Manuale di Conservazione DigiBox
di Engineering Ingegneria Informatica

EMISSIONE DEL DOCUMENTO

Azione	Data	Nominativo	Funzione
Redazione	01/08/2018	Stefano Mannori	Responsabile dello sviluppo e della manutenzione del sistema di conservazione
	01/08/2018	Francesca Pranzo Zaccaria	Responsabile funzione archivistica di conservazione
Verifica	05/07/2018	Andrea Pugi	Responsabile servizio di conservazione
	05/07/2018	Stefano Ciuffi	Responsabile Sicurezza dei sistemi per la conservazione
Approvazione	05/07/2018	Pizzonia Mario Carmelo	Responsabile ECM Competence Center

REGISTRO DELLE VERSIONI

N°Ver/ Rev/	Data emissione	Modifiche apportate	Osservazioni
beta	30/07/2014	Stesura iniziale	Distribuzione interna
v-1	25/09/2014	Seconda Stesura	Distribuzione interna
v-1	5/12/2014	Rilascio documento	Distribuzione interna
v1.1	27/1/2015	Modifiche per integrazione informazioni sicurezza e monitoraggio (manuale AgID ver.2)	
V2	4/3/2015	Integrazione con descrizione struttura PDD nel cap.4	
V4	15/1/2016	Redazione aderente allo schema v.2 pubblicato da AgID	
V5	10/2/2016	Correzioni a seguito di richiesta “accessibilità”	
V6	10/4/2017	Integrazioni per evolutive funzionali rilevanti nel processo di conservazione; aggiornamento contratto Resp. Tratt. Dati personali	
V8	20/6/2017	Versione interna workingprogress per aggiornamento al nuovo SW	Distribuzione interna
V9	2/8/2017	Integrazioni con nuove funzionalità per evoluzione prodotto sw di Conservazione	

V10	15/1/2018	Modifiche per cambio Proprietà Azienda (cambio logo)	
v11	15/5/2018	Modifiche per cambio societario: recepita l'incorporazione di Infogroup in Engineering; modificata organizzazione ed altri dettagli legati alla denominazione Aziendale	Cambio nome del documento
V12	05/07/2019	Modifiche per accogliere i suggerimenti evidenziati durante l'audit RINA di novembre 2018. Cap. 1 Condivisione con il cliente delle specificità contrattuali Cap. 4.8 Evidenziata la relazione tra il responsabile trattamento dati (AgID) e il Privacy Manager Engineering. Cap. 5.1 Aggiornati gli schemi organizzativi di Engineering e del Servizio Cap. 6.1 inserita verifica obsolescenza formati Cap. 7.2 Attivazione e cessazione del Servizio, riportato un richiamo al documento Piano di Cessazione del Servizio in caso di dismissione completa da parte di Engineering Cap. 8.3 aggiornato componenti tecnologiche Cap. 9.6 Verifica della compliance del servizio: pianificazione degli Audit interni (nuovo Capitolo)	

INDICE

1 Scopo e Ambito del Documento

Engineering Ingegneria Informatica dispone di due differenti servizi di Conservazione Digitale, uno denominato DigiDoc e l'altro denominato DigiBox (sistema ereditato dall'incorporazione di Infogroup); il presente documento costituisce il manuale di conservazione di DigiBox, (ex-Infogroup) adottato da Engineering Ingegneria Informatica S.p.A., nel seguito indicato come Eng, per il processo di conservazione della documentazione digitale ai sensi della vigente normativa in materia elencata nell'apposito capitolo del presente documento

Il presente manuale ha lo scopo di descrivere:

- il modello organizzativo adottato da Eng per l'erogazione del Servizio, in cui sono evidenziati i ruoli e le responsabilità attribuite ad attori interni o affidate a soggetti esterni;
- i processi di erogazione del servizio, facendo riferimento anche a documentazione operativa esterna per la descrizione di attività di dettaglio;
- le attività di controllo sul processo e sugli archivi in modo da verificare la corretta gestione dei processi di erogazione del servizio;
- l'infrastruttura tecnologica a supporto del servizio;
- le misure di sicurezza logiche e fisiche;

Il documento rappresenta il riferimento principale relativo a qualsiasi aspetto che regola il corretto funzionamento del Servizio.
In particolare, il presente documento, rappresenta la linea guida per la gestione della comunicazione tra Engineering e il Cliente, è verificato dal Responsabile del Servizio di Conservazione ed è approvato dal Responsabile del Competence Center ECM.
Le responsabilità assegnate nell'erogazione del servizio di conservazione vengono riportare nel capitolo specifico di questo manuale.
Si riportano, sempre all'interno del presente documento, i dettagli degli oggetti che vengono conservati, le modalità con cui vengono mantenuti nel tempo, le infrastrutture su cui tali servizi si poggiano ed i sistemi di monitoraggio che controllano l'erogazione.

