

MANUALE DI CONSERVAZIONE DI ALMAVIVA

<i>Redatto</i>	E. Locuratolo		◆ AlmavivA Security Practice
<i>Validato</i>	A. Mercurio } E. Locuratolo }	20/05/2017	◆ AlmavivA Security Practice ◆ Almaviva Responsabile servizio di conservazione
<i>Verificato</i>	R. Buonfiglio } A. Giaccone } A. Abaterusso }	20/05/2017	◆ AlmavivA Security Practice ◆ Managed Operations
<i>Lista di distribuzione</i>			◆ Intranet Aziendali

REGISTRO DELLE VERSIONI

N°Ver/Rev/Bozza	Data emissione	Modifiche apportate	Osservazioni
1.0	15.05.2015	Prima emissione	Nessuna
1.1	07.07.2016	Cambiamento Responsabile funzione archivistica	
1.2	01.12.2016	Cambiamento Responsabile sviluppo e manutenzione	
1.3	20.05.2017	Cambiamento Responsabile sviluppo e manutenzione – Cambiamento Infrastruttura server	

Sommario

1. SCOPO E AMBITO DEL DOCUMENTO	4
2. TERMINOLOGIA (GLOSSARIO, ACRONIMI).....	5
3. NORMATIVA E STANDARD DI RIFERIMENTO	9
3.1. Normativa di riferimento.....	9
3.2. Standard di riferimento.....	10
4. RUOLI E RESPONSABILITÀ	11
5. STRUTTURA ORGANIZZATIVA PER IL SERVIZIO DI CONSERVAZIONE	14
5.1. Organigramma.....	14
5.2. Strutture organizzative.....	17
6. OGGETTI SOTTOPOSTI A CONSERVAZIONE	20
6.1. Oggetti conservati.....	20
6.2. Pacchetto di versamento	23
6.3. Pacchetto di archiviazione.....	29
6.4. Pacchetto di distribuzione	34
7. IL PROCESSO DI CONSERVAZIONE.....	36
7.1. Creazione del servizio	38
7.2. Modalità di acquisizione dei pacchetti di versamento per la loro presa in carico	39
7.3. Verifiche effettuate sui pacchetti di versamento e sugli oggetti in essi contenuti	39
7.4. Accettazione dei pacchetti di versamento e generazione del rapporto di versamento di presa in carico	40
7.5. Rifiuto dei pacchetti di versamento e modalità di comunicazione delle anomalie	40
7.6. Creazione del pacchetto di archiviazione	41
7.7. Preparazione e gestione del pacchetto di archiviazione	44
7.8. Preparazione e gestione del pacchetto di distribuzione ai fini dell'esibizione	45
7.9. Produzione di duplicati e copie informatiche e descrizione dell'eventuale intervento del pubblico ufficiale nei casi previsti	47
7.10. Scarto dei pacchetti di archiviazione.....	47
7.11. Predisposizione di misure a garanzia dell'interoperabilità e trasferibilità ad altri conservatori.....	48
7.12. Cessazione del servizio	48
8. IL SISTEMA DI CONSERVAZIONE	49
8.1. Componenti Logiche	49
8.2. Componenti tecnologiche.....	50
8.3. Componenti Fisiche.....	51
8.4. Procedure di gestione e di evoluzione.....	52
8.4.1. Conduzione e manutenzione del sistema di conservazione.....	52
8.4.2. Gestione e conservazione dei log	54
8.4.3. Monitoraggio del sistema di conservazione	54
8.4.4. Change management	55
8.4.5. Verifica periodica di conformità a normativa e standard di riferimento	55
9. MONITORAGGIO E CONTROLLI.....	56
9.1. Procedure di monitoraggio	56
9.2. Log del sistema di conservazione.....	58
9.3. Verifica dell'integrità degli archivi.....	59
9.4. Soluzioni adottate in caso di anomalie	61

1. SCOPO E AMBITO DEL DOCUMENTO

Il presente documento costituisce il Manuale del sistema di conservazione di Al maviva, nel quale sono descritti :

- il modello organizzativo
- i ruoli e le responsabilità
- i processi e le procedure
- l'architettura logica e fisica

del suo sistema di conservazione.

Lo scopo del documento è quello di fornire ai soggetti pubblici e privati, le informazioni adeguate a conoscere i requisiti organizzativi, di processo, architetture, funzionali e di sicurezza, in conformità ai quali Al maviva eroga il servizio di conservazione al livello più elevato in termini di qualità e sicurezza.

Si evidenzia che Il servizio è erogato nel DC Al maviva, nel rispetto dei requisiti di continuità, sicurezza fisica e logica, back-up, monitoraggio, presidio operativo, sistemistico, infrastrutture logistiche (locali, ups, condizionatori) e gestione reti dati che il Data Center garantisce e descrive negli specifici documenti. Il DC è certificato ISO 27001:2013, ISO 9001:2008, ISO 20000-1:2011, 22301:2012.

Al maviva presta una particolare attenzione alla definizione, attuazione, verifica, implementazione del suo Sistema di Gestione della Sicurezza delle Informazioni (SGSI), che è supportato da un impianto di policy la cui articolazione è di seguito rappresentata, e che rappresenta il contesto di riferimento costante nella implementazione e conduzione del servizio di conservazione.

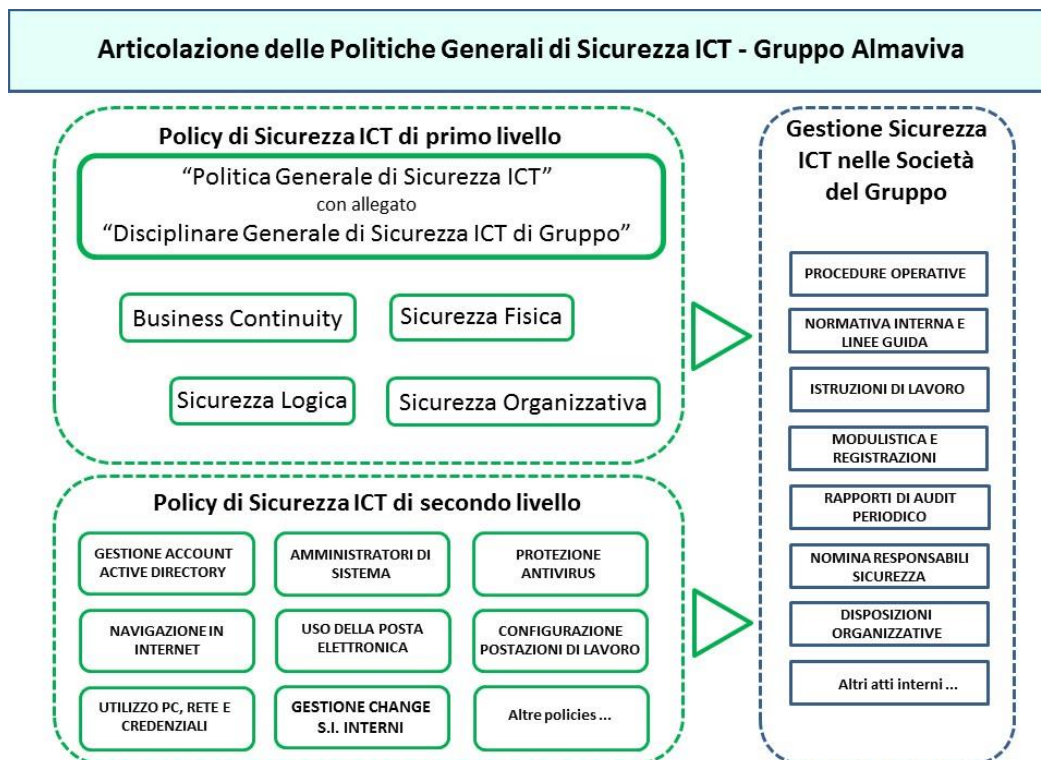


Figura 1 – Schema articolazione Politiche generali di sicurezza

La figura precedente (**Figura 1 – Schema articolazione Politiche generali di sicurezza**) espone in prima riga orizzontalmente il titolo “Articolazione delle Politiche Generali di Sicurezza ICT – Gruppo Almaviva”. Sotto questo titolo compare un primo riquadro in alto a sinistra intitolato “Policy di Sicurezza ICT di primo livello”; in questo riquadro sono inseriti altri cinque riquadri: nel primo è scritto “Politica Generale di Sicurezza ICT” con allegato “Disciplinare Generale di Sicurezza ICT di Gruppo”, nel secondo “Business Continuity”, nel terzo “Sicurezza fisica”, nel quarto “Sicurezza Logica”, nel quinto “Sicurezza Organizzativa”. Il primo riquadro (contenitore degli altri cinque) è indirizzato da una freccia verso un altro riquadro che si sviluppa in verticale a destra. Sempre a sinistra ma sotto il primo riquadro è inserito un secondo riquadro intitolato “Policy di Sicurezza ICT di secondo livello”; in questo riquadro sono inseriti altri nove riquadri: nel primo è scritto “Gestione Account Active Directory”, nel secondo è scritto “Amministratori di Sistema”, nel terzo è scritto “Protezione antivirus”, nel quarto è scritto “Navigazione in internet”, nel quinto è scritto “Uso della posta elettronica”, nel sesto è scritto “Configurazione postazioni di lavoro”, nel settimo è scritto “Utilizzo PC, rete e credenziali”, nell’ottavo è scritto “Gestione change S.I. interni”, nel nono è scritto “Altre policies...”. Anche il secondo riquadro è indirizzato da una freccia verso il riquadro che si sviluppa in verticale a destra. Il riquadro verticale a destra è intitolato “Gestione Sicurezza ICT nelle Società del Gruppo” e comprende otto riquadri; nel primo riquadro è scritto “Procedure operative”, nel secondo riquadro è scritto “Normativa interna e linee guida”, nel terzo riquadro è scritto “Istruzioni di lavoro”, nel quarto riquadro è scritto “Modulistica e registrazioni”, nel quinto riquadro è scritto “Rapporti di audit periodico”, nel sesto riquadro è scritto “Nomina responsabili sicurezza”, nel settimo riquadro è scritto “Disposizioni organizzative”, nell’ottavo riquadro è scritto “Altri atti interni...”.

[Torna al sommario](#)

2. TERMINOLOGIA (GLOSSARIO, ACRONIMI)

Termini	Definizioni
Accesso	Operazione che consente a chi ne ha diritto di prendere visione ed estrarre copia dei documenti informatici
Accreditamento	Riconoscimento, da parte dell’ Agenzia per l’Italia digitale , del possesso dei requisiti del livello più elevato, in termini di qualità e sicurezza ad un soggetto pubblico o privato, che svolge attività di conservazione o di certificazione del processo di conservazione
Affidabilità	Caratteristica che esprime il livello di fiducia che l’utente ripone nel documento informatico
Attestazione di conformità delle copie per immagine su supporto informatico di un documento analogico	Dichiarazione rilasciata da notaio o altro pubblico ufficiale a ciò autorizzato allegata o asseverata al documento informatico
Autenticità	Caratteristica di un documento informatico che garantisce di essere ciò che dichiara di essere, senza aver subito alterazioni o modifiche. L’autenticità può essere valutata analizzando l’identità del sottoscrittore e l’integrità del documento informatico

Termini	Definizioni
Certificatore accreditato	Soggetto, pubblico o privato, che svolge attività di certificazione del processo di conservazione al quale sia stato riconosciuto, dall’Agenzia per l’Italia digitale , il possesso dei requisiti del livello più elevato, in termini di qualità e di sicurezza
Ciclo di gestione	Arco temporale di esistenza del documento informatico, del fascicolo informatico, dell’aggregazione documentale informatica o dell’archivio informatico dalla sua formazione alla sua eliminazione o conservazione nel tempo
Classificazione	attività di organizzazione logica di tutti i documenti secondo uno schema articolato in voci individuate attraverso specifici metadati
Conservatore accreditato	Soggetto, pubblico o privato, che svolge attività di conservazione al quale sia stato riconosciuto, dall’Agenzia per l’Italia digitale , il possesso dei requisiti del livello più elevato, in termini di qualità e di sicurezza, dall’Agenzia per l’Italia digitale
Conservazione	Insieme delle attività finalizzate a definire ed attuare le politiche complessive del sistema di conservazione e a governarne la gestione in relazione al modello organizzativo adottato e descritto nel manuale di conservazione
Copia analogica del documento informatico	Documento analogico avente contenuto identico a quello del documento informatico da cui è tratto
Copia di sicurezza	Copia di <i>backup</i> degli archivi del sistema di conservazione prodotta ai sensi dell’articolo 12 delle presenti regole tecniche per il sistema di conservazione
Documento informatico	La rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti
Documento analogico	La rappresentazione non informatica di atti, fatti o dati giuridicamente rilevanti
Duplicazione dei documenti informatici	Produzione di duplicati informatici
Firma elettronica	L’insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica
Firma elettronica avanzata	Insieme di dati in forma elettronica allegati oppure connessi a un documento informatico che consentono l’identificazione del firmatario del documento e garantiscono la connessione univoca al firmatario, creati con mezzi sui quali il firmatario può conservare un controllo esclusivo, collegati ai dati ai quali detta firma si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati
Firma elettronica qualificata	Un particolare tipo di firma elettronica avanzata che sia basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma
Firma digitale	Un particolare tipo di firma elettronica avanzata basata su un certificato qualificato e su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare

Termini	Definizioni
	tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici
Esibizione	Operazione che consente di visualizzare un documento conservato e di ottenerne copia
Funzione di 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
Identificativo univoco	sequenza di caratteri alfanumerici associata in modo univoco e persistente al documento informatico, al fascicolo informatico, all'aggregazione documentale informatica, in modo da consentirne l'individuazione
Immodificabilità	caratteristica che rende il contenuto del documento informatico non alterabile nella forma e nel contenuto durante l'intero ciclo di gestione e ne garantisce la staticità nella conservazione del documento stesso
Impronta	la sequenza di simboli binari (bit) di lunghezza predefinita generata mediante l'applicazione alla prima di una opportuna funzione di hash
Integrità	insieme delle caratteristiche di un documento informatico che ne dichiarano la qualità di essere completo ed inalterato
Interoperabilità	capacità di un sistema informatico di interagire con altri sistemi informatici analoghi sulla base di requisiti minimi condivisi
Leggibilità	insieme delle caratteristiche in base alle quali le informazioni contenute nei documenti informatici sono fruibili durante l'intero ciclo di gestione dei documenti
Marca temporale	è il risultato di una procedura informatica – detta servizio di marcatura temporale – grazie alla quale si attribuisce a un documento informatico un riferimento temporale opponibile a terzi.
Memorizzazione	processo di trasposizione su un qualsiasi idoneo supporto, attraverso un processo di elaborazione, di documenti analogici o informatici
Metadati	insieme di dati associati a un documento informatico, o a un fascicolo informatico, o ad un'aggregazione documentale informatica per identificarlo e descriverne il contesto, il contenuto e la struttura, nonché per permetterne la gestione nel tempo nel sistema di conservazione
Pacchetto di archiviazione	pacchetto informativo composto dalla trasformazione di uno o più pacchetti di versamento secondo le modalità riportate nel manuale di conservazione
Pacchetto di distribuzione	pacchetto informativo inviato dal sistema di conservazione all'utente in risposta ad una sua richiesta
Pacchetto di versamento	pacchetto informativo inviato dal produttore al sistema di conservazione secondo un formato predefinito e concordato descritto nel manuale di conservazione
Presenza in carico	accettazione da parte del sistema di conservazione di un pacchetto di versamento in quanto conforme alle modalità previste dal manuale di

Termini	Definizioni
	conservazione
Produttore	persona fisica o giuridica, di norma diversa dal soggetto che ha formato il documento, che produce il pacchetto di versamento ed è responsabile del trasferimento del suo contenuto nel sistema di conservazione. Nelle Pubbliche amministrazioni, tale figura si identifica con responsabile della gestione documentale.
Rapporto di versamento	documento informatico che attesta l'avvenuta presa in carico da parte del sistema di conservazione dei pacchetti di versamento inviati dal produttore
Responsabile della conservazione	soggetto responsabile dell'insieme delle attività elencate nell'articolo 8, comma 1 delle regole tecniche del sistema di conservazione
Responsabile del trattamento dei dati	la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali
Responsabile della sicurezza	soggetto al quale compete la definizione delle soluzioni tecniche ed organizzative in attuazione delle disposizioni in materia di sicurezza
Riferimento temporale	informazione contenente la data e l'ora con riferimento al Tempo Universale Coordinato (UTC), della cui apposizione è responsabile il soggetto che forma il documento
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

Acronimi	Definizioni
AgID	Agenzia per l'Italia Digitale
CA	Certification Authority
FTP server	Programma che permette di accettare connessioni in entrata e di comunicare con un Client attraverso il protocollo FTP
IdP	strumento per rilasciare le informazioni di identificazione di tutti i soggetti che cercano di interagire con un Sistema; ciò si ottiene tramite un modulo di autenticazione che verifica un token di sicurezza come alternativa all'autenticazione esplicita di un utente all'interno di un ambito di sicurezza.
PdV	Pacchetto di Versamento
PdA	Pacchetto di Acquisizione
PdD	Pacchetto di Distribuzione
OAIS	ISO 14721:2012; Space Data information transfer system
ETSI	European Telecommunications Standards Institute

[Torna al sommario](#)

3. NORMATIVA E STANDARD DI RIFERIMENTO

3.1. Normativa di riferimento

1. Codice Civile [Libro Quinto Del lavoro, Titolo II Del lavoro nell'impresa, Capo III Delle imprese commerciali e delle altre imprese soggette a registrazione, Sezione III Disposizioni particolari per le imprese commerciali, Paragrafo 2 Delle scritture contabili], articolo 2215 bis - Documentazione informatica;
2. Legge 7 agosto 1990, n. 241 e s.m.i. – Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi;
3. 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;
4. Decreto Legislativo 30 giugno 2003, n. 196 e s.m.i. – Codice in materia di protezione dei dati personali;
5. Decreto Legislativo 22 gennaio 2004, n. 42 e s.m.i. – Codice dei Beni Culturali e del Paesaggio;
6. Decreto Legislativo 7 marzo 2005 n. 82 e s.m.i. – Codice dell'amministrazione digitale (CAD);
7. 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, comma 3, lettera b), 35, comma 2, 36, comma 2, e 71;

8. 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;
9. 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.
10. Decreto del Presidente del Consiglio dei Ministri 13 novembre 2014 - Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici nonché di formazione e conservazione dei documenti informatici delle pubbliche amministrazioni ai sensi degli articoli 20, 22, 23 -bis, 23 -ter, 40, comma 1, 41, e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005.

[Torna al sommario](#)

3.2. Standard di riferimento

1. ISO 14721:2012 OAIS (Open Archival Information System), Sistema informativo aperto per l'archiviazione;
2. ISO/IEC 27001:2013, Information technology - Security techniques - Information security management systems – Requirements, Requisiti di un ISMS (Information Security Management System);
3. ISO/IEC 20000-1:2011 Information technology -- Service management system requirements
4. 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;
5. 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;
6. UNI 11386:2010 Standard SInCRO - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali;
7. ISO 15836:2009 Information and documentation - The Dublin Core metadata element set, Sistema di metadata del Dublin Core.

[Torna al sommario](#)

4. RUOLI E RESPONSABILITÀ

Ruoli	Nominativo	Attività di competenza	Periodo nel ruolo
Responsabile del servizio di conservazione	Eleonora Locuratolo	<ul style="list-style-type: none">- 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;- monitoraggio della 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	
Responsabile Sicurezza dei sistemi per la conservazione	Andrea Mercurio	<ul style="list-style-type: none">- 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.	

<p>Responsabile funzione archivistica di conservazione</p>	<p>Annalisa Cerroni</p>	<ul style="list-style-type: none"> - Definizione e gestione del processo di conservazione, incluse le modalità di trasferimento da parte dell'ente produttore, di acquisizione, verifica di integrità e descrizione archivistica dei documenti e delle aggregazioni documentali trasferiti, di esibizione, di accesso e fruizione del patrimonio documentario e informativo conservato; - definizione del set di metadati di conservazione dei documenti e dei fascicoli informatici; - monitoraggio del processo di conservazione e analisi archivistica per lo sviluppo di nuove funzionalità del sistema di conservazione; - collaborazione con l'ente produttore ai fini del trasferimento in conservazione, della selezione e della gestione dei rapporti con il Ministero dei beni e delle attività culturali per quanto di competenza. 	<p>Dal 13.07.2016</p>
<p>Responsabile trattamento dati personali</p>	<p>Nunzio Cali</p>	<ul style="list-style-type: none"> - 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 	
<p>Responsabile sistemi informativi per la conservazione</p>	<p>Andrea Abaterusso</p>	<ul style="list-style-type: none"> . 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 erogati da terzi con segnalazione delle eventuali difformità al Responsabile del servizio di conservazione. 	

