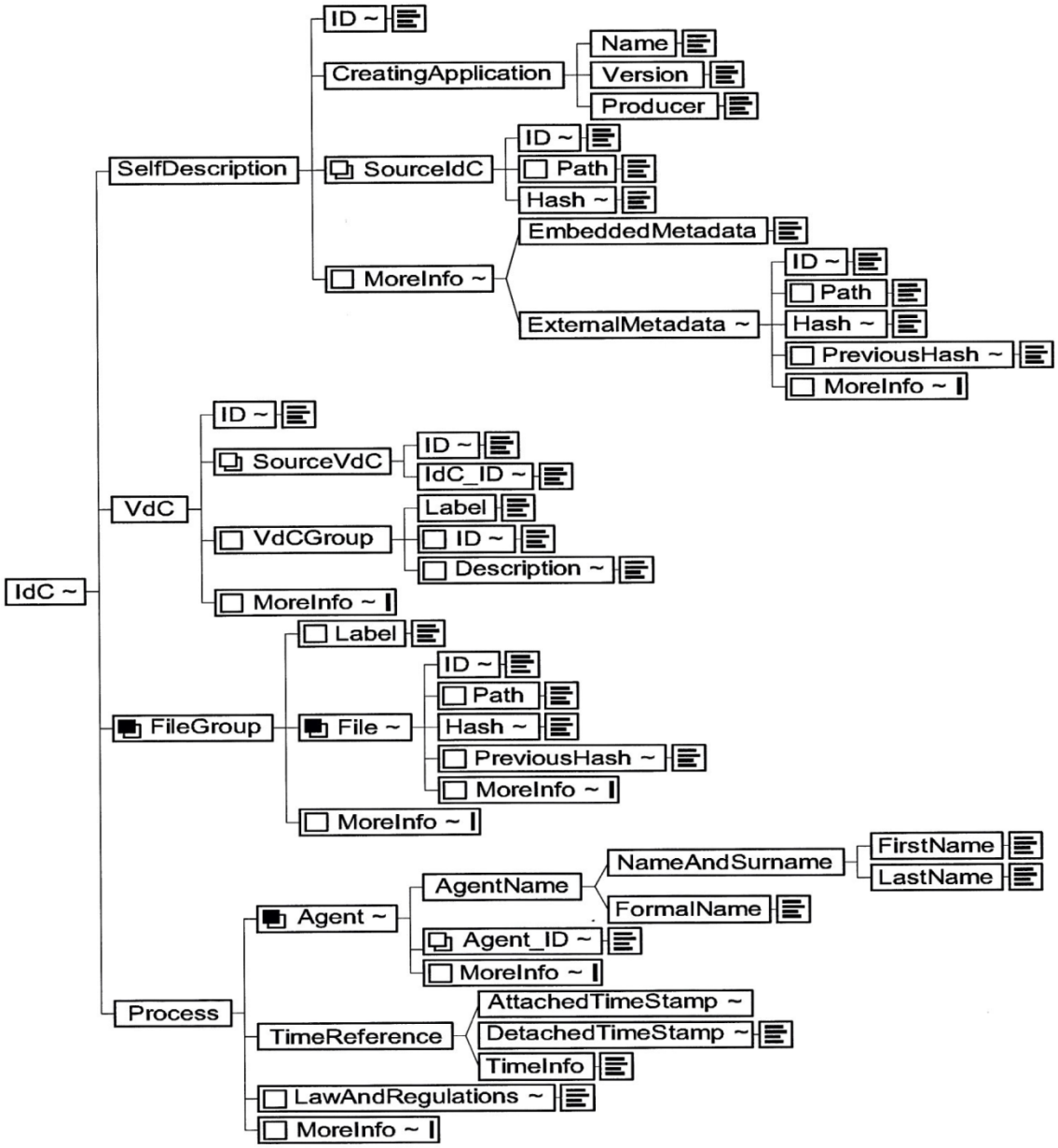


Figura 5 Struttura indice del pacchetto di archiviazione

Torna al sommario

6.3.1 Self description / VdC

Queste sezioni definiscono il pacchetto di archiviazione. Contengono **informazioni sulla conservazione** derivate dal processo di conservazione, ad esempio informazioni sulla provenienza e sulla creazione del pacchetto di archiviazione. La sezione VdC prevede una sezione “MoreInfo” embedded contenente informazioni sul produttore.

```
<sincro:SelfDescription>
    <sincro:ID></sincro:ID>
    <!-- Identificativo dell'indice dell'AIP dato dal Sistema -->
    <sincro:CreatingApplication>
        <sincro:Name></sincro:Name
        <!-- Nome del Sistema di Conservazione -->
        <sincro:Version></sincro:Version>
        <!-- Versione del Sistema di Conservazione -->
        <sincro:Producer></sincro:Producer>
        <!-- Produttore del Sistema di Conservazione -->
    </sincro:CreatingApplication>
    <sincro:SourceIdC>
        <sincro:ID></sincro:ID>
        <!-- Identificativo dell'indice dell'AIP Sorgente dato dal Sistema -->
        <sincro:Path></sincro:Path>
        <!-- Informazione sulla localizzazione del SourceIdC -->
        <sincro:Hash sincro:function="SHA256"></sincro:Hash>
        <!-- Hash dell'indice dell'AIP sorgente -->
    </sincro:SourceIdC>
</sincro:SelfDescription>
```

Figura 6 Struttura SelfDescription

```
<sincro:VdC>
    <sincro:ID></sincro:ID>
    <!-- Identificativo dell'AIP dato dal Sistema -->
    <sincro:SourceVdC>
        <sincro:ID></sincro:ID>
        <!-- Identificativo dell'AIP Sorgente dato dal Sistema -->
        <sincro:IdC_ID></sincro:IdC_ID>
        <!-- Identificativo dell'indice dell'AIP Sorgente dato dal Sistema -->
    </sincro:SourceVdC>
    <sincro:MoreInfo sincro:XMLScheme="unisincro_producerInfo.xsd">
        <sincro:EmbeddedMetadata>
            <ProducerInfo xmlns="">
                <ProducerCode></ProducerCode>
                <!-- Codice Produttore proprietario dell'AIP -->
                <ProducerType></ProducerType>
                <!-- Tipo Produttore proprietario dell'AIP -->
                <ProducerDen></ProducerDen>
                <!-- Descrizione Produttore proprietario dell'AIP -->
            </ProducerInfo>
        </sincro:EmbeddedMetadata>
    </sincro:MoreInfo>
</sincro:VdC>
```

Figura 7 Struttura VdC

Torna al sommario

6.3.2 FileGroup

Esistono tante sezioni FileGroup quante sono le Unità archivistiche o le Unità documentarie conservate nel pacchetto di archiviazione.

La sezione FileGroup prevede una sezione "MoreInfo" in forma embedded contenente **informazioni sulla conservazione** dell'unità conservata.

All'interno del FileGroup esistono tante sezioni File quante sono le componenti della Unità conservata:

- Nel caso di Unità documentarie le componenti presenti nell'equivalente pacchetto di versamento saranno archiviate in tante sezioni file; avremo quindi un file per la componente principale, tanti file quanti sono gli eventuali allegati e un file per i metadati (con le **informazioni sulla conservazione).** Vengono poi aggiunti altri tre file: l'indice del pacchetto di versamento, il rapporto di versamento ed il file delle informazioni descrittive generato dal sistema.
- Nel caso di Unità archivistica avremo il file di metadati, fornito nel pacchetto di versamento e contenente le **informazioni sulla conservazione,** l'indice del pacchetto di versamento, il rapporto di versamento e il file delle informazioni descrittive generato dal sistema.

La sezione File prevede una sezione "MoreInfo" in forma embedded contenente **informazioni sulla rappresentazione** della componente.

```
<sincro:FileGroup>
    <sincro:Label></sincro:Label>
    <!-- Etichetta Classe di appartenenza del contenuto -->
    <sincro:File sincro:encoding="binary" sincro:format="" sincro:extension="" >
        <sincro:ID></sincro:ID>
        <!-- Identificativo della componente dato dal Sistema -->
        <sincro:Path></sincro:Path>
        <!-- Informazione sulla localizzazione della componente -->
        <sincro:Hash sincro:function="SHA256"></sincro:Hash>
        <!-- Impronta della componente -->
        <sincro:MoreInfo sincro:XMLScheme="unisincro_fileInfo.xsd">
            <sincro:EmbeddedMetadata>
                <FileInfo xmlns="">
                    <Type></Type>
                    <!-- Tipologia di componente -->
                    <ShowOrder></ShowOrder>
                    <!-- Progressivo componente -->
                    <Description></Description>
                    <!--Descrizione della componente-->
                    <Language></Language>
                    <!-- Lingua componente -->
                    <Signed></Signed>
                    <!-- Indica se la componente e' firmata o meno -->
                    <Encrypted></Encrypted>
                    <!-- Indica se la componente e' criptata o meno -->
                    <EncryptedKeyId function=""></EncryptedKeyId>
                    <!-- Identifitivo della chiave di decriptazione -->
                    <FullFormat></FullFormat>
                    <!-- Formato completo della componente -->
                    <FullExtention></FullExtention>
                    <!-- Estensione completa della componente -->
                </FileInfo>
            </sincro:EmbeddedMetadata>
        </sincro:MoreInfo>
    </sincro:File>
    <sincro:MoreInfo sincro:XMLScheme="unisincro_fileGroupInfo.xsd">
            <sincro:EmbeddedMetadata>
                <FileGroupInfo xmlns="">
                    <SourceContentId></SourceContentId>
                    <!-- Identificativo del contenuto dato dall'applicativo Sorgente -->
                    <ForeverContentId></ForeverContentId>
                    <!-- Identificativo del contenuto dato dal Sistema -->
                    <ContentType></ContentType>
                    <!-- Tipologia di contenuto -->
                    <SubmissionTime></SubmissionTime>
                    <!-- Data in cui il contenuto e' stato versato -->
                    <RetentionTime></RetentionTime>
                    <!-- Periodo di retention del contenuto -->
                </FileGroupInfo>
            </sincro:EmbeddedMetadata>
        </sincro:MoreInfo>
</sincro:FileGroup>
```

Figura 8 Struttura FileGroup

Torna al sommario

6.3.3 Process

La sezione contiene ulteriori **Informazioni sulla conservazione** derivate dal processo di conservazione: identificativo del responsabile del servizio di conservazione, riferimento temporale.

La sezione Process prevede una sezione "MoreInfo" in forma embedded contenente **informazioni sulla conservazione** che precisa come il riferimento temporale sia generato pochi istanti prima dell'applicazione della marca temporale attached.

```
<sincro:Process>
        <sincro:Agent sincro:role="PreservationManager" sincro:type="person">
            <sincro:AgentName>
                <sincro:NameAndSurname>
                    <sincro:FirstName></sincro:FirstName>
                    <!-- Nome Responsabile Servizio Conservazione -->
                    <sincro:LastName></sincro:LastName>
                    <!-- Cognome Responsabile servizio Conservazione -->
                </sincro:NameAndSurname>
            </sincro:AgentName>
            <sincro:Agent_ID sincro:scheme="TaxCode"></sincro:Agent_ID>
            <!-- Codice Fiscale Responsabile Servizio Conservazione -->
        </sincro:Agent>
        <sincro:TimeReference>
            <sincro:AttachedTimeStamp sincro:normal=""></sincro:AttachedTimeStamp>
            <!-- Data di Creazione dell'indice dell'AIP -->
        </sincro:TimeReference>
        <sincro:MoreInfo sincro:XMLScheme="unisincro_timeReferenceInfo.xsd">
            <sincro:EmbeddedMetadata>
                <TimeReferenceInfo xmlns="">
                    <AttachedTimeStampInfo></AttachedTimeStampInfo>
                    <!-- Informazioni aggiuntive sulla marcatura temporale dell'indice dell'AIP -->
                </TimeReferenceInfo>
            </sincro:EmbeddedMetadata>
        </sincro:MoreInfo>
</sincro:Process>
```

Figura 5 Struttura Process

Torna al sommario

6.4 Pacchetto di distribuzione

Il Pacchetto di distribuzione viene generato dal sistema di conservazione, in risposta ad una richiesta da parte dell'Utente, a partire dai Pacchetti di archiviazione conservati ed è finalizzato a mettere a disposizione, in una forma idonea alle specifiche esigenze di utilizzo, gli oggetti sottoposti a conservazione.

Spesso non c'è coincidenza tra i DIP e gli AIP perché l'utente potrebbe:

- richiedere una selezione di unità documentarie/unità archivistiche presenti nel pacchetto di archiviazione
- richiedere unità documentarie/unità archivistiche presenti in più pacchetti di archiviazione

Per gestire l'interoperabilità tra sistemi di conservazione possono essere prodotti pacchetti di distribuzione coincidenti con i pacchetti di archiviazione.

