Manuale della Conservazione

Di

MEMAR MONTEASSEGNI S.p.A.

EMISSIONE DEL DOCUMENTO

Azione	Data	Nominativo	Funzione
Redazione	18/12/2017	Paolo Bolognese	*Responsabile sviluppo e manutenzione del sistema di conservazione*
Verifica	18/12/2017	Alessandro Di Francesco	*Responsabile Sicurezza Servizi di Conservazione*
Approvazione	18/12/2017		*Responsabile del Servizio di Conservazione*

REGISTRO DELLE VERSIONI

N°Ver/Rev/Bozza	Data emissione	Modifiche apportate	Osservazioni
1	02/01/2005	Prima redazione del manuale della conservazione	
2	02/01/2010	Seconda redazione del manuale	Modifiche piattaforma
3	02/01/2013	Terza redazione del manuale	Per modifiche procedurali
4	10/10/2015	Quarta redazione del manuale	Adeguamento alle nuove regole tecniche DPCM 3 dicembre 2013
5	06/04/2017	Quinta redazione del manuale	Variazione Responsabile Conservazione e Privacy

N°Ver/Rev/Bozza	Data emissione	Modifiche apportate	Osservazioni
6	17/12/2017	Sesta redazione del manuale	Variazione Responsabile Sicurezza dei sistemi per la conservazione, Responsabile funzione archivistica di conservazione, Responsabile sviluppo e manutenzione del sistema di conservazione, Responsabile trattamento dati personali

2

SOMMARIO

1. SCOPO E AMBITO DEL DOCUMENTO

MEMAR MONTEASSEGNI SpA opera da più di 40 anni nella Gestione Documentale soprattutto per i settori Industry e Bancario; il presente documento descrive struttura, processi e attività inerenti al Sistema di Conservazione sia sotto l'aspetto organizzativo che tecnico-operativo.

Il presente manuale (d'ora innanzi MdC) del sistema di conservazione Memar (d'ora in avanti SdCM), viene esposto alla clientela e su WEB attraverso un brand commerciale denominato EFATTURA (www.efattura.net) ma nel presente documento useremo per semplicità SdCM.

Nello specifico verranno descritti nel MdC:

- L'area aziendale e la sua organizzazione
- I ruoli e le persone che li rivestono
- Le architetture e le infrastrutture
- I processi e le attività del SdCM.
- La sicurezza ed i monitoraggi
- Il processo di manutenzione
- L'integrazione del sistema di conservazione nella struttura di produzione dei Servizi di gestione Documentale Memar.

Il documento dà supporto in modo descrittivo non solo alle procedure ISO ma anche a tutto ciò che regolamenta contrattualmente il servizio di fornitura, entrando a far parte integrale della stessa contrattualistica.
Il Servizio di Conservazione può riguardare classi e tipologie documentali diverse e può essere anche personalizzato, le eventuali personalizzazioni e specificità sono descritte nell'Allegato al presente manuale della conservazione denominato **Specificità del Contratto.**

Torna al sommario

2. TERMINOLOGIA (GLOSSARIO, ACRONIMI)

Termine	Descrizione
Accesso	operazione che consente a chi ne ha diritto di prendere visione ed estrarre copia dei documenti informatici
AGID	Agenzia per l'Italia Digitale
Aggregazione documentale informatica	aggregazione di documenti informatici o di fascicoli informatici, riuniti per caratteristiche omogenee, in relazione alla natura e alla forma dei documenti o in relazione all'oggetto e alla materia o in relazione alle funzioni dell'ente
AOO (Area Organizzativa Omogenea)	O unità operativa della Pubblica Amministrazione. Rappresenta un insieme di funzioni e di strutture, individuate dalla amministrazione, che opera su tematiche omogenee e che presenta esigenze di gestione della documentazione in modo unitario e coordinato ai sensi dell'articolo 50, comma 4, del D.P.R. 28 dicembre 2000, n. 445
ANORC	Associazione Nazionale per Operatori e Responsabili della Conservazione digitale
Archivio	complesso organico di documenti, di fascicoli e di aggregazioni documentali di qualunque natura e formato, prodotti o comunque acquisiti da un soggetto produttore durante lo svolgimento dell'attività
Archivio informatico	archivio costituito da documenti informatici, fascicoli informatici nonché aggregazioni documentali informatiche gestiti e conservati in ambiente informatico
ARXtoCOS	Software client che permette al Produttore di caricare i pacchetti di versamento dal proprio sistema ARXIVAR nel sistema di conservazione MEMAR
ARXIVAR	Software di gestione e workflow documentale
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 base di dati collezione di dati registrati e correlati tra loro — 53 — 12-3-2014 Supplemento ordinario n. 20 alla GAZZETTA UFFICIALE Serie generale - n. 59
CA (Certification Autorithy o 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
CAdES	Criptographic Message System Advanced Electronic Signature – formato di firma elettronica
Classe documentale	Aggregazione comprendente documenti omogenei per natura,funzione, modalità operative.
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 backup degli archivi del sistema di conservazione prodotta ai sensi dell'articolo 12 delle presenti regole tecniche per il sistema di conservazione
EFATTURA	Brand con cui viene commercializzato il sistema di Conservazione
Esibizione	Operazione che consente di visualizzare un documento conservato e di ottenerne copia
Evidenza informatica	Sequenza di simboli binari (bit) che può essere elaborata da una procedura informatica
Fascicolo informatico	Aggregazione strutturata e univocamente identificata di atti, documenti o dati informatici, prodotti e funzionali all'esercizio di una specifica attività o di uno specifico procedimento. Nella pubblica amministrazione il fascicolo informatico collegato al procedimento amministrativo è creato e gestito secondo le disposizioni stabilite dall'articolo 41 del Codice. — 54 — 12-3-2014 Supplemento ordinario n. 20 alla GAZZETTA UFFICIALE Serie generale - n. 59
Formato	modalità di rappresentazione della sequenza di bit che costituiscono il documento informatico; comunemente è identificato attraverso l'estensione del file
Funzione di Hash	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
HSM	Hardware Security Module, è l'insieme di hardware e software che realizza dispositivi sicuri per la generazione delle firme in grado di gestire in modo sicuro una o più coppie di chiavi crittografiche
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
Impronta	Sequenza di simboli binari (bit) di lunghezza predefinita generata mediante l'applicazione alla prima di una opportuna funzione di hash
Insieme minimo di metadati del documento informatico	Complesso dei metadati, da associare al documento informatico per identificarne provenienza e natura e per garantirne la tenuta
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
IPdA	Indice del pacchetto di archiviazione
ISO	International Organization for Standardization
Leggibilità	Insieme delle caratteristiche in base alle quali le informazioni contenute nei documenti informatici sono fruibili durante l'intero ciclo di gestione dei documenti
Log di sistema	Registrazione cronologica delle operazioni eseguite su di un sistema informatico per finalità di controllo e verifica degli accessi, oppure di registro e tracciatura dei cambiamenti che le transazioni introducono in una base di dati
Manuale di conservazione	Strumento che descrive il sistema di conservazione dei documenti informatici ai sensi dell'articolo 9 delle regole tecniche del sistema di conservazione — 55 — 12-3-2014 Supplemento ordinario n. 20 alla GAZZETTA UFFICIALE Serie generale - n. 59
Marca temporale	Time stamping rilasciato da Certification Autorithy
MEF	Registro di certificazione delle apparecchiature elettroniche
MEF CE 2.0	Tipo di Compliance certificata dal MEF
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;
NOC	Network Operating Center
OAIS	Open archival information system
PA	Pubblica Amministrazione
PdV (Pacchetto di Versamento)	Pacchetto informativo inviato dal produttore al sistema di conservazione secondo un formato predefinito e concordato descritto nel manuale di conservazione
PdA	Pacchetto di Archiviazione
PdD (Pacchetto di Distribuzione)	Pacchetto informativo inviato dal sistema di conservazione all'utente in risposta ad una sua richiesta
Piano della sicurezza del sistema di conservazione	Documento che, nel contesto del piano generale di sicurezza, descrive e pianifica le attività volte a proteggere il sistema di conservazione dei documenti informatici da possibili rischi nell'ambito dell'organizzazione di appartenenza.
Presa in carico	Accettazione da parte del sistema di conservazione di un pacchetto di versamento in quanto conforme alle modalità previste dal manuale di conservazione
Processo di conservazione	Insieme delle attività finalizzate alla conservazione dei documenti informatici di cui all'articolo 10 delle regole tecniche del sistema di conservazione — 56 — 12-3-2014 Supplemento ordinario n. 20 alla GAZZETTA UFFICIALE Serie generale - n. 59
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.
Rack mountable	Apparecchiature inseribili in armadi attrezzati per apparecchiature elettroniche (rack)
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
RdC (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
RdSC	Responsabile del Servizio di Conservazione
RdFAC	Responsabile della Funzione Archivistica di Conservazione
Responsabile della sicurezza	Soggetto al quale compete la definizione delle soluzioni tecniche ed organizzative in attuazione delle disposizioni in materia di sicurezza
RdSSdC	Responsabile della Sicurezza del Sistema della Conservazione
RdSIC	Responsabile dei Sistemi Informativi per la Conservazione
RpSM	Responsabile per lo sviluppo e manutenzione del sistema di conservazione
Repository	Zona di deposito di dati o file in un sistema informativo
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
SAP	Sistema informativo aziendale
SAPtoCOS	Software client che permette al Produttore di caricare i pacchetti di versamento dal proprio sistema gestionale SAP al sistema di conservazione MEMAR
Scarto	Operazione con cui si eliminano, secondo quanto previsto dalla normativa vigente, i documenti ritenuti privi di valore amministrativo e di interesse storico culturale
SdCM	Sistema di Conservazione MEMAR

Sistema di conservazione	Sistema di conservazione dei documenti informatici di cui all'articolo 44 del Codice sistema di gestione informatica dei documenti nell'ambito della pubblica amministrazione è il sistema di cui all'articolo 52 del D.P.R. 28 dicembre 2000, n. 445; per i privati è il sistema che consente la tenuta di un documento informatico
SLA	Service Level Agreement – estensione contrattuale che definisce le condizioni di erogazione di un servizio
Storage	Area di deposito o conservazione di dati o files in un sistema informativo
Time stamping	attestazione temporale
UNI SinCRO	UNI 11386:2010 - Supporto all'Interoperabilità nella conservazione e nel Recupero degli oggetti digitali
UPS	Uninterrutible Power Supply – sistema che garantisce la continuità dell'erogazione della corrente elettrica.
UPtoCOS	Software client che permette al produttore il caricamento del Pacchetto di versamento nel sistema di Conservazione Memar.
XAdES	XML Advanced Electronic Signature – formato di firma elettronica
XML	Extensible Markup Language – formato di file di dati
XSD	Schema di un file XML

Si richiama integralmente anche il glossario contenuto dell'Allegato 1 alle regole tecniche di cui al DPCM 3 dicembre 2013.

Torna al sommario

3. NORMATIVA E STANDARD DI RIFERIMENTO

3.1 Normativa di riferimento

Nella progettazione e realizzazione del SdCM si è tenuto conto della seguente normativa:

- Codice Civile [Libro Quinto Del lavoro, Titolo II Del lavoro nell'impresa, Capo III Delle imprese commerciali e delle altre imprese soggette a registrazione, Sezione III Disposizioni particolari per le imprese commerciali, Paragrafo 2 Delle scritture contabili], articolo 2215 bis - Documentazione informatica;
- Legge 7 agosto 1990, n. 241 e s.m.i. – Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi;
- Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 e s.m.i. – Testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa;
- Decreto Legislativo 30 giugno 2003, n. 196 e s.m.i. – Codice in materia di protezione dei dati personali;
- Decreto Legislativo 22 gennaio 2004, n. 42 e s.m.i. – Codice dei Beni Culturali e del Paesaggio;
- Decreto Legislativo 7 marzo 2005 n. 82 e s.m.i. – Codice dell'amministrazione digitale (CAD);
- Decreto del Presidente del Consiglio dei Ministri 22 febbraio 2013 – Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma3, lettera b), 35, comma 2, 36, comma 2, e 71;
- Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013 - Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5-bis, 23-ter, comma 4, 43, commi 1 e 3, 44 , 44-

bis e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005;

- Decreto del Ministero dell'Economia e delle Finanze del 17 giugno 2014 – Modalità di assolvimento degli obblighi fiscali relativi ai documenti informatici ed alla loro riproduzione sui diversi tipi di supporto.
- Decreto del Presidente del Consiglio dei Ministri del 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.
- Circolare AGID 10 aprile 2014, n. 65 - Modalità per l'accreditamento e la vigilanza sui soggetti pubblici e privati che svolgono attività di conservazione dei documenti informatici di cui all'articolo 44-bis, comma 1, del decreto legislativo 7 marzo 2005, n. 82.
- Deliberazione CNIPA del 21 maggio 2009, n.45 (come modificata dalla determinazione dirigenziale DigitPA n.69/2010). Regole per la creazione dei certificati di firma e di marca che quelle per il loro utilizzo, riconoscimento e verifica.
- Direttiva 2010/45/UE del 13 luglio 2010 recante modifica della direttiva 2006/112/CE relativa al sistema comune d'imposta sul valore aggiunto per quanto riguarda le norme in materia di fatturazione. Recepita in Italia dalla Legge 228/2012, legge di stabilità 2013 del 24 dicembre 2012.
- Circolare dell'Agenzia delle Entrate n.45/E del 19 ottobre 2005
- Circolare dell'Agenzia delle Entrate n.36/E del 06 dicembre 2006
- Circolare dell'Agenzia delle Entrate n.18/E del 24 giugno 2014
- Risoluzione dell'Agenzia delle Entrate n.161E del 9 luglio 2007
- Risoluzione dell'Agenzia delle Entrate n.158E del 15 giugno e nr. 196E del 30 luglio 2009
- Risoluzione dell'Agenzia delle Entrate n.81/E del 25 settembre 2015.