Responsabile sviluppo e manutenzione del sistema di conservazione	Andrea Mercurio	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.	
---	-----------------	---	--

[Torna al sommario](#)

5. STRUTTURA ORGANIZZATIVA PER IL SERVIZIO DI CONSERVAZIONE

5.1. Organigramma

Il servizio viene erogato nell'ambito ed attraverso le strutture di competenza della "Direzione Operations Infrastructure and Application Services", la cui struttura organizzativa è rappresentata nello schema seguente (con il simbolo ● sono evidenziate le Unità Organizzative direttamente interessate)

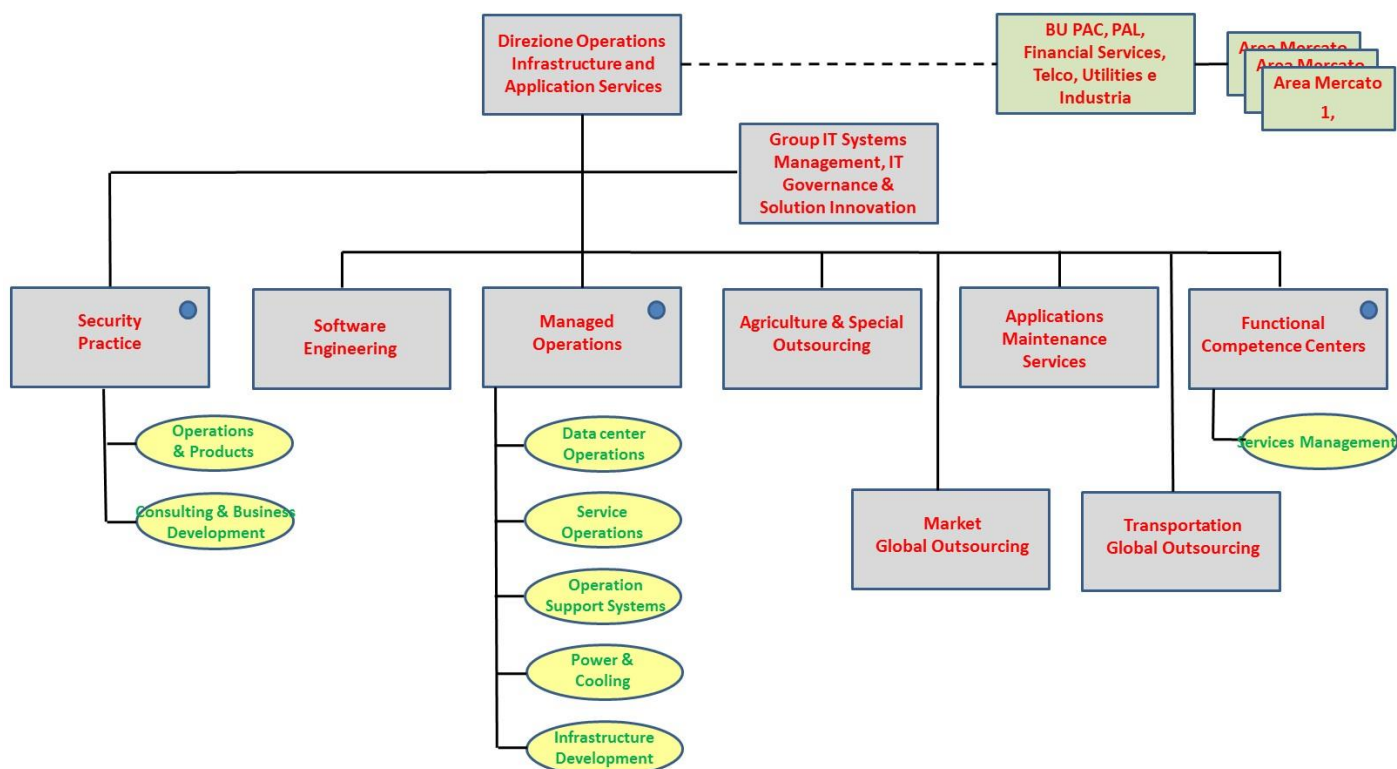


Figura 2 – Organigramma della Direzione Operations di Almagiva

La figura precedente (**Figura 2 – Organigramma della Direzione Operations di Almagiva**) evidenzia al primo livello gerarchico la "Direzione Operations Infrastructure and Applications services" ad essa rispondono le unità organizzative : "Group IT Systems Management, IT Governance & Solution Innovation", "Security Practice" (corresponsabile della governance del servizio di conservazione attraverso le aree funzionali "Operations & Products" e "Consulting & Business Development"), "Software Engineering", "Managed Operations" (corresponsabile della governance del servizio di conservazione attraverso le aree funzionali "Data center Operations", "Service Operations", "Operations Support Systems", "Power & Cooling", "Infrastructure Development"), "Agriculture & Social Outsourcing", "Market Global Outsourcing", "Applications Maintenance Services"; "Transportation Global Outsourcing", "Functional Competence Centers" (corresponsabile della governance del servizio di conservazione attraverso l'area funzionale "Services Management"). La "Direzione Operations Infrastructure and Applications services" collabora con la unità organizzativa "BU PAC, PAL, Financial Services, Telco, Utilities e Industria" a sua volta suddivisa in aree funzionali (Aree Mercato).

L'Unità Organizzativa "Security Practice" ha il compito, attraverso le sue unità funzionali, di :

- raccogliere e recepire, unitamente ai Functional Competence Centers ed ai referenti delle specifiche strutture aziendali, i requisiti di servizio per i clienti (esterni ed interni).
- monitorare i processi di conservazione affinché siano svolti nel rispetto dei requisiti di sicurezza, qualità e di servizio concordati con i clienti
- governare il processo di conservazione, garantendo la conformità alle norme ed agli standard
- analizzare e valutare al secondo livello gli eventi di sicurezza (monitorati dalla Unità Operativa "Managed Operations") per indirizzare le opportune azioni pro-attive e reattive
- supportare l'integrazione del servizio nel sistema di gestione della sicurezza delle informazioni aziendale, sia in fase di progettazione che di avviamento ed esercizio del servizio

L'Unità Organizzativa "Managed Operations" ha il compito, attraverso le sue unità funzionali, di :

- erogare la conduzione operativa e sistemistica del servizio
- garantire che le infrastrutture di supporto (hw, sw, network, storage,..) siano adeguate alle esigenze di volumi e di performance definiti contrattualmente
- monitorare i sistemi, sia per quanto riguarda l'utilizzo delle risorse sia per quanto riguarda gli aspetti di sicurezza (event and incident management)
- presidiare il change and configuration management

L'Unità Organizzativa "Functional Competence Centers" ha il compito, attraverso le sue unità funzionali, di :

- raccogliere e recepire, unitamente all'Unità Organizzativa "Security Practice" ed ai referenti delle specifiche Aree di Mercato, i requisiti di servizio per i clienti
- individuare e pianificare, unitamente all'Unità Organizzativa "Security Practice" le esigenze e le attività di change and configuration management supportando la struttura "Managed Operation"

Collocazione dei profili nella struttura organizzativa

Unità organizzativa	RSC	RSSC	RFAC	RTDP	RSIC	RSMSC
Security Practice	X	X	X	X		X
Managed Operations					X	

RSC = Responsabile del Servizio di Conservazione

RSSC = Responsabile Sicurezza dei Sistemi per la Conservazione

RFAC = Responsabile Funzione Archivistica di Conservazione

RTDP = Responsabile Trattamento Dati Personali

RSIC = Responsabile Sistemi Informativi per la Conservazione

RSMSC = Responsabile Sviluppo e Manutenzione del Sistema di Conservazione

Nella tabella precedente è schematizzata la collocazione dei profili nella struttura organizzativa. Nella "Security Practice" sono collocati i profili RSC, RSSC, RFAC, RDTP, RSMSC; nella "Managed Operations" è collocato il profilo RSIC.

Di seguito viene evidenziata la tabella RACI secondo i ruoli riportati dall'organigramma e secondo il processo di conservazione a norma OAIS :

Ruoli e responsabilità del processo di conservazione			
	Produttore	Cliente (colui che può accedere ai doc. conservati)	Responsabile della Conservazione
<i>1-Produzione documenti da archiviare e controllo contenuti</i>	R/E/V/A		
<i>2-Verifica Documento da Conservare e indicizzazione dello stesso</i>	R/E/V/A		
<i>3-Creazione del file conforme alle direttive di Archiviazione</i>	R/E/V/A		
<i>4-Invio documenti al sistema di conservazione</i>	R/E/V/A		
<i>5-Verifica e accettazione del documento da parte del sistema di Conservazione</i>			R/V/A
<i>6-Inserimento nel pacchetto di versamento e apposizione Firma e marca temporale</i>			R/E/V/A
<i>7-Memorizzazione , creazione copia sicurezza e chiusura del processo</i>			R/E/V/A
<i>8-Esibizione documento conservato tramite interfaccia Web</i>	V/A	V/A	R/E
<i>9-Verifica periodica della leggibilità dei documenti conservati e delle copie di BK</i>			R/E/V/A
<i>10-Dematerializzazione e Distruzione cartaceo documenti conservati.</i>		R/E	V/A

A=Approva R=Responsabile E=Esecutore V=Verifica

Nella tabella precedente sono schematizzati i ruoli e le responsabilità nel processo di conservazione. Nelle colonne sono indicati i ruoli : “Produttore”, “Cliente” (colui che può accedere ai doc. conservati), “Responsabile della Conservazione”. Nelle righe sono elencate le principali macro-attività del processo. Nell’incrocio tra righe e colonne è evidenziata la modalità con la quale un certo ruolo è coinvolto nella macro-attività. Nella macro-attività “1-Produzione documenti da archiviare e controllo contenuti” è coinvolto il Produttore con le seguenti modalità R/E/V/A. Nella macro-attività “2-Verifica Documento da Conservare e indicizzazione dello stesso” è coinvolto il Produttore con le seguenti modalità R/E/V/A. Nella macro-attività “3-Creazione del file conforme alle direttive di Archiviazione” è coinvolto il Produttore con le seguenti modalità R/E/V/A. Nella macro-attività “4-Invio documenti al sistema di conservazione” è coinvolto il Produttore con le seguenti modalità R/E/V/A. Nella macro-attività “5-Verifica e accettazione del documento da parte del sistema di Conservazione” è coinvolto il Responsabile della conservazione con le seguenti modalità R/V/A. Nella macro-attività “6-Inserimento nel pacchetto di versamento e apposizione Firma e marca temporale” è coinvolto il Responsabile della conservazione con le seguenti modalità R/E/V/A. Nella macro-attività “7-Memorizzazione , creazione copia sicurezza e chiusura del processo” è coinvolto il Responsabile della conservazione con le seguenti modalità R/E/V/A. Nella macro-attività “8-Esibizione documento conservato tramite interfaccia Web” sono coinvolti il Produttore con le seguenti modalità V/A, il Cliente con le seguenti modalità V/A, il Responsabile della conservazione con le seguenti responsabilità R/E. Nella macro-attività “9-Verifica periodica della leggibilità dei documenti conservati e delle copie di BK” è coinvolto il Responsabile della conservazione con le seguenti modalità R/E/V/A. Nella macro-attività “10-Dematerializzazione e Distruzione cartaceo documenti conservati.” sono coinvolti il il cliente con le seguenti modalità R/E, il Responsabile della conservazione con le seguenti modalità V/A.

Si ricorda che il Cliente, il Titolare dei documenti informatici posti in conservazione, nomina il proprio Responsabile della Conservazione, come richiesto dalla normativa.

Il suddetto Responsabile della conservazione, sotto la propria responsabilità, affida ad Al maviva, quale prestatore del servizio di conservazione digitale dei documenti informatici, il servizio di conservazione digitale dei documenti informatici del Cliente, affidando le attività previste dal relativo Contratto di servizio ad Al maviva stessa, che attraverso il suo responsabile del servizio di conservazione, svolgerà le opportune attività ad essa affidate dal Cliente

[Torna al sommario](#)

5.2.Strutture organizzative

Di seguito le matrici RACI tra le attività del servizio di conservazione e di gestione dei sistemi informativi, descritte nel presente documento, e le responsabilità che in esse competono ai ruoli.

Attività proprie di ciascun contratto di servizio di conservazione							
Attività	RSC	RSSC	RFAC	RTDP	RSIC	RSMSC	FCC
Attivazione del servizio di conservazione (a seguito della sottoscrizione di un contratto) [rif. § 7.1]	A/R	R	R	C	R	I	C
Acquisizione, verifica e gestione dei pacchetti di versamento presi in carico e generazione del rapporto di versamento [rif. § 7.2 - § 7.3 - § 7.4]	A/R	I	C	C	R	I	
Preparazione e gestione del pacchetto di archiviazione [rif. § 7.7]	A/R	C	R	R	R	I	
Preparazione e gestione del pacchetto di distribuzione ai fini dell'esibizione e della produzione di duplicati e copie informatiche su richiesta [rif. § 7.8]	A/R	R	C	R	R	I	
Scarto dei pacchetti di archiviazione [rif. § 7.10]	A/R	C	C	I	R	I	
Chiusura del servizio di conservazione (al termine di un contratto) [rif. § 7.12]	A/R	R	R	C	R	I	C

A=Approva

R=Responsabile

C=Consultato

I=Informato

RSC = Responsabile del Servizio di Conservazione
 RSSC = Responsabile Sicurezza dei Sistemi per la Conservazione
 RFAC = Responsabile Funzione Archivistica di Conservazione
 RTDP = Responsabile Trattamento Dati Personali
 RSIC = Responsabile Sistemi Informativi per la Conservazione
 RSMSC = Responsabile Sviluppo e Manutenzione del Sistema di Conservazione
 FCC = Functional Competence Center

Nella tabella precedente è schematizzata la relazione tra le attività proprie di ciascun contratto di servizio di conservazione ed i profili svolti nel servizio stesso. Nelle colonne sono indicati i profili RSC, RSSC, RFAC, RDTP, RSIC, RSMSC, FCC; nelle righe sono elencate le attività. All'incrocio tra righe e colonne sono evidenziate le modalità con cui un dato profilo è coinvolto nella specifica attività. Nella attività "Attivazione del servizio di conservazione (a seguito della sottoscrizione di un contratto) [rif. § 7.1]" sono coinvolti : RSC con le modalità A/R, RSSC con la modalità R, RFAC con la modalità R, RTDP con la modalità C, RSIC con la modalità R, RSMSC con la modalità I, FCC con la modalità C. Nella attività "Acquisizione, verifica e gestione dei pacchetti di versamento presi in carico e generazione del rapporto di versamento [rif. § 7.2 - § 7.3 - § 7.4]" sono coinvolti : RSC con le modalità A/R, RSSC con la modalità I, RFAC con la modalità C, RTDP con la modalità C, RSIC con la modalità R, RSMSC con la modalità I. Nella attività "Preparazione e gestione del pacchetto di archiviazione [rif. § 7.7]" sono coinvolti : RSC con le modalità A/R, RSSC con la modalità C, RFAC con la modalità R, RTDP con la modalità R, RSIC con la modalità R, RSMSC con la modalità I. Nella attività "Preparazione e gestione del pacchetto di distribuzione ai fini dell'esibizione e della produzione di duplicati e copie informatiche su richiesta [rif. § 7.8]" sono coinvolti : RSC con le modalità A/R, RSSC con la modalità R, RFAC con la modalità C, RTDP con

la modalità R, RSIC con la modalità R, RSMSC con la modalità I. Nella attività “*Scarto dei pacchetti di archiviazione [rif. § 7.10]*” sono coinvolti : RSC con le modalità A/R, RSSC con la modalità C, RFAC con la modalità C, RTDP con la modalità I, RSIC con la modalità R, RSMSC con la modalità I. Nella attività “*Chiusura del servizio di conservazione (al termine di un contratto) [rif. § 7.12]*” sono coinvolti : RSC con le modalità A/R, RSSC con la modalità R, RFAC con la modalità R, RTDP con la modalità C, RSIC con la modalità R, RSMSC con la modalità I, FCC con la modalità C.

Attività proprie di gestione dei sistemi informativi						
Attività	RSC	RSSC	RFAC	RTDP	RSIC	RSMSC
Conduzione e manutenzione del sistema di conservazione [rif 8.3.1]	A	R	I	C	R	I
Monitoraggio del sistema di conservazione [rif. § 8.3.3 - § 9.1]	A/R	R	R	C	R	I
Change management [rif 8.3.4]	A	C	C	C	R	R
Verifica periodica di conformità a normativa e standard di riferimento [rif. 8.3.5]	A/R	C	R	R	I	I

A=Approva

R=Responsabile

C=Consultato

I=Informato

RSC = Responsabile del Servizio di Conservazione

RSSC = Responsabile Sicurezza dei Sistemi per la Conservazione

RFAC = Responsabile Funzione Archivistica di Conservazione

RTDP = Responsabile Trattamento Dati Personali

RSIC = Responsabile Sistemi Informativi per la Conservazione

RSMSC = Responsabile Sviluppo e Manutenzione del Sistema di Conservazione

Nella tabella precedente è schematizzata la relazione tra le attività proprie di gestione dei sistemi informativi ed i profili svolti nella gestione. Nelle colonne sono indicati i profili RSC, RSSC, RFAC, RDTP, RSIC, RSMSC nelle righe sono elencate le attività. All’incrocio tra righe e colonne sono evidenziate le modalità con cui un dato profilo è coinvolto nella specifica attività. Nella attività “*Conduzione e manutenzione del sistema di conservazione [rif 8.3.1]*” sono coinvolti : RSC con la modalità A, RSSC con la modalità R, RFAC con la modalità I, RTDP con la modalità C, RSIC con la modalità R, RSMSC con la modalità I. Nella attività “*Monitoraggio del sistema di conservazione [rif. § 8.3.3 - § 9.1]*” sono coinvolti : RSC con le modalità A/R, RSSC con la modalità R, RFAC con la modalità R, RTDP con la modalità C, RSIC con la modalità R, RSMSC con la modalità I. Nella attività “*Change management [rif 8.3.4]*” sono coinvolti : RSC con la modalità A, RSSC con la modalità C, RFAC con la modalità C, RTDP con la modalità C, RSIC con la modalità R, RSMSC con la modalità R. Nella attività “*Verifica periodica di conformità a normativa e standard di riferimento [rif. 8.3.5]*” sono coinvolti : RSC con le modalità A/R, RSSC con la modalità C, RFAC con la modalità R, RTDP con la modalità R, RSIC con la modalità I, RSMSC con la modalità I.

Aggiornamento professionale

Il personale coinvolto nel servizio viene istruito su:

- le specificità tecniche e di sicurezza (vulnerabilità e minacce e relative contromisure adottate) dei sistemi/impianti da prendere in carico, anche attraverso opportuni manuali di gestione-amministrazione;
- il corretto utilizzo dei sistemi IT impiegati a supporto dell'attività quotidiana (e-mail, software ecc.);
- la generazione e la gestione delle password;
- la responsabilità ed il ruolo;
- il tracciamento delle attività.
- Regole tecniche in materia di sistema di conservazione (dpcm 3 dicembre 2013 [\[2\]](#) e successivi) e aspetti di sicurezza tipici di un progetto di conservazione digitale ovvero le
- contromisure che garantiscono autenticità, integrità, affidabilità, leggibilità e reperibilità dei documenti informatici, come previsto dal CAD (art.44). [\[1\]](#)

Sono inoltre previsti periodici piani di training e sessioni dedicate agli aspetti della sicurezza delle informazioni con particolare riguardo agli aspetti della conservazione.

La direzione Risorse Umane gestisce operativamente la formazione al termine del processo di rilevazione dei fabbisogni riportati nel Piano dei fabbisogni formativi.