Nel caso più completo di pacchetto di distribuzione si troveranno le seguenti informazioni per ciascun pacchetto informativo:

- gli oggetti dati della unità documentaria/unità archivistica
- le informazioni sulla rappresentazione comprensivi dei software di visualizzazione
- le informazioni di conservazione (i metadati)
- l'indice di conservazione firmato e marcato
- l'indice di versamento
- il rapporto di versamento
- le informazioni sulla richiesta di distribuzione
- il riferimento temporale relativo alla sua creazione a meno di accordi con il produttore per l'utilizzo di una marca temporale.
- I documenti attestanti eventuali precedenti conservazioni presso altri soggetti conservatori

Il pacchetto di distribuzione viene fornito attraverso una modalità sincrona, descritta nei paragrafi 7.6 e 8.2 e può essere sottoscritto digitalmente nei casi previsti dall'art. 7, comma 1, lett. d) Regole Tecniche.

Torna al sommario

7 Il processo di conservazione

Il processo di conservazione inizia in seguito alla ricezione della copia sottoscritta del contratto di affidamento del servizio di conservazione da parte del soggetto produttore

Si compone di due processi distinti:

- il versamento dei pacchetti informativi da parte del produttore che è un processo sincrono;
- l'archiviazione, ovvero la presa in carico da parte del conservatore delle risorse digitali per la loro trasformazione o il loro inserimento nell'archivio digitale legale, che è un processo asincrono.

Il processo di versamento prevede:

- l'acquisizione del SIP e l'autenticazione del produttore. La funzione di acquisizione dei versamenti può rappresentare un trasferimento legale della custodia del contenuto informativo di un pacchetto di versamento e questo comporta l'imposizione di controlli da parte del conservatore;
- la verifica del SIP da parte del conservatore;
- la generazione di un rapporto di versamento o di un rifiuto del versamento, nel caso in cui si riscontrino delle anomalie, e conseguente comunicazione al produttore.

Il processo di archiviazione prevede una procedura unica per tutti i produttori che affidano a InfoCamere il servizio di conservazione con due fasi:

- la gestione dei dati e l'archiviazione del SIP nel sistema di conservazione (generazione AIU)
- la generazione del pacchetto di archiviazione (AIP)

Torna al sommario

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

Il processo di versamento viene illustrato nella figura seguente e dettagliato nei paragrafi 7.1, 7.2, 7.3 e 7.4.

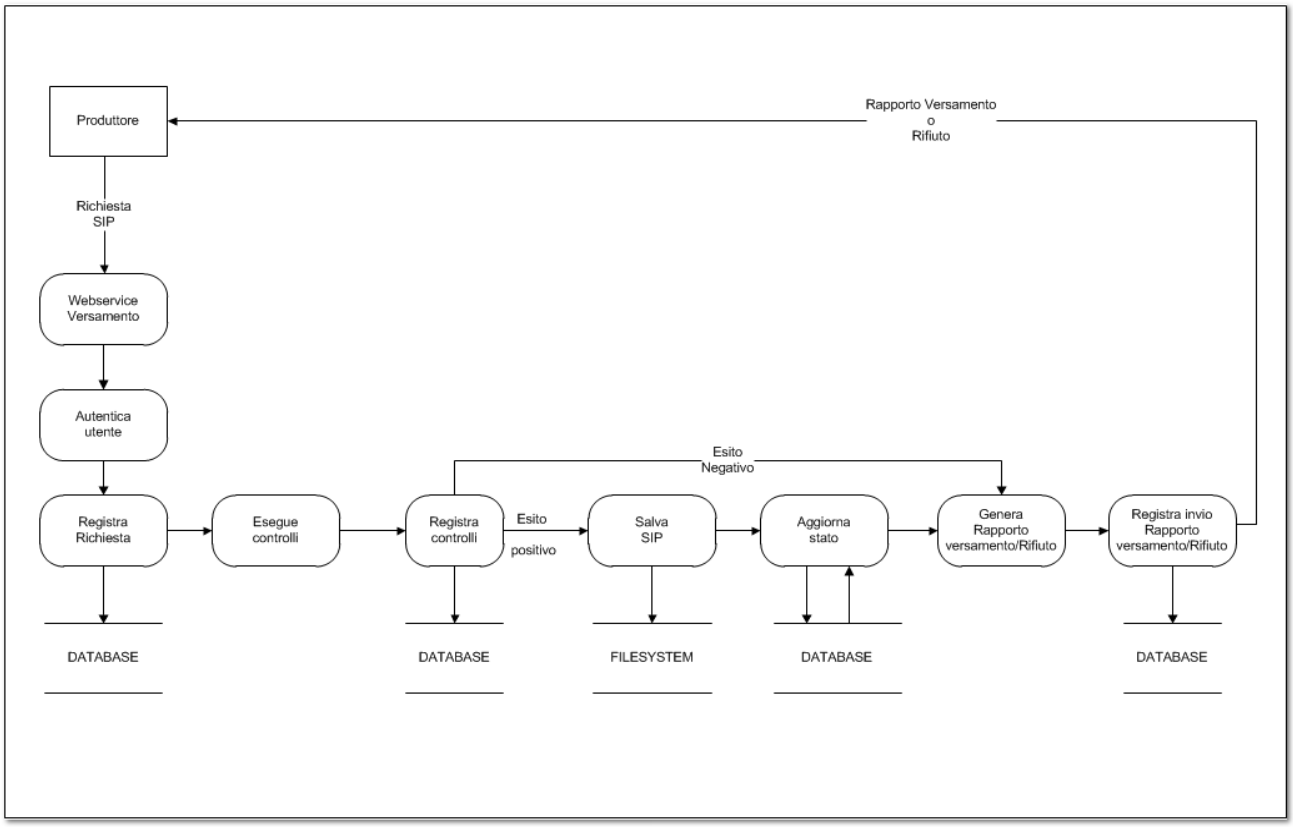


Figura 6 Acquisizione pacchetto di versamento

L'acquisizione delle diverse tipologie di pacchetti di versamento, indicate nel paragrafo 6.2 "pacchetti di versamento", avviene attraverso l'utilizzo di un web service. Non vengono previsti versamenti tramite supporti fisici e utilizzi di posta elettronica certificata.

Per ciascun produttore, le tipologie documentarie previste saranno dettagliate nell'ambito delle pattuizioni contrattuali stipulate con i singoli soggetti produttori.

Ad ogni pacchetto di versamento acquisito viene assegnato un identificativo univoco ed entra nella registrazione di log come indicato nel paragrafo 8.4 "procedure di gestione ed evoluzione" e ciò permetterà il controllo del sistema di conservazione come indicato nel paragrafo 9.1 "procedure di monitoraggio".

Per ogni pacchetto di versamento viene registrato in un record di log l'insieme delle informazioni che identificano la richiesta di versamento.

La stessa operatività è presente anche in tutti gli altri passi del processo di conservazione, illustrati nei paragrafi successivi, e permette con il tracciamento di tutte le fasi del processo l'analisi e il ripristino di eventuali criticità sorte nel trattamento dei pacchetti informativi.

Torna al sommario

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

Il web service esegue per tutti i pacchetti di versamento ricevuti i seguenti controlli obbligatori e bloccanti:

- l'identificazione del produttore
  la verifica consiste nell'autenticare il software versante, attraverso la verifica della firma apposta al file indice del pacchetto di versamento e nell'accertare la congruenza dello stesso con l'identificazione del produttore contenuta nel pacchetto di versamento.

- la conformità dell'Indice del pacchetto di versamento allo schema stabilito dal sistema di conservazione

- l'univocità degli identificativi dei contenuti versati.
  Ogni unità documentaria e unità archivistica devono poter essere univocamente identificate a livello di soggetto produttore

- la conformità delle tipologie documentarie che devono essere congruenti con quanto previsto nell'ambito delle pattuizioni contrattuali stipulate con i singoli soggetti produttori

- la conformità dei metadati che devono essere congruenti con le "strutture metadati contenuto" indicate nell'ambito delle pattuizioni contrattuali stipulate con i singoli soggetti produttori. Viene controllata in particolare la validità delle relazioni tra contenuti e la presenza dei metadati concordati come obbligatori

- l'integrità dei componenti verificando per ogni file versato che l'impronta fornita dal produttore coincida con quella calcolata dal sistema di conservazione.

- il controllo di ammissibilità dei formati
  Si verifica che i formati spediti siano tra quelli indicati nell'ambito delle pattuizioni contrattuali stipulate con i singoli soggetti produttori

- il controllo di conformità dei formati
  Si verifica che i formati dei file siano conformi a quanto dichiarato

Eventuali altri controlli opzionali sui pacchetti di versamento possono essere concordati con il produttore (es. verifica firma digitale). L'esecuzione ed esito di tali controlli dipende da quanto previsto nelle pattuizioni contrattuali.

Per ogni pacchetto di versamento viene registrato in un record di log l'elenco dei controlli effettuati ed il loro esito.

Torna al sommario

7.2.1 Riservatezza documenti e metodi di crittografia

- Per ogni contenuto versato il sistema permetterà al soggetto produttore di indicare il livello di privacy: Generico/Personale/Sensibile/Giudiziario.

- Per ogni contenuto versato il sistema permetterà al soggetto produttore di indicare il livello di riservatezza: Pubblico/Interno/Riservato.

- È in carico al soggetto produttore la criptazione o codifica dei contenuti (file e metadati):

    - nei casi in cui questo sia previsto dalla norma, tipicamente per i documenti contenenti informazioni sensibili o giudiziarie come indicato dall'art. 22 del codice della privacy (D.Lgs 196/2003), visto che questo obbligo deve iniziare dalla formazione del documento ed essere garantito per tutto il ciclo di vita del documento informatico
    - Nei casi in cui il produttore ha dei documenti riservati, compatibilmente con le norme vigenti.

- Nel caso in cui il soggetto produttore effettui il versamento in conservazione di un contenuto criptato dovrà segnalarlo al sistema di conservazione utilizzando un apposito metadato. Il soggetto produttore deve fornire le informazioni necessarie per identificare metodologia e chiave di criptazione utilizzata.

- InfoCamere si riserva di accettare, nell'ambito delle pattuizioni contrattuali, le seguenti tipologie di contenuto:

    - Contenuti con livello di privacy 'Sensibile' e 'Giudiziario'
    - Contenuti con livello di riservatezza 'Riservato'
    - Contenuti criptati

- È previsto che i canali di comunicazione tra soggetto produttore e sistema di conservazione siano criptati tramite l'uso di connessioni SSL/HTTPS.

Torna al sommario

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

Nel caso di esito positivo dei controlli indicati nel paragrafo 7.2 il web service produce un rapporto di versamento in formato XML contenente:

- identificativo del SIP a cui si riferisce il rapporto di versamento

- La lista dei contenuti versati con il SIP e le relative impronte
- Gli identificativi delle unità documentarie / archivistiche assegnati dal sistema di conservazione (id unità conservata)
- il riferimento temporale relativo alla creazione del rapporto, a meno di accordi con il produttore per l'utilizzo di una marca temporale attached.
- L'accettazione del pacchetto di versamento

Il rapporto di versamento viene conservato nel sistema di conservazione associato al relativo pacchetto di versamento e può essere consultato all'interno dei pacchetti di distribuzione.

Per ogni pacchetto di versamento accettato vengono registrati i seguenti record di log:

- Ricezione del pacchetto di versamento
- Controlli eseguiti sul pacchetto di versamento
- Salvataggio e cambio stato del pacchetto di versamento
- Invio del rapporto di versamento

Torna al sommario

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

Nel caso di esito negativo dei controlli indicati nel paragrafo 7.2 il web service fornisce la seguente risposta:

- l'identificativo del SIP a cui si riferisce la comunicazione delle anomalie;
- la lista dei contenuti versati con il SIP e le relative impronte;
- il riferimento temporale relativo alla sua creazione a meno di accordi con il produttore per l'utilizzo di una marca temporale attached;
- il rifiuto del pacchetto di versamento e l'anomalia riscontrata.

In caso di rifiuto del pacchetto di versamento, Non viene conservato il pacchetto di versamento e la relativa comunicazione nel caso questo abbia esito negativo.

Per ogni pacchetto di versamento rifiutato vengono registrati i seguenti record di log:

- Ricezione del pacchetto di versamento

- Controllo che ha causato il rifiuto del pacchetto di versamento

- Invio della comunicazione di rifiuto del pacchetto di versamento

Torna al sommario

7.5 Preparazione e gestione del pacchetto di archiviazione

Il processo di archiviazione è suddivisibile in due fasi che vengono illustrate utilizzando i due seguenti schemi grafici.