Torna al sommario

3.2 Standard di riferimento

Gli standard adottati per il Sistema di Conservazione sono i seguenti e sono anche riportati nell'allegato "Specificità del contratto" dove vengono periodicamente aggiornate:

- ISO 14721:2012 OAIS (Open Archival Information System), Sistema informativo aperto per l'archiviazione;
- ISO/IEC 27001:2013, Information technology - Security techniques - Information security management systems – Requirements, Requisiti di un ISMS (Information Security Management System);
- ETSI TS 101 533-1 V1.3.1 (2012-04) Technical Specification, Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part 1: Requirements for Implementation and

Management, Requisiti per realizzare e gestire sistemi sicuri e affidabili per la conservazione elettronica delle informazioni;

- ETSI TR 101 533-2 V1.3.1 (2012-04)Technical Report, Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part 2: Guidelines for Assessors, Linee guida per valutare sistemi sicuri e affidabili per la conservazione elettronica delle informazioni;
- UNI 11386:2010 Standard SInCRO - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali;
- ISO 15836:2009 Information and documentation - The Dublin Core metadata element set, Sistema di metadata del Dublin Core.

Torna al sommario

4. RUOLI E RESPONSABILITÀ

4.1 Ruoli esterni

Prima di definire i ruoli interni diamo una breve descrizioni degli attori esterni coinvolti nel processo di Conservazione:

- **Il Produttore**: è la persona fisica o giuridica che ha il compito di predisporre ed inviare al SdCM il Pacchetto di Versamento prodotto nel contesto del sistema di gestione documentale e contenente i documenti corredati dei necessari metadati descrittivi. Il Produttore produrrà i Pacchetti di Versamento (d'ora innanzi PdV) nello standard previsto dal SdCM o sarà affiancato dal Service MEMAR nella loro produzione nel caso sia necessario intervenire con processi software di conversione ed adattamento dei pacchetti del Cliente allo standard o nel caso di flussi cartacei da de-materializzare. In entrambi i casi la responsabilità sui contenuti dei documenti informatici è sempre del Produttore, che ha sempre, per specificità del Processo, il dovere di visionare ed autorizzare o scartare l'entrata dei documenti informatici nel SdCM. Convalidando un Pacchetto di Versamento il Produttore si assume tutte le responsabilità sui contenuti dei documenti versati o de-materializzati.
- **Il Responsabile della Conservazione:** è il soggetto che definisce ed attua le politiche complessive del sistema di conservazione e ne governa la gestione con piena responsabilità ed autonomia. Ai sensi dell'art. 44 del D.Lgs 82/2005 e dell'art. 5 del DPCM 3 dicembre 2013, il Responsabile della Conservazione può decidere di affidare la conservazione ad altri soggetti, pubblici o privati che offrono idonee garanzie organizzative e tecnologiche.
- **L'Utente**: è il personale del Cliente autorizzato all'accesso al SdCM con diversi ruoli e permission, definite e sottoscritte a livello contrattuale dal Produttore.

Torna al sommario

4.2 Ruoli Interni

Per quanto riguarda invece i ruoli interni del SdCM la supervisione del buon funzionamento del servizio erogato è affidata al Team del SdCM, nominato dalla Direzione Generale; questo team si riunisce mensilmente per la valutazione delle linee generali che riguardano:

- Valutazione ed evoluzione del SdCM
- Valutazione di Non Conformità, azioni correttive e verifiche delle stesse
- Aggiornamenti sulle variazioni normative

Il Team è composto da:

- Responsabile del Servizio di Conservazione (d'ora innanzi RdSC)
- Responsabile della Funzione Archivistica per la Conservazione (RdFAC)
- Responsabile della Sicurezza del Sistema della Conservazione (RdSSdC)
- Responsabile dei Sistemi Informativi per la Conservazione (RdSIC)
- Responsabile per lo sviluppo e manutenzione del sistema di conservazione (RpSM)
- Responsabile per il trattamento dei dati.

La Tabella a seguire definisce i ruoli interni e le responsabilità del personale dell'Azienda predisposto al buon funzionamento del SdCM.

Ruoli	nominativo	attività di competenza	periodo nel ruolo	eventuali deleghe
Responsabile del servizio di conservazione	Stefano Di Zenzo	- Definizione ed attuazione delle politiche complessive del sistema di conservazione, nonché del governo della gestione del sistema di conservazione; - definizione delle caratteristiche e dei requisiti del Sistema di conservazione in conformità alla normativa vigente; - corretta erogazione del servizio di conservazione all'ente produttore; - gestione delle convenzioni, definizione degli aspetti tecnici-operativi e validazione dei disciplinari tecnici che specificano gli aspetti di dettaglio e le modalità	Dal 2017 ad oggi	

		operative di erogazione dei servizi di conservazione.		
Responsabile Sicurezza dei sistemi per la conservazione	Alessandro Di Francesco	- Rispetto e monitoraggio dei requisiti di sicurezza del sistema di conservazione stabiliti dagli standard, dalle normative e dalle politiche e procedure interne di sicurezza; - Segnalazione delle eventuali difformità al Responsabile del servizio di conservazione e individuazione e pianificazione delle necessarie azioni correttive;	Dal 2017 ad oggi	
Responsabile funzione archivistica di conservazione	Stefano Di Zenzo	- 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 aggregazioni documentali trasferiti, di esibizione, di accesso e fruizione del patrimonio documentario e informativo conservato; - Definizione del set dei 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 gestione dei rapporti con il Ministero dei beni e delle attività culturali per quanto di competenza.	Dal 2017 ad oggi	
Responsabile trattamento dati personali	Adriano Ricchello	- Garanzie e rispetto delle vigenti disposizioni in materia di trattamento dei dati personali; - Garanzia che il trattamento dei dati affidati dal Cliente avverrà nel rispetto delle istruzioni impartite dal Produttore del trattamento dei dati personali, con garanzia di sicurezza e di riservatezza;	Dal 2017 ad oggi	

Responsabile sistemi informativi per la conservazione	Sergio Palumbo	- Gestione dell'esercizio dei 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.	Dal 2011 ad oggi	
Responsabile sviluppo e manutenzione del sistema di conservazione	Paolo Bolognese	- Coordinamento dello sviluppo e manutenzione delle componenti hardware e software del sistema di conservazione; - Pianificazione e monitoraggio dei progetti di sviluppo del sistema di conservazione; - Monitoraggio degli SLA relativi alla manutenzione del sistema di conservazione; - Interfaccia con l'ente produttore relativamente alle modalità di trasferimento dei documenti e fascicoli informatici in merito ai formati elettronici da utilizzare, all'evoluzione tecnologica hardware e software, alle eventuali migrazioni verso nuove piattaforme tecnologiche; - Gestione dello sviluppo di siti web e portali connessi al servizio di conservazione.	Dal 2017 ad oggi	

Per quello che riguarda le deleghe e nomine dei ruoli la politica di MEMAR MONTESSEGNI si fonda per questi ruoli sull'utilizzo di personale la cui responsabilità è intrinseca al grado rivestito dalla persona in Azienda. Di conseguenza il ruolo di Responsabile del Servizio di Conservazione è stato da sempre affidato alla funzione aziendale che nel momento di creazione del Servizio era il Direttore Tecnico ed ideatore del Servizio. L'RdSC nel tempo si è sempre contraddistinto per la sua evoluzione e formazione professionale partecipando anche attivamente alla vita associativa della ANORC come delegato territoriale.
Le altre figure sono comunque oggi i referenti aziendali come Direzione Tecnica, Responsabile Infrastrutture dei Sistemi Informativi, Responsabile Sviluppo Software aziendale, Produttore per il trattamento dei dati.

Il responsabile del Trattamento dei Dati è il Legale Rappresentante dell'Azienda a cui viene conferita la titolarità del ruolo dal Produttore della documentazione attraverso un documento di nomina sottoscritto dal Legale Rappresentante del Cliente, questo documento fa parte integrante del Contratto.

Torna al sommario

4.3 Terze parti

4.3.1 Certification Autorithy

SdCM ha adottato Namiral S.p.A. come Certification Authority che emette i certificati di firma automatica. Namiral S.p.A è accreditata ed iscritta nell'elenco pubblico dei certificatori presso l'Agenzia per l'Italia Digitale (http://www.agid.it/identita-digitali/firme -elettroniche/certificatori-attivi).

4.3.2 Firma digitale remota

Per l'apposizione delle firme in modalità remota viene usato un servizio di forma digitale automatica erogato tramite la soluzione Time4Mind di Intesi Group. La soluzione applicativa implementata, si basa sul prodotto PkBox, il server di sicurezza che permette di implementare nel sistema le funzionalità di firma digitale, crittografia ed autenticazione. Le chiavi private di firma dell'utente Produttore sono custodite da appositi HSM in grado di garantire il più elevato livello di sicurezza. Le funzionalità offerte dal servizio sono:

- la firma digitale automatica dei documenti
- la verifica di un documento elettronico firmato inclusa la verifica di validità del certificato tramite CRL oppure OCSP
- l'apposizione in fase di firma di una marca temporale.

I formati e le modalità di firma disponibili sono quelle previste dalla normativa italiana.

4.3.3 Data Center

Per dare garanzia di continuità e sicurezza del SdCM MEMAR ha ubicato il SdCM presso due Data Center di RETELIT. Il primo sito denominato Data Center Memar01 è ubicato in Castenaso (BO) mentre il secondo sito denominato Memar02 è ubicato in Roma. Tramite questa architettura RETELIT non solo garantisce la continuità del servizio ma anche il backup continuo del SdCM. Tutte le apparecchiature che erogano i servizi sono di proprietà di Memar che ne detiene il controllo informatico totale attraverso la Direzione Tecnica di Memar.
I Data Center RETELIT sono certificati ISO 9001, 14001, 27001:2013 e MEF CE 2.0 e sono caratterizzati da:

- Sale trasmissive dedicate
- Sale separate per la connessione carrier
- Sale Dati ad accesso riservato ed esclusivo
- Sale ad uso ufficio

Le sale dati sono dotate di pavimenti flottanti e controsoffitti con pannelli fonoassorbenti montati su strutture di sostegno sospese mediante pendinatura metallica regolabile. I dati tecnici generali dei siti, variabili per dotazione locale, sono i seguenti:

- Cabine di trasformazione di proprietà
- Trasformatori in configurazione n+1

- Gruppi di continuità cofanati con serbatoi giornaliero di varie capacità per sito e caratterizzati dal carico automatico da serbatoio interrato
- Serbatoio interrato doppia camera con controllo delle perdite di adeguate capienze
- Funzionamento dei Gruppi in parallelo
- UPS per i vari rami costituenti gli impianti (tipicamente Ramo A e Ramo B) dotati di sistema di sincronismo
- Stazioni di energia a 48V con raddrizzatori in configurazione n+2
- Condizionatori ad espansione diretta con doppio compressore e sistema di freecoling (Gas R410A).

L'accesso fisico alle sale avviene per mezzo di lettori di prossimità (badge) rilasciate alle risorse autorizzate individuate da Memar tra il proprio personale tecnico.

I DC sono provvisti di un sistema di antintrusione composto da contatti magnetici, sensori volumetrici e dispositivi di videosorveglianza.

I sistemi antincendio sono costituiti da impianti di rilevazione fumi e da impianti di spegnimento tra loro interconnessi. La rilevazione dei fumi avviene per mezzo di sensori ottici puntiformi installati nei pavimenti flottanti, negli ambienti e nei controsoffitti. I sistemi di spegnimento agiscono con scariche di Gas Argon gestite in automatico da apposite centraline.

Gli allarmi tecnologici sono centralizzati e gestiti attraverso un sistema di supervisione e monitorati H24 dal NOC Retelit.

Il servizio Internet di accesso primario e di backup al SdC è fornito dal fornitore Fastweb, con livelli di servizio concordati in sede contrattuale mentre l'interconnessione tra i siti è realizzata tramite il prodotto E-LINK di E-VIA di Retelit. Detto servizio prevede la fornitura di un circuito trasmissivo *always on* punto punto Ethernet di tipo Fast Ethernet con una capacità adeguata, a porta singola e percorso protetto con disponibilità contrattuale del servizio pari a 99,95%.

Torna al sommario

5. STRUTTURA ORGANIZZATIVE PER IL SERVIZIO DI CONSERVAZIONE

5.1 Organigramma

L'area Aziendale dedicata all'erogazione del servizio di conservazione è denominata EFATTURA, inizialmente dedicata al settore Industry successivamente si espande anche ad altri settori quali la PA ed il settore Bancario.
L'area fa capo direttamente alla Direzione Generale che ne è il Responsabile e Coordinatore.
L'Amministratore Delegato coordina le seguenti Strutture:

- Area Commerciale
- Area Amministrativa
- SdCM

Il seguente organigramma riassume i rapporti fra le strutture preposte all'erogazione del SdCM.

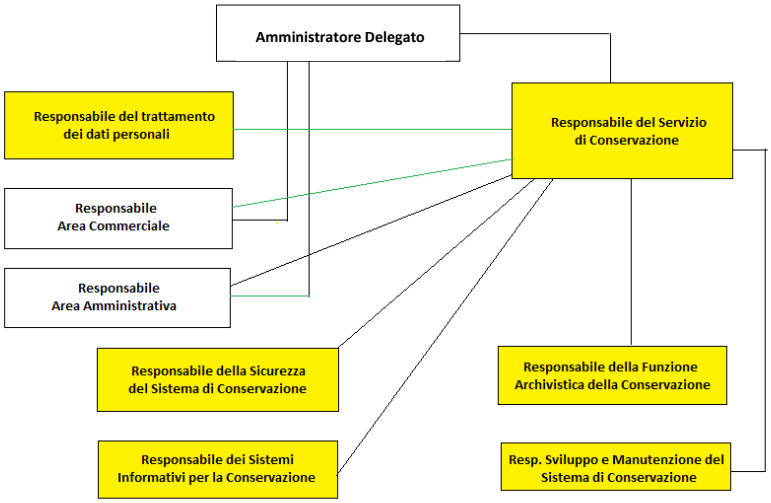

Figura 1. Organigramma del Servizio di Conservazione

Le linee verdi dell'organigramma rappresentano un rapporto di collaborazione. I ruoli definiti con fondo giallo rappresentano il Team che gestisce il Sistema di Conservazione.