Per il personale appartenente al servizio di conservazione sono previste :

- sessioni di formazione ove si tratti di personale in nuovo ingresso
- aggiornamento professionale, per tutto il personale interessato, a seguito di modifiche a norme e/o funzionalità e/o processi gestionali, e/o requisiti di sicurezza

[Torna al sommario](#)

6. OGGETTI SOTTOPOSTI A CONSERVAZIONE

6.1. Oggetti conservati

Gli oggetti sottoposti a conservazione possono essere i seguenti:

1. Documenti informatici e documenti amministrativi informatici prodotti dal cliente con metadati associati a seconda delle tipologia documentale oggetto di conservazione.
2. Fascicoli informatici: aggregazione di più documenti informatici con metadati associati a seconda sia della tipologia del fascicolo sia dei documenti.

I formati più comuni gestiti sono riassunti nella tabella sottostante

Tipo File	Visualizzatore	Versione
TIFF	Visualizzatore Windows	6.0
XML	Notepad, IE, Firefox	2.0
P7M	Dike	ETSI TS 101 733
PDF	Adobe Acrobat Reader	1.7
PDF(PADES)	Adobe Acrobat Reader	ETSI TS 102 778
XML(XADES)	Dike	ETSI TS 101 903

Nella tabella precedente sono elencati i formati più comuni gestiti (“tipo file”) ed il visualizzatore utilizzato, nonché la versione. Per il “tipo file” TFF il visualizzatore utilizzato è Windows versione 6.0; per il “tipo file” XML i visualizzatori utilizzati sono Notepad, IE, Firefox versione 2.0. Per il “tipo file” P7M il visualizzatore utilizzato è Dike versione ETSI TS 101 733. Per il “tipo file” PDF il visualizzatore utilizzato è Adobe Acrobat Reader versione 1.7. Per il “tipo file” PDF(PADES) il visualizzatore utilizzato è Adobe Acrobat Reader versione ETSI TS 102 778. Per il “tipo file” XML(XADES) il visualizzatore utilizzato è Dike versione ETSI TS 101 903.

Tutti gli oggetti portati in conservazione sono trattati dal sistema in forma di pacchetti informativi detti:

- Pacchetti di versamento (PdV)
- Pacchetti di archiviazione (PdA)
- Pacchetti di distribuzione (PdD)

Il sistema di conservazione di Al maviva gestisce la conservazione di qualunque tipologia documentale secondo quanto definito dal contratto di servizio verso il cliente, purché la tipologia documentale sia effettivamente dematerializzabile o conservabile nativamente in digitale, secondo le norme attuali. Il sistema di conservazione può prendersi carico di gestire i documenti secondo i processi di conservazione qui definiti. A titolo di esempio, vengono indicate alcune tipologie documentali di maggiore interesse :

FATTURE ELETTRONICA VERSO LA PUBBLICA AMMINISTRAZIONE.

Si ricorda che la FatturaPA è una fattura elettronica ai sensi dell'articolo 21, comma 1, del DPR 633/72 ed è la sola tipologia di fattura accettata dalle Amministrazioni che, secondo le disposizioni di legge, sono tenute ad avvalersi del Sistema di Interscambio. Dal 6 Giugno 2013 possono accettare solo fatture elettroniche le PA Centrali, mentre dal 31 Marzo 2015, l'obbligo si estende anche a tutti gli altri Enti Centrali.

La FatturaPA ha le caratteristiche di una fattura elettronica, ovvero :

- il contenuto è rappresentato, in un file XML (eXtensible Markup Language), secondo il formato della FatturaPA.
- l' autenticità dell' origine e l' integrità del contenuto sono garantite tramite l' apposizione della firma elettronica qualificata di chi emette la fattura,
- la trasmissione è vincolata alla presenza del codice identificativo univoco dell'ufficio destinatario della fattura riportato nell' Indice delle Pubbliche Amministrazioni.
- Per la firma del file FatturaPA consultare la sezione Firmare la FatturaPA.

FATTURA ATTIVA :

I metadati della Fattura Attiva gestiti dal sistema di conservazione e che vengono presi in carico per la generazione del pacchetto di archiviazione sono i seguenti e sono quelli richiesti dal DMEF del 17 Giugno del 2014 :

- Numero Fattura
- Partita IVA
- Codice Fiscale
- Data Fattura
- Denominazione

FATTURA PASSIVA :

I metadati della Fattura Passiva gestiti dal sistema di conservazione e che vengono presi in carico per la generazione del pacchetto di archiviazione sono i seguenti e sono quelli richiesti dal DMEF del 17 Giugno del 2014 :

- Numero Fattura
- Partita IVA
- Codice Fiscale
- Data Fattura
- Denominazione
- Numero di Registrazione / Protocollo
- Data di Registrazione / Protocollo

Le tipologie sopra descritte sono quelle maggiormente trattate dal sistema di conservazione, ma è chiaro che i processi qui descritti valgono anche per le altre tipologie documentali, indipendentemente se queste sono contabili, amministrativi o sanitari. La variazione tra una tipologia ed un'altra è data dalla diversità della tempistica di conservazione e della diversità dei metadati descritti del documento, come richiesto dagli allegati del DPCM del 3 Dicembre 2013 [\[2\]](#) e dal processo di gestione del documento e anche di formazione come definito e richiesto dal DPCM del 13 Novembre 2014 [\[3\]](#), riportante le Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici.

A titolo di esempio si ricorda che :

- La conservazione dei documenti fiscali e contabili, è annuale e quindi la tempistica per la generazione dei pacchetti di archiviazione/distribuzione, è fatta almeno una volta l'anno.
- La conservazione del libro unico del lavoro, è mensile con la produzione dei pacchetti di archiviazione/versamento fatta quindi almeno una volta al mese (Es. LUL di Gennaio 2015, conservati entro Febbraio 2015)
- La conservazione di una cartella clinica elettronica, richiede l'analisi dei processi documentali sanitari e dei documenti digitali da conservare.

Come si evidenzierà di seguito nel manuale, verranno descritti processi di versamento comuni anche alle tipologie sanitarie.

Gli esempi sopra descritti evidenziano una diversa tempistica ed ovviamente anche i metadati saranno diversi, ma visto che il sistema qui descritto gestisce vari Pacchetti di Versamento, sarà possibile conservare qualunque tipologia documentale con una sua determinata tempistica e con un determinato processo di conservazione e di versamento.

[Torna al sommario](#)

6.2. Pacchetto di versamento

Il sistema di conservazione riceve i documenti in diversi formati tramite canali concordati con il cliente e che comunque garantiscono l'integrità del versamento. A titolo di esempio ma non esaustivo si ricorda che il cliente potrebbe inviare i documenti per la generazione del pacchetto di versamento in questo modo (viene anche descritta la metodologia per garantire integrità) :

- FTPS o SFTP : il cliente può usufruire dei canali FTP con crittografia a 256 bit messi a disposizione per l'invio di documenti nel formato concordato con il Cliente. Il cliente viene identificato tramite login e password dedicate per ciascun canale aperto e l'integrità dei documenti versati e del loro formato, vengono garantiti subito dopo il versamento, avviando un controllo (check) della leggibilità dei singoli documenti. Si evidenzia che il formato non può comunque essere difforme da quanto definito dal DPCM del 3 Dicembre 2013. [2]

In questo caso sarà possibile schedulare un JOB secondo gli accordi con il Cliente che partendo da una cartella di polling, legge i documenti di uno dei formati evidenziati nel presente Manuale cui dovrà essere abbinato un file TXT o XML contenente i metadati per ogni singolo documento; tale job invia sulla raccolta SharePoint i documenti letti dalla cartella di polling. Nel momento in cui verranno archiviati i documenti su SharePoint, verrà effettuato un controllo sugli hash dei singoli documenti rispetto a quelli presente sulla cartella di polling. Il pacchetto di versamento in questo coinciderà con il processo di upload tramite Web Service dalla cartella FPT alla raccolta SharePoint.

- Web Services : il cliente tramite tecnologia SOAP può inviare i documenti tramite un servizio WEB messo a disposizione solo per il tempo necessario al versamento dei documenti e su canale sicuro SSL a 256 bit con certificato valido ed installato sul web server di comunicazione.

Tali documenti confluiscono in una raccolta SharePoint all'interno di un sito documentale dedicato al cliente per il caricamento dei documenti da sottoporre a conservazione.

La raccolta documentale SharePoint potrà ricevere un set di metadati già concordati con il cliente.

- Via WEB é possibile per il Produttore/Cliente caricare autonomamente il PdV attraverso la Sezione/Area su SharePoint riferita proprio alla gestione dei PdV. In questo caso il Cliente potrà fare l'upload del documento caricando i files (documenti) tramite interfaccia ed avere immediatamente riscontro della buonuscita dell'operazione.

A caricamento avvenuto il sistema effettua i seguenti controlli :

- che i files del PdV siano tutti firmati digitalmente, diversamente anche in questo caso il sistema avvisa il Cliente che ci sono dei files non firmati ed individua quelli non firmati, qualora il Cliente dovesse inviare documenti esclusivamente firmati digitalmente. Diversamente, se il contratto di servizio con il Cliente, prevede la conservazione di fatture analogiche e quindi non firmate digitalmente al momento dell'emissione, il sistema sarà in grado di ricevere i files non firmati e di procedere con la firma automatica massiva tramite HSM sicuro, per rendere le fatture analogiche, documenti informatici e provvedere successivamente alla conservazione come dettato dal Art. 4 recante gli Obblighi da osservare per la dematerializzazione di documenti e scritture analogici rilevanti ai fini tributari , del DMEF del 17 Giugno 2014.
- che il file sia integro e non corrotto, diversamente il sistema avvisa di rieffettuare il caricamento.

All'interno delle configurazioni dell'archiviazione e nel processo di versamento, sulla gestione degli utenti adibiti al versamento, sono gestite le informazioni degli utenti produttori.

Un utente produttore deve essere censito sul sistema con alcune informazioni obbligatorie:

- Tipo documento (Carta Identità, Codice fiscale)
- Numero documento
- Codice Fiscale
- Ente

L'utente produttore viene in questo modo collegato ad un Ente.

Il sistema gestisce un'anagrafica degli Enti centralizzata indipendentemente dai tenant facendo visualizzare su ogni tenant solo gli enti associati a quel tenant.

Un Ente possiede le seguenti informazioni:

- Ragione Sociale
- P Iva
- Indirizzo
- Città
- Telefono
- Contratto

Un utente produttore deve essere collegato ad un ente (anagrafica centralizzata).

Ogni ente è collegato a un contratto. L'anagrafica dei contratti è strutturata come segue:

- Id contratto
- Data inizio
- Data scadenza
- Descrizione
- Tipologia

A titolo di esempio, si evidenzia una struttura di un file ZIP contenente delle fatture elettroniche (PA), che è del seguente tipo

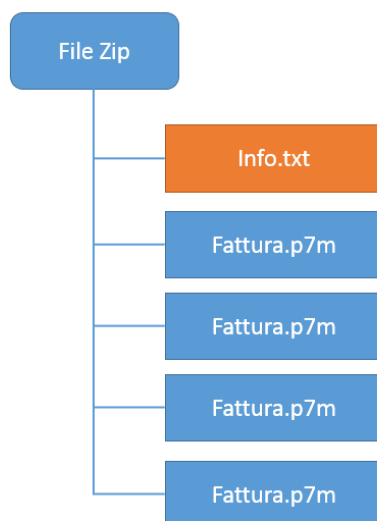


Figura 3 – Schema struttura file ZIP pacchetto fatture elettroniche PA

Nella “**Figura 3 – Schema struttura file ZIP pacchetto fatture elettroniche PA**” è schematizzato il contenuto di un file zip contenente le fatture elettroniche per la PA : un file testo (info.txt) e tutte le fatture firmate (Fattura.p7m)

All’interno del file Info.txt vengono descritti i metadati che devono essere riportati sul sistema di Conservazione all’interno del pacchetto di Versamento.

La struttura del file TXT info è rappresentata come segue:

Fatture Attive

DataFattura|FatturaElettronica/FatturaElettronicaBody/DatiGenerali/DatiGeneraliDocumento/Data
NumeroFattura|FatturaElettronica/FatturaElettronicaBody/DatiGenerali/DatiGeneraliDocumento/N
umero

ImportoTotale|FatturaElettronica/FatturaElettronicaBody/DatiGenerali/DatiGeneraliDocumento/Im
portoTotaleDocumento

La prima riga del file rappresenta la raccolta documentale (tipo documento) di destinazione del file ZIP estratto, mentre le seguenti righe rappresentano il metadato del documento separato da un carattere “|” che identifica la posizione del valore all’interno della struttura XML della fattura PA rispetto alla versione 1.1 definita sul sito fattura PA <http://www.fatturapa.gov.it/export/fatturazione/it/a-3.htm> .

Il sistema consente al cliente finale di caricare il pacchetto di versamento (es. file zip con fatture attive) attraverso un pannello in cui viene effettuato l’upload del file ed il controllo del file stesso. Sotto l’immagine del pannello per la creazione ed il controllo di un pacchetto di versamento

Crea Pacchetto Versamento

- PROCSOSTPaccVersamento

Società	Almaviva
Sito	http://dev2014-3/siti/almaviva
Carica pacchetto	

Salva

Figura 4 – Pannello per la creazione di un PdV

Nella “**Figura 4 – Pannello per la creazione di un PdV**” è rappresentato il form della funzione di creazione, nel quale devono essere valorizzati i campi : “Società” e “Sito”; successivamente si agisce sul pulsante “Carica pacchetto” ed una volta effettuato il caricamento si agisce sul pulsante “Salva”

Al caricamento del pacchetto il sistema effettua un controllo sulla validità del pacchetto stesso e se corretto crea una raccolta documentale che rappresenta il pacchetto a partire dalle configurazioni impostate nel file Info.txt (vedi precedente). Viene quindi proposta la lista dei vari pacchetti di versamento che il cliente ha caricato.

Di seguito vengono descritti i controlli che il sistema di conservazione effettua sul contenuto del pacchetto di versamento al fine di garantire l'integrità dello stesso (si fa riferimento allo specifico esempio) :

- Verifica che i files XML contenuti nel file ZIP siano integri e firmati digitalmente. Si verifica dunque che i files siano firmati in CASES o in XADES. Nel primo caso si verifica che i files abbiano l'estensione in P7M e che la busta della firma sia integra. Nel secondo caso si verifica che sia presente all'interno della struttura XML, il campo <Signature> del XADES e che la busta della firma sia integra.
- Verifica che il nome dei files rispetti le regole dettate dal Sistemi di Interscambio
- Verifica integrità dei files con controllo sui bit di parità
- Verifica della presenza di eventuali altri files che non siano XML.

Qualora almeno una delle verifiche e dei controlli di cui sopra dovesse risultare positiva, allora viene inviato sia al Produttore sia al Responsabile della Conservazione, un alert contenente il risultato della verifica positiva. L'errore viene storicizzato nel sistema documentale sharepoint e viene individuato il pacchetto ZIP che contiene i files errati. Viene inviato al Produttore una richiesta di rinvio di quel pacchetto che deve essere nuovamente versato e ricontrollato. Nel sistema documentale SharePoint rimarrà comunque un registro degli errori.

Sono gestiti anche degli errori bloccanti qualora si verificano una delle seguenti :

- il PdV non corrisponde al formato richiesto

- i files contenuti nel PdV non sono firmati digitalmente (quando previsto)
- il PdV è corrotto
- se il file XML della Fattura Elettronica PA non è conforme allo standard richiesto da SOGEI per il Sistema di Interscambio

Nei casi precedentemente indicati, si presenta un errore bloccante che restituisce al Cliente/Produttore l'errore presentato. In questo caso viene avvisato anche il Responsabile della Conservazione che avvia tutte le procedure per risolvere gli errori e decide se e quando richiedere al Produttore nuovi files per la generazione dei PdA.

Nel momento in cui il versamento dei documenti del Produttore finisce, viene generato dal sistema un rapporto di versamento che viene firmato digitalmente dal Responsabile del servizio di conservazione e che conterrà non solo il riferimento di tutti i files contenuti nei pacchetti, ma anche i rispettivi metadati legati e allegati a ciascun documento e relativo time stamping, in modo tale da identificarlo in modo univoco ed in modo tale da rendere al Produttore il dettaglio del versamento. Il rapporto di versamento conterrà anche la lista di eventuali files errati e che non hanno passato la fase di verifica e controllo sopra descritta. Il rapporto di versamento dovrà essere inviato al Produttore tramite PEC. Si ricorda che ogni singolo pacchetto di versamento ha un suo nome univoco ed identificabile.

Di seguito viene evidenziata un'immagine che descrive il flusso di firma del rapporto di versamento

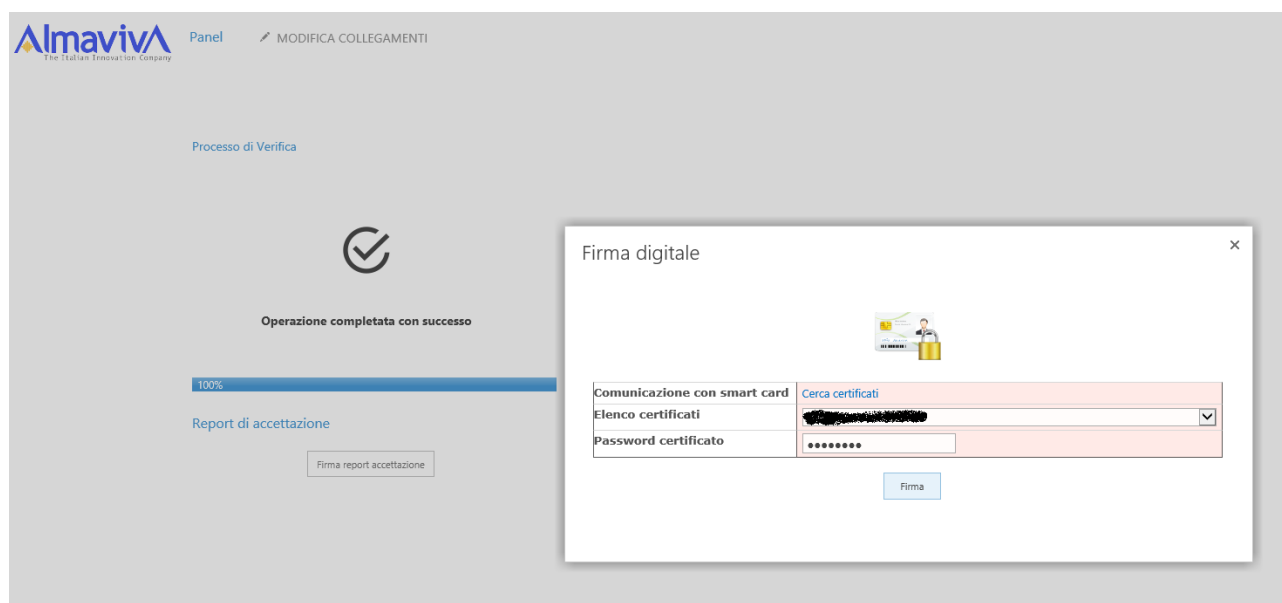


Figura 5 – Pannello per la firma del rapporto di versamento

Nella “**Figura 5 – Pannello per la firma del rapporto di versamento**” è rappresentato il form della funzione di firma, nel quale, dopo essere stato selezionato il certificato di firma, esposto nella combobox “elenco certificati”, deve essere valorizzata la password nel campo “password certificato”. Infine deve essere attivato il pulsante “Firma”.