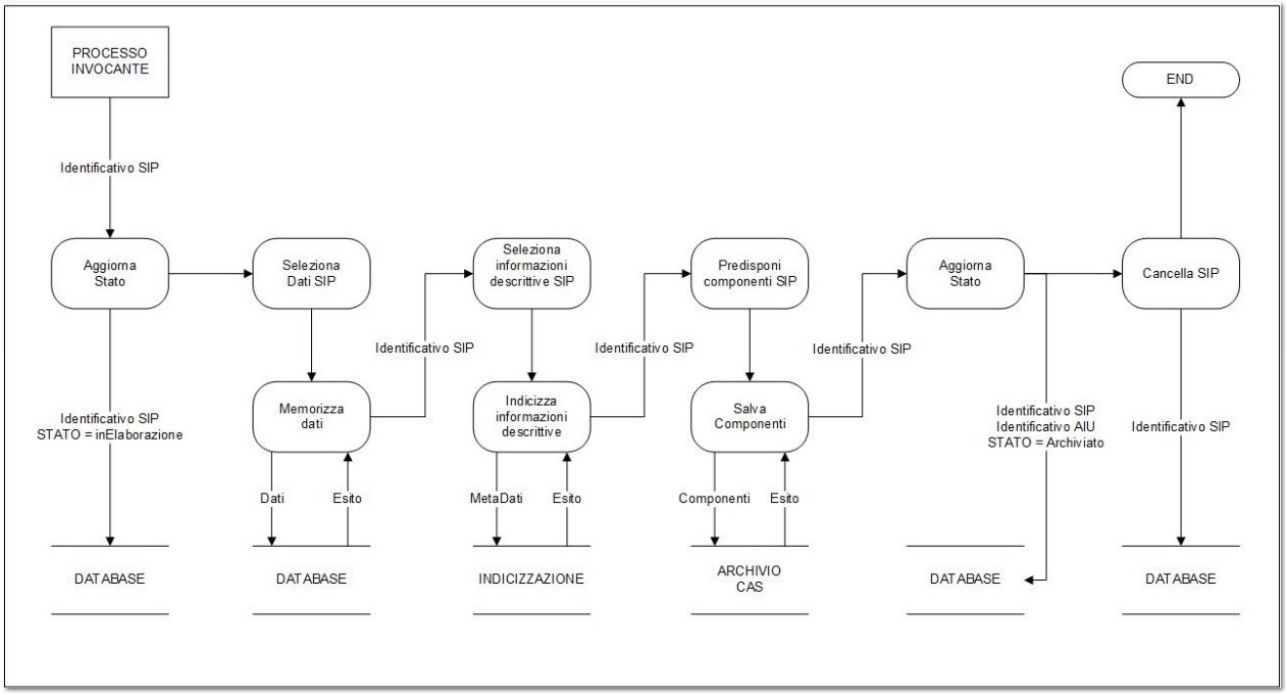


Figura 11 Pacchetto di archiviazione - prima fase

La prima fase consiste nel consolidare il SIP nel sistema di conservazione. Per ogni SIP, generato il rapporto di versamento, verranno effettuate queste operazioni:

- memorizzazione delle informazioni del SIP nel database. Nel database vengono registrate tutte le informazioni necessarie per la gestione dei dati; vengono quindi utilizzate le principali informazioni dei metadati e vengono collegate alle informazioni necessarie per i sistemi di indicizzazione e l'archivio CAS.

- recupero delle informazioni descrittive e inserimento nel sistema di indicizzazione. Per ogni "struttura metadati contenuto" vengono selezionati gli attributi che sono oggetto di ricerca e forniti al sistema di indicizzazione.

- archiviazione dei componenti nell'archivio CAS. Tutti gli oggetti dati presenti nel SIP e il rapporto di versamento vengono salvati nel supporto dedicato per la conservazione.

- Consolidamento dell'acquisizione del SIP nel sistema di conservazione. Utilizzando la terminologia OAIS il pacchetto informativo creato è un AIU (Archival Information Unit), considerato sottotipo del pacchetto di archiviazione.

- Cancellazione delle informazioni del SIP, intendendo con questa operazione la cancellazione delle informazioni registrate su supporti diversi da quelli di riferimento del sistema di conservazione (in genere file system).

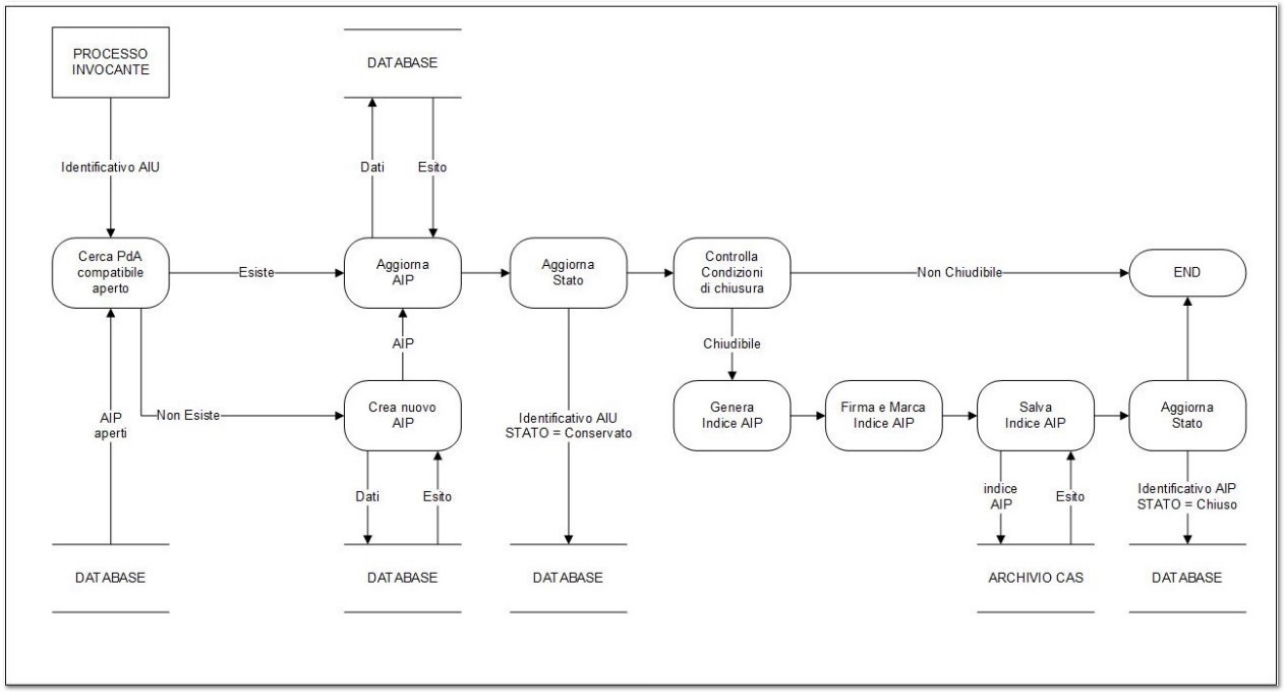


Figura 12 Pacchetto di archiviazione - seconda fase

Nella seconda fase viene creato il pacchetto di archiviazione (AIP) che, come indicato nel paragrafo 6.3, contiene più pacchetti di versamento, consolidati nella prima fase del processo sotto forma di AIU.

I criteri di raggruppamento sono quelli di essere appartenenti allo stesso produttore e secondariamente di avere una omogeneità di informazioni (tipicamente medesimo "codice sistema versante", "struttura metadati contenuto" e "tempo di conservazione").

In base a tali criteri viene effettuata l'associazione del pacchetto informativo con l'AIP relativo nel caso di AIP già esistente, altrimenti ne viene creato uno nuovo. La creazione dell'indice del pacchetto di archiviazione avviene seguendo lo standard UniSincro e le indicazioni contenute nel paragrafo 6.3 del manuale di conservazione. Si precisa che tutti i pacchetti di archiviazione sono identificati univocamente all'interno del sistema di conservazione.

Per gestire la chiusura del pacchetto di archiviazione si adottano i seguenti criteri:

- Numerosità
  Indica il numero massimo di unità documentarie/unità archivistiche per l'AIP
- Dimensione
  Indica la dimensione massima che può raggiungere l'AIP
- Durata
  Indicare il limite massimo di giorni che un AIP può rimanere aperto (in genere mai superiore all'anno)
- Data limite conservazione
  Si tratta di un metadato impostabile nei pacchetti di versamento dal produttore per indicare la data entro la quale serve conservare l'AIP. Questo parametro è utilizzato per alcune Tipologie documentarie, come ad esempio le fatture, per le quali la norma richiede il completamento della conservazione entro certe tempistiche.

Quando si raggiunge uno dei criteri di chiusura per il singolo pacchetto di archiviazione verranno eseguiti i seguenti passi:

- Creazione dell'indice del pacchetto di archiviazione
- firma dell'indice del pacchetto di archiviazione da parte del responsabile del servizio di conservazione
- apposizione della marca temporale all'indice del pacchetto di archiviazione
- archiviazione dell'indice dell'AIP nell'archivio CAS
- memorizzazione di alcune informazioni del pacchetto di archiviazione nel database

Il produttore, con un apposito web service, ha la possibilità di conoscere lo stato di conservazione di ogni contenuto versato, che restituisce l'informazione del pacchetto di archiviazione in cui è stato inserito e il suo stato.

Anche questo processo mantiene nei log tutti i singoli passi sopradescritti e il loro esito.

Nel caso di operazioni manuali sui pacchetti di archiviazione, necessari per ripristinare alcune fasi andate in errore, sono tracciati in modo opportuno tutti gli interventi.

Questo permette nelle analisi periodiche di verificare la correttezza di tutti i pacchetti di archiviazione creati.

Torna al sommario

7.6 Preparazione e gestione del pacchetto di distribuzione ai fini dell'esibizione

Il processo di distribuzione, illustrato nella figura seguente, avviene attraverso due web services:

- il web service di ricerca
- il web service di generazione DIP

L'accesso a questi servizi avviene mediante autenticazione dell'utente, che consiste

- nella verifica che la firma apposta al file indice della richiesta di ricerca e/o della richiesta di pacchetto di distribuzione sia congruente l'identificazione dell'utente
- nella verifica che l'utente sia abilitato ad accedere al contenuto richiesto

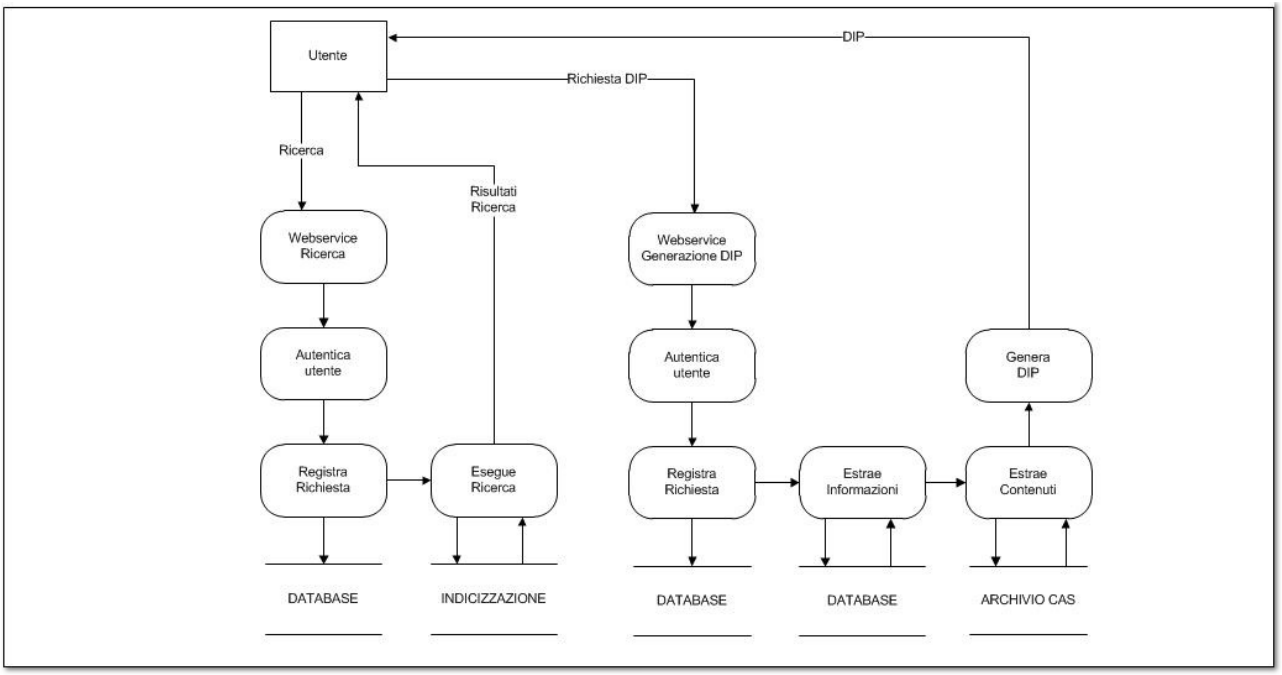


Figura 13 Generazione pacchetto di distribuzione

Il web service di ricerca accetta in input i dati da ricercare in funzione dei metadati delle informazioni descrittive, come definito nella "struttura metadati contenuto". Ricerca tali informazioni nel sistema di indicizzazione e fornisce le informazioni identificative di tutte le unità documentarie e unità archivistiche che contengono le informazioni ricercate.