Eventuali modifiche e aggiornamenti a questo documento potranno essere effettuate dal Responsabile del servizio di Conservazione, previa condivisione con il Responsabile del trattamento dei dati personali, il Responsabile della Sicurezza e con il Responsabile dei Sistemi Informativi.

Qualora si concordi con uno specifico cliente o per uno specifico servizio di conservazione, di operare in modo differente rispetto a quanto riportato nel presente manuale, le particolarità definite saranno riportate in uno specifico allegato, riferito allo specifico contratto o servizio, denominato "specificità contrattuali". Il documento di specificità contrattuale viene condiviso con il cliente e diventerà parte integrante della documentazione del servizio erogato.

torna al sommario

2 Terminologia (glossario/acronimi)

In questo paragrafo sono riportate in ordine alfabetico le principali definizioni, termini, e concetti direttamente riferiti o collegati al processo di conservazione a norma

2.1 Glossario

TERMINE	DEFINIZIONE
accesso	operazione che consente a chi ne ha diritto di prendere visione ed estrarre copia dei documenti informatici
accreditamento	riconoscimento, da parte dell'Agenzia per l'Italia digitale, del possesso dei requisiti del livello più elevato, in termini di qualità possesso dei requisiti del livello più elevato, in termini di qualità e sicurezza ad un soggetto pubblico o privato, che svolge attività di conservazione o di certificazione del processo di conservazione
affidabilità	caratteristica che esprime il livello di fiducia che l'utente ripone nel documento informatico
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
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
area organizzativa omogenea	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
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
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

TERMINE	DEFINIZIONE
ciclo di gestione	arco temporale di esistenza del documento informatico, del fascicolo informatico, dell'aggregazione documentale informatica o dell'archivio informatico dalla sua formazione alla sua eliminazione o conservazione nel tempo
classificazione	attività di organizzazione logica di tutti i documenti secondo uno schema articolato in voci individuate attraverso specifici metadati
Codice	decreto legislativo 7 marzo 2005, n. 82 e successive modificazioni e integrazioni
codice eseguibile	insieme di istruzioni o comandi software direttamente elaborabili dai sistemi informatici
conservatore accreditato	soggetto, pubblico o privato, che svolge attività di conservazione al quale sia stato riconosciuto, dall'Agenzia per l'Italia digitale, il possesso dei requisiti del livello più elevato, in termini di qualità e di sicurezza, dall'Agenzia per l'Italia digitale
conservazione	insieme delle attività finalizzate a definire ed attuare le politiche complessive del sistema di conservazione e a governarne la gestione in relazione al modello organizzativo adottato e descritto nel manuale di conservazione
Coordinatore della Gestione Documentale	responsabile della definizione di criteri uniformi di classificazione ed archiviazione nonché di comunicazione interna tra le AOO ai sensi di quanto disposto dall'articolo 50 comma 4 del DPR 445/2000 nei casi di amministrazioni che abbiano istituito più Aree Organizzative Omogenee
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
destinatario	identifica il soggetto/sistema al quale il documento informatico è indirizzato
duplicazione dei documenti informatici	produzione di duplicati informatici
esibizione	operazione che consente di visualizzare un documento conservato e di ottenerne copia
estratto per riassunto	documento nel quale si attestano in maniera sintetica ma esaustiva fatti, stati o qualità desunti da dati o documenti in possesso di soggetti pubblici
evidenza informatica	una 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.
formato	modalità di rappresentazione della sequenza di bit che costituiscono il documento informatico; comunemente è identificato attraverso l'estensione del file