Torna al sommario

5.2 Strutture organizzative

Le attività di ciascuna area o di servizi che a vario titolo intervengono nel regolare svolgimento delle attività del SdCM sono definite di seguito:

a) Area Commerciale, è composta da una Direzione Commerciale e da commerciali, l'area si occupa di:
   - Apporto di nuove commesse per il Servizio di Conservazione
   - Ricercare opportunità di mercato che possano incrementare lo sviluppo del Sistema di Conservazione.
   - Coordinarsi in sede di Offerta con il RdSC per lo studio della fattibilità della commessa

- Tenere i rapporti con il cliente in fase di post-vendita e rapportarsi con RdSC per eventuali chiarimenti, lamentele o altro inerente al servizio.
- Attivare ed ottenere dalla CA i certificati di firma per quel Cliente qualora il produttore ne faccia richiesta, censire i soggetti con autorizzazione di firma e le scadenze dei certificati.
- Censire con il Produttore gli accessi e le permission al SdCM.

Le responsabilità specifiche di questa area sono:

- La definizione dei requisiti del cliente;
- Il coordinamento della comunicazione fra cliente ed i reparti preposti all'erogazione del servizio;
- L'individuazione del livello di soddisfazione del cliente rispetto al servizio di conservazione;
- La penetrazione di mercato
- Verificare in fase preliminare l'aderenza dei requisiti oggetto della commessa con i requisiti del SdCM.

b) Area Amministrativa:
   - Registrazione dei documenti contrattuali
   - Apertura e chiusura delle commesse

   Le responsabilità specifiche di questa area sono:

   - La corretta contabilizzazione della commessa;
   - La comunicazione con i reparti preposti all'erogazione del servizio in caso di interruzioni o sospensioni della commessa;

c) Servizio IT:
   Si occupa direttamente dello sviluppo software, delle configurazioni di siti e piattaforme, dell'infrastruttura Hardware e di Sicurezza. Il Servizio IT, sotto la responsabilità del suo Direttore Tecnico si articola in diverse sezioni:
   - Area Sviluppo Software: area di sviluppo software coordinata da un responsabile dello sviluppo.
   - Area Sistemistica e della Sicurezza: si occupa dello sviluppo e manutenzione delle infrastrutture hardware e di sicurezza informatica

   Il servizio IT per il normale funzionamento del SdCM provvede alle seguenti funzioni operative:
   - Compilazione del Rapporto di Attivazione
   - Configurazione di nuovi servizi sulla base del Rapporto di Attivazione
   - Test delle fasi preliminari di trasferimento pacchetti PdV
   - Monitoraggio dei trasferimenti
   - Generazione dei Rapporti di Versamento
   - Gestione dei Rapporti di rifiuto del PdV nei confronti del Produttore
   - Monitorare la creazione automatica dei PdA
   - Monitorare la creazione automatica dei PdD
   - Monitorare la leggibilità e integrità dei PdA conservati mediante strumenti di automazione.
   - Gestire lo scarto da SdCM dei pacchetti di scarto
   - Help Desk di primo livello: è realizzato attraverso una piattaforma web che permette la segnalazione di problemi e l'apertura di ticket di assistenza.
   - Help Desk di secondo livello è svolto dal personale del servizio IT.
   - Sviluppo, manutenzione e sicurezza dell'infrastruttura hardware

   Le responsabilità specifiche di questa area sono:

- L'aderenza fra i requisiti del cliente ed il verbale di attivazione;
- Segnalare tempestivamente i requisiti del cliente che non sono compatibili con i requisiti del SdCM;
- La corretta configurazione del servizio su SdCM;
- La corretta esecuzione dei test preliminari e collaudi
- Il monitoraggio delle attività di versamento e la tempestiva apertura di non conformità;
- Il monitoraggio delle attività di conservazione e la tempestiva apertura di non conformità;
- L'analisi del log di sistema e degli "alert" del sistema stesso;
- Il pronto intervento nell'assistenza ai ticket;
- Il monitoraggio dei sistemi di sicurezza;

d) Area Progettistica: si occupa, attraverso i suoi Project manager, della analisi e gestione dei progetti informatici, nella specificità del SdCM si occupa direttamente di:
   - Elaborazione del Rapporto di Attivazione: questionario iniziale che riporta tutte le informazioni di dettaglio sulle classi documentali da conservare, relativi metadati obbligatori ed accessori, definizione delle modalità di trasferimento, referenti e contatti dell'ente produttore.
   - Elaborazione e richiesta al servizio IT per lo sviluppo di varianti di controllo e/o monitoraggio richieste da quel specifico contratto.

   Le responsabilità specifiche di questa area sono:

   - L'aderenza fra i requisiti del cliente e la configurazione del cliente sul SdCM
   - L'indicazione delle specifiche necessarie allo sviluppo di personalizzazioni e nuove funzionalità;
   - Il test e collaudo delle implementazioni.

Torna al sommario

6. OGGETTI SOTTOPOSTI A CONSERVAZIONE

6.1 Oggetti conservati

Gli oggetti che vengono sottoposti a conservazione nel SdCM sono documenti informatici o aggregazioni degli stessi inviati al SdCM dal produttore e sempre autorizzati dal Produttore stesso al processo di conservazione.

I documenti da conservare possono appartenere a differenti classi documentali e secondo la classe possono essere diversi nel formato, nei metadati di accompagnamento e nelle regole di conservazione.

Il formato, i metadati ed i tempi di conservazione e di tenuta, specifici per ogni Cliente, sono descritti nel Rapporto di Attivazione che è stato predisposto ed accettato dal Responsabile del Servizio di Conservazione e della Funzione Archivistica in congiunto e condiviso con il Responsabile della Conservazione.

Le generalità sui formati, metadati e tempi di conservazione e di tenuta sono descritti nel documento **Specificità del contratto** del presente manuale.

Ogni singolo documento informatico può avere degli allegati che sono collegati ai documenti principali e possono essere conservati su scelta del Produttore.

I Pacchetti di Versamento (d'ora innanzi PdV) sono omogenei per classe documentale o per registro qualora la classe sia rappresentata da suddivisioni negli stessi, come per esempio nel caso di documenti fiscali e tributari, l'appartenenza di un documento informatico ad un determinato registro o classe è un'informazione prodotta dal Produttore ed inserita nel PdV.

Poiché al momento della formazione dei PdA per un singolo Produttore possono essere presenti più PdV ed anche PdV appartenenti a Classi e registri diversi il SdCM si comporta nel seguente modo:

- I PdA sono omogenei per Produttore e classe documentale.
- Nel caso il Produttore sia un Gruppo di Aziende il PdA è omogeneo per ogni singola Ragione Sociale del Gruppo e classe documentale.
- Nel caso di PA il PdA è omogeneo per Area Organizzativa Omogenea e classe documentale.
- Nel caso in cui una singola classe documentale corrisponda a più registri questi ultimi vengono identificati alla classe ed i PdA sono così omogenei per classe documentale o registro.

Torna al sommario

6.2 Pacchetto di versamento (PdV)

Una apposita sezione del SdCM mostra al Produttore i PdV caricati dal produttore, compresi gli esiti dei controlli. Presa visione del pacchetto caricato, il Produttore può confermare o annullare (in tutto o parzialmente) il pacchetto caricato. Confermando il pacchetto di caricamento questo si trasforma nel PdV attraverso il processo di firma del Produttore del PdV. Questo momento rappresenta il punto di non ritorno nel senso che una volta confermato il PdV i documenti entrano in uno stato "protetto" che non permetterà più né modifiche né cancellazioni. Il PdV passa così allo stato "pronto" per la conservazione.

Confermando il PdV il Produttore firma digitalmente con dispositivo HSM tutti i documenti che entrano a far parte del PdV.

Il SdCM una volta caricato il PdV procede alla generazione della Ricevuta del PdV, nella quale il RdSC firma e marca con marca temporale l'hashing dei documenti informatici contenuti nel PDV e restituisce copia al Produttore, la Ricevuta contiene il Rapporto di versamento o di rifiuto.

Il rapporto di versamento è un file XML firmato secondo lo standard XAdES, questa operazione è svolta dal Responsabile del Servizio di Conservazione.

In base alle caratteristiche ed alle regole di conservazione di quella classe o registro documentale sono stabiliti dei tempi massimi per lo stazionamento dei PdV allo stato pronto, ovvero per la sua conversione in PdA.

Un apposito sistema di monitoraggio tiene sempre sotto controllo i pacchetti di input caricati e la loro trasformazione in PdV, segnalando pacchetti di input sospesi da troppo tempo ed i pacchetti andati a buon fine e di PdV in scadenza per la conservazione.

Si rinvia al allegato **Specificità del Contratto** la descrizione di dettaglio della struttura dei PdV.

Torna al sommario

6.3 Pacchetto di Archiviazione (PdA)

Un sistema di monitoraggio di SdCM verifica i tempi di conservazione dei PdV allo stato "pronto" ed allo scadere del tempo limite procede all'aggregazione e conservazione dei PdV in PdA.

L'aggregazione avviene per classi e per singolo Produttore o AOO per la PA e crea un PdA con relativo IPdA (formato XML) in formato UNI SINCRO.

I singoli PdA vengono processati solo se vengono validate le regole di conservazione correlate a quelle tipologie documentali.

Una volta validato il PdA viene creato il relativo IPdA e questo viene firmato dal RdSC e marcato temporalmente, questa operazione vien svolta dal Responsabile del Servizio di Conservazione. Il IPdA viene così incorporato nel PdA formando così il Pacchetto di Conservazione.

I metadati associati o descrittivi del PdA vengono messi a sistema nel Database di SdCM.

All'interno del IPdA si trovano:

- informazioni riguardanti l'azienda e il prodotto che generano l'indice;
- informazioni riguardanti l'azienda Produttore dei documenti, per la quale viene prodotto l'indice;
- informazioni riguardanti la classe documentale e il periodo di riferimento dei documenti conservati;
- informazioni specifiche di ogni documento. In questa sezione trovano posto l'ID univoco del documento, il nome del file, la sua impronta e tutti i metadati ad esso correlati;
- informazioni riguardanti tutti i soggetti (fisici e giuridici) interessati dal processo di conservazione. In tale sezione trovano posto il soggetto che appone la firma all'IPdA e l'azienda che offre il servizio di conservazione;

L'indice del pacchetto di archiviazione viene firmato in modalità CAdES e marcato temporalmente.

Il pacchetto di archiviazione (PdA), prodotto al termine del processo di conservazione, è composto da un insieme di file e directory, gli elementi che lo compongono:

- L'IPdA firmato in modalità CAdES e marcato;
- La directory contenente tutti i documenti facenti parte del PDA
- L'applicazione java (visualizzatore) che consente la verifica della firma apposta sull'IPdA e la visualizzazione del PDA stesso.
- La directory contenente i certificati necessari per la verifica della firma apposta sull'indice del pacchetto di archiviazione;
- Il file contenente le istruzioni per avviare automaticamente l'applicazione di visualizzazione.

tutti gli elementi appena descritti vengono inseriti in un unico file .ISO che costituisce il pacchetto di archiviazione.
Il formato .ISO fa si che, se necessario, il PDA possa comodamente essere masterizzato su DVD.