L'utente, in base alle informazioni restituite dal servizio di ricerca, effettua una o più richieste di pacchetti di distribuzione attraverso il web service di generazione DIP.

E' possibile richiedere che nel pacchetto di distribuzione siano inclusi i visualizzatori necessari per l'esibizione delle componenti fornite.

Per tutte le componenti distribuite viene effettuata la verifica che l'impronta conservata nel pacchetto di archiviazione coincida con quella calcolata al momento della preparazione del pacchetto di distribuzione. I contenuti saranno resi disponibili in modalità sincrona e forniti attraverso un file zip.

Tutte le richieste vengono registrate nel log del sistema di conservazione, comprese le motivazioni di eventuali errori/rifiuti.

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 è realizzata con i servizi che forniscono i pacchetti di distribuzione. L'utente potrà chiedere copie di sicurezza o la restituzione dei propri dati solo per via telematica.
Non è prevista da parte del sistema di conservazione la fornitura su supporti rimovibili o tramite posta elettronica certificata.

In merito alla produzione delle copie sarà cura del soggetto produttore produrre le copie conformi e richiedere, quando necessario, la presenza di un pubblico ufficiale. L'attestazione di conformità, anche nel caso sia necessario un cambio di formato, rimarrà a carico del soggetto produttore. Il sistema di conservazione prevede appositi metadati per il tracciamento delle operazioni di copia e garantisce il legame tra le diverse versioni delle unità documentarie.

Torna al sommario

7.8 Scarto dei pacchetti di archiviazione

L'art. 9 comma 2, lett. k) delle Regole Tecniche stabilisce che deve essere effettuato lo scarto dal sistema di conservazione, alla scadenza dei termini di conservazione previsti dalla norma, dandone informativa al soggetto produttore.

Nei casi previsti dalle norme, è a carico del produttore fornire all'autorità di vigilanza competente la lista dei pacchetti di archiviazione da scartare. Il soggetto produttore, una volta ricevuto il nulla-osta provvede ad adeguare, se necessario, l'elenco di scarto alle decisioni dell'autorità.

Il produttore richiede lo scarto dei pacchetti di archiviazione, allegando eventuali documenti a comprova della autorizzazione.

Il processo di scarto provvede a:

- eliminare fisicamente, per ogni AIP gli AIU presenti nell'Archivio CAS, le informazioni descrittive presenti nel sistema di indicizzazione e le informazioni degli AIU presenti nel database che non siano essenziali per il tracciamento della operazione di scarto.
- mantenere l'indice del pacchetto di archiviazione scartato (contenente la lista delle Unità documentarie e delle Unità archivistiche cancellate)
- conservare richiesta di scarto con gli eventuali allegati
- registrare le informazioni sul processo di scarto

Torna al sommario

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

Come garanzia di interoperabilità e trasferibilità ad altri conservatori delle informazioni di un produttore conservate nel sistema di conservazione di InfoCamere è disponibile un pacchetto di distribuzione che coincide con il pacchetto di archiviazione; il pacchetto di distribuzione così prodotto utilizza lo standard UniSincro per la gestione dell'impacchettamento dei dati. La distribuzione di questi pacchetti avviene in modalità asincrona.

Nel contratto di affidamento del servizio di conservazione è previsto, nel caso di recesso del produttore o di cessazione della attività del soggetto conservatore, che i pacchetti di archiviazione siano disponibili al produttore in formato UniSincro sul sistema di conservazione per una adeguata finestra temporale definita nell'ambito delle pattuizioni contrattuali.

Il sistema di conservazione, progettato secondo lo standard OAIS, è altresì in grado di importare e archiviare pacchetti di distribuzione generati da altri sistemi e forniti secondo lo standard UniSincro, in base ad accordi con il soggetto produttore.

Torna al sommario

8 Il sistema di conservazione

8.1 Componenti Logiche

La figura che segue, realizzata sul modello OAIS di rappresentazione delle entità funzionali, schematizza dal punto di vista logico le principali relazioni tra i soggetti interessati al processo di conservazione e le componenti più significative del sistema di conservazione di InfoCamere.

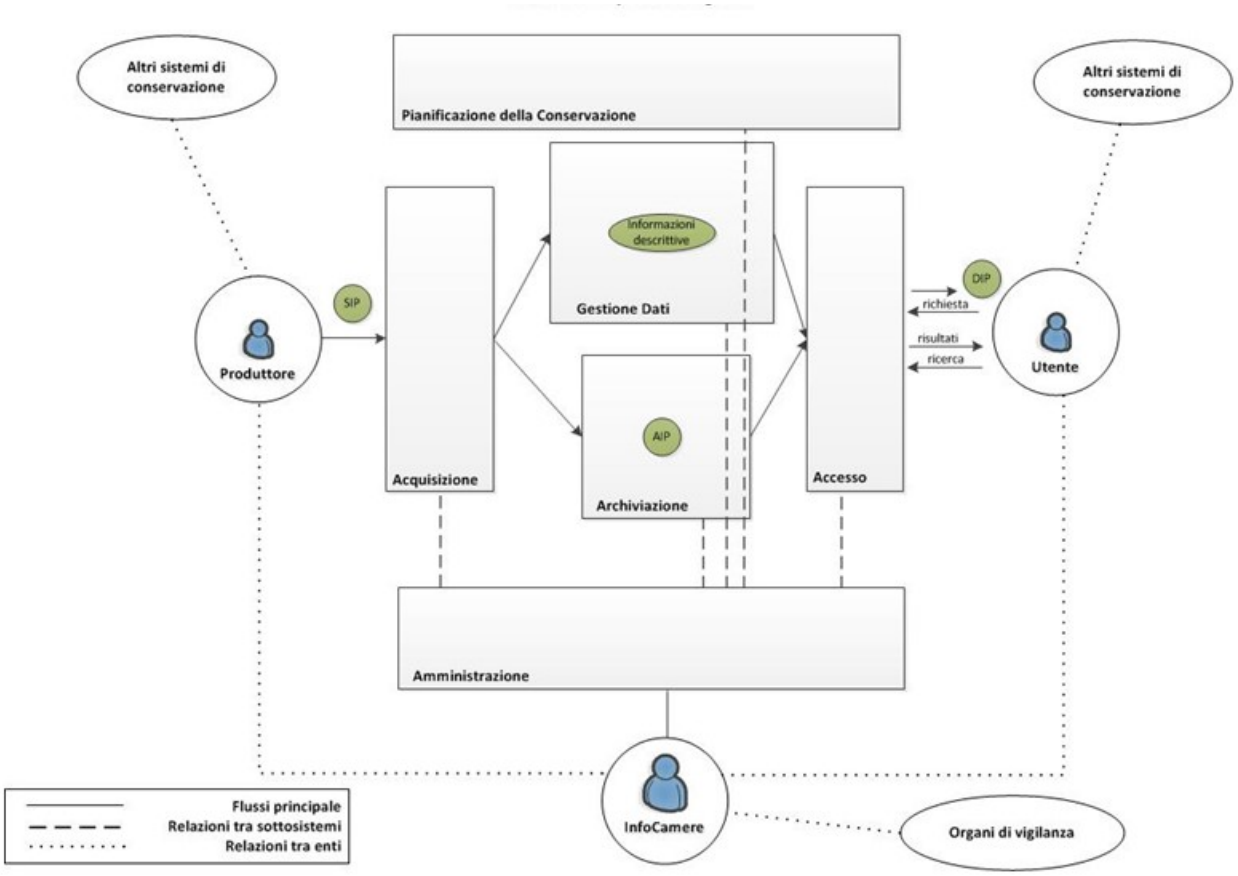


Figura 14 Schema componenti logiche

Per la descrizione dei ruoli di *Produttore, Utente, InfoCamere* e *Organi di vigilanza* si rimanda al Capitolo 5 del presente manuale.

La funzionalità di *Acquisizione* gestisce la fase di ricezione e presa in carico del processo di conservazione**:** ricezione e verifica dei *SIP* versati nel sistema dal soggetto produttore, generazione del rapporto di versamento, produzione dei relativi *AIP* e delle Informazioni descrittive associate.

La funzionalità di *Gestione Dati* prevede la memorizzazione, manutenzione e aggiornamento all'interno del sistema delle *Informazioni descrittive* necessarie a ricercare gli AIP (ricevute nella fase di *Acquisizione*) e dei dati necessari per la gestione dei pacchetti informativi.

La funzionalità di *Archiviazione* prevede la memorizzazione, migrazione dei supporti, backup, Disaster Recovery ed eliminazione (scarto) degli AIP conservati nel Sistema.

La funzionalità di *Amministrazione* governa l'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 ed il monitoraggio del sistema.

La funzionalità di *pianificazione della Conservazione* interviene 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 o da procedure strutturate. Si tratta di una serie di attività finalizzate a raccogliere informazioni, confrontarsi con la Comunità di riferimento, effettuare test e verifiche sugli oggetti conservati. Al termine di queste operazioni si ottengono indicazioni utili a mantenere il processo di conservazione aggiornato sia in relazione all'evoluzione tecnologica, sia alle esigenze della Comunità di riferimento (aggiornamento dei pacchetti informativi in base a nuovi standard, adeguamento del Software a nuove librerie, test su nuovi componenti hardware, etc).

La funzionalità di *accesso* gestisce la fase di generazione del DIP del processo di conservazione con cui l'utente può ricercare e ottenere gli oggetti conservati nel Sistema e le informazioni necessarie alla loro visualizzazione.

Al fine di garantire l'interoperabilità tra i sistemi di conservazione, *InfoCamere,* in base a quanto previsto dalle Regole Tecniche e secondo accordi con il *Produttore,* è in grado di ricevere da *altri sistemi di conservazione* pacchetti di versamento contenenti oggetti già sottoposti a conservazione presso un altro ente conservatore, e di generare pacchetti di distribuzione coincidenti con i pacchetti di archiviazione in modo da permetterne il versamento in altri Sistemi di conservazione.

Torna al sommario

8.2 Componenti Tecnologiche

Il sistema di conservazione è stato progettato e realizzato considerando quanto segue:

- deve garantire autenticità, integrità, affidabilità, leggibilità, reperibilità degli oggetti sottoposti a conservazione. Per questo motivo vengono impiegate tecnologie ampliamente testate, affidabili, utilizzate diffusamente in contesti professionali. Tutte le tecnologie utilizzate nel sistema garantiscono inoltre elevati livelli di sicurezza

- gli oggetti sottoposti a conservazione vengono mantenuti all'interno del sistema di conservazione per un lasso di tempo potenzialmente molto esteso. Per questo motivo sono utilizzare tecnologie in grado di offrire un elevato grado di maturità/stabilità, caratterizzate da un diffuso knowhow e un'ampia comunità di riferimento. Le tecnologie sono state scelte

tenendo in considerazione gli impatti legati ad aggiornamenti tecnologici e eventuali migrazione di dati

- la numerosità degli oggetti che il sistema di conservazione deve gestire è potenzialmente molto elevata. Per questo motivo sono utilizzate tecnologie che permettono la scalabilità del sistema di conservazione

- deve garantire la tracciabilità dei sui processi e la gestione/ripristino delle anomalie. Per questo motivo sono utilizzate tecnologie che garantiscono la conoscenza precisa di dove e come vengono memorizzati i dati. Si è evitato l'uso di tecnologie che prevedono l'uso di elevati livelli di astrazione o in cloud, le quali complicano la localizzazione esatta dei dati. I processi si avvalgono di un Business Process Manager che ne permette un'elevata tracciabilità

- deve garantire performance e livelli di servizio elevati. Per questo motivo sono state utilizzate tecnologie che garantiscono facilità di manutenzione, alta affidabilità e scalabilità

- deve avere una sostenibilità finanziaria nel tempo. Per questo motivo sono stati valutati i costi d'esercizio delle tecnologie impiegate

- deve tenere in attenta considerazione anche rischi legati a fattori esterni al soggetto produttore. Per questo motivo sono state privilegiate soluzioni che limitano la dipendenza da specifici fornitori e che implementano standard internazionali e/o si basano su software open source. Nei casi in cui si utilizzano tecnologie proprietarie, queste sono fornite da fornitori con ampia stabilità finanziaria

Per i motivi sopra esposti:

- Il software è scritto in Java: linguaggio open source, tra i più diffusi al mondo. Il software fa uso delle specifiche Java Enterprise e dei più diffusi e conosciuti standard, tra cui: EJB, JPA, JTA, SOAP, REST. Vengono utilizzati webserver e application server open source. Il software utilizza una componente di BPM in cui sono definiti flussi con notazioni basate su standard internazionali

- Si utilizza un database relazionale per la memorizzazione delle informazioni strutturate dei pacchetti informativi, in cui sono state definite strutture SQL standard e si è limitato al massimo l'uso di funzionalità proprietarie, al fine di massimizzarne la portabilità della base dati

- Un sistema di indicizzazione delle informazioni descrittive, basato su un software open source che è tra i leader mondiali in questo campo

- Un archivio CAS utilizzato per memorizzare gli AIP, che implementa i più elevati standard di sicurezza e garantisce una maggior sostenibilità e scalabilità rispetto ai filesystem tradizionali

La figura che segue descrive le principali componenti tecnologiche del sistema di conservazione con cui si realizzano le funzionalità logiche precedentemente descritte.