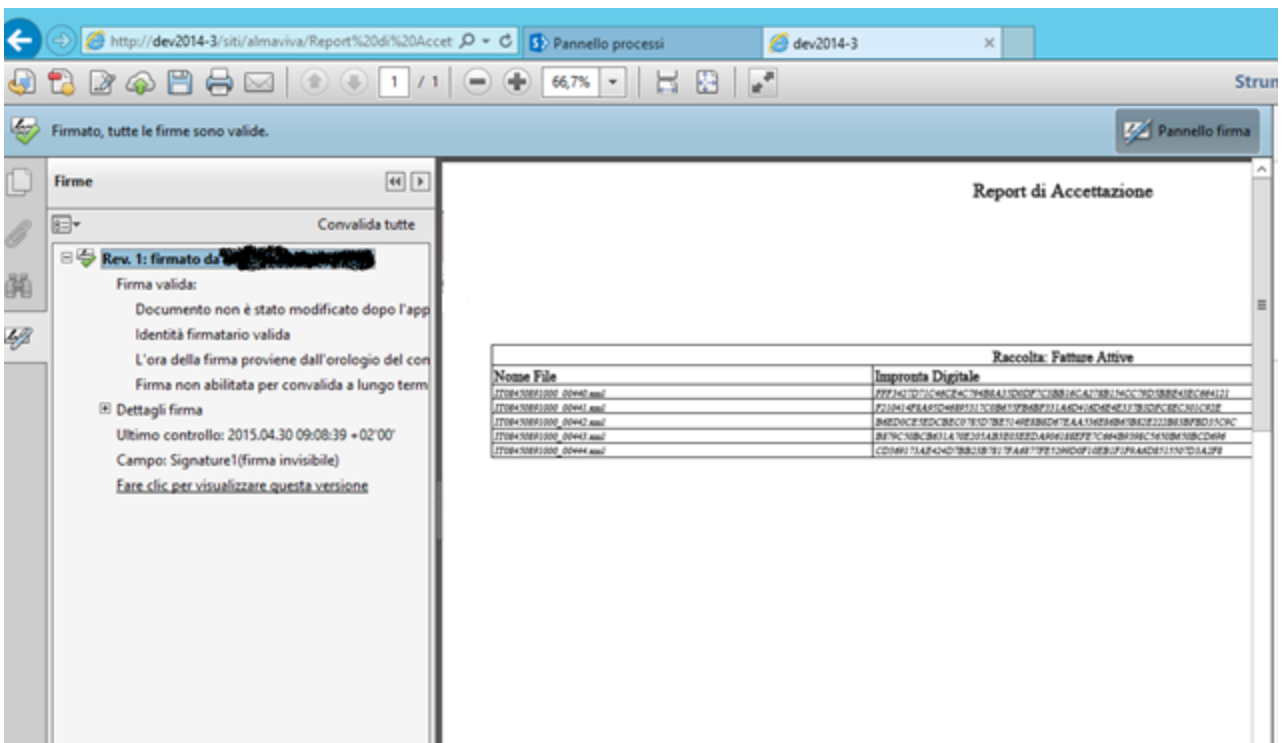


Figura 6 – Dettagli del rapporto di versamento

Nella “Figura 6 – Dettagli del rapporto di versamento” è rappresentato il form dei dettagli di firma del rapporto di versamento; per ogni “Nome File” relativo alle fatture versate viene evidenziata l’ “Impronta digitale”.

Di seguito invece viene evidenziata un’immagine che descrive i pacchetti di versamento accettati e che saranno oggetto del processo di conservazione e generazione del pacchetto di Archiviazione :



Figura 7 – Pannello di visualizzazione dei PdV accettati

Nella “**Figura 7 – Pannello di visualizzazione dei PdV accettati**” è rappresentato il form dei dettagli dei pacchetti di versamento accettati; per ogni “Società” è indicato il “Sito sorgente” (indirizzo del pacchetto), la “Raccolta” (tipologia di documenti) e lo “ID versamento” (codice identificativo del pacchetto di versamento).

Si evidenzia comunque che il sistema di conservazione consente agli utenti produttori di produrre pacchetti di versamento in modo autonomo, rispettando i vincoli pre-concordati con il produttore (ovvero Cliente) stesso. Tali pacchetti di versamento possono essere annullati e quindi eliminati dal sistema direttamente dagli utenti stessi, prima della produzione del rapporto di versamento. Tale operazione è loggata dal sistema. I pacchetti di Versamento vengono eliminati fisicamente dal sistema e ne rimane dunque traccia nel sistema dei Log che ovviamente viene conservato anch'esso secondo quanto descritto nel presente Manuale.

Qualora il produttore abbia la necessità di cancellare un documento già versato e già presente nel rapporto di versamento, dovrà essere fatta una segnalazione tramite un'interfaccia dedicata e che verrà inviata direttamente sul cruscotto gestito dal responsabile del servizio di conservazione, il quale dovrà riprodurre un nuovo rapporto di versamento, privo del documento cancellato, ma che contenga comunque il riferimento al rapporto di versamento precedente, compreso il rispettivo hash. Qualora invece il Produttore voglia sostituire un documento già versato e per il quale sia già stato prodotto un rapporto di versamento, invierà sempre una segnalazione tramite un'interfaccia dedicata e che verrà sempre notificata sul cruscotto del responsabile del servizio di conservazione, il quale chiederà un versamento correttivo e/o aggiuntivo. In questo caso, il produttore, secondo le metodologie già descritte di versamento, potrà inviare il documento corretto e sarà prodotto un nuovo rapporto di versamento che conterrà sempre il riferimento al precedente rapporto di versamento con relativa impronta.

Il sistema di conservazione quindi consente il caricamento di tutte le tipologie di file oltre a quelli più diffusi (pdf e xml) purchè questi siano sempre firmati digitalmente in CADE, PADES o XADES o se non firmati, solo ed esclusivamente siano documenti contabili analogici identificati dal DMEF del 17 Giugno 2014.

Nella generazione dell'indice di conservazione IdC si terrà sempre conto dei metadati necessari ad individuare ed archiviare in modo corretto il documento. Oltre ai metadati minimi identificati sia dagli allegati del DPCM del 3 Dicembre 2013 [2] e dal DMEF del 17 Giugno 2014, potranno essere aggiunti metadati scelti secondo accordo con il Cliente.

[Torna al sommario](#)

6.3. Pacchetto di archiviazione

Un pacchetto di archiviazione contiene un numero variabile di documenti informatici e il loro relativo indice di conservazione (in formato XML standard Sincro).

L'indice di conservazione definito come IdC è un file in formato XML che riporta per ogni documento archiviato alcune informazioni del file stesso tra cui una stringa URN e un'impronta HASH.

L'URN è una stringa che rappresenta in maniera univoca il file stesso senza determinarne l'ubicazione mentre la stringa di HASH rappresenta un'impronta del documento ricavata dalla sequenza di bit del file stesso che garantisce nel tempo il controllo della corrispondenza esatta del contenuto originale.

Di seguito viene riportato lo schema del file XML dell'IdC (che risponde allo standard Sincro UNI 11386:2010 <http://www.uni.com>) ed un suo esempio:

Figura 8 –Struttura file XML IdC

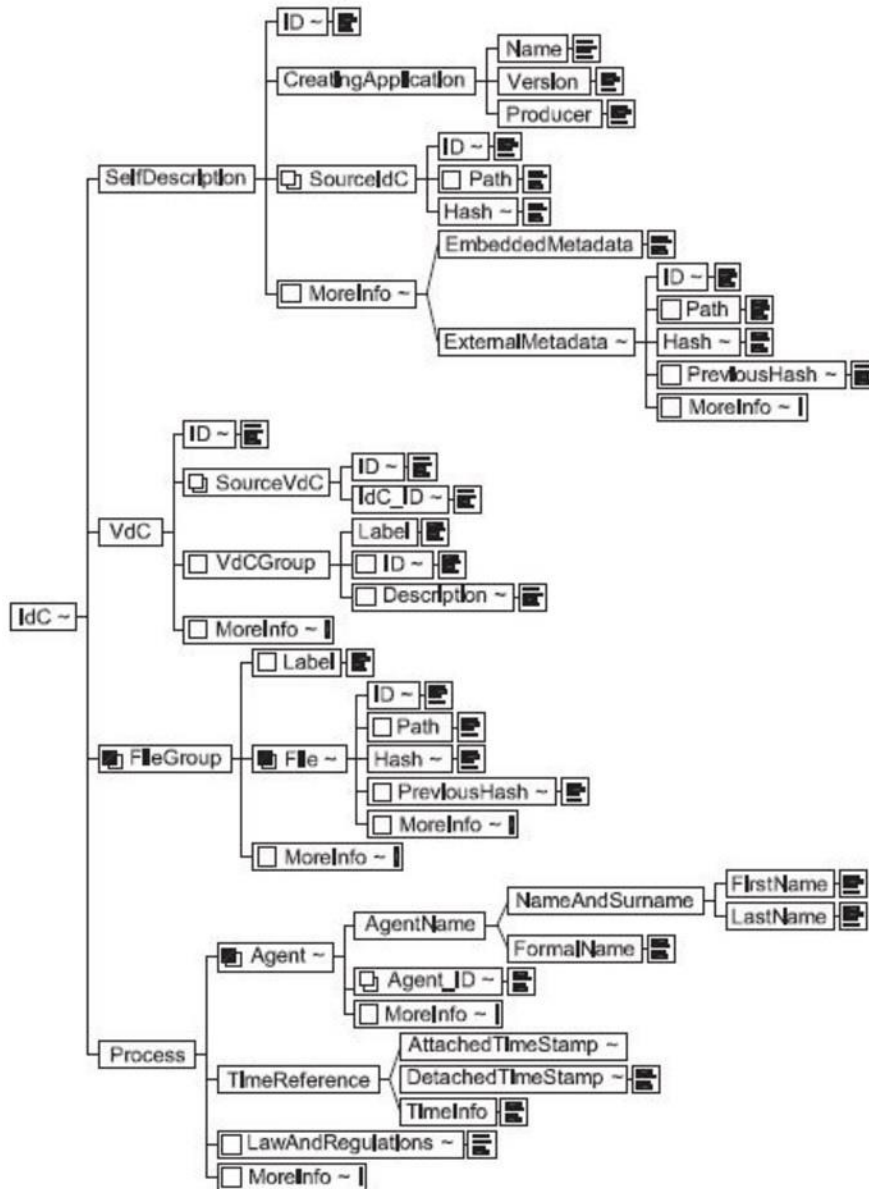


Figura 8 –Struttura file XML IdC

Nella “**Figura 8 – Struttura file XML IdC**” è rappresentata la struttura del file indice del pacchetto di conservazione (Indice di Conservazione). Il primo elemento è proprio lo “IdC” ovvero l’indice che contiene le informazioni relative al pacchetto di archiviazione; comprende (rappresentato nella figura da una parentesi graffa) : l’elemento “SelfDescription”, l’elemento “VdC”, l’elemento “FileGroup”, l’elemento “Process”. L’elemento “SelfDescription” comprende (rappresentato nella figura da una parentesi graffa) : l’elemento “ID”, l’elemento “CratingApplication”, l’elemento “SourceIdC”, l’elemento “MoreInfo”. L’elemento “CratingApplication” a sua volta comprende (rappresentato nella figura da una parentesi graffa) : l’elemento “Name”, l’elemento “Version” e l’elemento “Producer”. L’elemento “SourceIdC” a sua volta comprende (rappresentato nella figura da una parentesi graffa) :

l'elemento "Id", l'elemento "Path" e l'elemento "Hash". L'elemento "MoreInfo" a sua volta comprende (rappresentato nella figura da una parentesi graffa) : l'elemento "EmbeddedMetadata" e l'elemento "ExternalMetadata", che a sua volta comprende (rappresentato nella figura da una parentesi graffa) : l'elemento "Id", l'elemento "Path", l'elemento "Hash", l'elemento "PreviousHash" e l'elemento "MoreInfo". L'elemento "VdC" (pari livello dell'elemento "SelfDescription") comprende (rappresentato nella figura da una parentesi graffa) : l'elemento "Id", l'elemento "SourceVdC", l'elemento "VdCGroup" e l'elemento "MoreInfo". L'elemento "SourceVdC" a sua volta comprende (rappresentato nella figura da una parentesi graffa) : l'elemento "Id" e l'elemento "IdC_ID". L'elemento "VdCGroup" a sua volta comprende (rappresentato nella figura da una parentesi graffa) : l'elemento "Label", l'elemento "Id" e l'elemento "Description". L'elemento "FileGroup" (pari livello dell'elemento "VdC") comprende (rappresentato nella figura da una parentesi graffa) : l'elemento "Label", l'elemento "File", e l'elemento "MoreInfo". L'elemento "File" a sua volta comprende (rappresentato nella figura da una parentesi graffa) : l'elemento "Id", l'elemento "Path", l'elemento "Hash", l'elemento "PreviousHash" e l'elemento "MoreInfo". L'elemento "Process" (pari livello dell'elemento "FileGroup") comprende (rappresentato nella figura da una parentesi graffa) : l'elemento "Agent", l'elemento "TimeReference", l'elemento "LawAndRegulations" e l'elemento "MoreInfo". L'elemento "Agent" a sua volta comprende (rappresentato nella figura da una parentesi graffa) : l'elemento "AgentName", l'elemento "Agent_ID" e l'elemento "MoreInfo". L'elemento "AgentName" a sua volta comprende (rappresentato nella figura da una parentesi graffa) : l'elemento "NameAndSurname" e l'elemento "FormalName". L'elemento "NameAndSurname" a sua volta comprende (rappresentato nella figura da una parentesi graffa) : l'elemento "FirstName" e l'elemento "LastName". L'elemento "TimeReference" comprende (rappresentato nella figura da una parentesi graffa) : l'elemento "AttachedTimeStamp", l'elemento "DetachedTimeStamp" e l'elemento "TimeInfo".

La soluzione adottata è compliant con lo standard UNI 11386 [UNI 11386:2010 - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali (SinCRO)]. [\[4\]](#) All'interno della sottocommissione DIAM/SC11 (Gestione dei documenti archivistici) dell'Ente nazionale italiano di unificazione (UNI), un apposito gruppo di lavoro denominato SInCRO, ha definito la struttura dell'insieme dei dati a supporto del processo di conservazione individuando gli elementi informativi necessari alla creazione di un Indice di Conservazione.


```
<?xml version="1.0" encoding="UTF-8"?>
<syncro:IdC xmlns:syncro="http://www.uni.com/U3011/sincro/" syncro:url="http://www.uni.com/U3011/sincro/" syncro:version="1.0">
  <syncro:SelfDescription>
    <syncro:ID>Processo_x0020_conservazione_x0020_sostitutiva</syncro:ID>
    <syncro:CreatingApplication>
      <syncro:Name>Name</syncro:Name>
      <syncro:Version>6.0.22</syncro:Version>
      <syncro:Producer> Producer</syncro:Producer>
    </syncro:CreatingApplication>
  </syncro:SelfDescription>
  <syncro:VdC>
    <syncro:ID>302322ed-b343-4dea-8ae2-7f88e4283528</syncro:ID>
  </syncro:VdC>
  <syncro:FileGroup>
    <syncro:Label>c0bda191-100d-434e-b515-98d680d53946</syncro:Label>
    <syncro:File>
      <syncro:ID>1:c0bda191-100d-434e-b515-98d680d53946</syncro:ID>
      <syncro:Path>http://iwgdemo:7000/siti/Volume '2014/Fatture%20Attive_2/IT08450891000_00440.xml</syncro:Path>
      <syncro:Hash syncro:function="SHA256">FFF3427D71C46CE4C79488A35D0DF7C38816CA2788154CC79D588E43EC664121</syncro:Hash>
      <syncro:MoreInfo syncro:XMLScheme="file://metadata.xsd">
        <syncro:EmbeddedMetadata>
          <syncro:Denominazione>-</syncro:Denominazione>
          <syncro:PartitaIVA>Partita IVA</syncro:PartitaIVA>
          <syncro:CodiceFiscale>Codice Fiscale</syncro:CodiceFiscale>
          <syncro:NumeroFattura>-</syncro:NumeroFattura>
          <syncro>DataFattura>11-10-2014</syncro>DataFattura>
          <syncro:RagioneSociale>Ragione Sociale</syncro:RagioneSociale>
        </syncro:EmbeddedMetadata>
      </syncro:MoreInfo>
    </syncro:File>
  </syncro:FileGroup>
</syncro:IdC>
```

Figura 9 – Porzione esempio file XML IdC

Nella “Figura 9 – Porzione esempio file XML IdC” è rappresentata una porzione di XML di un IDC. L’elemento “SelfDescription” è valorizzato nel seguente modo : “Id” = “Processo_xD020_conservazione_xD020_sostitutiva”; “CreatingApplication”_”Name” = “Name”, “CreatingApplication”_”Version” = “6.0.22”, “CreatingApplication”_”Produce” = “Producer”. L’elemento “VdC” è valorizzato nel seguente modo : “ID” = “302322ed-b343-4dea-8ae2-7f88e4283528”. L’elemento “FileGroup” è valorizzato nel seguente modo : “Label” = “c0bda191-100d-434e-b515-98d680d53946”; l’elemento “File”_”ID” = “1: c0bda191-100d-434e-b515-98d680d53946”; l’elemento “File”_”Path” = http://iwgdemo:7000/siti/Volume 2014/Fatture%20Attive_2/IT08450891000_00440.xml; l’elemento “File”_”Hash” = “SHA56>FFF3427D71C46CE4C79488A35D0DF7C38816CA2788154CC79D588E43EC664121”; l’elemento “File”_”MoreInfo” = file://metadata.xsd; l’elemento “File”_”EmbeddedMetadata”_”Denominazione” = “-“; l’elemento “File”_”EmbeddedMetadata”_”PartitaIVA” = “Partita IVA”; l’elemento “File”_”EmbeddedMetadata”_”CodiceFiscale” = “Codice Fiscale”; l’elemento “File”_”EmbeddedMetadata”_”NumeroFattura” = “-“; l’elemento “File”_”EmbeddedMetadata”_”DataFattura” = “11-10-2014”; l’elemento “File”_”EmbeddedMetadata”_”RagioneSociale” = “Ragione Sociale”.

L’implementazione di tale indice, del quale SInCRO ha descritto sia la semantica sia l’articolazione, permette di utilizzare una struttura-dati condivisa e raggiungere un soddisfacente grado d’interoperabilità nei processi di migrazione, mediante l’adozione di uno Schema XML appositamente elaborato.

Il pacchetto di archiviazione verrà quindi firmato e marcato temporalmente dal responsabile del

servizio di conservazione, entro i limiti di tempo di conservazione imposti dalle normative in vigore e garantendo quindi integrità, autenticità, robustezza, certezza e immutabilità del file XML IdC e quindi del file UNISINCRO. Di seguito un'immagine che evidenzia un indice di conservazione firmato e marcato temporalmente e verificato con il visualizzatore gratuito Dike e che attesta che il documento è firmato con un certificato valido e con marca temporale valida. Si precisa inoltre che il sistema di conservazione qui presentato, ovviamente effettua un controllo sulla validità del certificato di firma del responsabile del servizio di conservazione e sulla validità e disponibilità delle marche temporali.

Nome File	Esito Verifica	Verifica alla Data	Algoritmo Digest	Firmatario	Ente Certificatore	Cod. Fiscale	Stato	Organizzazione
IdC_Fatture_30-04-2015_09.10.14.xml.p7m (Firme totali apposte: 2)	Firma CADES OK	<input checked="" type="checkbox"/> verifica alla data? clicca qui...	SHA-256	MASSIMO MAGGIORA	ArubaPEC S.p.A. NG CA 3	MGGMSM55E05L219X	IT	non presente
	Marca sulla Firma OK Data Marca: 30/04/2015 07.10.31 (UTC Time)		SHA-256	ICEDTS04201504	InfoCert Time Stamping Authority 2		IT	INFOCERT SPA

Figura 10 – Pannello che evidenzia le informazioni del PdA

Nella “Figura 10 – Pannello che evidenzia le informazioni del PdA” è rappresentato il form delle informazioni dei pacchetti di archiviazione; per ogni “Nome File” è indicato : “Esito Verifica” (es. Firma CADES OK, Marca sulla firma OK Data marca.....), “Verifica alla Data” (campo da selezionare se si vuole verificare i dettagli della firma), “Algoritmo Digest” (es. SHA-256), “Firmatario” (Nome del firmatario), “Ente Certificatore” (es. ArubaPEC, InfoCert), “Codice Fiscale”, “Stato” (IT), “Organizzazione” (es. InfoCert).