Struttura schema XML del PdA:

```
<?xml version="1.0" encoding="utf-8"?>
<xs:schema xmlns="http://memar.it/tDoc/pacchetto.xsd"
    xmlns:xs="http://www.w3.org/2001/XMLSchema"
    targetNamespace="http://memar.it/tDoc/pacchetto.xsd"
    elementFormDefault="qualified">
  <xs:element name="pacchetto">
    <xs:complexType>
      <xs:sequence>
        <xs:element name="company" type="xs:string" />
        <xs:element name="doctype" type="xs:string" />
        <xs:element name="period" type="xs:gYear" />
        <xs:element name="previous" minOccurs="0">
          <xs:complexType>
            <xs:simpleContent>
              <xs:extension base="xs:hexBinary">
                <xs:attribute name="id" type="xs:string" use="optional" />
              </xs:extension>
            </xs:simpleContent>
          </xs:complexType>
        </xs:element>
      </xs:sequence>
    </xs:complexType>
  </xs:element>
</xs:schema>
```

Struttura xsd dei metadati:

```
<?xml version="1.0" encoding="utf-8"?>
<xs:schema xmlns="http://memar.it/tDoc/metadata.xsd"
       xmlns:xs="http://www.w3.org/2001/XMLSchema"
    targetNamespace="http://memar.it/tDoc/metadata.xsd"
    elementFormDefault="qualified">
  <xs:element name="metadata">
    <xs:complexType>
      <xs:sequence>
        <xs:element name="meta" maxOccurs="unbounded">
          <xs:complexType>
            <xs:attribute name="class" type="xs:string" use="optional" />
```

```
            <xs:attribute name="name"  type="xs:string" use="required" />
            <xs:attribute name="value" type="xs:string" use="required" />
          </xs:complexType>
        </xs:element>
      </xs:sequence>
    </xs:complexType>
  </xs:element>
</xs:schema>
```

Struttura del xsd del SINCRO:


```
<?xml version="1.0" encoding="utf-8"?>
<xs:schema xmlns:sincro="http://www.uni.com/U3011/sincro/"
       xmlns:xs="http://www.w3.org/2001/XMLSchema"
targetNamespace="http://www.uni.com/U3011/sincro/"
       elementFormDefault="qualified" attributeFormDefault="qualified">
  <xs:annotation>
    <xs:documentation xml:lang="en">
      Definition of simple
      types
    </xs:documentation>
  </xs:annotation>
  <xs:simpleType name="Label">
    <xs:restriction base="xs:string" />
  </xs:simpleType>
  <xs:simpleType name="Path">
    <xs:restriction base="xs:anyURI" />
  </xs:simpleType>
  <xs:simpleType name="Name">
    <xs:restriction base="xs:string" />
  </xs:simpleType>
  <xs:simpleType name="Version">
    <xs:restriction base="xs:string" />
  </xs:simpleType>
  <xs:simpleType name="Producer">
    <xs:restriction base="xs:string" />
  </xs:simpleType>
  <xs:simpleType name="TimeInfo">
    <xs:restriction base="xs:dateTime" />
  </xs:simpleType>
  <xs:simpleType name="FirstName">
    <xs:restriction base="xs:string" />
  </xs:simpleType>
  <xs:simpleType name="LastName">
    <xs:restriction base="xs:string" />
  </xs:simpleType>
  <xs:simpleType name="FormalName">
    <xs:restriction base="xs:string" />
  </xs:simpleType>
  <xs:simpleType name='EmptyString'>
    <xs:restriction base='xs:string'>
      <xs:maxLength value="0" />
    </xs:restriction>
  </xs:simpleType>
  <xs:annotation>
    <xs:documentation xml:lang="en">
```

```
    Definition of attributes
  </xs:documentation>
</xs:annotation>
<xs:attribute name="version" type="xs:NMTOKEN" fixed="1.0" />
<xs:attribute name="url" type="xs:anyURI"
           fixed="http://www.uni.com/U3011/sincro/" />
<xs:attribute name="XMLScheme" type="xs:anyURI" />
<xs:attribute name="scheme" type="xs:string" default="local" />
<xs:attribute name="canonicalXML" type="xs:boolean" />
<xs:attribute name="function" type="xs:NMTOKEN" default="SHA-1" />
<xs:attribute name="extension" type="xs:NMTOKEN" />
<xs:attribute name="language" type="xs:language" default="it" />
<xs:attribute name="format" type="xs:string" />
<xs:attribute name="encoding">
  <xs:simpleType>
    <xs:restriction base="xs:NMTOKEN">
      <xs:enumeration value="7bit" />
      <xs:enumeration value="8bit" />
      <xs:enumeration value="base64" />
      <xs:enumeration value="binary" />
      <xs:enumeration value="quotedprintable" />
      <xs:enumeration value="xtoken" />
    </xs:restriction>
  </xs:simpleType>
</xs:attribute>
<xs:attribute name="normal" type="xs:dateTime" />
<xs:attribute name="type">
  <xs:simpleType>
    <xs:restriction base="xs:NMTOKEN">
      <xs:enumeration value="person" />
      <xs:enumeration value="organization" />
    </xs:restriction>
  </xs:simpleType>
</xs:attribute>
<xs:attribute name="otherRole" type="xs:string" />
<xs:attribute name="role">
  <xs:simpleType>
    <xs:restriction base="xs:NMTOKEN">
      <xs:enumeration value="PreservationManager" />
      <xs:enumeration value="Operator" />
      <xs:enumeration value="PublicOfficer" />
      <xs:enumeration value="Delegate" />
      <xs:enumeration value="OtherRole" />
    </xs:restriction>
  </xs:simpleType>
</xs:attribute>
<xs:annotation>
  <xs:documentation xml:lang="en">
    Definition of
    complex types
  </xs:documentation>
</xs:annotation>
<xs:complexType name="EmbeddedMetadata">
  <xs:complexContent>
    <xs:extension base="xs:anyType"></xs:extension>
  </xs:complexContent>
</xs:complexType>
<xs:complexType name="Identifier">
  <xs:simpleContent>
    <xs:extension base="xs:NMTOKEN">
```

```
      <xs:attribute ref="sincro:scheme" />
    </xs:extension>
  </xs:simpleContent>
</xs:complexType>
<xs:complexType name="Agent_ID">
  <xs:simpleContent>
    <xs:extension base="xs:string">
      <xs:attribute name="scheme" use="required">
        <xs:simpleType>
          <xs:restriction base="xs:NMTOKEN">
            <xs:enumeration value="TaxCode" />
            <xs:enumeration value="VATRegistrationNumber" />
            <xs:enumeration value="NationalHealthCareAuthority" />
            <xs:enumeration value="OtherScheme" />
          </xs:restriction>
        </xs:simpleType>
      </xs:attribute>
      <xs:attribute name="otherScheme" type="xs:string" />
    </xs:extension>
  </xs:simpleContent>
</xs:complexType>
<xs:complexType name="Description">
  <xs:simpleContent>
    <xs:extension base="xs:string">
      <xs:attribute ref="sincro:language" />
    </xs:extension>
  </xs:simpleContent>
</xs:complexType>
<xs:complexType name="MoreInfo">
  <xs:choice>
    <xs:element name="EmbeddedMetadata" type="sincro:EmbeddedMetadata" />
    <xs:element name="ExternalMetadata" type="sincro:File" />
  </xs:choice>
  <xs:attribute ref="sincro:XMLScheme" use="required" />
</xs:complexType>
<xs:complexType name="Hash">
  <xs:simpleContent>
    <xs:extension base="xs:string">
      <xs:attribute ref="sincro:canonicalXML" />
      <xs:attribute ref="sincro:function" use="required" />
    </xs:extension>
  </xs:simpleContent>
</xs:complexType>
<xs:complexType name="PreviousHash">
  <xs:simpleContent>
    <xs:extension base="sincro:Hash">
      <xs:attribute name="relatedIdC" type="xs:NMTOKEN" use="required" />
    </xs:extension>
  </xs:simpleContent>
</xs:complexType>
<xs:complexType name="CreatingApplication">
  <xs:sequence>
    <xs:element name="Name" type="sincro:Name" />
    <xs:element name="Version" type="sincro:Version" />
    <xs:element name="Producer" type="sincro:Producer" />
  </xs:sequence>
</xs:complexType>
<xs:complexType name="LawAndRegulations">
  <xs:simpleContent>
    <xs:extension base="xs:string">
```

```
      <xs:attribute ref="sincro:language" />
    </xs:extension>
  </xs:simpleContent>
</xs:complexType>
<xs:complexType name="SourceIdC">
  <xs:sequence>
    <xs:element name="ID" type="sincro:Identifier" />
    <xs:element name="Path" type="sincro:Path" minOccurs="0" />
    <xs:element name="Hash" type="sincro:Hash" />
  </xs:sequence>
</xs:complexType>
<xs:complexType name="SourceVdC">
  <xs:sequence>
    <xs:element name="ID" type="sincro:Identifier" />
    <xs:element name="IdC_ID" type="sincro:Identifier" />
  </xs:sequence>
</xs:complexType>
<xs:complexType name="VdCGroup">
  <xs:sequence>
    <xs:element name="Label" type="sincro:Label" />
    <xs:element name="ID" type="sincro:Identifier" minOccurs="0" />
    <xs:element name="Description" type="sincro:Description"
                minOccurs="0" />
  </xs:sequence>
</xs:complexType>
<xs:complexType name="VdC">
  <xs:sequence>
    <xs:element name="ID" type="sincro:Identifier" />
    <xs:element name="SourceVdC" type="sincro:SourceVdC"
                minOccurs="0" maxOccurs="unbounded" />
    <xs:element name="VdCGroup" type="sincro:VdCGroup"
                minOccurs="0" />
    <xs:element name="MoreInfo" type="sincro:MoreInfo"
                minOccurs="0" />
  </xs:sequence>
</xs:complexType>
<xs:complexType name="FileGroup">
  <xs:sequence>
    <xs:element name="Label" type="sincro:Label" minOccurs="0" />
    <xs:element name="File" type="sincro:File" maxOccurs="unbounded" />
    <xs:element name="MoreInfo" type="sincro:MoreInfo"
                minOccurs="0" />
  </xs:sequence>
</xs:complexType>
<xs:complexType name="File">
  <xs:sequence>
    <xs:element name="ID" type="sincro:Identifier" />
    <xs:element name="Path" type="sincro:Path" minOccurs="0" />
    <xs:element name="Hash" type="sincro:Hash" />
    <xs:element name="PreviousHash" type="sincro:PreviousHash"
                minOccurs="0" />
    <xs:element name="MoreInfo" type="sincro:MoreInfo"
                minOccurs="0" />
  </xs:sequence>
  <xs:attribute ref="sincro:encoding" default="binary" />
  <xs:attribute ref="sincro:extension" />
  <xs:attribute ref="sincro:format" use="required" />
</xs:complexType>
<xs:complexType name="SelfDescription">
  <xs:sequence>
```

```
    <xs:element name="ID" type="sincro:Identifier" />
    <xs:element name="CreatingApplication" type="sincro:CreatingApplication" />
    <xs:element name="SourceIdC" type="sincro:SourceIdC"
                minOccurs="0" maxOccurs="unbounded" />
    <xs:element name="MoreInfo" type="sincro:MoreInfo"
                minOccurs="0" />
  </xs:sequence>
</xs:complexType>
<xs:complexType name="NameAndSurname">
  <xs:sequence>
    <xs:element name="FirstName" type="sincro:FirstName" />
    <xs:element name="LastName" type="sincro:LastName" />
  </xs:sequence>
</xs:complexType>
<xs:complexType name="AgentName">
  <xs:choice>
    <xs:element name="NameAndSurname" type="sincro:NameAndSurname" />
    <xs:element name="FormalName" type="sincro:FormalName" />
  </xs:choice>
</xs:complexType>
<xs:complexType name="Agent">
  <xs:sequence>
    <xs:element name="AgentName" type="sincro:AgentName" />
    <xs:element name="Agent_ID" type="sincro:Agent_ID"
                minOccurs="0" maxOccurs="unbounded" />
    <xs:element name="MoreInfo" type="sincro:MoreInfo"
                minOccurs="0" />
  </xs:sequence>
  <xs:attribute ref="sincro:type" use="required" />
  <xs:attribute ref="sincro:role" use="required" />
  <xs:attribute ref="sincro:otherRole" />
</xs:complexType>
<xs:complexType name="Process">
  <xs:sequence>
    <xs:element name="Agent" type="sincro:Agent" maxOccurs="unbounded" />
    <xs:element name="TimeReference" type="sincro:TimeReference" />
    <xs:element name="LawAndRegulations" type="sincro:LawAndRegulations"
                minOccurs="0" />
    <xs:element name="MoreInfo" type="sincro:MoreInfo"
                minOccurs="0" />
  </xs:sequence>
</xs:complexType>
<xs:complexType name="TimeReference">
  <xs:choice>
    <xs:element name="DetachedTimestamp" type="sincro:DetachedTimeStamp" />
    <xs:element name="AttachedTimeStamp" type="sincro:AttachedTimeStamp" />
    <xs:element name="TimeInfo" type="sincro:TimeInfo" />
  </xs:choice>
</xs:complexType>
<xs:complexType name="AttachedTimeStamp">
  <xs:simpleContent>
    <xs:extension base="sincro:EmptyString">
      <xs:attribute ref="sincro:normal" use="required" />
    </xs:extension>
  </xs:simpleContent>
</xs:complexType>
<xs:complexType name="DetachedTimeStamp">
  <xs:simpleContent>
    <xs:extension base="xs:anyURI">
      <xs:attribute ref="sincro:normal" use="required" />
```

```
        <xs:attribute ref="sincro:encoding" default="binary" />
        <xs:attribute ref="sincro:format" use="required" />
      </xs:extension>
    </xs:simpleContent>
  </xs:complexType>
  <xs:complexType name="IdC">
    <xs:sequence>
      <xs:element name="SelfDescription" type="sincro:SelfDescription" />
      <xs:element name="VdC" type="sincro:VdC" />
      <xs:element name="FileGroup" type="sincro:FileGroup"
                  maxOccurs="unbounded" />
      <xs:element name="Process" type="sincro:Process" />
    </xs:sequence>
    <xs:attribute ref="sincro:version" />
    <xs:attribute ref="sincro:url" />
  </xs:complexType>
  <xs:annotation>
    <xs:documentation xml:lang="en">
      Definition of root
      element
    </xs:documentation>
  </xs:annotation>
  <xs:element name="IdC" type="sincro:IdC" />
</xs:schema>
```


Torna al sommario

6.4 Pacchetto di Distribuzione (PdD)

Qualora il Produttore o persona autorizzata richieda una estrazione di documenti conservati, SdCM provvede alla creazione del PdD.

La creazione di un PdD può essere richiesta dal Produttore o via mail o attraverso una interfaccia web dedicata nel portale del SdCM.