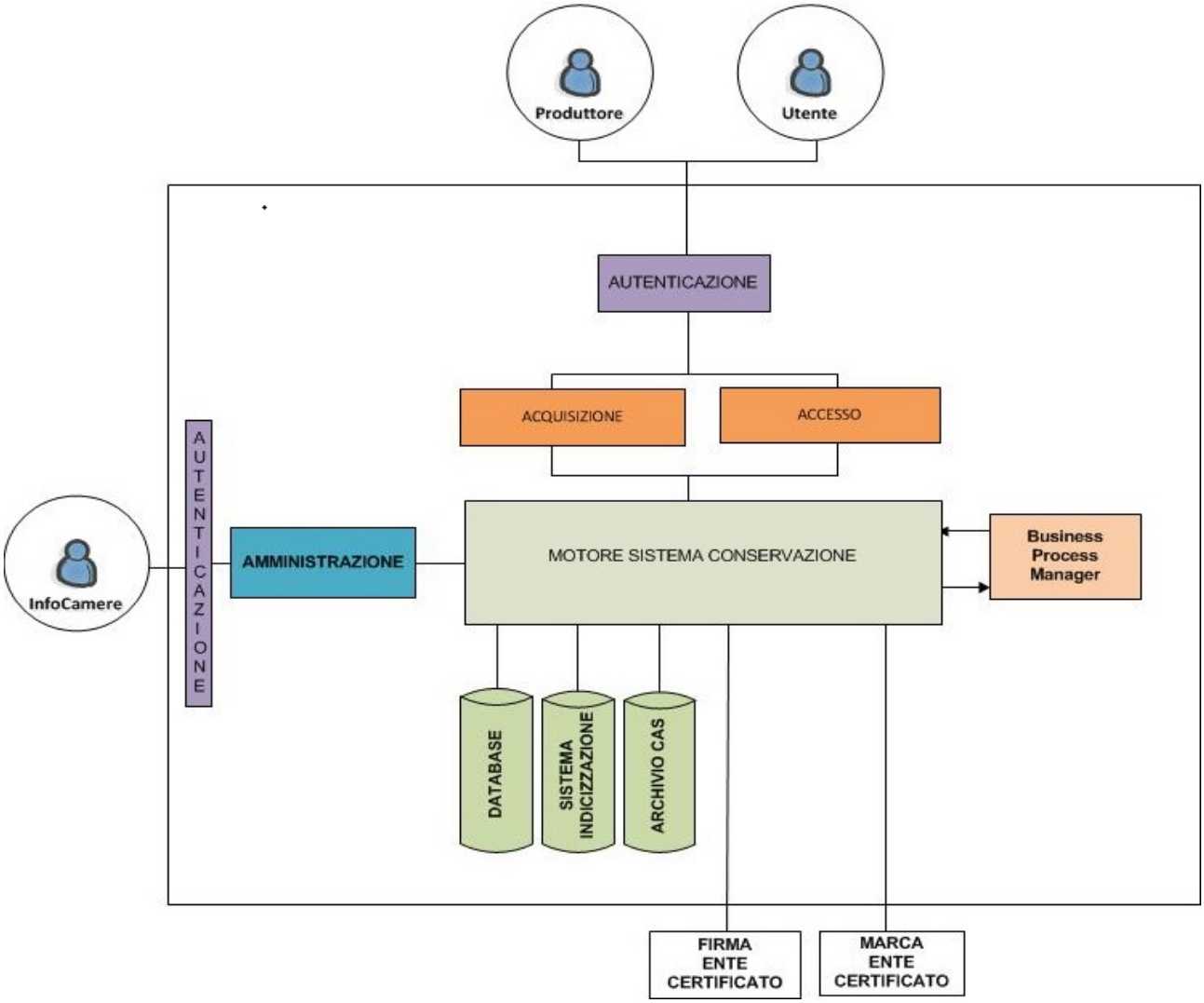


Figura 15 Schema componenti tecnologiche

Il sistema di conservazione è integrato con una componente di *autenticazione* che identifica e verifica l'autorizzazione delle richieste di produttore, utente ed InfoCamere. L'autenticazione avviene o attraverso autenticazione basata su username e password o attraverso la verifica della firma. Maggiori dettagli sulle politiche di accesso adottate sono disponibili nel piano della sicurezza.

Sono possibili due modalità di interazione con il sistema di conservazione:

- Interfaccia application-2-application: attraverso l'uso di Web Services (con tecnologia SOAP e REST) per le funzionalità di *acquisizione* e *accesso* al sistema.
- Interfaccia web: per l'amministrazione del sistema di conservazione

Le comunicazioni tra soggetto produttore/utente e sistema di conservazione utilizzano connessioni sicure attraverso il protocollo HTTPS e certificati SSL.

La componente di *acquisizione* permette la gestione dei pacchetti di versamento, le richieste di scarto ed il monitoraggio del processo di conservazione.

La componente di *accesso* permette la ricerca dei pacchetti informativi presenti nel sistema di indicizzazione, la richiesta e la generazione dei pacchetti di distribuzione.

Il *motore sistema conservazione* contiene la logica di business del sistema. In questa componente sono presenti tutti i processi per la *gestione dati*, l'*archiviazione* e le interfacce con le componenti esterne ad InfoCamere. Il sistema utilizza un Business Process Manager(BPM) *al fine di garantire* una gestione chiara, struttura e tracciabile dei flussi elaborativi.

Per la memorizzazione delle informazioni descrittive e l'archiviazione degli AIP vengono utilizzate le seguenti componenti tecnologiche:

- Database
- Sistema di Indicizzazione
- Archivio CAS

La componente di *amministrazione* permette la gestione e configurazione del sistema di conservazione.

Relativamente ai processi di firma digitale e marca temporale, InfoCamere si avvale di servizi terzi forniti da enti certificati accreditati da AgID.

Torna al sommario

8.3 Componenti Fisiche

Le piattaforme tecnologiche del Sistema di Conservazione sono installate presso il sito InfoCamere di Padova e quello di Milano che, con riferimento alla disaster recovery, costituiscono rispettivamente il sito primario e il sito secondario di erogazione dei servizi;

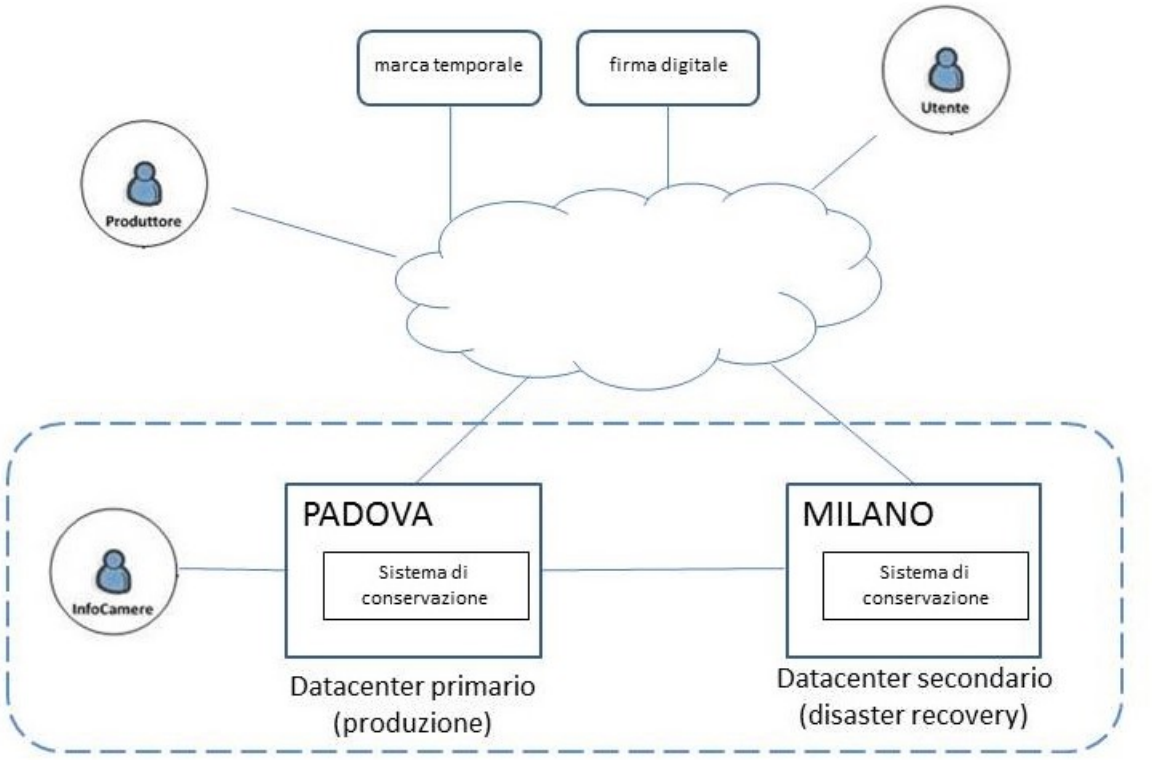


Figura 16 Schema dei siti di conservazione

Per i servizi di firma digitale e marca temporale InfoCamere si avvale di enti certificatori iscritti come Certification Authority presso AgID, attraverso una procedura di gara aperta.

I servizi utilizzano protocolli di comunicazione standard e sono forniti in modalità sincrona.

Torna al sommario

8.3.1 Componenti fisiche sito di Padova

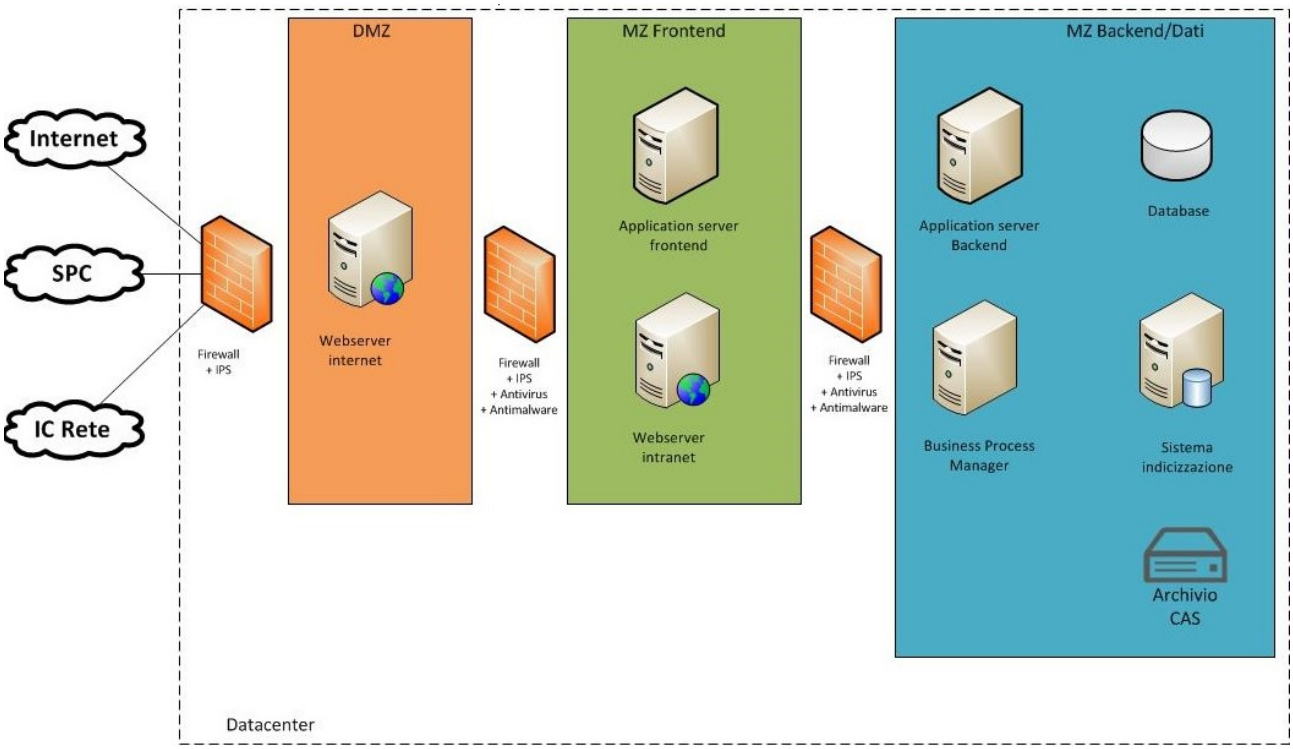


Figura 17 Schema componenti fisiche

Architettura di rete

L'infrastruttura di rete utilizzata per il Sistema di Conservazione prevede la protezione ed il controllo degli accessi tramite un'architettura a tre zone di sicurezza (DMZ, MZ Front-end, MZ Back-end) isolate verso internet e tra di loro da altrettanti firewall. Tale infrastruttura non utilizza reti wireless.