Come si nota nell'immagine di sopra, il nome del PdA è certamente univoco in quanto viene costituito dalla data e dall'ora . Si precisa anche che il sistema è in grado di verificare che il PdA corrisponde esattamente all'indice di conservazione di cui fanno parte i documenti conservati e che non possono essere presente metadati vuoti. Qualora un metadati non sia valorizzato, il suo valore nel PdA corrisponde a n/a in modo tale da identificare la mancanza di quel valore per quel particolare tipo di documento. Oltre alla firma digitale , come si nota nell'immagine di sopra, viene evidenziata anche la marca temporale atta a garantire che i documenti conservati nel PdA da quella data certa in poi non potranno essere più modificati. Si ricorda, infatti, che un controllo successivo permetterà di controllare e verificare che l'impronta del documento rimanga invariata nel tempo anche a seguito della marca temporale e della firma digitale effettuate in un determinato giorno

E' inoltre controllato che un documento già archiviato non venga nuovamente portato in archiviazione. Prima che venga effettuato il rapporto di versamento, il sistema calcolerà l'impronta hash di ogni file (l'impronta che verrà messa nel rapporto di versamento) per poter verificare all'interno dei volumi di conservazione se il documento è già presente.

Nel caso in cui il documento sia già presente verrà generato un report di controllo con la descrizione di tale problema, specificando il documento doppio.

Per la firma digitale del PdA, sarà possibile inoltre utilizzare più CA. La funzionalità in pratica consente di censire per ogni tenant un'anagrafica di CA da utilizzare per la firma digitale e la marca temporale.

In configurazione è possibile definire un numero n di CA con le seguenti informazioni:

- Nome CA
- Descrizione
- Indirizzo web service firma digitale
- Indirizzo web service marca temporale
- Tipo di credenziali

Se un tenant ha configurato più di una CA, al momento di effettuare la firma digitale il sistema chiederà quale CA utilizzare.

Inoltre in base alla tipologia di documento che ogni PdA contiene, il sistema permette all'utente di effettuare una ricerca sui PdA creati.

Il sistema permette all'utente finale di scegliere la tipologia di documento su cui cercare.

In base alla tipologia il sistema propone i campi di ricerca generici relativi a quella tipologia e consente di ricercare su tutti i PdA di quella tipologia.

Un pacchetto di archiviazione una volta concluso e generato può essere annullato. A differenza del pacchetto di versamento un pacchetto di archiviazione quando viene annullato non viene eliminato fisicamente ma solo logicamente, per permettere al responsabile del servizio di conservazione, di avere un controllo esclusivo e sicuro anche sui pacchetti cancellati.

Un pacchetto di archiviazione può essere annullato dal responsabile del servizio di conservazione, previa informativa/condivisione con il produttore e trasmissione mail dell'avvenuto annullamento. Tutti i pacchetti nello stato annullato potranno essere inseriti come riferimento ai nuovi pacchetti di archiviazione per poter definire un riferimento ai pacchetti annullati da parte dei nuovi PdA.

Tale riferimento sarà presente all'interno dell'indice di conservazione del nuovo pacchetto di archiviazione secondo lo standard UniSINCRO. [4]

[Torna al sommario](#)

6.4. Pacchetto di distribuzione

Il sistema permette la ricerca nel tempo di tutti i pacchetti di archiviazione precedentemente creati, tramite interfaccia web con un sistema di autenticazione e autorizzazione.

A fronte di una ricerca da parte dell'utente il sistema mette a disposizione un oggetto detto pacchetto di distribuzione.

L'accesso a tale oggetto avviene in un area riservata al cliente soggetta ad autenticazione e inserito in un archivio a norma contenente l'indice di conservazione dell'oggetto stesso (IPdA).

Il pacchetto di distribuzione generato da un PdA e fornito al cliente contiene i seguenti oggetti:

1. Elenco dei documenti contenuti nel PdA con i relativi metadati su raccolta SharePoint
2. IdC.xml.p7m firmato e marcato

Si precisa che il PdD coincide con il PdA e che è possibile per l'utente che ne richiede l'esibizione, avere accesso riservato all'Area dedicata alla consultazione dei PdD che quindi sono autoconsistenti

e che potranno essere distribuiti al di fuori del sistema di conservazione qualora fosse richiesto dagli Organi Competenti. Qualora questo avvenga, il PdD verrà firmato digitalmente al momento della distribuzione al di fuori del sistema dal responsabile del servizio di conservazione che ne attesta l'integrità e la piena corrispondenza non solo con il PdA ma anche con quanto richiesto .



Nome PdA	TEST
Società	Almaviva
Responsabile Conservazione	[REDACTED]
Password certificato	<input type="text"/>

Crea pacchetto Distribuzione

Figura 11 –Pannello di creazione PdD

Nella “**Figura 11 – Pannello di creazione PdD**” è rappresentato il form di firma del PdD; è indicato : il “NomePdA” (da cui viene prodotto il PdD), la “Società”, il “Responsabile Conservazione” ed il campo “Password certificato” nel quale il responsabile valorizza la password per la firma.



Home PdD  MODIFICA COLLEGAMENTI

Fatture Attive - 08-05-2015 11-09-39 (PdD)

Home page

Fatture Attive - 08-05-2015
11-09-39 (PdD)

 MODIFICA COLLEGAMENTI

 nuovo documento o trascinare i file qui

Tutti i documenti ...

✓ 	Nome	Data/ora modifica	Autore ultima modifica
	Fatture Attive - 08-05-2015 11-09-39 (PdD) ✱	... Pochi secondi fa	<input type="checkbox"/> Account di sistema
	IdC_08-05-2015_11.09.47.xml ✱	... Pochi secondi fa	<input type="checkbox"/> Account di sistema
	IT08450891000_00440 ✱	... Pochi secondi fa	<input type="checkbox"/> Account di sistema
	IT08450891000_00441 ✱	... Pochi secondi fa	<input type="checkbox"/> Account di sistema
	IT08450891000_00442 ✱	... Pochi secondi fa	<input type="checkbox"/> Account di sistema
	IT08450891000_00443 ✱	... Pochi secondi fa	<input type="checkbox"/> Account di sistema
	IT08450891000_00444 ✱	... Pochi secondi fa	<input type="checkbox"/> Account di sistema

Figura 12 –Dettaglio informazioni PdD

Nella “**Figura 12 – Dettaglio informazioni PdD**” è rappresentato il form che elenca le informazioni di dettaglio del PdD, comprendenti : il file IdC.xml, e tutti i documenti (nel caso esposto, fatture).

Al termine o alla cessazione del contratto di un determinato Ente-Cliente, il sistema mette a disposizione al cliente finale (produttore) la possibilità di estrarre tutti i pacchetti di archiviazione generati fino a quel momento generando un file ZIP per ogni PdD

Il sistema consente tramite l'apposita funzionalità sul pannello di configurazione di generare un export di file ZIP contenenti ognuno un PdD. Il sistema crea in automatico un'area temporanea in cui vengono messi il file ZIP per il download da parte dell'utente produttore.

Alla richiesta di export il sistema tramite un processo timer genera i file ZIP e li deposita nell'apposita area temporanea.

Tale area è disponibile per i successivi tre mesi dalla cessazione del contratto.

[Torna al sommario](#)

7. IL PROCESSO DI CONSERVAZIONE

Di seguito lo schema sintetico delle fasi del processo di conservazione



Figura 13 –Schema sintetico del processo di conservazione

Nella “**Figura 13 – Schema sintetico del processo di conservazione**” sono evidenziati i passi principali del processo di conservazione. Il processo inizia con la fase “Pacchetto di versamento (web services, upload spool stampa, acquisizione metadati, marcatura con datamatrix), poi la fase “Processo di verifica” (verifiche numerazione, verifiche metadati, verifiche datamatrix, PDF corrotti/vuoti, calcolo impronte), che produce un “Report di verifica” (errori/scarti, anomalie numerazione); a seguito dell’esito della verifica può innescarsi una “Attività di correzione “ (analisi documenti errati, aggiornamento PdV, sincronizzazione gestionale) oppure si ha un “Avanzamento processo” (registrazione estrazione) che produce un “Rapporto di versamento” (firma report di verifica); il successivo “Avanzamento processo” (firma rapporto di versamento) porta alla fase di “Estrazione elementi” (totale/parziale); il nuovo “Avanzamento di processo” (registrazione estrazione) porta alla fase della creazione del “Pacchetto di archiviazione” (unico XML con metadati, standard Sincro/OAIS); un ulteriore “Avanzamento processo “ (PdA completato) porta alla fase di creazione del “Pacchetto di distribuzione” (PdA firmato, firma e marca temporale); infine l’ultimo “Avanzamento di processo” (PdD completato) porta alla fase “Versamento archivi” (creazione copie di sicurezza, archiviazione locazioni definite) che pone fine al processo.

Il processo di conservazione dunque si avvale delle seguenti fasi :

- Gestione e Presa in carico del Pacchetto di Versamento;
- Processo di Verifica di ogni singolo PdV e gestione degli errori e delle segnalazioni;
- Report di verifica che riporta eventuali errori e o anomalie sul Pacchetto di Versamento inviato. Tale report non viene firmato digitalmente dal responsabile del servizio di conservazione, ma evidenzia esclusivamente un report/statistiche sul numero dei documenti inviati dal Produttore e sullo stato del Pacchetto di Versamento
- Attività di correzione, in presenza di eventuali errori bloccanti, per la generazione di alert verso il Produttore e rinvio dei documenti per la generazione e presa in carico di un nuovo PdV, che sostituisce quello precedente che ha il suo interno degli errori;
- Avanzamento del processo di gestione e presa in carico del PdV a seguito di controlli con firma digitale da parte del responsabile del servizio di conservazione del rapporto di versamento
- Estrazione degli elementi facenti parte del PdV
- Generazione del Pacchetto di Archiviazione secondo norme UNI Sincro e OAIS; [4]
- generazione del Pacchetto di Distribuzione, che coincide esattamente con il PdA, su richiesta del cliente
- Versamento dei Pacchetti di Archiviazione e Distribuzione su server certificati ISO 27001 o Supporto Idoneo alla conservazione.
- Il sistema di conservazione effettua il log di ogni azione che viene effettuata sul sistema, dalla modifica delle configurazioni alla firma digitale e marca temporale.

Le categorie di log del sistema si possono riassumere in:

- Azioni intraprese in Configurazioni (inserimento, modifica, eliminazione di qualsiasi anagrafica)
- Azioni intraprese in PdV
- Azioni intraprese in PdA
- Azioni intraprese in PdD

[Torna al sommario](#)

7.1. Creazione del servizio

Il servizio di Conservazione per ogni Cliente viene attivato al termine di un processo di configurazione che segue queste fasi fondamentali:

- a) Condivisione con il produttore (cliente) delle tipologie di documenti che saranno conferiti al servizio di conservazione
- b) Condivisione informazioni tecniche di richiesta configurazione PDV: questa fase comprende la definizione di dettaglio dei PDV che il produttore (o Cliente) andrà a produrre ed i controlli che verranno attivati sul sistema di conservazione.
- c) Creazione del tenant SharePoint messo a disposizione del cliente per il caricamento dei pacchetti di Versamento e la creazione dei relativi volumi di conservazione e pacchetti di archiviazione.
- d) Validazione delle configurazioni da parte del Responsabile del servizio di conservazione e del Responsabile sistemi informativi per la conservazione;
- e) Condivisione con il cliente ed attivazione dei canali di comunicazione per la ricezione dei Pacchetti di Versamento
- f) Configurazione ambiente di produzione e start-up del servizio;
- g) Generazione e Firma del Report di Versamento;

- h) Gestione Controlli e Verifiche;
- i) Validazione e fasi successive per la creazione del Pacchetto di Archiviazione
- j) Conservazione del Pacchetto di Archiviazione e disponibilità dello stesso con generazione del Pacchetto di Distribuzione.

Nella fase di attivazione del servizio vengono definiti i canali utilizzati per lo scambio informativo tra produttore e conservatore.

Tali canali avranno caratteristiche di sicurezza ed identificazione del mittente:

- SFTP
- https
- Certificato lato Client

[Torna al sommario](#)

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

La corretta ricezione dei PdV, proveniente dal Cliente, è monitorata dal Servizio Sistemistico tramite presidio del canale di comunicazione concordato. Tale presidio viene effettuato non solo tramite intervento umano, ma anche tramite automatismi di ascolto che generano informazioni di presa in carico dei pacchetti di versamento verso il responsabile della conservazione, che si ricorda ne detiene la responsabilità.

Ogni azione di ricezione/caricamento del pacchetto di versamento viene loggata sul sistema. In caso di ricezione di un pacchetto di versamento il sistema registra le seguenti informazioni:

- Data/ora
- Utente che ha effettuato l'operazione
- Descrizione dell'operazione
- Url sito in cui è avvenuto il caricamento
- Eventuali note

In caso di anomalie il Supporto Operativo prende in carico la segnalazione proveniente dal Servizio Sistemistico, contattando i riferimenti tecnici del cliente.

[Torna al sommario](#)

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

I controlli minimi effettuati sul pacchetto sono:

- Verifica presenza dei metadati minimi e di quelli concordati
- Verifica che l'ente produttore sia autorizzato all'invio dei documenti
- Verifica ed Identificazione univoca del soggetto produttore
- Verifica che il formato dichiarato dal Produttore sia corrispondente a quanto concordato

- Verifica della firma digitale su ogni documento (ove previsto)
- Verifica che la firma digitale sui documenti sia quella del soggetto Produttore

Nel caso in cui uno o più controlli non vadano a buon fine il sistema genera due tipi di eccezioni, una di warning e una di alert bloccante. La prima decreta la differenza tra quanto atteso e quanto prodotto, la seconda blocca l'utente attendendo un secondo caricamento.

Le operazioni di versamento, come tutte le operazioni di rilievo normativo, vengono tracciate in specifici log applicativi, su tabelle del database ovvero su file system, a seconda della tipologia delle informazioni ivi contenute.

I log memorizzati su database vengono mantenuti online per tutta la durata del periodo di conservazione, mentre quelli su file system vengono opportunamente suddivisi per mese / anno per una maggior facilità di consultazione.

Per maggiori dettagli sul log vedere il capitolo 9 del seguente documento, mentre per maggiori informazioni circa l'integrità del Pacchetto di Versamento e del Processo di Versamento si rimanda al paragrafo 6.2. [5]

[Torna al sommario](#)

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

Se i controlli sul pacchetto di versamento sono andati a buon fine e quindi il sistema restituisce un esito positivo

Il sistema memorizza i documenti all'interno di una raccolta SharePoint dedicata al pacchetto di Versamento predisponendo il pacchetto per essere usato per iniziare un processo di conservazione o eventualmente firmare obbligatoriamente digitalmente i documenti non firmati e poi iniziare un processo. Si ricorda a tal fine, infatti, che non è possibile conservare documenti privi di firma digitale, secondo quanto richiesto dal DMEF del 17 Giugno del 2014. A tal fine, si ricorda che nel paragrafo 6.2 [5] vengono indicati gli errori bloccanti in caso appunto di mancata firma digitale sui documenti contenuti nel Pacchetto di Versamento e che devono essere conservati.

Ogni azione di ricezione/caricamento del pacchetto di versamento viene loggata sul sistema.

In caso di accettazione o rifiuto di un pacchetto di versamento il sistema registra le seguenti informazioni:

- Data/ora
- Utente che ha effettuato l'operazione
- Descrizione dell'operazione
- Url sito in cui è avvenuto il caricamento
- Eventuali note sulla motivazione del rifiuto

[Torna al sommario](#)

7.5. Rifiuto dei pacchetti di versamento e modalità di comunicazione delle anomalie

Se il controllo del pacchetto di versamento rileva degli errori, il sistema presenta l'elenco degli errori

riscontrati, in un report di controllo, come in figura sotto

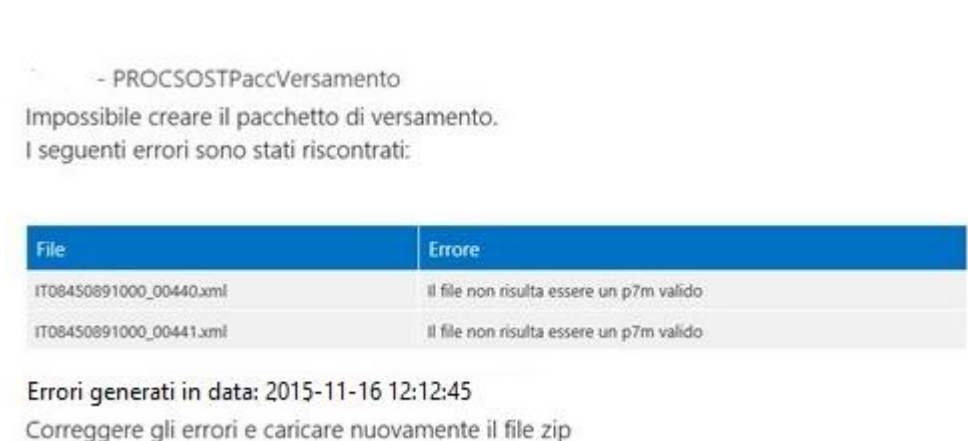


Figura 14 – evidenza errori PdV

Nella “**Figura 14 – evidenza errori PdV**” è rappresentato il form che elenca le informazioni di errore evidenziati dall’analisi del PdV, ovvero “file” e “errore” (descrizione)

Se il sistema riscontra almeno un errore il pacchetto di versamento viene rifiutato e non viene caricato sul sistema. In questo caso si richiede al Produttore di inviare un Pacchetto di Versamento corretto. I vari errori che possono essere riscontrati sono:

- Il file non risulta essere un p7m valido
- Il pacchetto fornito non presenta il file di descrizione info.txt fornito per le fatture elettroniche
- Il file non risulta essere firmato digitalmente (caso firma PADES)
- Il file è corrotto.

Viene fornito il riferimento temporale (timestamp) di tale report, tale timestamp viene generato dall’orario del server che è sincronizzato con l’NTP.

[Torna al sommario](#)

7.6. Creazione del pacchetto di archiviazione

Inizio del processo e verifica metadati

Il processo di conservazione può effettuare alcuni controlli obbligatori e non:

- Verifica apertura file (obbligatorio)
- Verifica datamatrix e metadati: questa procedura effettua la lettura del datamatrix presente all’interno del documento pdf (se presente) e si occupa di controllare che il contenuto del datamatrix sia uguale ai metadati memorizzati sulla raccolta documentale (facoltativo)

Nella “**Figura 16 – Rapporto di versamento**” è rappresentato il form che elenca le informazioni di rapporto di versamento : “nome file”, “impronta digitale”

In caso di esito negativo il sistema genera un report di controllo in cui viene effettuata una distinta che contiene l’elenco dei documenti che hanno riscontrato un problema nel controllo. Inoltre il problema viene visualizzato in una tabella di fianco a ciascun documento, indicando quindi il motivo del rifiuto.

I vari errori che possono essere riscontrati sono:

- Il file non risulta essere un p7m valido
- Il pacchetto fornito non presenta il file di descrizione info.txt fornito per le fatture elettroniche
- Il file non risulta essere firmato digitalmente (caso firma PADES)
- Il file è corrotto.

Viene fornito il riferimento temporale (timestamp) di tale report, tale timestamp viene generato dall’orario del server che è sincronizzato con l’NTP.

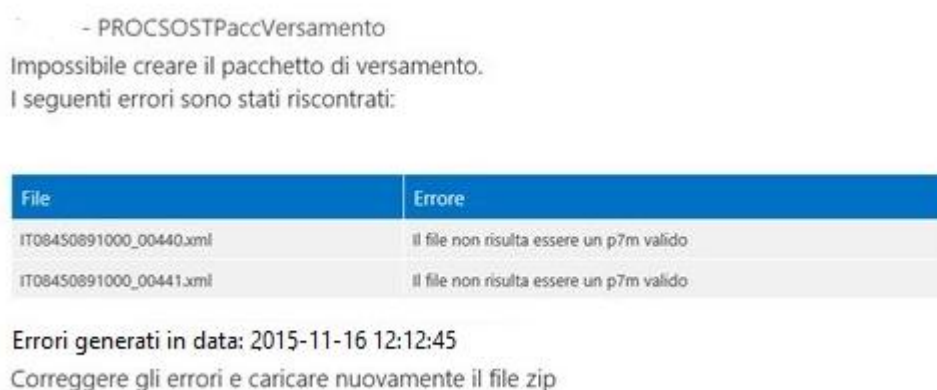


Figura 17 – Report di controllo

Nella “**Figura 17 – Report di controllo**” è rappresentato il form che elenca le informazioni relative agli errori riscontrati nel PdV : “file”, “errore” (es. “il file non risulta essere un p7m valido”).