TERMINE	DEFINIZIONE
funzionalità aggiuntive	le ulteriori componenti del sistema di protocollo informatico necessarie alla gestione dei flussi documentali, alla conservazione dei documenti nonché alla accessibilità delle informazioni
funzionalità interoperative	le componenti del sistema di protocollo informatico finalizzate a rispondere almeno ai requisiti di interconnessione di cui all'articolo 60 del D.P.R. 28 dicembre 2000, n. 445
funzionalità minima	la componente del sistema di protocollo informatico che rispetta i requisiti di operazioni ed informazioni minime di cui all'articolo 56 del D.P.R. 28 dicembre 2000, n. 445
funzione di hash	una funzione matematica che genera, a partire da una evidenza informatica, una impronta in modo tale che risulti di fatto impossibile, a partire da questa, ricostruire l'evidenza informatica originaria e generare impronte uguali a partire da evidenze informatiche differenti
generazione automatica di documento informatico	formazione di documenti informatici effettuata direttamente dal sistema informatico al verificarsi di determinate condizioni
identificativo univoco	sequenza di caratteri alfanumerici associata in modo univoco e persistente al documento informatico, al fascicolo informatico, all'aggregazione documentale informatica, in modo da consentirne l'individuazione
immodificabilità	caratteristica che rende il contenuto del documento informatico non alterabile nella forma e nel contenuto durante l'intero ciclo di gestione e ne garantisce la staticità nella conservazione del documento stesso
impronta	la sequenza di simboli binari (bit) di lunghezza predefinita generata mediante l'applicazione alla prima di una opportuna funzione di hash
insieme minimo di metadati del documento informatico	complesso dei metadati, la cui struttura è descritta nell'allegato 5 del presente decreto, 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
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
manuale di gestione	strumento che descrive il sistema di gestione informatica dei documenti di cui all'articolo 5 delle regole tecniche del protocollo informatico ai sensi delle regole tecniche per il protocollo informatico D.P.C.M. 31 ottobre 2000 e successive modificazioni e integrazioni
memorizzazione	processo di trasposizione su un qualsiasi idoneo supporto, attraverso un processo di elaborazione, di documenti analogici o informatici

TERMINE	DEFINIZIONE
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; tale insieme è descritto nell'allegato 5 del decreto "regole tecniche in materia di Conservazione"
pacchetto di archiviazione	pacchetto informativo composto dalla trasformazione di uno o più pacchetti di versamento secondo le specifiche contenute nell'allegato 4 del presente decreto e secondo le modalità riportate nel manuale di conservazione
pacchetto di distribuzione	pacchetto informativo inviato dal sistema di conservazione all'utente in risposta ad una sua richiesta
pacchetto di versamento	pacchetto informativo inviato dal produttore al sistema di conservazione secondo un formato predefinito e concordato descritto nel manuale di conservazione
pacchetto informativo	contenitore che racchiude uno o più oggetti da conservare (documenti informatici, fascicoli informatici, aggregazioni documentali informatiche), oppure anche i soli metadati riferiti agli oggetti da conservare
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
piano della sicurezza del sistema di gestione informatica dei documenti	documento, che, nel contesto del piano generale di sicurezza, descrive e pianifica le attività volte a proteggere il sistema di gestione informatica dei documenti da possibili rischi nell'ambito dell'organizzazione di appartenenza
piano di conservazione	strumento, integrato con il sistema di classificazione per la definizione dei criteri di organizzazione dell'archivio, di selezione periodica e di conservazione ai sensi dell'articolo 68 del D.P.R. 28 dicembre 2000, n. 445
piano generale della sicurezza	documento per la pianificazione delle attività volte alla realizzazione del sistema di protezione e di tutte le possibili azioni indicate dalla gestione del rischio 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
produttore	persona fisica o giuridica, di norma diversa dal soggetto che ha formato il documento, che produce il pacchetto di versamento ed è responsabile del trasferimento del suo contenuto nel sistema di conservazione. Nelle pubbliche amministrazioni, tale figura si identifica con responsabile della gestione documentale.
rapporto di versamento	documento informatico che attesta l'avvenuta presa in carico da parte del sistema di conservazione dei pacchetti di versamento inviati dal produttore