Il pacchetto di distribuzione (PdD), prodotto al termine del processo di richiesta, è un file in formato ZIP che comprende i seguenti elementi:

- L'insieme dei documenti ricercati attraverso l'interfaccia di esibizione suddivisi per Azienda, classe documentale e per PDA di appartenenza;
- L'insieme degli IPdA di appartenenza dei documenti ricercati
- L'applicazione java che consente la visualizzazione di tutti i documenti contenuti nel pacchetto di distribuzione e dei relativi metadati. L'applicazione consente anche di verificare le firme apposte sugli IPdA contenuti nel pacchetto e di fare ricerche interne al PDD;
- La directory contenente i certificati necessari per la verifica delle firme apposte sugli indici del pacchetto di archiviazione;
- La directory contenente gli schemi XSD che descrivono la struttura degli indici dei pacchetti di archiviazione.
- Il file contenente le istruzioni per avviare automaticamente l'applicazione di visualizzazione.
- Il file indice del PdD è firmato dal RdSC secondo il formato CAdES. Il file contiene l'elenco degli IPdA contenuti nel PDD e dei relativi hash. Questa operazione vien svolta dal Responsabile del Servizio di Conservazione

Il file indice fornisce garanzie di autenticità e di integrità circa gli IPdA contenuti nel pacchetto. A loro volta gli IPdA contengono l'elenco dei documenti e dei relativi hash, e, essendo firmati, garantiscono l'autenticità e l'integrità di tutti i documenti contenuti nel PdD.
La presenza di un file così strutturato all'interno del PdD fornisce le stesse garanzie che fornirebbe una firma CAdES esterna al pacchetto, con il vantaggio di evitare proprio la firma esterna al PdD, che potrebbe essere tecnicamente improponibile vista la potenziale dimensione di un PDD, che potrebbe raggiungere decine o centinaia di GigaByte.

Torna al sommario

7. PROCESSO DI CONSERVAZIONE

Il Processo di Conservazione si può rappresentare schematicamente nel seguente modo:

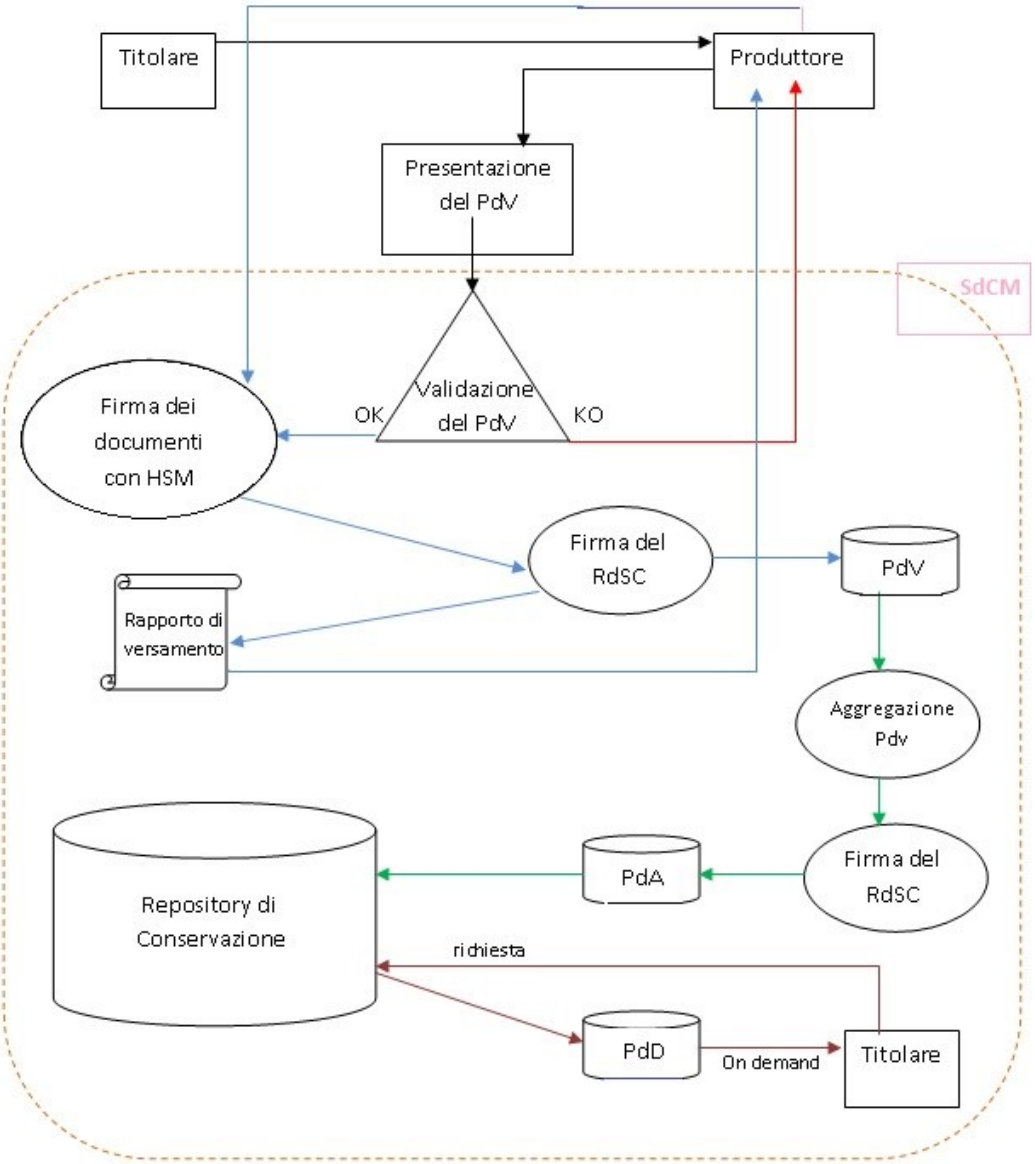

Figura 2. Schema generale del Processo di Conservazione

L'attivazione di un nuovo contratto di conservazione nasce dall'Amministrazione, la quale, ricevuto un contratto firmato dall'Area Commerciale e verificata la consistenza dei documenti, apre la commessa nel gestionale aziendale e ne dà comunicazione al RdSC, responsabile per l'erogazione del servizio di conservazione.

Una volta attivato il contratto con il Produttore da un punto di vista amministrativo, seguono le vere e proprie attività di startup, ovvero:

a) Verifica dei requisiti dichiarati in fase di pre-vendita relativi al servizio di conservazione con i parametri contrattuali, dichiarazione di eventuali non conformità all'Area Commerciale. Questa verifica è attuata dal RdSC.

b) Compilazione da parte di un project manager del Questionario di Attivazione

c) Valutazione di coerenza del Questionario di attivazione con gli standard del SdCM.

d) Configurazione del nuovo servizio nel SdCM

e) Eventuale richiesta e rilascio dei certificati di firma digitale da parte della CA.

Il Questionario di Attivazione è un documento preliminare necessario a poter configurare il nuovo servizio sul SdCM, in esso sono contenute informazioni importanti quali le classi documentali, i tipi documento, numerazioni e registri di riferimento, i metadati obbligatori da abbinare ai documenti informatici, i tempi di conservazione e di tenuta, gli utenti del Produttore autorizzati ai processi di firma, le modalità di trasferimento dei PdV, gli estremi dei certificati di firma, i riferimenti aziendali per le procedure tecniche, amministrative e commerciali.

Il Questionario di Attivazione viene compilato da un nostro operatore congiuntamente con il Produttore e viene sottoscritto ed accettato anche da quest'ultimo, contiene le SLA del processo di consegna dei PdV e le regole di conservazione. Il questionario è validato infine dal RdSC.

Il questionario fa parte integrante del Contratto di servizio e descrive anche con quale sistema il produttore caricherà i PdV nel SdCM.

Torna al sommario

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

Il SdCM ha un suo standard di attivazione che secondo la tipologia di documento prevede un determinato formato di input e dei controlli accessori. Il tutto è definito da dei parametri di configurazione formati nella fase di attivazione in base al Questionario di Attivazione.

Spesso il Produttore non è in grado di fornire gli input nel formato richiesto ed in questo caso o il Produttore sviluppa in proprio un "Conversore" oppure la nostra Azienda lo affiancherà in tale attività.

Nell'ultimo caso l'attività di Conversione non fa parte del SdCM bensì del processo di produzione dell'input e resta in capo al Produttore come onere e responsabilità.

Per il SdCM il processo di Conservazione inizia con la consegna da parte del Produttore del PdV.

E' anche presente il caso in cui il Produttore ci consegni documenti cartacei da trasformare in documenti informatici, anche in questo caso la nostra Azienda fornisce un servizio di de-materializzazione che permette

dal cartaceo di produrre il pacchetto di input destinato a diventare il PdV, anche questo servizio non entra a far parte del SdCM essendo un servizio preliminare alla formazione del PdV. In ogni caso questo processo è governato da procedure di produzione di qualità che permettono la quadratura degli oggetti e di tracciare le coordinate dell'archivio cartaceo per il periodo intermedio di produzione dei PdV.

Una volta quindi prodotto il Pacchetto di input (PdV) questo viene trasferito al SdCM. Il trasferimento avviene attraverso un canale di trasmissione gestito dal SdCM per il controllo e la verifica del trasferimento.

A secondo del produttore del PdV l'attività di trasferimento è così gestita:

a) Attraverso un software dedicato denominato UpToCOS
b) Attraverso un software dedicato denominato SAPtoCOS per gli utenti che possiedono SAP.
c) Attraverso un software dedicato denominato ARXtoCOS per gli utenti che possiedono workflow Arxivar.
d) Attraverso un software di produzione Memar denominato MemarToCOS, nel caso di de-materializzazione di documenti analogici.

I diversi xxToCOS non fanno parte del SdCM ma ne rappresentano l'alimentazione, governano le trasmissioni sFTP e si assicurano dell'integrità e completezza del trasferimento, effettuano quindi dei controlli di primo livello ai fini di bloccare in partenza dei pacchetti problematici. I controlli riguardano la presenza dei metadati obbligatori.

Una volta trasferito al SdCM il pacchetto di Input viene elaborato e se per quella tipologia o classe documentale sono previsti controlli di qualità di secondo livello questi vengono effettuati.

Questa parte del processo rappresenta una fase delicata dell'intero processo ed è per questo che è sottoposta a test e collaudo.

Nella fase di attivazione quindi vengono elaborati tanti tipi di input quanti sono le classi documentali che il Produttore invierà a SdCM. Per ogni tipo vengono fatti test di conversione e caricamento in ambiente di test, il collaudo viene sottoposto ad accettazione da parte del Cliente.

Dalla sottoscrizione dell'accettazione il Cliente si assume tutte le responsabilità delle fasi di trasformazione che creano il PdV, avendo comunque l'onere e la responsabilità di convalidare e firmare i singoli PdV prima che questi vengano inviati alla conservazione.

La sottoscrizione avviene postuma rispetto a test e collaudi nello stesso documento Questionario di attivazione che fa parte integrante del contratto.

Tutti i PdV vengono caricati in SdCM attraverso un SFTP-SSH2 dedicato di SdCM con protocollo di crittografia sia del canale di trasmissione che dei pacchetti trasmessi, tutti i log delle azioni fatte sul database di SdCM vengono conservati e consultabili in automatico da sistema.

Tutti i log di accesso al server su cui risiede il SdCM vengo storicizzati e conservati in real time su un sistema remoto di conservazione (K-audit).

Torna al sommario

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

Una volta caricati su SdCM i pacchetti di versamento, questi subiscono una serie di controlli se previsti dalla configurazione di quel cliente e di quella classe documentale, solo i documenti informatici che superano questi "controls" sono pronti per diventare PdV.

I controls principali sono i seguenti:

- Identificazione dell'utente della convalida: viene effettuato non solo attraverso l'ID e password dell'utente abilitato ma anche con l'inserimento da parte dell'utente del PIN di convalida del certificato di firma.
- L'identificazione certa del soggetto che ha prodotto il documento e dell'ente produttore è fatta in fase di convalida in quanto il SdCM garantisce l'accesso alle funzioni di caricamento solo a determinati utenti configurati sul sistema, allo stesso modo vengono configurati sul sistema i certificati di firma corrispondenti agli utenti autorizzati ai caricamenti, l'inserimento del PIN, oltre le credenziali di accesso, garantiscono senza possibilità di dubbio che l'utente che sta facendo l'operazione è il titolare del certificato di firma autorizzato.
- Se il service MEMAR affianca il produttore la convalida dei PdV è sempre comunque fatta dal'utente del Produttore che firma i PdV.
- Verifica dell'esistenza della classe documentale sul SdCM per quel Produttore.
- Verifica della presenza e del formato dei metadati obbligatori definiti nella classe documentale.
- Verifica, se necessaria per quella classe di numerazione, duplicazione e inversioni di date.
- Verifica del formato del file che viene caricato.

Attraverso una interfaccia dedicata il produttore può visualizzare l'esito dei controlli e confermare il versamento. Attraverso questa conferma i documenti che faranno parte del PdV vengono firmati digitalmente dal Produttore attraverso un sistema di firma remota HSM, viene così consolidato il PdV e generato il rapporto di versamento; da questo momento in avanti i documenti ed i loro metadati non possono più essere modificati.

Il SdCM presenta una maschera che elaborando i log di sistema permette sempre all'utente di verificare le operazioni effettuate, i documenti andati a buon fine ed i documenti registrati. Questo meccanismo non rende necessaria l'analisi dei log in quanto già attuati dalla stessa interfaccia (pur rimanendo comunque i log consultabili al personale tecnico del SdCM).

Per gestire correttamente il Processo SdCM effettua una serie di monitoraggi descritti nel paragrafo 9.1.

Torna al sommario

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

Una volta che il pacchetto di versamento ha superato i controls ed è stato convalidato dalla persona autorizzata alla convalida ed identificato attraverso il PIN del certificato di firma, inizia il processo di formazione del PdV che viene eseguito in automatico dal SdCM.

Una volta convalidati i documenti presenti nel pacchetto di versamento vengono tutti firmati con modalità HSM dall'utente.

Per ogni PdV viene generato automaticamente un Rapporto di Versamento relativo al pacchetto di versamento, univocamente identificato dal sistema di conservazione e contenente un riferimento temporale, specificato con riferimento al Tempo universale coordinato (UTC), e una o più impronte, calcolate sull'intero contenuto del pacchetto di versamento.

Il PdV è un file XML firmato dal RdSC in modalità XAdES, la cui struttura o schema XSD è definito nel documento **Specificità del Contratto**, allegato al presente manuale.

Ogni PdV viene archiviato e conservato in una classe documentale predefinita per mantenere evidenza storica del pacchetto di versamento.