Firma digitale rapporto di versamento

Generato il rapporto di versamento quest’ultimo deve essere firmato digitalmente dal responsabile del servizio di conservazione. Il processo del sistema prosegue consentendo di firmare digitalmente il documento PDF che rappresenta il suddetto report.

[Torna al sommario](#)

7.7. Preparazione e gestione del pacchetto di archiviazione

Firmato il rapporto di versamento il sistema procede alla creazione del pacchetto di archiviazione rispetto al pacchetto di versamento da portare in conservazione.

Il pacchetto di archiviazione è rappresentato da una raccolta SharePoint contenente tutti i documenti del pacchetto di versamento e l'indice di Conservazione firmato e marcato.

La conservazione dei documenti digitali vera e propria ha inizio con la formazione del PdA e la costruzione dell'indice.

Parte integrante di questo processo è la sottoscrizione digitale dell'Indice (Sincro) da parte del responsabile del servizio di conservazione. In questa fase è inclusa anche l'apposizione di un "time-stamp", ovvero un riferimento temporale certificato che costituisce evidenza dell'esistenza e dell'esatta composizione del file collegato all'istante indicato (Tcons).

Apponendo un time stamp all'indice lo si "sigilla" e contemporaneamente si fissa il riferimento temporale.

Inoltre vengono memorizzati i Log sia temporali sia operativi da parte del sistema di conservazione, nel momento in cui viene creato il pacchetto di archiviazione, riportando anche il riferimento del rispettivo rapporto di versamento precedentemente prodotto. Si veda il paragrafo 7.4 [\[6\]](#)

Con questo procedimento, dunque, si viene a costituire un riferimento temporale per ognuno dei file inclusi nel PdA.

In conclusione di tale processo abbiamo il PDA così costituito:

- idPdA.xml.p7m (firmato dal RdC)
- idPdA.xml.tsr (marca temporale)
- documenti con metadati (collocati su SharePoint)

Nome File	Esito Verifica	Verifica alla Data	Algoritmo Digest	Firmatario	Ente Certificatore	Cod. Fiscale	Stato	Organizzazione
IdC_Fatture_31-03-2015_01.06.21.xml.p7m (Firme totali apposte: 2)	Firma CADES OK	verifica alla data? clicca qui...	SHA-256	[REDACTED]	ArubaPEC S.p.A. NG CA 3	[REDACTED]	IT	non presente
	Marca sulla Firma OK Data Marca: 31/03/2015 11.06.34 (UTC Time)		SHA-256	ICEDTS04201501	InfoCert Time Stamping Authority 2		IT	INFOCERT SPA

Figura 18 – Indice PdA firmato e marcato

Nella “**Figura 18 – Indice PdA firmato e marcato**” è rappresentato il form che elenca le informazioni relative all'indice PdA (firmato e marcato); per ogni “Nome File” è indicato : “Esito Verifica” (es. Firma CADES OK, Marca sulla firma OK Data marca), “Verifica alla Data” (campo da selezionare se si vuole verificare i dettagli della firma), “Algoritmo Digest” (es. SHA-256), “Firmatario” (Nome del firmatario), “Ente Certificatore” (es. ArubaPEC, InfoCert), “Codice Fiscale”, “Stato” (IT), “Organizzazione” (es. InfoCert).

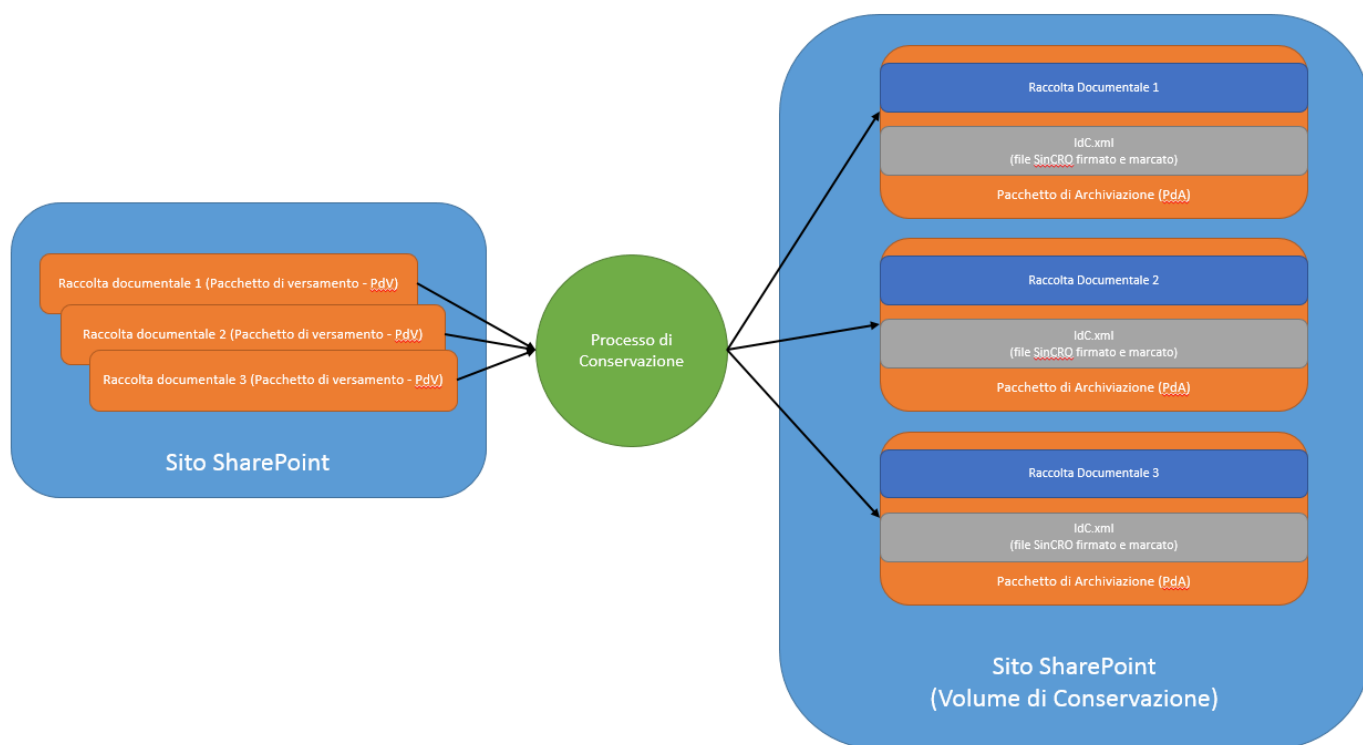


Figura 19 – Schema strutturale generazione PdA

Nella “**Figura 19 – Schema strutturale generazione PdA**” è sintetizzato lo schema della transizione dal PdV al PdA, tramite il servizio di conservazione. Nel riquadro a sinistra è evidenziato che nel sito sharepoint vengono trasferite le Raccolte documentali [“Raccolta documentale 1.. n (Pacchetto di versamento – PdV)”]. Queste Raccolte documentali puntano (attraverso le frecce) al sistema di conservazione che crea nel riquadro a destra (sito sharepoint-Volume di conservazione) altrettanti PdA costituiti ognuno da : Raccolta documentale n, IdC xml, file Sincro firmato e marcato, Pacchetto di archiviazione (PdA).

[Torna al sommario](#)

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

L'utente può richiedere al sistema di conservazione l'accesso ai documenti per acquisire le informazioni di interesse nei limiti previsti dalla legge.

Tali informazioni vengono fornite ai soggetti autorizzati tramite l'accesso diretto, anche da remoto, al documento informatico conservato, attraverso la produzione di un pacchetto di distribuzione selettivo tramite specifica ricerca nel sistema di Conservazione a Norma.

Per quanto riguarda l'attività di ricerca e l'esibizione a norma dei documenti conservati (anche a fronte di una verifica ispettiva da parte delle Autorità competenti) lo strumento di accesso all'archivio documentale del Cliente è consentito da un'interfaccia web esposta dall'applicazione.

Il Cliente, tramite l'interfaccia messa a disposizione, può pertanto richiedere la visualizzazione di tutti i documenti conservati al fine di:

- Visionare e scaricare il documento conservato all'interno dell'archivio a norma;
- Verificare ed eventualmente scaricare le prove di conservazione (idPdA);

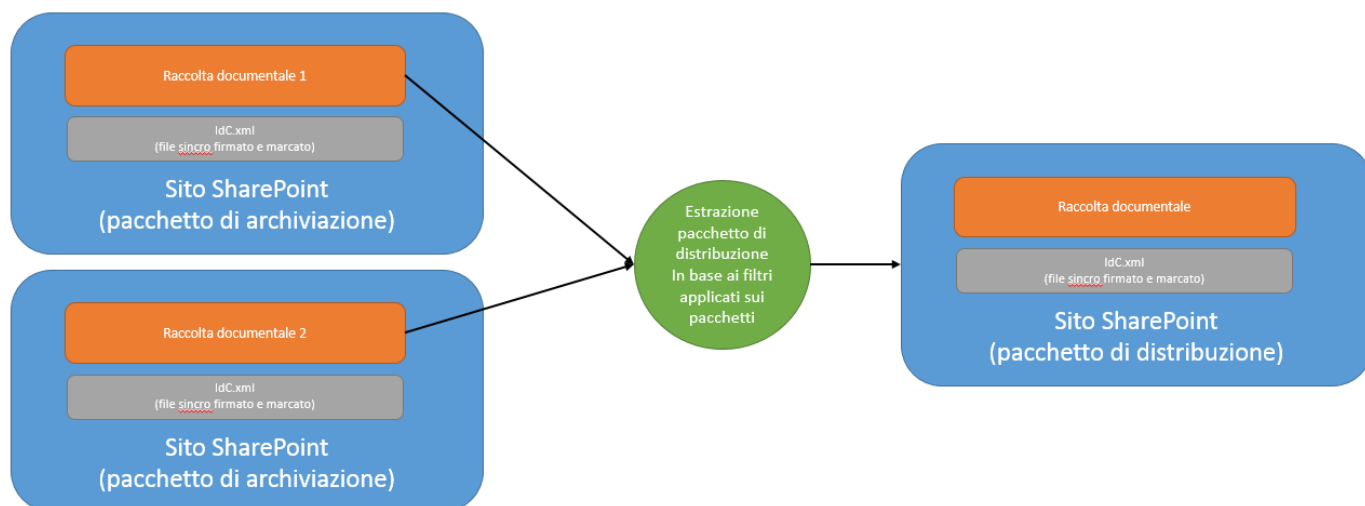
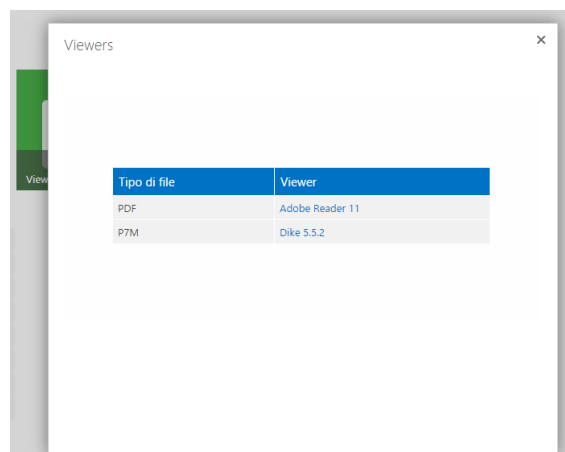


Figura 20 – Schema strutturale generazione PdD

Nella “**Figura 20 – Schema strutturale generazione PdD**” è sintetizzato lo schema della transizione dal PdA al PdD, tramite il servizio di conservazione. Nei riquadri a sinistra è evidenziato che nel sito sharepoint sono conservati i PdA costituiti ognuno da : Raccolta documentale n, IdC xml, file Sincro firmato e marcato, Pacchetto di archiviazione (PdA). Tramite il processo di estrazione del pacchetto di distribuzione, in base ai filtri applicati sui pacchetti, viene estratto il PdD (sempre nel sito sharepoint (Pacchetto di distribuzione) costituito da : raccolta documentale, IdC xml (file Sincro firmato e marcato).

Viewer di sistema

Ogni tipo di file portato in conservazione ha sul sistema associato un programma definito “viewer” che consente la visualizzazione di quel tipo di documento a distanza di tempo. E’ presente un mapping tra il tipo file ed il viewer associato



Tipo di file	Viewer
PDF	Adobe Reader 11
P7M	Dike 5.5.2

Figura 21 – Schermata dei viewer

Nella “**Figura 21– Schermata dei viewer**” è rappresentato il form che elenca i viewer utilizzati in base ai tipi file. Nelle colonne sono evidenziati i campi “Tipo di File” e “Viewer”; nelle righe sono evidenziati i valori assunti (nella figura : PDF → Adobe Reader 11, P7M → Dike 5.5.5)

[Torna al sommario](#)

7.9. Produzione di duplicati e copie informatiche e descrizione dell’eventuale intervento del pubblico ufficiale nei casi previsti

Tale processo si attua nel seguente modo :

“Riversamento diretto”

processo che trasferisce uno o più documenti conservati da un supporto di memorizzazione ad un altro, non alterando la loro rappresentazione digitale

"Riversamento sostitutivo"

processo che trasferisce uno o più documenti conservati da un supporto di memorizzazione (o da un sistema di conservazione) ad un altro, modificando la loro rappresentazione digitale. Per tale processo si deve allegare al PdA aggiornato, anche il precedente PdA evidenziando i cambiamenti in riferimento all’impronta del singolo documento e predisponendo la generazione del nuovo PdA che contenga il PdA da cambiare. Il PdA precedente deve essere trattato, dunque, come un nuovo PdA ma evidentemente con informazioni aggiuntive rispetto ad un normale e comune PdA qui descritto nel paragrafo 6.2. [5]

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 si necessiti un cambio di formato, rimarrà a carico del soggetto produttore.

[Torna al sommario](#)

7.10. Scarto dei pacchetti di archiviazione

Alla scadenza dei termini di conservazione relativi alla specifica tipologia documentale e comunque definiti in sede contrattuale con il Cliente, avviene lo scarto del Pacchetto di Archiviazione dal sistema

di conservazione a norma.

Per dare la possibilità di poter prolungare i termini di conservazione prima dello scarto, verrà data informativa al produttore con congruo anticipo (almeno 6 mesi) al fine di confermare la cancellazione ovvero mantenere in conservazione i PdA per un ulteriore anno.

Nel caso di archivi pubblici o privati di particolare interesse culturale, le procedure di scarto avvengono previa autorizzazione del Ministero dei beni e delle attività culturali e del turismo. Ad esempio qualora fosse necessaria la completa dematerializzazione di documenti sanitari, compresa la cartella clinica elettronica, verrà richiesta autorizzazione per lo scarto alla Soprintendenza Archivistica Regionale competente.

La cancellazione avverrà soltanto dopo che sono state eseguite le fasi di approvazione esplicita da parte del RdC e soltanto dopo aver consegnato al Cliente e Titolare dei documenti, il rispettivo Pacchetto di Distribuzione come specificato dalla norma. Inoltre il Pacchetto di Distribuzione deve essere autoconsistente e riportare all'interno : il manuale della conservazione, i documenti conservati, i files UNISincro, il visualizzatore di documenti firmati e marcati temporalmente, interfaccia di qualsiasi tipo per interrogare e cercare i documenti.

[Torna al sommario](#)

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

Le modalità con le quali garantire la interoperabilità e trasferibilità sono concordate con i singoli clienti e formalizzate nel contratto di servizio; la creazione dei PdD corrispondenti ai PdA è una delle modalità con le quali tale requisito è garantito.

[Torna al sommario](#)

7.12. Cessazione del servizio

Il processo di cessazione del servizio di Conservazione per ogni Cliente/Famiglia Documentale segue queste fasi principali:

- a) Condivisione informazioni tecniche di richiesta cessazione;
- b) Consolidamento delle informazioni tecniche propedeutiche alla cessazione del servizio, definizione della data formale di Cessazione;
- c) Condivisione della chiusura e delle sue modalità con il Responsabile della Conservazione;
- d) Cessazione tecnica;
- e) Attivazione di un piano di riversamento su richiesta del cliente. Il Responsabile della conservazione in questo caso valuta l'opportunità di riversare in un nuovo sistema di conservazione gli archivi precedentemente formati o di mantenerli invariati fino al termine di scadenza di conservazione dei documenti in essi contenuti. In questo caso, il processo può seguire una delle seguenti modalità :
 - i. "riversamento diretto" : processo che trasferisce uno o più documenti conservati da un supporto di memorizzazione ad un altro, non alterando la loro rappresentazione digitale. Per tale processo non sono previste particolari modalità, se non l'indicazione nel Manuale della Conservazione del processo di riversamento e la descrizione dettagliata del flusso di riversamento;

- ii. "riversamento sostitutivo": processo che trasferisce uno o più documenti conservati da un supporto di memorizzazione (o da un sistema di conservazione) ad un altro, modificando la loro rappresentazione digitale. Per tale processo oltre all'indicazione nel Manuale della Conservazione sia delle metodologie adottate sia del flusso, bisognerà allegare alla PdA aggiornato, anche il precedente PdA evidenziando i cambiamenti in riferimento all'impronta del singolo documento e predisponendo la generazione del nuovo PdA che contenga il PdA da cambiare. Il PdA precedente deve essere trattato, dunque, come un nuovo PdA ma evidentemente con informazioni aggiuntive rispetto ad un normale e comune PdA qui descritto nel paragrafo 6.2 [\[5\]](#)

[Torna al sommario](#)

8. IL SISTEMA DI CONSERVAZIONE

8.1. Componenti Logiche

Il sistema di conservazione basa le sue componenti logiche e strutturali sulla piattaforma SharePoint 2013.

L'intero sistema è posizionato all'interno di SharePoint 2013 utilizzandone le funzionalità.

Il Panel è il pannello di controllo dove viene gestito l'intero processo di conservazione. Tramite il Panel vengono gestiti gli accessi dei vari soggetti coinvolti nel processo: produttore, responsabile servizio di conservazione, archiviazione, amministratore e controllore.

Il Panel si trova all'interno della soluzione che è sviluppata interamente su SharePoint.

I pacchetti di Versamento, di archiviazione e di distribuzione sono delle raccolte documentali SharePoint completamente gestite e controllate per poter determinare gli accessi e i ruoli all'interno del processo di conservazione .

Tutti i dati (log compresi) sono storicizzati all'interno del server SQL Server.