Sistemi di protezione

A tutela della sicurezza del sistema di conservazione sono utilizzati i seguenti dispositivi: firewall, IPS, antivirus e antimalware.

Tali dispositivi sono "appliance" dedicati a tale scopo e prodotti da fornitori leader di mercato. Tali dispositivi garantiscono i più elevati standard di qualità, sicurezza, affidabilità e performance.

Al fine di garantirne la massima disponibilità: i sistemi di protezione sono in alta affidabilità in configurazioni ridondate, con meccanismi di bilanciamento e sono soggetti a backup delle configurazioni. Sono inoltre presenti sistemi di "data exchange" ed accountability / audit.

Server

Il sistema di conservazione utilizza server con sistema operativo open source linux, a cui vengono applicate policy di hardening.

La maggior parte dei server sono ospitati su una piattaforma di virtualizzazione in grado di garantire l'alta affidabilità, a fronte di guasti hardware. E' inoltre garantita la ridondanza nell'accesso alla rete e allo storage.

I server fisici utilizzati hanno componenti ridondate per l'alimentazione, il raffreddamento, l'accesso alla rete e allo storage.

Web server

La suddivisione dello strato di accesso in più livelli garantisce la separazione e l'isolamento tra le diverse zone: DMZ, MZ Front-end, MZ Back-end.

I webserver internet sono collocati nella DMZ e permettono il raggiungimento degli application server di Front-end dalla rete internet. I webserver intranet sono collocati nella MZ Front-end e sono utilizzati per il raggiungimento, dalla rete intranet, degli application server di Front-end e Back-end

I webserver utilizzati nel sistema di conservazione sono "Apache HTTP Server": software open source, tra i più diffusi ed utilizzati nel web. Il carico elaborativo dei webserver è bilanciato attraverso appositi dispositivi di rete, tra istanze in alta affidabilità distribuite su più server virtuali.

Application server

La suddivisione dello strato applicativo in più livelli garantisce la separazione e l'isolamento tra MZ Front-end e MZ Back-end.

Gli application server sono suddivisi tra application server di Front-end collocati nella MZ Front-end, e application di Back-end collocati nella MZ Back-end. A garanzia della sicurezza del sistema di conservazione:

- L'accesso agli application server e possibile solo dai webserver autorizzati
- I soggetti produttori e utenti non possono accedere allo strato applicativo di Back-end, ma le loro richieste devono sempre essere elaborate e validate dallo strato applicativo di Front-end
- L'accesso ai dati del sistema di conservazione(database, sistema di indicizzazione, archivio CAS) è possibile solo da parte dello strato applicativo di Back-end presente nella MZ Back-end.

Gli application server utilizzati nel sistema di conservazione sono Redhat Jboss: software open source, tra i più diffusi ed utilizzati nel web, che implementa i più moderni standard tecnologici e le più recenti specifiche java enterprise. Il carico elaborativo degli application server è bilanciato tra istanze in alta affidabilità distribuite su più server virtuali, tramite meccanismi propri dei webserver e degli application server.

Gli application server del motore di conservazione sono isolati dal resto dell'infrastruttura. La visibilità e l'accesso a questi server sono limitati alle sole persone autorizzate.

Database

I dati del sistema di conservazione sono ospitati su un database relazionale costituito da un cluster Oracle "Real Application Clusters" (RAC) distribuito su più server fisici; i server sono collocati sulla rete di Massima Sicurezza.

L'architettura impiegata ha in sé notevoli caratteristiche di alta affidabilità che consentono di:

- garantire il funzionamento del database anche a fronte della caduta di uno o più nodi
- effettuare in alcuni casi l'aggiornamento di componenti del software di base Oracle in modalità di "rolling upgrade" (aggiornamento che consente di mantenere in servizio i sistemi mentre l'aggiornamento prosegue gradualmente); è così possibile aggiornare un sistema per volta mantenendo la possibilità di dare servizio sugli altri ambienti, al più interrompendo temporaneamente le connessioni su un server;
- aggiungere nodi e istanze al cluster e ridistribuire il carico applicativo in modalità dinamica

Il cluster Oracle RAC è realizzato secondo un'architettura database "Extended Cluster" che consente una recovery molto veloce anche in caso di malfunzionamento dell'intero datacenter; consente inoltre di avere tutti i nodi attivi su tutti i siti, elaborando le transazioni applicative come se fossero eseguite su un unico cluster database.

Un'ulteriore caratteristica è costituita dalla funzionalità Data Guard Oracle che consente la replicazione dei dati tra siti diversi; tale funzionalità è applicata nella modalità asincrona "Maximum Performance" ai siti di Padova e Milano per la Disaster Recovery; i dati del Sistema di Conservazione presenti nel sito primario vengono completamente aggiornati sul sito secondario.

Il database fornisce meccanismi di audit che garantiscono il tracciamento delle modifiche.

I dati del sistema di conservazione sono isolati dal resto dell'infrastruttura. La visibilità e l'accesso ai dati è limitato alle sole persone/componenti software autorizzate.

Business Process Manager (BPM)

I flussi elaborativi presenti nel sistema di conservazione utilizzano una componente BPM leader di mercato, della famiglia di prodotti IBM FileNet per la gestione documentale e del workflow di processo. Il BPM consente di progettare flussi di processo complessi, basati su standard internazionali, con una gestione integrata degli errori e delle anomalie. I server del BPM sono collocati sulla rete MZ Back-end di massima sicurezza.

Il carico elaborativo del BPM è in alta affidabilità con bilanciamento su più server virtuali.

I flussi del sistema di conservazione sono isolati dal resto dell'infrastruttura. La visibilità e l'accesso ai dati è limitato alle sole persone/componenti software autorizzate.

Sistema di indicizzazione

Il sistema di indicizzazione viene utilizzato per permettere la ricerca dei pacchetti informativi versati nel sistema di conservazione in base alle informazioni descrittive associate. A garanzia della sicurezza dei dati conservati, i server sono collocati sulla rete MZ Back-end di massima sicurezza.

Il sistema di indicizzazione utilizzato è Fusion di LucidWorks: un software open source tra i più diffusi nel web, basato su Apache Solr. L'architettura impiegata garantisce un elevato livello di alta affidabilità e ridondanza attraverso il bilanciamento del carico su più server virtuali.

I dati di indicizzazione del sistema di conservazione sono isolati dal resto dell'infrastruttura. La visibilità e l'accesso ai dati è limitato alle sole persone/componenti software autorizzate.

Archivio CAS

L'archivio CAS (Content Addressable Storage) è un dispositivo di memorizzazione progettato per l'archiviazione a lungo termine di dati non modificabili, in cui vengono memorizzati i pacchetti informativi del sistema di conservazione. A garanzia della sicurezza dei dati conservati, il dispositivo è collocato sulla rete MZ Back-end di massima sicurezza.

L'archivio CAS utilizza una piattaforma EMC ECS (Elastic Cloud Storage) che garantisce l'autenticità, l'immodificabilità, l'integrità, la reperibilità, il governo dei contenuti nel rispetto delle normative vigenti per i sistemi di conservazione. Questa piattaforma è l'evoluzione della piattaforma EMC Centera.

I dati del sistema di conservazione sono isolati dal resto dell'infrastruttura. La visibilità e l'accesso ai dati è limitato alle sole persone/componenti software autorizzate.

Torna al sommario

8.3.2 Componenti fisiche sito di Milano

Nel sito di Disaster Recovery sono presenti gli analoghi dispositivi tecnologici utilizzati dal sistema di conservazione nel sito di produzione. Le caratteristiche di sicurezza del sito di Disaster Recovery sono le medesime del sito di produzione.

La seguente figura descrive il collegamento tra il sito di Produzione presente nel datacenter InfoCamere di Padova e il sito InfoCamere di Disaster Recovery di Milano.

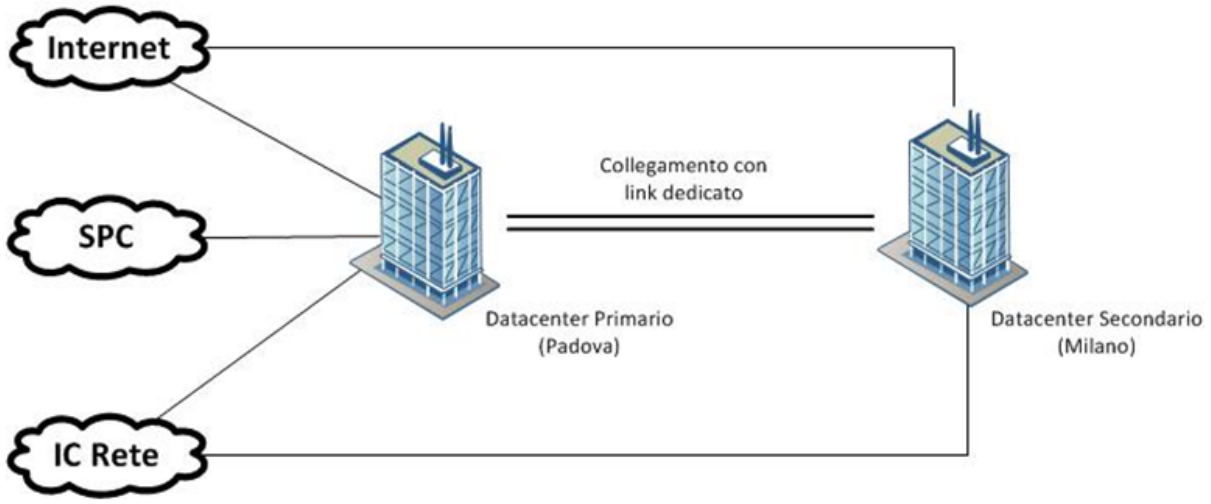


Figura 18 Schema geografico

Tra i 2 siti esiste un processo di replica che mira a garantire gli RPO e RTO previsti per la Disaster Recovery. La replica continua dei dati del Sistema di Conservazione sul sito di disaster recovery, permette di mantenere costantemente allineati i dati presenti nel sito primario, sul sito secondario.

Il collegamento dedicato tra i due siti è realizzato con link "Dark Fiber" in alta affidabilità.

Torna al sommario

8.4 Procedure di gestione e di evoluzione

La conduzione del sistema di conservazione è regolata da una serie di processi certificati ISO 9001:2008 e ISO/IEC 27001:2013. Questa organizzazione permette di:

- garantire la riservatezza, l'integrità, la leggibilità, la reperibilità e la disponibilità dei documenti e dati nel sistema di conservazione
- formalizzare e garantire i requisiti del sistema in conformità alla normativa vigente;
- gestire la manutenzione del servizio
- gestire in modo ottimizzato le anomalie
- valutare i livelli di rischio e di continuità operativa
- monitorare i livelli di sicurezza e gestire le attività di sicurezza

Torna al sommario

8.4.1 Conduzione e manutenzione sistema conservazione

I processi che regolano la conduzione del sistema di conservazione sono:

- Il **processo di Resource Capacity Management** garantisce che il complesso dell'infrastruttura tecnologica sia sempre in grado di soddisfare i livelli di servizio richiesti, in maniera tempestiva e con costi adeguati.