TERMINE	DEFINIZIONE
registrazione informatica	insieme delle informazioni risultanti da transazioni informatiche o dalla presentazione in via telematica di dati attraverso moduli o formulari resi disponibili in vario modo all'utente
registro particolare	registro informatico di particolari tipologie di atti o documenti; nell'ambito della pubblica amministrazione è previsto ai sensi dell'articolo 53, comma 5 del D.P.R. 28 dicembre 2000, n. 445
registro di protocollo	registro informatico di atti e documenti in ingresso e in uscita che permette la registrazione e l'identificazione univoca del documento informatico all'atto della sua immissione cronologica nel sistema di gestione informatica dei documenti
repertorio informatico	registro informatico che raccoglie i dati registrati direttamente dalle procedure informatiche con cui si formano altri atti e documenti o indici di atti e documenti secondo un criterio che garantisce l'identificazione univoca del dato all'atto della sua immissione cronologica
responsabile della gestione documentale o responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi	dirigente o funzionario, comunque in possesso di idonei requisiti professionali o di professionalità tecnico archivistica, preposto al servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi, ai sensi dell'articolo 61 del D.P.R. 28 dicembre 2000, n. 445, che produce il pacchetto di versamento ed effettua il trasferimento del suo contenuto nel sistema di conservazione.
responsabile della conservazione	soggetto responsabile dell'insieme delle attività elencate nell'articolo 8, comma 1 delle regole tecniche del sistema di conservazione
responsabile del trattamento dei dati	la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali
responsabile della sicurezza	soggetto al quale compete la definizione delle soluzioni tecniche ed organizzative in attuazione delle disposizioni in materia di sicurezza
riferimento temporale	informazione contenente la data e l'ora con riferimento al Tempo Universale Coordinato (UTC), della cui apposizione è responsabile il soggetto che forma il documento
scarto	operazione con cui si eliminano, secondo quanto previsto dalla normativa vigente, i documenti ritenuti privi di valore amministrativo e di interesse storico culturale
sistema di classificazione	strumento che permette di organizzare tutti i documenti secondo un ordinamento logico con riferimento alle funzioni e alle attività dell'amministrazione interessata
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
staticità	Caratteristica che garantisce l'assenza di tutti gli elementi dinamici, quali macroistruzioni, riferimenti esterni o codici eseguibili, e l'assenza delle informazioni di ausilio alla redazione, quali annotazioni, revisioni, segnalibri, gestite dal prodotto software utilizzato per la redazione

TERMINE	DEFINIZIONE
transazione informatica	particolare evento caratterizzato dall'atomicità, consistenza, integrità e persistenza delle modifiche della base di dati
integrità e persistenza delle modifiche della base di dati	Testo unico decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, e successive modificazioni
ufficio utente	riferito ad un area organizzativa omogenea, un ufficio dell'area stessa che utilizza i servizi messi a disposizione dal sistema di protocollo informatico
utente	persona, ente o sistema che interagisce con i servizi di un sistema di gestione informatica dei documenti e/o di un sistema per la conservazione dei documenti informatici, al fine di fruire delle informazioni di interesse
versamento agli archivi di stato	operazione con cui il responsabile della conservazione di un organo giudiziario o amministrativo dello Stato effettua l'invio agli Archivi di Stato o all'Archivio Centrale dello Stato della documentazione destinata ad essere ivi conservata ai sensi della normativa vigente in materia di beni culturali

torna al sommario

2.2 Acronimi

AgID	Agenzia per l'Italia Digitale
ASP	Application Service Providing
CA	Certification Authority (indica l'Autorità di certificazione di un dispositivo di firma digitale)
CAD	Codice Amministrazione Digitale
CAGE	Spazio Tecnico presente all'interno di un DC ad uso esclusivo dell'affittuario.
CD	Compact Disk
DL	Decreto Legge
D.Lgs	Decreto Legislativo
DM	Decreto ministeriale
DMEF	Decreto del Ministero dell'Economia e delle Finanze
DMS	Document Management System
DPCM	Decreto Presidente del Consiglio dei Ministri
DPR	Decreto Presidente della Repubblica
DVD	Digital Versatile Disk
FTP	File Transfer Protocol
GC	Gestore della Conservazione
GU	Gazzetta Ufficiale
HTTP	Hyper Text Transfer Protocol (identificativo convenzionale per un sito)
HTTPS	Secure Hyper Text Transmission Protocol. Protocollo sviluppato allo scopo di cifrare e decifrare le pagine Web che vengono inviate dal server ai client.
IPDA	Indice del Pacchetto di Archiviazione
HW	Hardware
L	Legge
NTP	Network Time Protocol
PdA	Pacchetto di Archiviazione
PdD	Pacchetto di Distribuzione
PDF	Portable Document Format
PdV	Pacchetto di Versamento
PEC	posta elettronica certificata
PKI	Public Key Infrastructure (infrastruttura necessaria per creare, gestire, conservare e revocare i certificati delle firme elettroniche basati su crittografia a chiave pubblica)
RDC	Responsabile della Conservazione
RdV	Rapporto di Versamento
SLA	Service Level Agreement
SSL	Secure Socket Layer. Protocollo che consente, grazie a tecniche di crittografia, il trasferimento di dati tramite la rete Internet in modo sicuro.
STORAGE	Infrastruttura tecnologica composta da più Dischi Ottici ad alta capacità di immagazzinamento dati.
SW	Software
TSA	Time Stamping Authority
TU	Testo Unico
URL	Uniform Resource Locator (indica la modalità per individuare univocamente un sito Internet)
UTC	Universal Time Coordinated (Misura del tempo così come stabilito dall'International Radio Consultative Committee – CCIR)