Di seguito si riporta lo schema delle componenti logiche costituenti il sistema

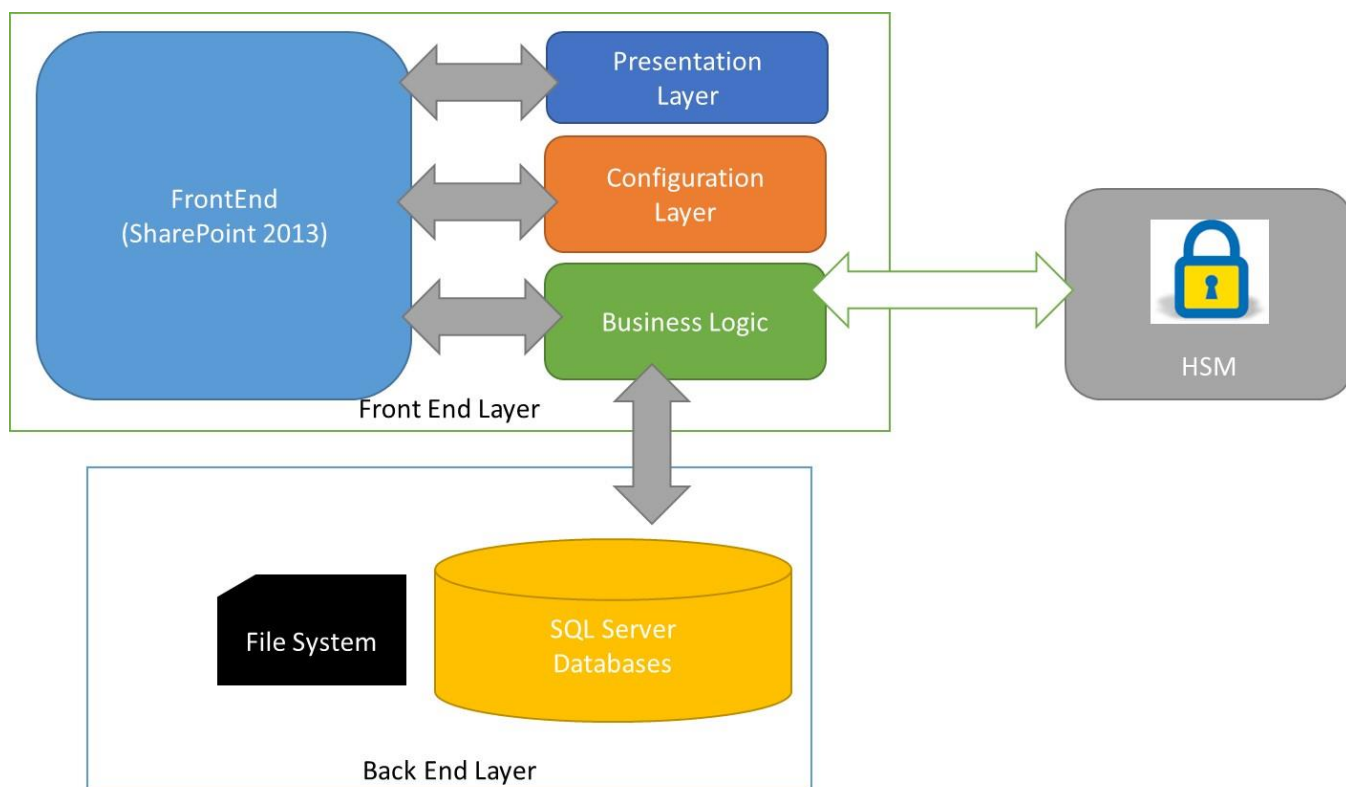


Figura 22 – Schema delle componenti logiche

Nella “**Figura 22– Schema delle componenti logiche**” è rappresentato un riquadro grande, intitolato “Front End Layer”, all’interno del quale sono evidenziati : un ulteriore riquadro azzurro, intitolato “FrontEnd (SharePoint 2013)”, posto a sinistra, collegato con tre frecce bidirezionali ad altrettanti riquadri posti a destra, intitolati (partendo dall’alto verso il basso) : “Presentation Layer” (riquadro blu), “Configuration Layer” (riquadro arancione), “Business Logic” (riquadro verde). Il riquadro “Front End Layer” è collegato con una freccia bidirezionale ad un riquadro sottostante, intitolato “Back End Layer” , all’interno del quale sono evidenziati : un ulteriore riquadro nero intitolato “File System” ed un cilindro di color giallo, intitolato “SQL Server Databases”. Sempre il riquadro “Front End Layer” è collegato con una freccia bidirezionale ad un riquadro a destra intitolato “HSM”, nel quale è rappresentato un lucchetto.

[Torna al sommario](#)

8.2. Componenti tecnologiche

L’interfaccia web per gli utenti e gli amministratori è compatibile con i browser Internet Explorer, Chrome e Firefox. Le versioni per cui è garantita piena compatibilità sono definite dai requisiti di Sharepoint 2013:

- Internet Explorer (versione 8 e superiore)
- Chrome (ultima versione rilasciata)
- Firefox. (ultima versione rilasciata)

Il Front-End Layer è strutturato su Architettura 3-tier:

- Presentation Layer: è basato sulla User Interface di Sharepoint 2013. I moduli custom, come i pannelli per gli utenti e gli amministratori, appositamente realizzati per il Sistema di Conservazione, sono realizzati con tecnologia ASP.NET 4.5, C#, Javascript.
- Configuration Layer: è stato realizzato tramite funzionalità native di Sharepoint, richiamate tramite API C#.
- Business Logic: è lo strato che interconnette le funzionalità dei due strati superiori con il Back-End. La comunicazione con Sharepoint avviene tramite API C#, mentre le chiamate verso il Back-End (File System / Sql Server) avvengono tramite librerie standard .NET e sono realizzate sempre in C#.

Il Back-End Layer è costituito da:

- File System NTFS su Windows Server 2012
- DBMS SQL Server 2012

[Torna al sommario](#)

8.3. Componenti Fisiche

Il servizio è erogato, nel rispetto dei requisiti di continuità, sicurezza fisica e logica, back-up, monitoraggio, presidio operativo, sistemistico, infrastrutture logistiche (locali, ups, condizionatori) e gestione reti dati che il Data Center garantisce e descrive negli specifici documenti.

L'infrastruttura è stand-alone e si basa su server virtuali realizzati su tecnologia VMWARE ESX. In caso di fault dei sistemi la ripartenza è garantita sfruttando la HA VMWARE, che prevede la configurazione di un POD UCS di backup su cui viene riavviato il nodo primario.

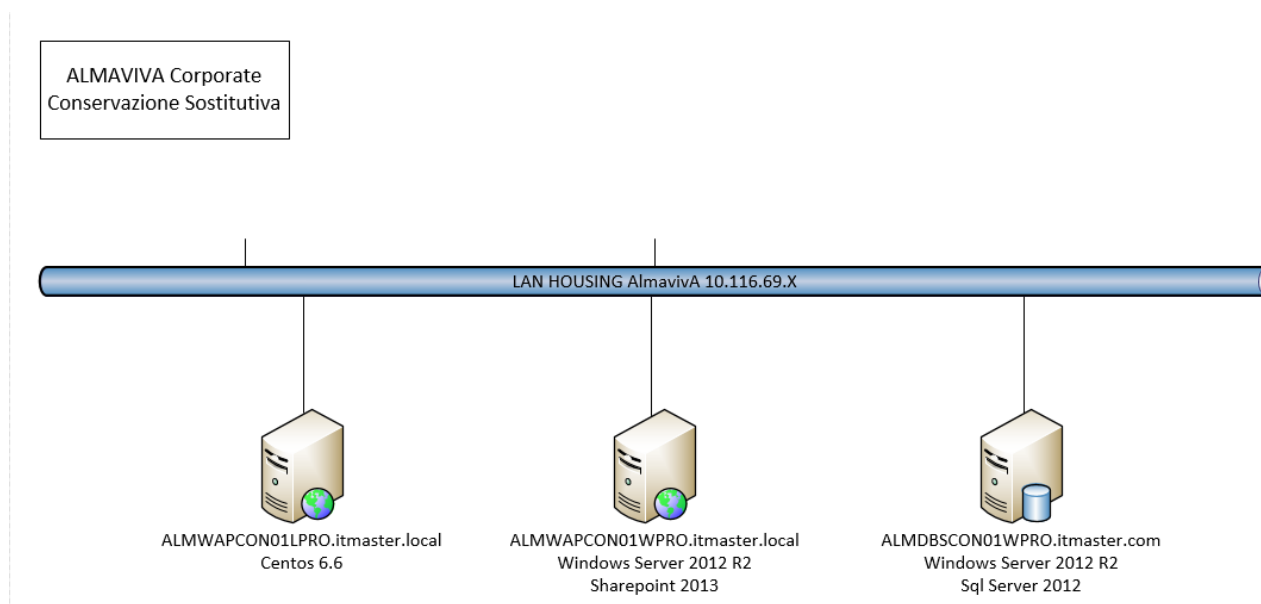


Figura 23 – Schema delle componenti fisiche

Nella “Figura 23– Schema delle componenti fisiche” è evidenziata la sequenza di server che compongono la Almayiva, schermata da Firewall rispetto all’accesso da Internet ; dalla LAN si accede

al server di gestione della firma, all'application server ed al DB Server, gestiti da VMWARE ESX

Web server

- Sistema Operativo: Centos 6.6
- Tomcat
- Agent Tivoli di monitoraggio base

Application server

- Sistema Operativo: Windows Server 2012 EE x64
- Microsoft Sharepoint Foundation 2013
- Agent Tivoli di monitoraggio base
- Agent Tivoli Storage Manager per il backup delle directory applicative, log, etc

DB server

- Sistema Operativo: Windows Server 2012 EE x64
- DBMS: SQL Server 2012
- Agent Tivoli di monitoraggio SQL
- Agent Tivoli Storage Manager per il backup del DB SQL

L'infrastruttura VMware del CED è basata su

- VMware vSphere Enterprise Plus 5.x
- VMware vCenter Server 5 Standard

e l'infrastruttura che compone la farm vmware è costituita da sistemi con caratteristiche differenziate per quanto riguarda : processori, CPU, RAM, I/O (come descritto in dettaglio nel Piano della Sicurezza del Sistema di Conservazione).

Il sito di Disaster Recovery del Sistema di Conservazione è realizzato in un CED Almagiva distante geograficamente, su cui sono installati sistemi identici nelle caratteristiche rispetto a quelli del sito primario.

[Torna al sommario](#)

8.4. Procedure di gestione e di evoluzione

8.4.1. Conduzione e manutenzione del sistema di conservazione

Nel documento “*Linee guida di sviluppo e manutenzione*” Almagiva ha definito le linee guida relative allo sviluppo, alla manutenzione e alla conduzione dei Sistemi Informativi che intende applicare in ambito aziendale, sulla base delle prescrizioni di legge, degli impegni contrattuali e delle indicazioni del Comitato per la Sicurezza, al fine di proteggere il proprio patrimonio informativo e quello dei suoi Clienti.

Le indicazioni contenute nel documento hanno i seguenti obiettivi principali:

- garantire la corretta e sicura operatività delle infrastrutture di elaborazione delle informazioni;
- proteggere l'integrità del software e delle informazioni;
- garantire la salvaguardia dei dati in transito sulle reti e la protezione delle infrastrutture di supporto;
- prevenire errori, perdite, modifiche non autorizzate o abuso delle informazioni nelle applicazioni;
- mantenere la sicurezza del software dei sistemi applicativi e delle informazioni

Le richieste di cambiamento su sistemi già in esercizio sono essenzialmente originate da:

- malfunzionamenti riguardanti il software di base, hardware, software applicativo;
- esigenze di miglioramento delle prestazioni, manutenibilità ed usabilità del sistema;
- esigenze di adeguamento ai mutamenti intervenuti nell'ambiente tecnico/operativo. L'innovazione tecnologica può essere a sua volta indotta (causa/effetto) da esigenze di miglioramento del software applicativo (capacity management);
- introduzione di nuove funzionalità esplicitamente richieste dall'utente.

I cambi da operare su sistemi in Esercizio sono classificabili in base a diversi parametri, quali ad esempio:

- l'entità dell'impatto sia sull'operatività del servizio erogato, sia sui componenti HW e SW implicati;
- la tipologia dell'intervento, espresso in termini di manutenzione correttiva, evolutiva, adeguativa;
- l'urgenza degli interventi, pianificabili o meno (es. interventi per i quali è necessario un fermo del sistema che può essere programmato o accidentale, a seconda delle cause che lo determinano).

Nell'ambito delle attività che insistono sui sistemi di produzione è possibile definire una classificazione tra attività che per loro natura sono **pianificabili** ed attività **non pianificabili**.

Per le prime dovranno essere individuati dei criteri di allocazione temporale in modo da evitare, il più possibile, impatti negativi sui livelli di servizio concordati.

Per le seconde saranno individuate delle finestre temporali nelle quali si cercherà di svolgerle comunque, fermo restando che eventuali attività ritenute critiche o di assoluta necessità, potranno essere effettuate in qualsiasi momento, all'occorrenza anche durante il normale orario di esercizio e quindi al di fuori delle finestre temporali individuate, potendo comportare, in questo caso, una riduzione dei livelli di disponibilità concordati.

Il processo di cambiamento è attuato in conformità a quanto definito nel documento "*Change Management*".

Nella conduzione e manutenzione del servizio, Al maviva adotta una politica di gestione delle utenze, dei ruoli e privilegi d'accesso, delle credenziali, conforme a quanto definito nei documenti di Policy di Sicurezza Logica, Procedura di Sicurezza Logica, Policy di gruppo sull'utilizzo delle credenziali, applicate nella gestione dei DC e nella progettazione e gestione dei servizi.

Nella conduzione del servizio vengono altresì applicate le policy di sicurezza Al maviva inerenti la gestione degli asset, dei supporti di memorizzazione, delle "scrivanie e schermi puliti".

[Torna al sommario](#)

8.4.2. Gestione e conservazione dei log

Almaviva considera i log di sistema facenti parte del proprio patrimonio informativo meritevole di protezione da tutto ciò che è in grado di minacciarlo; per tale motivo ha definito le politiche relative alla gestione dei log, che applica nei suoi DC, sulla base delle prescrizioni di legge, degli impegni contrattuali e delle indicazioni del Comitato per la Sicurezza, al fine di proteggere il proprio patrimonio informativo e quello dei propri Clienti.

Queste politiche riguardano essenzialmente :

- la rete internet
- la posta elettronica
- i server e gli apparati di rete
- l'operatività degli amministratori di sistema

I log degli amministratori di sistema sono gestiti dalla procedura Log Management Almaviva che ha, tra l'altro, l'obiettivo di assolvere agli obblighi di legge inerenti il Prov. del Garante Privacy sugli Amm. di Sistema.

[Torna al sommario](#)

8.4.3. Monitoraggio del sistema di conservazione

Il monitoraggio dei sistemi viene effettuato con le seguenti modalità:

- monitoraggio istantaneo; vengono utilizzati strumenti per una rapida ed efficace gestione degli eventi; un evento anomalo può essere classificato per l'ambito in cui accade (hardware, software, rete), per il contesto (servizio online, eccezione in un'esecuzione batch, back-up, ecc.) e per la gravità (impatto totale, parziale o nullo sul servizio, ecc.); a seconda della classificazione vengono inviate segnalazioni ad una console presidiata;
- monitoraggio andamentale; vengono utilizzati strumenti che permettono una raccolta storica dei dati di monitoraggio, effettuandone delle aggregazioni secondo opportune configurazioni; oltre a permettere una verifica della disponibilità del servizio (SLA), permettono un'efficace presa visione dell'andamento delle risorse ai fini di un corretto Capacity Planning

Sono previste inoltre soluzioni di monitoraggio atte a fornire ai clienti visibilità sulla effettiva fruibilità dei servizi di loro interesse e/o dell'infrastruttura coinvolta. Queste vengono suddivise in:

- strumenti di monitoraggio end-to-end; vengono utilizzati strumenti che permettono di misurare la disponibilità ed i tempi di risposta di transazioni campione delle applicazioni, attraverso motori che le eseguono a intervalli regolari da apposite postazioni dislocate sul territorio, simulando il comportamento di un generico utente;
- strumenti di BSM (Business System Manager) che collezionano lo stato di tutte le risorse tecnologiche di un intero ambiente utilizzando a tale scopo anche diversi strumenti di monitoraggio; forniscono una visibilità completa (sistemi, rete,..) sull'infrastruttura IT coinvolta nell'erogazione di un servizio.

Il monitoraggio comporta, tra le altre, le seguenti attività

- definizione, (Service Control Room e Application Management) delle procedure del Piano di Esercizio (CAR);
- gestione delle attività di gestione di incident fault e performance management (,(in conformità con quanto con quanto prescritto dalla *Linee guida di gestione incidenti e continuità operativa data*

center)

- attività di supporto tecnico, on demand, nella fasi di manutenzione o deployment delle applicazioni;
- esecuzione delle prove di accettazione e certificazione sotto il profilo del rispetto degli standard di esercibilità, del software rilasciato;
- controllo della corretta esecuzione delle elaborazioni batch automatiche ed intervento in caso di malfunzionamento;

[Torna al sommario](#)

8.4.4. Change management

Almaviva per assicurare completezza ed efficienza nella gestione delle richieste di cambiamento al servizio erogato, ha definito delle norme che regolamentano le modalità di presa in carico, valutazione ed autorizzazione di tali richieste.

Pertanto, in applicazione di quanto espressamente richiesto dalla Norma ISO/IEC 20000-1, inglobata nel Sistema di Gestione Qualità aziendale, viene registrata ogni richiesta di modifica e seguita ogni fase della sua lavorazione, fino alla messa in esercizio della stessa modifica. Lo scopo è quello di garantire che non si verifichino problemi o malfunzionamenti dovuti ad una effimera e ingannevole valutazione delle conseguenze sui servizi già erogati per le variazioni che vengono introdotte.

Il documento “*Change Management*” descrive il processo che governa la gestione delle modifiche agli ambienti di produzione, definendo ruoli, responsabilità, prodotti in ingresso ed uscita, nonché modalità di registrazione ed attuazione delle fasi del processo.

[Torna al sommario](#)

8.4.5. Verifica periodica di conformità a normativa e standard di riferimento

Il Responsabile del servizio di conservazione ha, tra i suoi compiti, quello di definire le caratteristiche ed i requisiti del sistema di conservazione in conformità alla normativa vigente e monitorarne l’attuazione.

Ai fini della verifica di conformità sono periodicamente effettuati degli audit interni applicando la procedura appositamente definita da Almaviva, che stabilisce attività ruoli e responsabilità nelle attività, prodotti in ingresso, prodotti in uscita.

Il responsabile della Funzione Qualità & Customer Satisfaction (CS&Q) decide l'estensione e la profondità del proprio intervento di verifica in funzione dei risultati di precedenti verifiche, delle caratteristiche di attività e strutture aziendali da auditare.

Le verifiche ispettive sono eseguite sui documenti e/o prodotti delle attività esaminate e sulle registrazioni risultanti dallo svolgimento delle attività.

Qualora contrattualmente richiesto, la procedura si estende al personale e alle attività di eventuali sub-fornitori.

Il processo di audit si compone dei seguenti passi :

1. Pianificazione : è predisposto il Piano delle verifiche ispettive (sulla base di una serie di elementi tra cui le non conformità riscontrate, gli obiettivi ed i piani di miglioramento) in modo che venga verificata l’efficacia del Sistema di Gestione Integrato e che tutti i processi di rilievo siano visti di norma una volta l’anno.
2. Assegnazione : a partire da una lista a disposizione del CS&Q sono scelti gli ispettori, sulla base di specifici criteri di formazione e qualificazione, per tipologia di norma da verificare

3. Accordo di visita : l'ispettore concorda la data di visita con il responsabile da esaminare richiedendo l'eventuale documentazione necessaria
4. Esecuzione visita ispettiva : l'ispettore esegue la verifica dei requisiti del Sistema che fanno capo al responsabile esaminato, confrontando le evidenze delle attività svolte con le procedure previste per quelle attività.
5. Verifica chiusura non conformità : l'ispettore verifica e valuta le correzioni effettuate e ne dichiara la (eventuale) risoluzione
6. Riepilogo delle non conformità : viene redatto il riepilogo delle non conformità (indirizzato, nei momenti pianificati, al riesame della Direzione)

[Torna al sommario](#)

9. MONITORAGGIO E CONTROLLI

Il processo di monitoraggio e controlli di Al maviva è una componente del suo Sistema di Gestione della Sicurezza Informatica (SGSI), rivolto, in conformità ai requisiti della ISO 27001, a valutare le prestazioni della sicurezza delle informazioni e l'efficacia del sistema di gestione per la sicurezza delle informazioni.

Tale processo è definito in un corpo documentale costituito da :

- Policy
- Linee guida
- Procedure

L'insieme di persone, processi, attività, tecnologie, software specializzati, ambienti fisici utilizzati, rappresentano il Dominio Logico, Fisico e Tecnico sotto monitoraggio e sono definiti TOE DC (Target of Evaluation Data Center) mutuando questa definizione, ma mantenendone il significato, dalla terminologia ITSEC Common Criteria.

Il TOE DC per assolvere al proprio mandato, si avvale di asset in proprio uso esclusivo; le componenti riguardano, oltre ai locali fisici che ospitano le infrastrutture, apparecchiature ICT e applicazioni software quali:

- i server su cui sono ospitate le applicazioni utilizzate per la gestione e il monitoraggio delle apparecchiature presenti nelle sale CED;
- gli strumenti di gestione e monitoraggio dei sistemi;
- gli strumenti di sicurezza e di gestione e monitoraggio della rete.