- Il **processo Operation & Event Management** garantisce il rilevamento di tutti gli eventi che si verificano nell'infrastruttura IT al fine di monitorare e controllare le deviazioni dalle performance attese, la gestione delle attività di routine riguardanti la manutenzione ordinaria dei servizi, attraverso la schedulazione automatica delle attività (batch),le attività e le procedure quotidiane di gestione dell'infrastruttura IT, condotte dal personale della Sala di Controllo, affinché i servizi erogati raggiungano i livelli qualitativi prefissati.

- Il **processo di Change & Release Management** assicura che le richieste di cambiamento siano registrate, valutate nel loro impatto, implementate e documentate in modo strutturato, che le attività di passaggio in produzione dei rilasci siano pianificate ed eseguite in accordo con i tempi e con le risorse previste, assicurando il rilascio in esercizio di nuovi servizi e le modifiche ai servizi esistenti.

- Il processo di **Incident Management & Problem Management** descrive come ripristinare le normali operazioni di servizio il più velocemente possibile con il minimo impatto sul business e come determinare la causa primaria degli incidenti e la loro gestione.
- Il processo di **Service Catalogue & Service Level Management** illustra come:

    - garantire la disponibilità di un Catalogo dei Servizi Tecnologici, fonte consistente d'informazione, attraverso la raccolta, l'inserimento, l'aggiornamento e l'eliminazione di informazioni sui servizi in Esercizio o in fase di realizzazione.
    - misurare il Service Level Agreement (SLA) dei Servizi catalogati

- Il processo di **Configuration Management** ha lo scopo di fornire e mantenere nel tempo un modello logico dell'infrastruttura IT, attraverso l'identificazione, il controllo, la manutenzione e la verifica della versione degli oggetti di configurazione.

Viene mantenuta tutta la documentazione relativa alle azioni gestionali ed ai processi amministrativi rilevanti per la conservazione.

Torna al sommario

8.4.2 Gestione e conservazione dei log

Nella gestione del Sistema di Conservazione InfoCamere intende tenere sotto controllo gli eventi anomali legati a:
- malfunzionamenti
- performance

e intende registrarli ai fini di:
- riesame
- audit.

La gestione dei log è pertanto finalizzata a gestire tali eventi prevedendo le seguenti attività periodiche:
- analisi periodica degli errori non evidenziati
- analisi periodica delle performance del sistema

e le seguenti attività straordinarie generate da segnalazioni:
- analisi dei malfunzionamenti segnalati dai soggetti produttori, utenti o dal personale dell'ente conservatore
- analisi dei malfunzionamenti segnalati dai processi automatici del sistema
- analisi della sequenza di eventi generatisi dalla sollecitazione di una funzionalità su richiesta dei soggetti produttori, utenti o dal personale dell'ente conservatore

catalogazione dei log
Il Sistema di Conservazione prevede la gestione di tre grandi categorie di log:
- log infrastrutturali: ovvero i log delle componenti software (acquisite da fornitori) e dei sistemi hardware che compongono l'infrastruttura su cui si attesta il Sistema di Conservazione
- log applicativi: ovvero i log delle applicazioni software (sviluppate da InfoCamere) con rilevanza dal punto di vista di monitoraggio delle funzionalità del sistema di conservazione
- log eventi: ovvero i log nei quali si effettuano registrazioni per il tracciamento di talune categorie di eventi, derivanti dall'accesso al Sistema, con rilevanza dal punto di vista della sicurezza e della normativa.

log infrastrutturali
I log di tale categoria sono ulteriormente catalogabili in *Hardware / Software,* cioè riferiti ai log delle componenti infrastrutturali hardware e software.

log applicativi

I log di tale categoria sono ulteriormente catalogabili in base alla componente software a cui si riferiscono:

- *Motore di conservazione*: log relativi alla componente centrale e core del Sistema di Conservazione che offre funzionalità dotate di interfaccia web-service;
- Amministrazione: log relativi alla componente dedicata all'amministrazione del Sistema di Conservazione attraverso un'interfaccia grafica;
- Gestore archivio CAS: log relativi alla componente di interfaccia con l'archivio CAS nel quale vengono memorizzati i pacchetti informativi.

log eventi

I log di tale categoria sono ulteriormente catalogabili in:

- *Sicurezza*: log in cui vengono registrati eventi con riferimento alla sicurezza delle informazioni e ai dati personali;
- Tracciamento Normativo: log in cui vengono registrati eventi relativi a funzionalità normative che non coinvolgono né la sicurezza delle informazioni né i dati personali;

Nella tabella seguente indichiamo alcune delle possibili informazioni tracciate nei log eventi.

Classificazione delle informazioni del log	
Tipo informazione	Contenuto
Tipo log eventi	Sicurezza Identifica tutti i log con informazioni utili ai fini dell'attività di analisi e monitoraggio della sicurezza del sistema (in primis i log relativi agli accessi) Tracciamento Normativo Identifica tutti i log per in tracciamento delle attività del sistema di conservazione
Livello criticità	Criticità del messaggio loggato. Ad esempio: Info, Warning, Error
Cliente	Viene tracciato l'identificativo del richiedente: produttore, utente, InfoCamere
User	Viene tracciata la user della persona che esegue l'operazione
Timestamp	Viene tracciata la data/ora dell'evento
Tipologia operazione	Viene classificata la tipologia di operazione. Ad esempio: • Richiesta pacchetto di versamento • Richiesta di archiviazione • Richiesta pacchetto di distribuzione
Descrizione operazione	Vengono tracciate informazioni di dettaglio della operazione/processo

Maggiori dettagli sulla gestione del log si trovano nel piano della sicurezza.

Torna al sommario

8.4.3 Monitoraggio del sistema di conservazione

Processo di Resource Capacity Management

Vengono regolarmente effettuate previsioni sull'andamento dei consumi di risorse nel tempo, sia in funzione della stagionalità e della crescita fisiologica, sia a fronte di interventi modificativi quali nuovi rilasci o implementazioni significative dei software esistenti o a fronte di sostanziali modifiche all'infrastruttura.

Quando dall'analisi emerge l'avvicinamento ai limiti di attenzione, vengono avviate azioni di ridimensionamento dell'hardware o di ottimizzazione del software, tali da garantire l'erogazione del servizio in condizioni controllate.

Processo Operation & Event Management

Descrive le modalità di coordinamento ed esecuzione delle attività e dei processi richiesti per fornire e gestire servizi ai clienti secondo livelli di qualità concordati, in conformità alle Pratiche di Successo ITIL V3 fase Service Operation.

Nello specifico, il documento concentra la sua attenzione sui processi:

- Event Management, per il rilevamento di tutti gli eventi che si verifichino nell'infrastruttura IT al fine di monitorare e controllare le deviazioni dalle performance attese.
- Scheduling Management, per la gestione delle attività di routine riguardanti la manutenzione ordinaria dei servizi, attraverso la schedulazione automatica delle attività (batch).
- IT Operation & Service Desk, per tutte le attività e procedure quotidiane di gestione dell'infrastruttura IT, condotte dal personale della Sala di Controllo, affinché i servizi erogati raggiungano i livelli qualitativi prefissati.

Il processo:

- assicura il monitoraggio ed il controllo del corretto funzionamento dell'infrastruttura IT;
- esegue le attività necessarie affinché ai sistemi ed alle procedure applicative siano rese disponibili le risorse necessarie al corretto funzionamento;
- è focalizzato su attività giornaliere o di breve termine eseguite da personale specializzato, ripetute in modo continuativo per lunghi periodi;
- garantisce un supporto 7x24 attraverso turnazioni e reperibilità in tele-assistenza.

Torna al sommario

8.4.4 Change Management

Le modifiche apportate al sistema vengono tracciate seguendo quanto previsto dalla procedura, in particolare vengono tracciate:

- tutte le modifiche hardware al sistema
- tutti gli aggiornamenti del software di sistema (sistemi operativi, rete, middleware, database)
- tutte le modifiche architetturali e strutturali
- tutti gli aggiornamenti di software applicativo

Il processo assicura:

- che le richieste di cambiamento siano registrate, valutate nel loro impatto, implementate e documentate in modo strutturato;
- la pianificazione e l'esecuzione delle attività di passaggio in produzione dei rilasci in accordo con i tempi e con le risorse previste, assicurando il rilascio in esercizio di nuovi servizi e le modifiche ai servizi esistenti.

Grazie all'uso degli strumenti di change management aziendali, il richiedente classifica la propria richiesta in maniera tale che possa essere poi presa in carico dal gruppo di lavoro competente, per cui ogni change ha associato uno o più gruppi di competenza.

Le informazioni gestite con gli strumenti aziendali per le richieste e registrazione modifiche costituiscono la documentazione a supporto dei cambiamenti ed in particolare assicurano che ogni cambiamento significativo sia stato:

- analizzato e valutato dal personale coinvolto
- autorizzato dal responsabile
- eseguito dalle persone autorizzate
- eseguito nei tempi richiesti
- adeguatamente testato

Relativamente alla gestione del software applicativo del sistema di conservazione esiste una istruzione tecnica specifica per cui vengono mantenute tutte le versione di software.

Torna al sommario

8.4.5 Verifica periodica di conformità a normativa e standard di riferimento ed evoluzione del sistema di conservazione

Nell'ambito del rapporto quadrimestrale sull'andamento del sistema di conservazione saranno effettuate le seguenti attività:

- verifica conformità alla normativa del responsabile del servizio di conservazione
- verifica conformità alla normativa del responsabile sicurezza dei sistemi per la conservazione
- verifica conformità alla normativa del responsabile trattamento dati personali
- resoconto sul monitoraggio complessivo del sistema di conservazione da parte del responsabile dei sistemi informativi per la conservazione
- resoconto sul corretto funzionamento dei processi applicativi del responsabile del servizio di conservazione e dello sviluppo e manutenzione del sistema di conservazione

Qualora si rendesse necessario possono essere indette delle riunioni per degli eventi particolari (ad esempio cambi tecnologici urgenti, novità normative critiche, etc).

Nell'ambito della "Governance Aziendale" e più nello specifico nell'ambito del "Sistema di Controllo" interno, InfoCamere recepisce ed integra il modello delle "tre linee di difesa" previste dagli standard internazionali e nazionali; i 3 livelli di controllo sono così rappresentati:

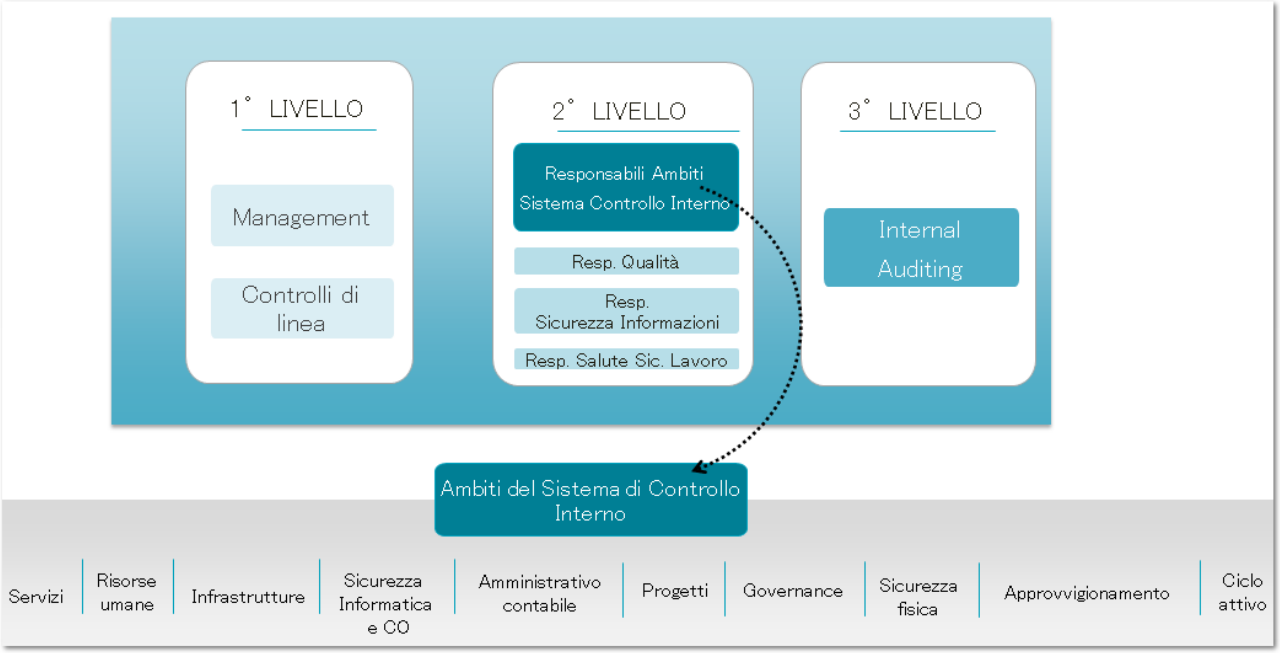


Figura 19 Schema di controllo interno InfoCamere

I diversi responsabili verificano, sulla base di specifiche procedure operative e/o istruzioni tecniche e con periodicità ivi definite, la conformità delle proprie aree di riferimento alle politiche di sicurezza, standard ed ogni altro requisito di sicurezza. Tali controlli periodici di primo e secondo livello rientrano nel normale esercizio della mission assegnata al management.