I log di questa operazione vengono storicizzati e conservati nel SdCM.

Il Rapporto di Versamento viene firmato dal RdSC e conservato in un'area dedicata del SdCM dalla quale il Produttore può ritirarne una copia.

Torna al sommario

7.4 Rifiuto del pacchetto di versamento e modalità di comunicazione delle anomalie.

Il rifiuto totale o parziale di un pacchetto di versamento è una operazione implicita nel meccanismo di versamento utilizzato dal SdCM. Ogni pacchetto di documenti, omogenei per classe, dopo aver subito i controls, viene mostrato analiticamente all'Utente che convalida il PdV e vengono segnalati tutti i documenti che non hanno superato i controls; per ogni documento che non supera i controls viene descritto lo stato di anomalia e la causale specifica che ha creato l'anomalia. Tutti i documenti con stato di anomalia automaticamente non vengono accettati dal sistema e quindi non possono passare nel Rapporto di versamento, vengono semplicemente ignorati. L'eliminazione di questi documenti anomali è fatta direttamente dall'Utente fino a quando i restanti documenti da caricare non presentano anomalie, solo in questo stato il PdV può essere formato dando luogo al Rapporto di versamento. In questo modo non è necessario alcun Rapporto di rifiuto o comunicazione di anomalie in quanto queste sono interattive con l'operato dell'Utente. In ogni caso i log relativi ai documenti di pacchetti rifiutati vengono registrati all'interno dei report descritti nel paragrafo 9.1.4 (monitoraggio dei PdV).

Le anomalie che determinano il rifiuto parziale o totale di documenti sono le stesse dei controls elencati nel paragrafo 7.2.

Torna al sommario

7.5 Preparazione e gestione del pacchetti di archiviazione

Una volta che i pacchetti di versamento sono stati formati, SdCM con una scadenza definita nelle regole di conservazione della configurazione Cliente inizia la fase di creazione dei PdA. Le modalità di aggregazione dei vari PdV disponibili per ogni produttore avviene con le regole di conservazione definite per quel produttore e quella classe o registro documentale. Una volta creati i PdA e firmati dal RdSC i documenti nel sistema SdCM passano dallo stato "Pronto" allo stato "Archiviato", per terminare il processo il PdA dovrà essere

trasferito sui supporti di conservazione, cosa che gli conferirà lo stato di "Conservato". Il pacchetto di archiviazione (PDA), prodotto al termine del processo di conservazione, è composto da un insieme di file e directory, gli elementi che lo compongono sono i seguenti:

- ***Pacchetto.xml.p7m***: indice del pacchetto di archiviazione firmato in modalità CAdES e marcato;
- ***docs***: directory contenente tutti i documenti facenti parte del PDA
- ***viewer.jar***: applicazione java che consente la verifica della firma apposta sull'IPdA e la visualizzazione del PDA stesso. L'applicazione (fuigua 1) consente di visualizzare i documenti contenuti nel PDA con i relativi metadati e consente di fare ricerche interne al PDA;
- ***certs***: directory contenente i certificati necessari per la verifica della firma apposta sull'indice del pacchetto di archiviazione;
- ***autorun.inf***: file contenente le istruzioni per avviare automaticamente l'applicazione viewer.jar.

tutti gli elementi appena descritti vengono inseriti in un unico file .ISO che costituisce il pacchetto di archiviazione.
Il formato .ISO fa si che il PDA possa comodamente essere masterizzato su DVD.

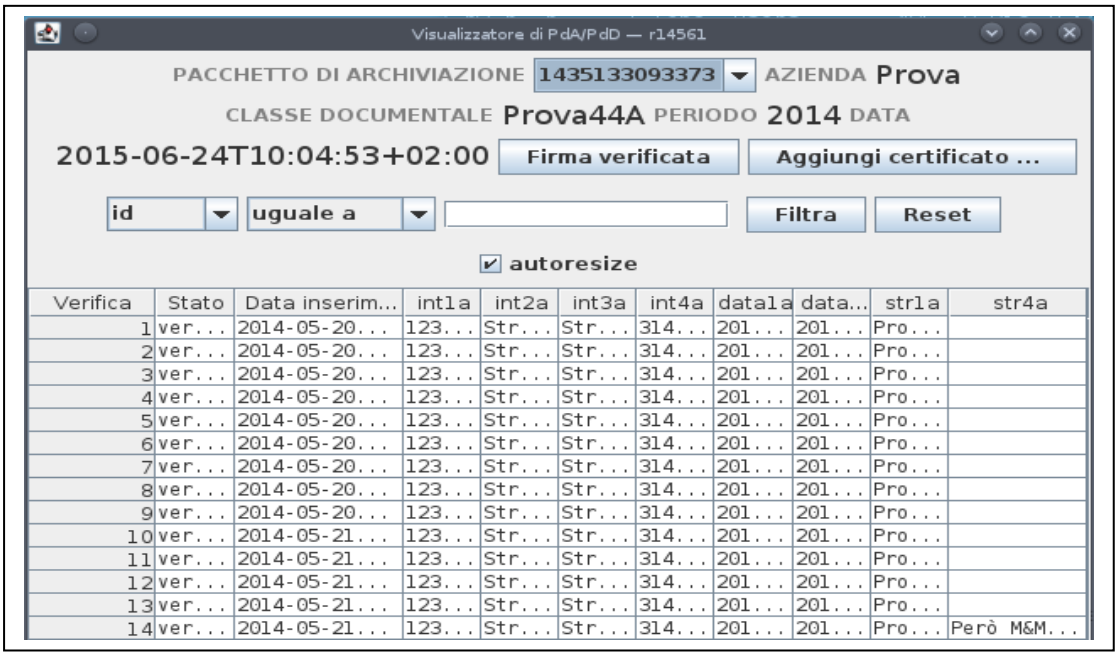

Figura 3: Visualizzatore di PDA
(maschera di visualizzazione del viewer che mostra i documenti contenuti nel Pacchetto di Archiviazione, attraverso questo Viewer è possibile, oltre a verificare le firme anche ricercare singoli documenti appartenenti al PdA e visualizzarli unitamente ai metdadati.)

Anche per la creazione dei PdA il SdCM crea e conserva i log relativi alla loro formazione. Una volta creati e per caratteristica del SdCM i PdA non possono essere in alcun modo manipolati o cancellati, gli accessi alle aree di conservazione sono sotto monitoraggio dei sistemi di log degli accessi.

La leggibilità e integrità dei PdA è verificata automaticamente dal SdCM secondo le tempistiche definite dalle regole di conservazione e monitorata come descritto nel paragrafo 9.1.5 e 9.1.6.

Torna al sommario

7.5.1 Invio dei PdA al repository di Conservazione

Il SdCM risiede su server virtuali Memar ma è fisicamente residente in due Data Center esterni.

In questi Data Center sono ospitati i due storage di conservazione che sono fra loro backuppati e sincronizzati.

La garanzia di conservazione a norma è assicurata dalle SLA e dalle certificazioni del Data Center esterno.

Il trasferimento dei PdA negli storage di Conservazione cambia lo stato dei documenti da "Archiviato" a "Conservato"

Torna al sommario

7.5.2 La gestione dei PdA

La gestione dei PdA fondamentalmente consiste nei seguenti controlli:

a) Quadratura fra PdV e PdA

b) Quadratura fra documenti allo stato "Pronto" con documenti allo stato "Archiviato"

c) Quadratura fra documenti allo stato "Archiviato" con documenti allo stato "Conservato"

d) Controlli di struttura dei PdA

Le modalità di monitoraggio e controllo sono descritte nel paragrafo 9.1.

I report di quadratura possono essere anche lanciati manualmente in qualsiasi momento.

Per quanto riguarda invece i controlli sulla struttura e integrità dei PdA si rimanda al paragrafo 9.1.

Torna al sommario

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

Il sistema di conservazione deve permettere ai soggetti autorizzati l'accesso diretto, anche da remoto, ai documenti informatici conservati.
Per esibizione si intende dunque l'operazione che consente a tali soggetti la visualizzazione di uno o più documenti conservati e la loro esportazione dal sistema di conservazione attraverso la produzione di un pacchetto di distribuzione selettiva.
Queste operazione sono tutte effettuate in modo interattivo attraverso una interfaccia dedicata del SdCM.

La creazione di un PdD è un processo automatico realizzato attraverso una interfaccia dedicata ad uso dell'utente autorizzato, tuttavia questo processo viene monitorato nel seguente modo:

- Ogni volta che viene richiesto un PdD dal Produttore la richiesta viene segnalata al RdSC
- Il RdSC controlla che il processo di richiesta sia stato correttamente svolto e che il PdD sia stato effettivamente scaricato (download) dal richiedente.
- In caso di richiesta che non ha prodotto il PdD il RdSC contatta il cliente per completare l'operazione.
- In caso sia stato prodotto un PdD ma non sia seguito il downolad dello stesso il RdSC contatta il cliente per capire se c'è stato un malfunzionamento (e a questo seguiranno azioni correttive) oppure se semplicemente c'è un rimando.

- Il controllo del RdSC intercetta anche la presenza di usi scorretti del sistema di richiesta.
- Tutte le comunicazioni fra Cliente e RdSC vengono firmate e conservate dallo stesso nel diario della Conservazione.
- Gli utenti del Produttore abilitati alle richieste di PdD sono descritti nel Questionario di Attivazione e configurati con idonee ID e Password che ne definiscono le permission sul SdCM.

I PdD possono in via eccezionale essere consegnati su supporto fisico, come ad esempio nel caso di cessazione del servizio o in caso di volumi importanti. In questo caso il supporto fisico, generalmente un Hard Disk esterno USB, viene consegnato con vettore nazionale al destinatario, nessuna indicazione è presente sul pacchetto che possa identificarne il contenuto. Lo stesso contenuto è protetto da un sistema di crittografia le cui chiavi di decrittografia vengono comunicate in modo riservato al destinatario.

In caso di richiesta di invio e-mail di un PdD si utilizza esclusivamente il sistema di posta certificata PEC.

Il pacchetto di distribuzione (PdD), prodotto al termine del processo di esibizione, è un file in formato ZIP che comprende i seguenti elementi:

- L'insieme dei documenti ricercati attraverso l'interfaccia di esibizione suddivisi per Azienda, classe documentale e per PDA di appartenenza;
- L'insieme degli IPdA di appartenenza dei documenti ricercati
- viewer.jar: applicazione java che consente la visualizzazione di tutti i documenti contenuti nel pacchetto di distribuzione e dei relativi metadati.

L'applicazione consente anche di verificare le firme apposte sugli IPdA contenuti nel pacchetto e di fare ricerche interne al PDD;

- certs: directory contenente i certificati necessari per la verifica delle firme apposte sugli indici del pacchetto di archiviazione;
- schemas: directory contenente gli schemi XSD che descrivono la struttura degli indici dei pacchetti di archiviazione.
- autorun.inf: file contenente le istruzioni per avviare automaticamente l'applicazione viewer.jar.
- index.txt.p7m: file indice del PDD firmato dal responsabile del servizio di conservazione secondo il formato CAdES.

Il file contiene l'elenco degli IPdA contenuti nel PDD e dei relativi hash.
Questo fa si che il file indice fornisca garanzie di autenticità e di integrità circa gli IPdA contenuti nel pacchetto. A loro volta gli IPdA contengono l'elenco dei documenti e dei relativi hash e, essendo firmati, garantiscono l'autenticità e l'integrità di tutti i documenti contenuti nel PDD.

Torna al sommario

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

Il SdCM prevede la possibilità di creare duplicati e/o copie informatiche dei documenti conservati. La richiesta fatta dal Produttore viene presa in carico direttamente dal RdSC che procede alla creazione delle copie e/o duplicati che erediteranno i metadati originali. Il RdSC rilascerà congiuntamente una attestazione di conformità all'originale, firmata elettronicamente.

Qualora richiesto dalla natura del documento l'attestazione di conformità potrà essere rilasciata e firmata con firma elettronica qualificata da un pubblico ufficiale.

Il RpSM valuterà caso per caso la necessità di adeguare le copie o i PdA a nuovi sistemi di leggibilità e ne comunicherà eventualmente la necessità al Produttore e al RdSC. L'adeguamento ai nuovi formati verrà in caso sia necessario espletato dal RdSC.

Nel caso generale in cui sia necessario l'intervento di un Pubblico Ufficiale il SdCM ne assicura la presenza e ne fornisce assistenza e supporto per l'espletamento delle sue attività.

Torna al sommario

7.8 Scarto dei pacchetti di archiviazione

Per ogni classe documentale o registro SdCM contiene all'interno delle configurazioni la durata della tenuta in conservazione del PdA.

Il RdSC ha a sua disposizione una interfaccia che gli permette di selezionare tutti i PdA il cui tempo di conservazione è espirato. Una volta selezionati i pacchetti il RdSC controlla l'effettiva scadenza in base alle classi documentali ed una volta validata la scadenza segnala al Produttore la presenza di PdA da poter scartare.

Se il Produttore è una azienda privata l'operazione di scarto consiste in:

- Emissione di un documento di autorizzazione allo scarto firmata digitalmente dal RdSC e che deve essere controfirmata per accettazione dal Produttore. Questo documento di dichiarazione firmato da entrambe le parti viene conservato in una apposita sezione dei Diari di Conservazione del RdSC.
- Una volta autorizzato viene creato un PdD che viene consegnato al Produttore.
- Una volta verificato il download da parte del Produttore del PdD, si invia al Produttore una dichiarazione di ricevimento che viene firmata dallo stesso.
- Una volta prodotta la ricevuta si procede alla eliminazione fisica dei PdA dal Repository di Conservazione attraverso la procedura o interfaccia di svecchiamento. Tale procedura è accessibile solo al RdSC ed è protetta dall'uso del suo certificato di firma.