[Torna al sommario](#)

9.1. Procedure di monitoraggio

Il sistema di conservazione viene monitorato tramite i seguenti agent :

- Agent Tivoli di monitoraggio base
- Agent Tivoli di monitoraggio SQL

Tali agent monitorano :

- L'accessibilità delle funzioni (richiamo URL)
- I parametri di sistema (CPU, RAM, occupazione disco)
- Lo stato dell'istanza SQL e dei rispettivi database

Su ogni componente delle macchine sono impostate delle soglie: in caso di superamento di queste soglie scatteranno deli alert sulla console del gruppo di competenza. Le soglie sono:

- NT_System_CPU_Critical scatta nel caso in cui la CPU supera un valore maggiore uguale del 95 % e la situazione si verifica per almeno 2 volte. Il controllo viene effettuato ogni 5 minuti.
- TSF_NT_0001_DiskSpaceCrit scatta quando la soglia del disco è inferiore al 95%, scatta l'allarme. Il controllo viene effettuato ogni 15 minuti.
- TSF_NT_0026_Memory_Usage scatta quando l'uso disponibile della RAM è inferiore al 5% e la situazione si verifica per almeno 5 volte consecutive. Il controllo viene effettuato ogni 5 minuti.
- TSF_NT_0018_Paging_Crità scatta quando sulla RAM c'è Paging e l'uso è maggiore al 95%. Il controllo viene effettuato ogni 10 minuti.
- TSF_NT_0025_ServRestart_Crità scatta quando un servizio si trova nello stato "Stopped" & "Automatic". In questo caso se uno dei servizi si trova in questo stato, l'agent prova ad eseguire un primo Restart (anche se non di tutti, visto che ci sono delle eccezioni).
- MS_OFFline à scatta nel caso in cui la macchina è down o non raggiungibile.
- TSF_MSSQL_0001_SQLServer_Status_Criticalà scatta se l'istanza SQL si trova nello stato Inactive.
- TSF_MSSQL_0003_DBNumErrors_Crit à scatta se trova errori nel DB
- TSF_MSSQL_0009_DBStatus_Crit à scatta nel caso in cui il Database non è disponibile.

Le risultanze delle misurazioni sono storicizzate ed analizzate periodicamente (es, attraverso grafici) dal Capacity Manager.

Il monitoraggio applicativo effettua le seguenti verifiche

- Le impronte dei singoli documenti che vengono conservati con relativo ricalcolo e confronto
- Controllo sui Bit di Parità di ciascun file, per garantire integrità
- Controllo dei Log del sistema, sia verificando le temporalità dei Log sia l'integrità degli stessi
- Verifica di tutti i documenti prodotti dal sistema di conservazione, compreso i rapporti di versamento
- Controllo e check dei componenti hardware attraverso analisi di KPI

A fronte di eventi anomali segnalati dal sistema di monitoraggio, gli operatori intervengono secondo le modalità descritte nelle schede-evento; a seconda della tipologia di evento la scheda può descrivere le azioni che l'operatore può effettuare direttamente, ovvero indica la struttura cui l'operatore deve trasmettere la segnalazione per competenza (sistemisti, db administrator, network administrator, presidio applicativo, responsabile del servizio).

[Torna al sommario](#)

9.2. Log del sistema di conservazione

Il sistema di conservazione effettua il log di tutte le operazioni effettuate, all'interno del Database SQL dedicato.

Le informazioni che vengono tracciate dal sistema relative al log sono:

- Data e ora dell'operazione
- Utente che ha effettuato l'operazione
- Operazione effettuata
- Sito dell'operazione effettuata
- Note

Sotto un'immagine che descrive la ricerca di un log.

BACK

Categoria	Nessuna categoria ▼
Da	<input type="text" value="01/05/2015"/>
A	<input type="text" value="08/05/2015"/>

Data	Utente	Operazione	Sito	Note
08/05/2015 11:57:00	Andrea Bologna	Creazione pacchetto di versamento	http://dev2014-3/siti/almaviva	Creato pacchetto di versamento 886991ef-2ae0-44ad-9d50-8a3a575f127a
08/05/2015 11:09:38	Andrea Bologna	Creazione pacchetto di distribuzione	http://dev2014-3/vdc/almaviva/2014/pdd	Creato PdD: http://dev2014-3/vdc/almaviva/2014/pdd
05/05/2015 11:05:16	Andrea Bologna	Creazione pacchetto di versamento	http://dev2014-3/siti/almaviva	
04/05/2015 15:44:53	Andrea Bologna	Creazione pacchetto di distribuzione	http://dev2014-3/vdc/almaviva/2014/pdd	Creato PdD: http://dev2014-3/vdc/almaviva/2014/pdd
04/05/2015 13:07:23	Andrea Bologna	Creazione pacchetto di distribuzione	http://dev2014-3/vdc/almaviva/2014/pdd	Creato PdD: http://dev2014-3/vdc/almaviva/2014/pdd
04/05/2015 12:51:59	Andrea Bologna	Creazione pacchetto di distribuzione	http://dev2014-3/vdc/almaviva/2014/pdd	Creato PdD: http://dev2014-3/vdc/almaviva/2014/pdd
04/05/2015 12:43:44	Andrea Bologna	Creazione pacchetto di distribuzione	http://dev2014-3/vdc/almaviva/2014/pdd	Creato PdD: http://dev2014-3/vdc/almaviva/2014/pdd
04/05/2015 12:25:05	Andrea Bologna	Creazione pacchetto di distribuzione	http://dev2014-3/vdc/almaviva/2014/pdd	Creato PdD: http://dev2014-3/vdc/almaviva/2014/pdd
04/05/2015 11:50:48	Andrea Bologna	Creazione pacchetto di distribuzione	http://dev2014-3/vdc/almaviva/2014/pdd	Creato PdD: http://dev2014-3/vdc/almaviva/2014/pdd
04/05/2015 11:48:49	Andrea Bologna	Creazione pacchetto di distribuzione	http://dev2014-3/vdc/almaviva/2014/pdd	Creato PdD: http://dev2014-3/vdc/almaviva/2014/pdd
04/05/2015 11:34:42	Andrea Bologna	Creazione pacchetto di versamento	http://dev2014-3/siti/almaviva	
04/05/2015 11:29:55	Andrea Bologna	Creazione pacchetto di versamento	http://dev2014-3/siti/almaviva	
04/05/2015 11:26:37	Andrea Bologna	Creazione pacchetto di distribuzione	http://dev2014-3/vdc/almaviva/2014/pdd	Creato PdD: http://dev2014-3/vdc/almaviva/2014/pdd
04/05/2015 09:11:41	Andrea Bologna	Creazione pacchetto di distribuzione	http://dev2014-3/vdc/almaviva/2014/pdd	Creato PdD: http://dev2014-3/vdc/almaviva/2014/pdd
03/05/2015 22:51:02	Andrea Bologna	Creazione pacchetto di distribuzione	http://dev2014-3/vdc/almaviva/2014/pdd	Creato PdD: http://dev2014-3/vdc/almaviva/2014/pdd
02/05/2015 22:08:05	Andrea Bologna	Creazione pacchetto di versamento	http://dev2014-3/siti/almaviva	Creazione pacchetto di versamento in http://dev2014-3/siti/almaviva
02/05/2015 12:27:07	Andrea Bologna	Creazione pacchetto di versamento	http://dev2014-3/siti/almaviva	Creazione pacchetto di versamento in http://dev2014-3/siti/almaviva

Figura 24 – Pannello di ricerca ed esposizione log

Nella “Figura 24– Pannello di ricerca ed esposizione log” sono evidenziate due form : la prima consente di selezionare i log da visualizzare sulla base dei seguenti elementi : “Categoria” Data “Da” e Data “A”, sono inoltre a disposizione due bottoni per cercare o esportare i log selezionati. Nella seconda form sono evidenziate le informazioni dei log selezionati : “Data”, “Utente”, “Operazione”, “Stato”, “Note”.

L'accesso ai log è consentito solo all'amministratore del sistema e al responsabile del servizio di

conservazione, che hanno la possibilità di effettuare un export in PDF del log ricercato, firmato e marcato dal responsabile. Sotto un'immagine dell'export firmato e marcato.

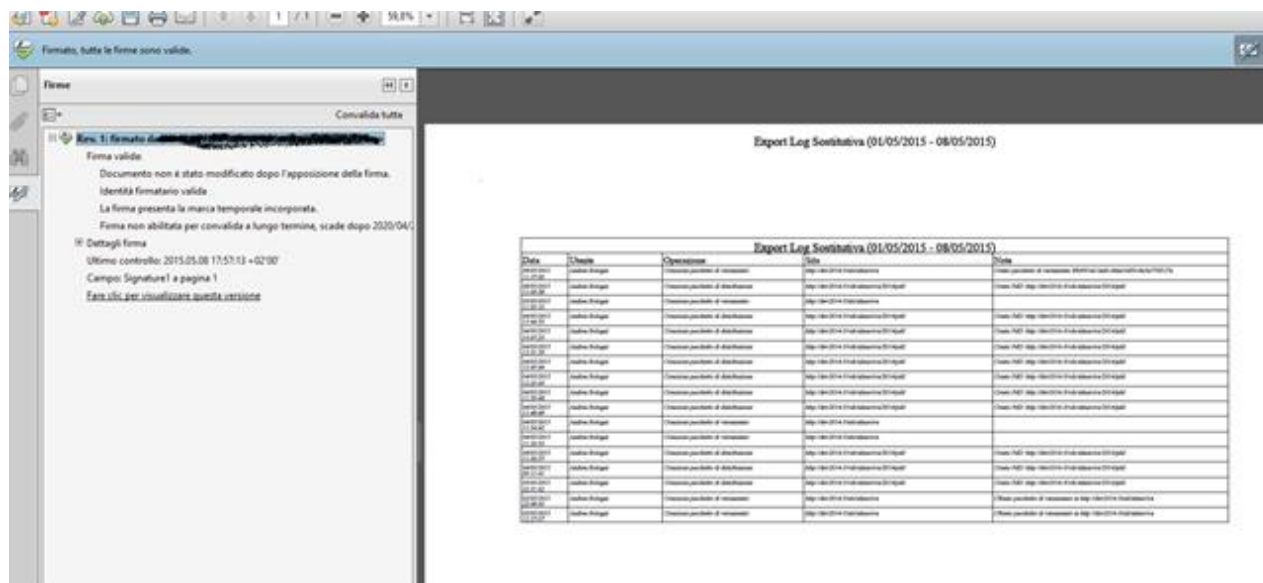


Figura 25 – Export del log firmato e marcato

Nella “**Figura 25– Export del log firmato e marcato**” è evidenziato il PDF, firmato e marcato, che contiene i log selezionati; il PDF ha il titolo “Export Log Sostitutiva (data da – data a)” ed evidenzia le seguenti informazioni : “Data”, “Utente”, “operazione”, “Stato”, “Note”.

Il sistema dei Log permette anche di attivare controlli preventivi e di attivare azioni al fine di avere un assistenza pro attiva. Qualora venga segnalato un monitoraggio non positivo, come ad esempio indicato nel 9.1, viene mandata una notifica al responsabile del servizio di conservazione, al responsabile dei sistemi informativi e al responsabile della sicurezza. Tutti i risultati prodotti dai controlli preventivi, vengono archiviati in una raccolta di SharePoint dedicata ai Log e al Monitoraggio.

[Torna al sommario](#)

9.3. Verifica dell'integrità degli archivi

Il sistema di conservazione , secondo quanto richiesto dal DPCM del 3 Dicembre 2013 [2], garantisce la conservazione a lungo termine dei documenti e quindi dei PdA conservati, attraverso una verifica periodica e non superiore ai tre mesi, dell'integrità dei PdA conservati per mezzo delle seguenti operazioni, effettuate dal responsabile del servizio di conservazione :

- Verifica che le impronte dei documenti contenuti nel PdA non siano mutate, attraverso una ricerca automatica che confronta l'hash precedentemente memorizzato con quello calcolato al momento della verifica
- Verifica che il PdA sia firmato digitalmente e marcato temporalmente e che la firma digitale non sia scaduta, ovvero che il certificato qualificato del responsabile del servizio di conservazione non

sia scaduto.

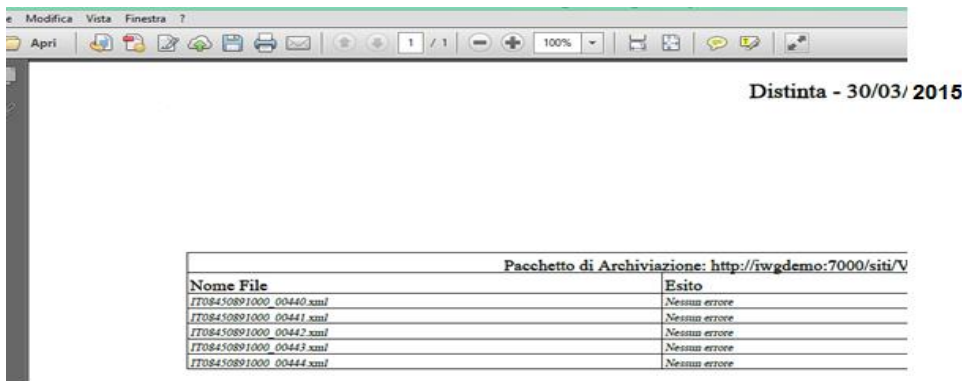
- Verifica che l'archivio sia consistente ed integro

Se almeno una delle verifiche di cui sopra, dovesse risultare positiva, il responsabile del servizio di conservazione avvierà le procedure atte a garantire il ripristino dei documenti conservati attraverso il riversamento dei documenti e specificando le operazioni intraprese nel presente Manuale .

A seconda dei casi, verrà individuata l'azione necessaria per il ripristino dei dati, sia come riversamento diretto sia come riversamento sostitutivo.

Il processo di riversamento sostitutivo di documenti informatici, avviene mediante la memorizzazione su un altro supporto, alterandone la rappresentazione binaria e termina con la generazione di un nuovo pacchetto di archiviazione della marca temporale e della firma digitale da parte del responsabile del servizio di conservazione che attesta il corretto svolgimento del processo. Il processo di riversamento diretto avviene mediante la memorizzazione su un altro supporto non alterandone la rappresentazione binaria. Anche in questo caso il processo termina con la generazione di un nuovo pacchetto di archiviazione della marca temporale e della firma digitale da parte del responsabile del servizio di conservazione che attesta il corretto svolgimento del processo

La funzionalità di verifica dell'integrità può essere richiamata in qualsiasi momento sul pannello dei processi di conservazione eseguiti. Al termine del controllo il sistema genera una distinta che consente di verificare puntualmente tutti i file controllati con i relativi esiti



Pacchetto di Archiviazione: http://iwgdemo:7000/siti/V	
Nome File	Esito
IT08450891000_00440.xml	Nessun errore
IT08450891000_00441.xml	Nessun errore
IT08450891000_00442.xml	Nessun errore
IT08450891000_00443.xml	Nessun errore
IT08450891000_00444.xml	Nessun errore

Figura 26 – Distinta dell'esito di verifica degli archivi

Nella “**Figura 26 – Distinta dell'esito di verifica degli archivi**” sono evidenziate le informazioni dell'esito della verifica dei singoli PdA. Il titolo della distinta è “Pacchetto di archiviazione : http://...../...” (indirizzo del PdA), e le informazioni contenute sono : “Nome file” e “Esito”.

[Torna al sommario](#)

9.4. Soluzioni adottate in caso di anomalie

Le possibili anomalie, riscontrate anche dai sistemi di monitoraggio, possono essere essenzialmente di due tipi :

- Anomalie dei sistemi
- Anomalie della applicazione

Di seguito si riportano sinteticamente alcune possibili anomalie e le relative soluzioni da adottare

Anomalie dei sistemi

In questo contesto si includono :

- Anomalie dell'hardware :
 - il monitoraggio continuo e l'analisi dei risultati consente in genere di individuare possibili situazioni di crisi ed intervenire proattivamente usufruendo dei servizi di manutenzione stipulati con i fornitori;
 - eventuali anomalie improvvise sono risolte trasferendo su altra macchina fisica, manualmente od automaticamente i sistemi virtuali operanti, sfruttando i meccanismi di alta affidabilità della versione ESX Vmware disponibile sull'infrastruttura
- Anomalie dei sistemi operativi, dei servizi (es. application server) e delle reti :
 - in alcuni casi il presidio operativo può intervenire direttamente (ad esempio riavviando i servizi, anche sulla base di quanto previsto nel manuale operativo)
 - nei casi più significativi il presidio operativo attiva i presidi sistemistico/di rete; questi ultimi valuteranno la situazione specifica (es. processi che stanno occupando risorse CPU o spazio disco eccessivo, trasmissione in rete bloccata) per intervenire adeguatamente, eventualmente anche consultando il presidio applicativo.
- Anomalie dei DB :

ove si riscontri un'anomalia dei DB si può procedere in modo differenziato in base alla gravità dell'evento;

 - si può effettuare un ripristino dei dati dalle copie di back-up
 - creare una nuova istanza del DB su un'altra macchina e poi ripristinare i dati

Anomalie della applicazione

Tali anomalie sono evidenziate dai log applicativi e sono alla attenzione del responsabile del servizio di conservazione ed ai responsabili degli altri servizi; e possono riguardare

- Anomalie funzionali :
 - vengono segnalate al fornitore della piattaforma applicativa che interverrà in conformità con quanto prescritto dai contratti di manutenzione, nel rispetto degli sla previsti nello stesso, e pianificando con il responsabile del servizio di conservazione, il responsabile dei sistemi informativi, il responsabile dello sviluppo e della manutenzione, i tempi e le modalità dell'intervento; il processo si attua in conformità a quanto definito dai documenti di change management facenti parte dell'impianto documentale del Sistema di Gestione della Qualità integrato Al maviva
- Anomalie nella integrità dei pacchetti :
 - il responsabile del servizio di conservazione, di concerto anche con il responsabile della sicurezza dei sistemi individuerà le cause della anomalia, e provvederà, qualora necessario, a ripristinare copie di backup, avendo cura di verificare l'integrità dei pacchetti e dandone evidenza al Produttore.

Le modalità di gestione degli incidenti di sicurezza sono riportate nel Piano della Sicurezza del Servizio di Conservazione

Un pacchetto di archiviazione può essere annullato dal responsabile della conservazione. Tale annullamento è un annullamento logico e non una cancellazione fisica che viene registrato all'interno del log del sistema. Sotto un'immagine della funzionalità di annullamento

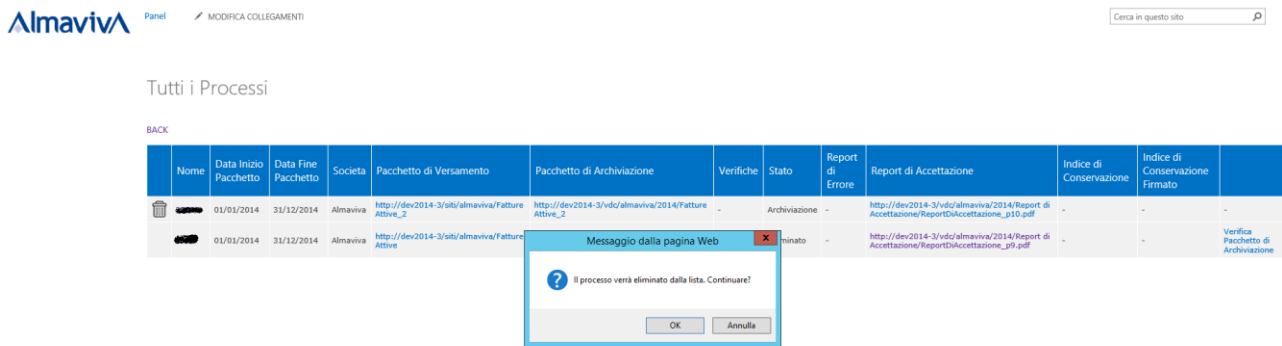


Figura 27 – Annullamento di un PdA

Nella “Figura 27 – Annullamento di un PdA” viene riportato il form mediante il quale si può procedere all’annullamento di un PdA. Nel form che elenca tutti i processi (PdA) sono evidenziate le seguenti informazioni : “Nome”, Data Inizio Pacchetto”, “Data fine Pacchetto”, “Società”, Pacchetto di versamento” (URI), Pacchetto di Archiviazione” (URI), “Verifiche”, “Stato”, “Report di errore”, “Report di accettazione” (URI), “Indice di conservazione”, “Indice di conservazione firmato”. All’estrema sinistra di tali informazioni può essere presente il simbolo del cestino. Selezionando il cestino appare un messaggio di richiesta conferma “Il processo verrà eliminato dalla lista. Confermare?”, a tale messaggio si può rispondere selezionando la scelta “OK” oppure la scelta “Annulla”.

[Torna al sommario](#)