InfoCamere annualmente predispone ed esegue un Piano di Audit approvato dal Consiglio di Amministrazione che accoglie le attività di controllo (audit) di terzo livello; il piano prevede Audit di tipo Operational, Compliance, Financial e IT (inclusi penetration test e vulnerability assessment).

Su richiesta del Responsabile del Servizio di Conservazione, il Piano di Audit prevede attività di audit sul Servizio stesso.

InfoCamere assicura adeguata informazione nei confronti del personale complessivamente coinvolto (interno ed esterno) per le possibili problematiche derivanti dalle non conformità alle tematiche di sicurezza e l'attuazione di eventuali audit di 2° parte.

E' mantenuta e resa disponibile adeguata documentazione a supporto delle attività complessivamente svolte e dei risultati ottenuti dalle verifiche.

A fronte delle attività precedenti possono essere necessari degli interventi al sistema di conservazione. L'evoluzione del sistema di conservazione è pianificata annualmente e rivista semestralmente e verrà gestita con:

- l'apertura di progetti, controllati mensilmente con degli stati di avanzamento lavori quando l'entità dell'intervento è significativa
- modifiche al prodotto quando l'entità dell'intervento è poco significativa.

Torna al sommario

9 Monitoraggio e controlli

9.1 Procedure di monitoraggio

La parte della Procedura "Operation & Event Management" che interessa il monitoraggio è quella relativa all'Event Management, che descrive il rilevamento di tutti gli eventi che si verifichino nell'infrastruttura IT al fine di monitorare e controllare le deviazioni dalle performance attese.

Una prima fase riguarda la predisposizione e la configurazione degli strumenti di Event e Scheduling Management; vengono eseguite le attività:

- effettuazione e valutazione della richiesta per la creazione di un nuovo controllo
- configurazione dello strumento di Event e Scheduling Management
- definizione dei monitoraggi, controlli e schedulazioni atti a garantire l'erogazione del servizio.

Una seconda fase riguarda l'avvio dei servizi e l'esecuzione del monitoraggio, per i quali vengono effettuate le attività di:

- attivazione in automatico delle componenti di sistema e applicative dallo strumento di Scheduling Management
- verifica dell'avvenuta attivazione
- esecuzione del monitoraggio sulla funzionalità dei servizi tramite gli strumenti di Event Management
- eventuale intervento di "workaround" per il ripristino del corretto funzionamento dei servizi
- eventuale attivazione del Processo di Incident & Problem Management
- registrazione delle attività eseguite nel "Logbook".

Una terza fase riguarda la gestione delle azioni correttive / preventive a seguito del riscontro di eventi anomali; vengono eseguite le attività di:

- verifica quotidiana delle schedulazioni andate in errore e in caso di superamento delle soglie di tolleranza, registrazione dell'evento e pianificazione della conseguente azione di miglioramento

- verifica settimanale dell'esito dell'allineamento tra i server controllati e quelli presenti nell'infrastruttura tecnologica; nel caso di superamento delle soglie di tolleranza, registrazione dell'evento e la conseguente azione di miglioramento

- con frequenza almeno annuale, ed ogni volta se ne verifichi la necessità, identificazione delle attività di evoluzione e miglioramento del processo che vengono descritte nel Riesame Manageriale di processo e inserite nel documento di pianificazione.

- specificamente per il Sistema di Conservazione viene eseguita una serie di controlli manuali sui log giornalieri per controllare il buon andamento dei processi e verificare che le segnalazioni di errore siano sempre motivate (es. pacchetti di versamento bloccati perché non conformi alle specifiche ecc).

La strumentazione per il monitoraggio dei servizi è essenzialmente costituita dalle componenti:

- sonde di rilevazione
- registrazione degli eventi
- console
- messaggistica
- escalation.

sonde
Le sonde di rilevazione sono costituite da componenti software che, con periodicità di circa 5 – 10 minuti, attivano dei programmi di controllo.

Un tipo di sonde attiva dei programmi di navigazione del web permettendo così una costante verifica sulla disponibilità e funzionalità dei servizi (sonde di tipo "applicativo"). Un elenco di sonde, non esaustivo, permetterà il controllo sul funzionamento dei seguenti componenti applicativi:

- web service di versamento
- web service di distribuzione
- web service di scarto

Un altro tipo di sonde attiva dei programmi di verifica sulla disponibilità delle risorse delle componenti hardware / software di base (sonde di tipo "sistemistico"). Un elenco di sonde, non esaustivo, permetterà il controllo sul funzionamento dei seguenti componenti sistemistici:

- processi elaborativi / di sistema
- occupazione dei filesystem
- data base
- application server
- web server
- istanze jboss e apache
- prestazioni dei sistemi (CPU, memoria)
- contenuti nei file di log
- connettività di rete

registrazione degli eventi
Gli eventi rilevati dalle sonde sono registrati automaticamente nel sistema di Incident per poter gestire il ciclo di vita dell'evento.
Possono essere registrati anche eventi a seguito di controlli manuali.

console
Gli eventi rilevati dalle sonde o dai controlli manuali sono inviati a delle console dove sono visualizzati secondo definiti criteri di evidenziazione.

messaggistica
A fronte di eventi particolarmente critici per l'erogazione dei servizi, secondo regole definite nella strumentazione di supporto viene automaticamente inviato un messaggio SMS e/o di posta elettronica al personale coinvolto.

escalation
In genere gli eventi critici rilevati dalle sonde attivano automaticamente il processo di Incident & problem Management interagendo con la relativa strumentazione.
Il supporto operativo può aprire manualmente un incidente anche nei casi in cui non è previsto l'automatismo.

Torna al sommario

9.2 Verifiche dell'integrità degli archivi

I controlli si possono distinguere di quattro tipologie:

- garanzia dell'integrità in entrata
- verifica dell'integrità dell'archivio di conservazione
- verifica di leggibilità a campione dell'archivio di conservazione
- garanzia dell'integrità in uscita

La prima tipologia avviene durante il processo di acquisizione del pacchetto di versamento con la verifica, per ogni componente ricevuto, che l'impronta fornita dal produttore coincida con l'impronta calcolata dal sistema di conservazione (vedi paragrafo 7.2).

La seconda tipologia viene effettuata con due operazioni:

- Una verifica annuale dell'integrità dei documenti conservati nell'archivio CAS.
  In analogia al controllo sui pacchetti di versamento, per ogni componente quindi si verifica che l'impronta fornitaci dal produttore e conservata nell'archivio CAS coincida con l'impronta ricalcolata sulla componente conservata nell'archivio CAS

- Almeno una volta ogni cinque anni l'allineamento dei dati dell'archivio CAS con le informazioni contenute nel database.
  Questo controllo permette di verificare che per tutti i riferimenti ad unità archivistiche, unità documentarie e componenti relative, presenti nel database, siano presenti nell'archivio CAS i corrispondenti file.

La terza tipologia consiste nel controllo della leggibilità dei documenti.
Almeno una volta ogni cinque anni viene estratto un campione di contenuti informativi presenti nell'archivio di conservazione. Tale campione verrà composto seguendo criteri di rappresentatività (produttore, data di conservazione, formato documenti, etc) e fornito al responsabile del servizio di conservazione.
Questi dovrà verificarne la leggibilità utilizzando i visualizzatori del sistema di conservazione e produrre un verbale sull'esito del controllo, che verrà registrato nella documentazione del sistema di conservazione.

L'ultima tipologia di controllo riguarda la produzione dei pacchetti di distribuzione.
Per tutte le componenti fornite agli utenti del sistema di conservazione, viene effettuata la verifica che l'impronta conservata nel pacchetto di archiviazione coincida con quella calcolata al momento della preparazione del pacchetto di distribuzione. Eventuali anomalie sono tracciate nel sistema di conservazione per la analisi e soluzione del problema (vedi paragrafo 7.6).

Torna al sommario

9.3 Soluzioni adottate in caso di anomalie

Le anomalie vengono affrontate seguendo le indicazione del processo "Incident & Problem Management".

Il Processo di "Incident & Problem Management" definisce:
- per l'Incident Management, come ripristinare le normali operazioni di servizio il più velocemente possibile con il minimo impatto sul business;
- per il Problem Management, la determinazione della causa primaria degli incidenti e la loro gestione.

Il Processo si applica a tutti gli incidenti e problemi attinenti alle aree:
- Tecnologica (hardware, sistemi operativi e middleware),
- Applicativa
- Sicurezza delle informazioni
- Servizi tecnici impianti;

L'Incident Management è composto dalle fasi:
- gestire segnalazione
- gestire incidente di 1° livello
- gestire incidente di 2° livello
- chiudere incidente
- monitorare incidenti

Il Problem Management è composto dalle fasi:
- individuare il problema
- risolvere il problema
- riesaminare i problemi.

Torna al sommario

9.3.1 Incident Management

gestire segnalazione
Le segnalazioni sono ricevute:
- per via telefonica o telematica dai clienti
- dal personale InfoCamere in conseguenza dell'analisi degli eventi registrati sui log o evidenziati nelle console

- dal personale InfoCamere in conseguenza alla diretta osservazione di eventi anomali.

Esse sono analizzate, registrate e classificate nello strumento informatico di tracciatura.
Se sono risolte con l'utilizzo di procedure operative ordinarie, vengono chiuse.
Se invece non sono risolte, vengono promosse ad incidente di 1° o 2° livello ed assegnate al soggetto che ne effettuerà la gestione.

gestire incidente di 1° livello
Si effettua la diagnosi dell'incidente e lo si risolve con l'utilizzo di procedure operative ordinarie.
Se l'incidente non è risolto, viene assegnato ad un Team Operativo specialistico per la gestione di 2° livello; se la durata del disservizio supera – o si prevede possa superare – la soglia di escalation, viene coinvolto l'Incident Manager che segue il relativo Processo.

gestire incidente di 2° livello
Si effettua la diagnosi approfondita dell'incidente e lo si risolve con l'utilizzo di procedure operative ad-hoc.
Se l'incidente non è risolto e supera – o si prevede possa superare – la soglia di escalation, vengono coinvolte le figure che seguono il relativo Processo

chiudere incidente
Si chiude l'incidente effettuando le opportune registrazioni e comunicando la chiusura ai responsabili di S.O. eventualmente coinvolti in precedenza.

Eventuali operazioni manuali sui dati del sistema di conservazione, necessarie per ripristinare i processi di sistema, sono tracciate nei log del sistema di conservazione.

monitorare incidenti
Ad ogni passaggio di fase e cambiamento di stato, le informazioni sull'incidente sono aggiornate nello strumento informatico di tracciatura.
Con cadenza giornaliera gli incidenti sono riesaminati, vengono aggiornate le relative informazioni.
Mensilmente viene redatto un report sull'andamento del Processo.
Sono prodotti e pubblicati indicatori per un'efficace gestione.

Torna al sommario

9.3.2 Problem Management

individuare il problema
Si analizza l'elenco degli incidenti per individuare la causa di origine. Se la causa è riconducibile ad un problema già esistente, l'incidente viene a questo associato tramite lo strumento informatico di Ticketing; se la causa non è riconducibile ad un problema esistente, viene registrato un nuovo problema associandovi l'incidente.
Il problema è assegnato alla persona di riferimento (Focal Point) per la sua soluzione.

risolvere il problema
Il Focal Point gestisce la soluzione del problema coinvolgendo gli specialisti tecnici necessari ed utilizzando le ordinarie procedure operative.

Si aggiorna lo stato di avanzamento della soluzione, si verifica la correttezza della soluzione attuata, si chiude il problema aggiornando le relative informazioni.

riesaminare i problemi
Con cadenza mensile i problemi sono riesaminati ed è aggiornato il loro stato di avanzamento, viene redatto e pubblicato un documento di riesame operativo, viene alimentato un repository contenente tutte le registrazioni degli errori e dei problemi noti (Known Error DataBase).

Torna al sommario

9.3.3 Comunicazioni ai produttori e utenti

Con le modalità definite nel contratto di affidamento, il responsabile dei sistemi informativi per la conservazione, responsabile del monitoraggio del sistema di conservazione, e il responsabile del servizio di conservazione predispongono la comunicazione delle anomalie e delle risoluzioni ai produttori o agli utenti in funzione delle tipologie di servizi coinvolti.

Torna al sommario