Nel caso di archivi pubblici o privati di particolare interesse culturale la procedura è la seguente:

- Emissione di un documento di autorizzazione allo scarto firmata digitalmente dal RdFA. Questo documento di dichiarazione deve tornare firmato dal Produttore con allegata l'autorizzazione allo scarto da parte del Ministero dei Beni e delle Attività Culturali e del Turismo.

- Una volta autorizzato viene creato un PdD che viene consegnato al Produttore.
- Una volta verificato il download da parte del Produttore del PdD si invia al Produttore una dichiarazione di ricevimento che viene firmata dallo stesso.
- Una volta prodotta la ricevuta si procede alla eliminazione fisica dei PdA dal Repository di Conservazione attraverso la procedura o interfaccia di svecchiamento. Tale procedura è accessibile solo al RdSC ed è protetta dall'uso del suo certificato di firma.

Torna al sommario

7.8.1 La gestione di fine rapporto

E' diversa dalla procedura di scarto in quanto in realtà non si vanno a cancellare i pacchetti di archiviazione bensì a restituire i pacchetti di conservazione al Produttore o al nuovo Conservatore da lui indicato. Il fine rapporto prevede le seguenti attività:

- Comunicazione da parte dell'Area Commerciale della fine rapporto contrattuale con un Produttore, parziale (ovvero solo per alcune classi) o totale, la comunicazione è fatta con un documento informatico
- Nulla osta da parte dell'Amministrazione sull'attivazione della fine rapporto e restituzione della documentazione attraverso documento informatico.
- Produzione di PdD omogenei per classi documentali
- Produzione di una ricevuta di essere in possesso di tutta la documentazione e liberatoria da parte del Produttore per la cancellazione dei PdA di quel Produttore, questa ricevuta deve essere un documento informatico prodotto e sottoscritto dal Produttore.
- Tutte le dichiarazioni e ricevute vengono conservate nel Diario del Conservatore.

Tutti gli anni il RdSC produce un documento verso l'Amministratore Delegato contenente l'elenco di tutti i nuovi clienti pervenuti durante l'anno ed il numero di clienti cessati. Un aumento dell'indice dei clienti cessati sulla totalità dei clienti viene considerato una Non Conformità di Processo, seguiranno quindi analisi delle cause ed azioni correttive.

Torna al sommario

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

Ai fini di garantire l'interoperabilità e trasferibilità da e verso altri conservatori, il SdCM è predisposto per l'accettazione di PdD provenienti da altri sistemi di conservazione purchè siano compliant con lo standard UNI SinCRO.

Un apposito uploader verifica la compatibilità dello standard del PdD ricevuto e lo converte in un pacchetto di versamento che viene poi preso in carico dal SdCM. In questo modo i pacchetti di archiviazione vengono trasferiti da un sistema all'altro.

Allo stesso modo il SdCM produce PdD con standard UNI SinCRO che, grazie alla identicità dei PdA con il PdD ne garantisce l'interoperabilità e la normale presa in carico da parte di un altro Sistema di conservazione.

Torna al sommario

8. IL SISTEMA DI CONSERVAZIONE

In questo paragrafo viene descritto il sistema di Conservazione denominato SdCM (Sistema di Conservazione MEMAR) nelle sue componenti logiche, tecnologiche e fisiche. Tutti gli aspetti riguardanti la sicurezza, le procedure di Backup & Disaster Recovery e la Business Continuity sono invece demandati al documento Piano della Sicurezza.

8.1 Componenti logiche

Le tre componenti logiche principali del SdCM sono:

- Componente Applicativa (la struttura software denominata EFATTURA)
- Componente fisica (server, storage)
- Il dispositivo o server di firma remota HSM (denominato kryptoEvolution, devoluto all'apposizione delle firme elettroniche)

L'applicativo di SdCM gestisce le interazioni con:

- Il sistema di firma remoto HSM per la firma dei documenti
- Il repository di conservazione per la memorizzazione dei documenti da conservare
- Con sistemi di alimentazione esterni (SAPtoCOS) ed interni (MemarToCOS), oltre che con servizi dedicati alla stampa o agli invii mail (MDS)
- Con la gestione, amministrazione i monitoraggi del RdSC
- Con i Titolari per ricerche e download
- Con i sistemi delle CA per la verifica dei certificati di firma
- Con la Time Stamping Authority certificata per l'apposizione di marche temporali

L'applicativo viene erogato dalle componenti tecnologiche del SdCM in logica SaaS (Software as a Service). Opportuni ambienti di sviluppo e di test sono fisicamente separati dal SdCM.

Torna al sommario

8.2 Componenti tecnologiche

La struttura tecnologica si avvale di sistemi virtualizzati che ospitano sistemi operativi Linux e Microsoft adeguati a supportare il modello applicativo prescelto.

Gli apparati hardware sono costituiti da apparecchiature rack mountable corrispondenti al carico di lavoro richiesto per lo svolgimento del servizio di Conservazione di esclusiva proprietà e sotto il totale controllo informatico di Memar.

Gli apparati coinvolti nel servizio sono i seguenti:

Componente	Quantità	Descrizione
PRIMERGY RX2520	2	Cabinet Rack Mountable 19" (2U), chipset Intel C600, 2 processori Intel Xeon, 24 slots per RAM [DDR3 RAM ECC a 1333 o 1600 o 1866 MHz (fino a 1536 GB (con memorie registered), 6 alloggiamenti da 3.5 Hot Plug ready o 8/12/16 alloggiamenti da 2.5" Hot Plug ready, 1 alloggiamento da 5.25" esterno, 2 schede di rete 10/100/1000 integrate su motherboard, Remote Management Controller integrato, 2 slots PCI Express x16 Low Profile (3.0) - 5 slots PCI Express x8 (3.0) [con un processore si gestiscono fino a 5 slots], 1 seriale, 8 USB (2 USB addizionali interni), ServerView Suite, Alimentatore Hot Plug ventole Hot Plug e ridondanti. Dimensioni (H x W x D): 87 x 483 x 770 mm. Peso: circa 25 Kg
ETERNUS DX100 S3	2	Dual Ctrl con 2 moduli con 2 porte FC da 8 Gb/s ciascuno (8192 MB cache protetta), 22 x 600 GB Serial Attached SCSI (SAS) Hot Swap 6Gb/s 10k, licenza software per Snapshot Basic, 2 alimentatori Hot Plug.
WS-C3850-48T-L	2	Cisco Catalyst 3850 48 Port Data LAN Base
ISR4331-SEC/K9	2	Cisco ISR 4331 Sec bundle w/SEC license U.S. Export Restriction Compliance license for 4330 series Performance on Demand License for 4330 Series

La manutenzione degli stessi è assicurata come da tabella che segue:

Componente	Quantità	Piano di manutenzione assegnato
PRIMERGY RX2520	2	TP 5 year OS Svc,NBD, ON-SITE, lun-ven 9.00-18.00
ETERNUS DX100 S3	2	TP 5 year OS Svc,NBD, ON-SITE, lun-ven 9.00-18.00, intervento entro 4 ore
WS-C3850-48T-L	2	3 year,NBD, ON-SITE, lun-ven 9.00-18.00
ISR4331-SEC/K9	2	3 year,NBD, ON-SITE, lun-ven 9.00-18.00

Torna al sommario

8.3 Componenti fisiche

Il sito primario di conservazione è ubicato presso il Data Center Memar 01 posto nel data center Retelit di Bologna (DCM01 Retelit Bologna) sito in Castenaso (BO). Il sito secondario di conservazione è ubicato presso il Data Center Memar 02 posto nel data center Retelit di Roma (DCM02 Retelit Roma) sito in Roma (RM).

Le componenti applicative sono eseguite su server virtuali in ambiente VMWare posti in configurazione attiva-attiva. Tutti gli oggetti di conservazione sono custoditi in apparati storage dedicati e fisicamente distinti. L'apposizione di firme digitali è effettuata per mezzo di dispositivo HSM di firma remota integrato denominato kryptoEvolution, interfacciabile con i più significati Certificatori Accreditati di firma digitale.

Applicazioni e dati sono replicati tra le infrastrutture attraverso una connessione permanente E-Link da 200 Mbps. Le procedure di replica sono basate su RSYNC ed impiegano un tunnel crittografico VPN IPSEC.

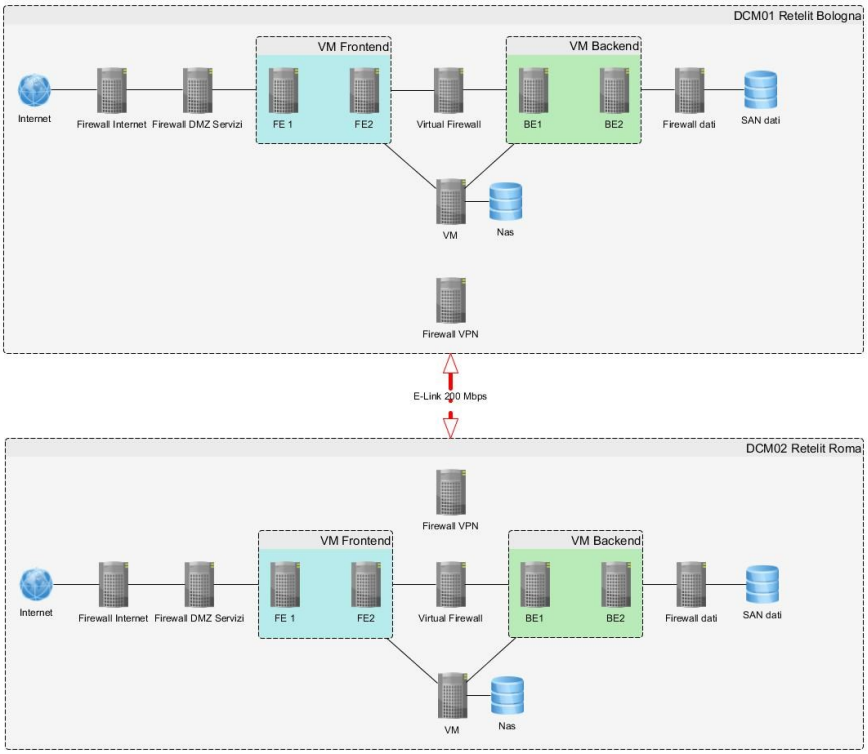

Figura 4: (schema del sistema di replica): mostra come la struttura di macchine virutali, repository SAN e sistemi di sicurezza vengono ridondati fra i due centri geograficamente distinti del Data Center di Bologna e Roma.

Torna al sommario

8.4 Procedure di gestione ed evoluzione

Per la gestione del servizio e dei cambiamenti che possono rendersi necessari o in seguito ad incidenti o a specifiche richieste dei clienti viene utilizzata la procedura di Change Management.

Obiettivo del Change Management è assicurare che metodi e procedure standard vengano utilizzati per una efficiente e pronta gestione di tutti i cambiamenti applicativi e di infrastruttura IT, al fine di minimizzare l'impatto e gli incidenti in capo ai servizi erogati.

Il Change Management è responsabile della gestione del cambiamento che coinvolge tutto il SdCM, come ad esempio:

- Strutture logiche
- Strutture tecnologiche
- Strutture fisiche
- Tutta la documentazione e le procedure legate alla gestione, supporto e manutenzione dell'ambiente.

E' quindi il processo di change management che dovrà fornisce l'approvazione ad ogni richiesta di cambiamento. L'organo che ha l'autorità per prendere la decisione è il Change Advisory Board (CAB), il quale è principalmente costituito dal Team del SdCM.

Per una visione complessiva delle attività del processo di Change Management si espongono di seguito gli elementi chiave e gli attori coinvolti nel processo.

Richiesta di cambiamento (RFC)

La RFC è l'unico meccanismo previsto per richiedere un cambiamento all'infrastruttura. La RFC deve contenere tutte le informazioni necessarie affinché un cambiamento possa essere valutato, approvato e implementato. Tra i motivi per i quali può essere richiesta una RFC, si trovano:

- Risoluzione di un Incidente o di un Problema;
- Insoddisfazione di un cliente su un servizio (attraverso il SLM);
- Introduzione, upgrade o rimozione di un CI (Configuration Item);
- Cambiamenti in seguito a richieste del business;
- Spostamenti di sede;
- Cambiamenti legislativi;
- Cambiamenti di prodotti o servizi da parte di fornitori.

Change Manager

I compiti principali del change manager, alcuni dei quali possono essere delegati, sono i seguenti:

- Ricevere, tracciare e assegnare la priorità a tutte le RFC. Rigettare subito le richieste impraticabili;
- Predisporre tutte le RFC da presentare al CAB, definirne l'agenda e fornire anticipatamente a tutti i membri la lista di RFC in modo che possano effettuare delle valutazioni preliminari.
- Decidere quali sono le persone che è opportuno invitare al meeting
- Convocare in caso di urgenza un Emergency CAB
- Presiedere a tutti i CAB meeting
- Cooperare con tutte le strutture coinvolte per coordinarne l'implementazione e i test secondo la pianificazione definita
- Verificare tutti i change eseguiti per assicurarsi che si sono raggiunti gli obiettivi prefissati
- Analizzare tutti i change per individuare eventuali trend in atto o problemi emergenti
- Chiudere le RFC
- Produrre dei report regolari e accurati da presentare al management

Change Advisory Board (CAB)

I compiti principali dei membri del CAB sono elencati di seguito:

- Analizzare tutte le RFC che vengono proposte in sede di CAB, determinandone gli impatti e le risorse necessarie per l'implementazione.
- Partecipare a tutti i meeting del CAB, esprimendo il proprio parere sui change in agenda al fine di autorizzarne l'esecuzione.
- Nel caso di CAB convocati per EC (Emergency Change) essere disponibili per una consultazione.

Schedulazione del cambiamento (SDC)

Il SDC o calendario dei cambiamenti è un output del processo, contiene i dettagli e la pianificazione di tutti i Change approvati. E' utilizzato per consentire a tutti i gruppi coinvolti di pianificare i propri rilasci. Il SDC ha una schedulazione dettagliata per il breve periodo, e una pianificazione di massima per il lungo periodo. Contiene inoltre, quando previsti, i periodi di downtime da comunicare agli utilizzatori.

Projected Service Availability (PSA)

Il PSA è un documento utilizzato dal Change Management per delineare gli effetti del cambiamento sui livelli di disponibilità definiti nei Service Level Agreement (SLA). Questo documento è collegato al RFC. Entrambi questi documenti vengono concordati con cliente.

Il Processo

Ogni membro dell'organizzazione è autorizzato a richiedere un cambiamento, questo consente di incoraggiare l'innovazione e di far emergere potenziali problemi. Primo compito del Change Manager, come già illustrato, è quello di filtrare tutte le RFC rigettando quelle inapplicabili, dopodiché verificare se sono presenti Emergency Change a cui dare priorità.

Scopo della fase di "Approvazione" è la discussione e valutazione di tutte le proposte di cambiamento proposte dai centri di competenza, al fine di evitare il verificarsi di effetti indesiderati nell'ambiente di produzione. Il livello di approvazione del cambiamento è legato al livello di rischio del change. Per garantire la valutazione di impatto, costi, benefici e rischi ci sono tre processi di approvazione:

- Tecnico
- Finanziario
- Business, che consiste nello sviluppo di giustificazioni di business al cambiamento.

Concluso il processo di approvazione è possibile passare all'esecuzione del Change.

Scopo della fase di "Esecuzione" e quello di gestire e coordinare le implementazioni richieste dalla RFC, al fine di rilasciarle nell'ambiente di produzione. Molta attenzione si pone, quando si implementa il Change, per

evitare impatti indesiderati sui servizi erogati, a questo scopo vengono implementati sia la fase di test che il back-out, ovvero la procedura da seguire per annullare il change e ritornare alla configurazione iniziale.

La fase di "Chiusura " è quella che conferma il buon esito dell'implementazione della RFC. Tutte le RFC vengono verificate dopo un periodo predefinito per assicurarsi che siano stati raggiunti gli effetti desiderati e che le risorse utilizzate siano state stimate accuratamente. In fine il Change Manager si assicura che tutta la documentazione sia stata aggiornata.

I benefici specifici derivanti da un efficace implementazione del processo di Change Management sono:

- miglior allineamento tra i servizi IT e le esigenze di business
- maggior visibilità e comunicazione dei cambiamenti sia da parte del business che da parte del service support
- miglior valutazione del rischio
- minor impatto negativo dei cambiamenti sulla qualità dei servizi e sugli SLA (livelli di servizio)
- miglior valutazione dei costi del cambiamento prima che vengano effettuati
- minor numero di cambiamenti per cui sarà necessario il back-out
- maggior produttività degli utenti, grazie ad una diminuzione dei disservizi e ad una maggiore qualità dei servizi erogati
- maggior capacità di gestire ampi volumi di change
- miglior percezione dell'IT da parte del business grazie ad una maggiore qualità dei servizi e ad un approccio professionale

Torna al sommario

9. MONITORAGGIO E CONTROLLI

Molti dei processi descritti sono regolamentati da procedure del Sistema Qualità, nello specifico:

- **Gestione degli incidenti e reclami**: PSQ 802 - Gestione delle Non Conformità, Incidenti e Azioni correttive, preventive e di miglioramento; MQ - Manuale della qualità e della sicurezza delle informazioni
- **Trattamento delle Non Conformità e delle azioni correttive**: PSQ 802 - Gestione delle Non Conformità, Incidenti e Azioni correttive, preventive e di miglioramento; MQ - Manuale della qualità e della sicurezza delle informazioni
- **Assistenza Clienti:** MQ - Manuale della qualità e della sicurezza delle informazioni; PSQ 701 - Gestione del processo di marketing e commercializzazione dei servizi
- **Controllo dei processi**: PSO901 - Servizio DataManagement; PSO903 - Servizio GED; PSO 912 - Organizzazione della filiale operativa; PSO 915 - Servizio di Back e Middle Office; Elenco delle IL
- **Erogazione dei servizi**: PSO 919 - Coordinamento produzione; PSO901 - Servizio DataManagement; PSO903 - Servizio GED; PSO 912 - Organizzazione della filiale operativa; PSO 915 - Servizio di Back e Middle Office; Elenco delle IL
- **Gestione del rischio**: PSQ 501 - Gestione della qualità e sicurezza delle informazioni; PSQ 803 - Gestione della sicurezza dei dati e delle informazioni; PSQ 804 - Risk Assessment report; PSQ 806 - Ambito;

Torna al sommario

9.1 Procedure di monitoraggio

A seguire l'elenco completo dei monitoraggi.

9.1.1 Rilevamento della tempistica di attivazione

Il rilevamento della tempistica di attivazione viene effettuato attraverso la comparazione delle date di: firma contratto, comunicazione dell'amministrazione della attivazione al RdSC, questionario di attivazione, rilascio dei certificati di firma, caricamento del primo PdV. Dalla data di firma del contratto le successive devono seguire rispettivamente i seguenti intervalli in giorni lavorativi: 5 per la comunicazione dell'amministrazione, 10 dalla precedente per il questionario di attivazione, 5 dalla precedente per il rilascio e consegna dei certificati, 10 per la chiusura di test e collaudi. Tutta la startup prevede quindi un tempo massimo di 25 giorni lavorativi dalla comunicazione di apertura del servizio da parte della amministrazione. Tempi più lunghi del previsto vengono valutati dal RdSC in base alla complessità del servizio e possono dare luogo a Non Conformità ed azioni correttive.

9.1.2 Coerenza del contratto di servizio

La coerenza del contratto di servizio con il manuale della conservazione o con le indicazioni date in fase di pre-sale viene verificata dal RdSC. Discordanze bloccanti danno luogo a Nota di Non Conformità ed azioni correttive che vengono firmate e conservate dal RdSC nel Diario della Conservazione.

9.1.3 Positività dei test e collaudi di attivazione

La positività dei test ed i collaudi di attivazione sono controfirmati digitalmente anche dal Produttore, il documento entra a far parte integrante al contratto di servizio. Il non superamento dei test richiede nuovo test e collaudo.

9.1.4 Monitoraggio dei PdV

Per gestire correttamente il Processo SdCM effettua una serie di controlli:

- Numero di pacchetti caricati sul FTP dai vari produttori
- Per ogni pacchetto caricato su FTP:
- Quantità di documenti presenti
- Quantità di documenti validati
- Quantità di documenti rifiutati
- Validità dei formati
- Date di espirazione dei singoli pacchetti per il periodo di latenza fra caricamento e convalida del versamento
- Pacchetti convalidati in PdV

Inoltre per ogni PdV convalidato vengono rilevati:

- Data della convalida
- Presenza della firma digitale del Produttore
- Validità del certificato di firma del Produttore
- Data massima per la conservazione
- Presenza delle firme del RdC del Produttore e del RdSC
- Valutazione della struttura del PdV

Tutti questi dati possono dar luogo o ad un esito di “normalità” che è un semplice avviso fatto per e-mail al RdSC che la situazione è normale, oppure genera un Report di anomalia per squadratura dei dati e quindi una segnalazione di allarme che viene inviata tramite mail al RdSC, al Responsabile della Funzione Archivistica (RdFA) ed all’Amministratore Delegato. Il report sulla situazione dei PdV viene prodotto in automatico dal SdCM settimanalmente ma può essere richiesto manualmente dal RdSC o dal RdFA in qualsiasi momento.

A seguito di un Report squadrato di anomalia viene aperto un ticket di assistenza al Reparto IT al quale fa seguito una giustificazione dell’accaduto.

La giustificazione viene valutata dal RdSC che pondera se aprire una Nota di Non Conformità sul processo a cui seguiranno le implementazioni delle azioni correttive.

Può accadere che nei documenti conservati in serie vi siano salti di numerazione, pur essendo comunque una responsabilità del produttore, SdCM avverte in automatico con una mail di servizio settimanale un alert che avvisa il produttore dell'eventuale salto di numerazione in un registro.

Tutte le comunicazioni inviate ai produttori riguardanti il servizio vengono anche inviate per conoscenza ad una casella interna Memar, questo ai fini di poter immediatamente intercettare cambiamenti negli indirizzi e-mail non comunicati dal cliente.

Tutti i Rapporti di Versamento e gli stessi pacchetti PDA vengono conservati all'interno del sdCM.

9.1.5 Monitoraggio della creazione dei PdA

La gestione dei PdA fondamentalmente consiste nei seguenti controlli:

a) Quadratura fra PdV e PdA

b) Quadratura fra documenti allo stato "Pronto" con documenti allo stato "Archiviato"

c) Quadratura fra documenti allo stato "Archiviato" con documenti allo stato "Conservato"

d) Controlli di struttura dei PdA

Le azioni a,b,c vengono calcolate in automatico settimanalmente da SdCM ed i risultati possono essere di 2 tipi:

- Risultato positivo: viene prodotta una mail verso il RdSC che SdCM non ha nulla da segnalare
- Risultato negativo: viene prodotta una mail di alert automatica verso il RdSC, il RdFA e l'Amministratore Delegato con allegato il report sulla situazione dei PdA. Viene prodotto in automatico dal SdCM settimanalmente ma può essere richiesto manualmente dal RdSC o dal RdFA in qualsiasi momento.

A seguito di un Report squadrato di anomalia viene aperto un ticket di assistenza al Reparto IT al quale fa seguito una giustificazione dell'accaduto.

La giustificazione viene valutata dal RdSC che pondera se aprire una Nota di Non Conformità sul processo a cui seguiranno le implementazioni delle azioni correttive.

I report di quadratura possono essere anche lanciati a mano in qualsiasi momento.

9.1.6 Monitoraggio dei PdA espirati

Monitoraggio dei PdA espirati: attraverso un report vengono valutate le date scadenza conservazione con la data di scarto o la mancata data di scarto, essendo il tempo di controllo mensile il tempo massimo di tolleranza fra data espirazione e data scarto è di due mesi. Eccezioni al tempo massimo danno luogo a Nota di Non Conformità nei confronti del RdFA.

9.1.7 Ritardi e incompletezze

Tutti i ritardi nella conferma dei PdV o nel loro caricamento o nella eliminazione di buchi di numerazione non vengono sottoposti a monitoraggio in quanti sono gestiti direttamente da SdCM con comunicazioni automatiche al Produttore e regolamentati dal contratto di servizio.

9.1.8 Log

Tutti i log di accesso ai server del SdCM vengono registrati ed inviati in real time al sistema di conservazione esterno a Memar dove vengono firmati e conservati.

9.1.9 Presidio

Mensilmente il team del SdCM si riunisce per l'analisi di non conformità, la segnalazione di disservizi, la valutazione di buon funzionamento del SdCM la valutazione di proposte migliorative. La riunione produce un verbale di riunione che viene firmato e conservato dal RdSC ed inviato all'Amministratore Delegato.

9.1.10 Monitoraggio Infrastruttura del SdCM

La componente hardware e software è controllata attraverso l'uso del tool Nagios, un software open source per il monitoraggio di server e servizi di rete. Esso opera in ambiente Linux/Unix e gestisce sistemi di notificazione basati su email, messaggistica, SMS.

Lo strumento dispone di un'interfaccia web visualizzabile con un comune browser e nella quale sono gestite specifiche autorizzazioni di accesso.

Grazie alla sua applicazione vengono effettuati il monitoraggio e la gestione ad esempio:

- di servizi di rete (SMTP, POP3, HTTP, ecc)
- di processi e applicazioni in ambiente Linux/Unix/Microsoft
- di risorse di storage
- delle risorse hardware dei server (carico del processore, utilizzo dei dischi e della memoria)
- di situazioni ambientali (temperatura)
- di notifiche e allarmi differenziati per gruppi e utenti
- di log dettagliati sulle attività svolte.

Torna al sommario

9.2 Verifica dell'integrità degli archivi

La verifica si basa sul controllo di struttura di leggibilità e integrità dei PdA e viene effettuato automaticamente dal SdCM che mensilmente invia un report di positività o anomalia al RdSC, al RdFA e alla DIREZIONE AZIENDALE. La presenza di PdA corrotti all'interno del sistema avvia le seguenti azioni correttive:

- Individuazione delle cause
- Recupero delle copie di backup
- Disaster recovery
- Se il disaster recovery ha esito positivo: ripristino del PdA, dichiarazione firmata dal RdSC sulla sostituzione effettuata, che verrà conservata nel diario della conservazione.

Se il disaster recovery ha esito negativo per la presenza di copie anch'esse corrotte la procedura prevede:

- l'apertura di incidente con emissione delle note di non conformità e conseguenti azioni correttive;
- comunicazione del RdSC al Produttore con valutazione di possibilità di recupero di una copia del documento;
- assunzione di responsabilità da parte del RdSC;
- annotazione e conservazione della documentazione nel Diario della Conservazione;
- nel caso di PA coinvolgimento nelle comunicazioni alla Soprintendenza dei Beni Culturali

Torna al sommario

9.3 Soluzioni adottate in caso di anomalie

Tutte le anomalie riscontrate dai monitoraggi, gli incidenti, le Non Conformità vengono prese in considerazione in prima istanza dal RdSC che ne valuta i tempi di risoluzione e, in caso di urgenza, convoca una riunione straordinaria del Team della Conservazione, oppure, in caso di non urgenza rilascia il trattamento dell'anomalia alla riunione mensile normalmente pianificata del Team della Conservazione.

Sarà poi il team a stabilire le azioni correttive e verificarne la attuazione ed efficacia.

Torna al sommario