torna al sommario

3 Normativa e Standard di Riferimento

3.1 Normativa di riferimento

La Conservazione a Norma di documenti informatici (e delle loro impronte), avviene attraverso la memorizzazione in supporti idonei e si completa con l'apposizione del riferimento temporale (marca temporale) e della firma digitale da parte del Responsabile del servizio di Conservazione (o del RdC se espressamente richiesto dal Cliente) che ne attesta il corretto svolgimento del processo.
Il documento conservato deve essere reso leggibile, in qualunque momento, presso il sistema di Conservazione ed esibito per via telematica.
Il servizio di Conservazione a norma recepisce le seguenti normative di riferimento:

- 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;
- 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.

torna al sommario

3.2 Standard di riferimento

- ISO 14721:2012 OAIS (Open Archival Information System), Sistema informativo aperto per l'archiviazione.
- ISO/IEC 27001:2013, Information technology - Security techniques - Information security management systems – Requirements, Requisiti di un ISMS (Information Security Management System).

- 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

Il Servizio di Conservazione a Norma Digibox, che Eng eroga ai propri clienti, prevede la seguente struttura Organizzativa:

- Produttore;
- Utente;
- Responsabile del Servizio di Conservazione;
- Responsabile dell'erogazione del Servizio;
- Responsabile Applicativo;
- Responsabile dei Sistemi Informativi;
- Responsabile della Sicurezza;
- Responsabile della Privacy;

torna al sommario

4.1 Produttore

E' il responsabile della creazione del pacchetto di versamento e del suo invio verso il sistema di Conservazione. Verifica l'esito della presa in carico da parte del Servizio di conservazione tramite opportuni sistemi di rendicontazione (on line o batch) che il sistema restituisce al mittente, ed eventualmente con il controllo del Rapporto di Versamento (RdV).

torna al sommario

4.2 Utente

Persona, ente o sistema in grado di richiedere al Sistema di Conservazione a Norma l'esibizione del pacchetto di distribuzione ovvero fruire delle informazioni di interesse.

I ruoli **interni all'organizzazione per l'erogazione del servizio** sono stati così assegnati:

PROFILO	Nominativo	Periodo nel Ruolo	Contratto
Responsabile del Servizio di Conservazione	Andrea Pugi	2009	Tempo indeterminato
Responsabile della funzione **archivistica** di conservazione	Francesca Pranzo Zaccaria	2010	Tempo indeterminato
Responsabile della **sicurezza** dei sistemi per la conservazione	Stefano Ciuffi	2008	Tempo indeterminato
Responsabile del **trattamento dei dati personali**	Cosimo Nigro	2018	Tempo Indeterminato

PROFILO	Nominativo	Periodo nel Ruolo	Contratto
Responsabile dei **sistemi informativi** per la conservazione	Enzo Cati	2011	Tempo indeterminato
Responsabile dello sviluppo e della manutenzione del sistema di conservazione (Resp. **Applicativo**)	Stefano Mannori	2009	Tempo indeterminato

I 6 profili richiesti per l'accreditamento dall'Agenzia sono stati mappati su figure professionali i cui compiti sono dettagliati nei paragrafi seguenti.

torna al sommario

4.3 Responsabile del Servizio di conservazione

Opera d'intesa con il responsabile del trattamento dei dati personali, con il responsabile della sicurezza e con il responsabile dei sistemi informativi oltre che con il responsabile della gestione documentale e:

- definisce le caratteristiche e i requisiti del sistema di conservazione in funzione della tipologia dei documenti da conservare, della quale tiene evidenza, in conformità alla normativa vigente;
- se richiesto dal cliente genera e sottoscrive il pacchetto di distribuzione con firma digitale o firma elettronica qualificata, nei casi previsti dal manuale di conservazione;
- assicura la verifica periodica, con cadenza non superiore ai cinque anni, dell'integrità degli archivi e della leggibilità degli stessi;
- al fine di garantire la conservazione e l'accesso ai documenti informatici, adotta misure per rilevare tempestivamente l'eventuale degrado dei sistemi di memorizzazione e delle registrazioni e, ove necessario, per ripristinare la corretta funzionalità; adotta analoghe misure con riguardo all'obsolescenza dei formati;
- provvede alla duplicazione o copia dei documenti informatici in relazione all'evolversi del contesto tecnologico, secondo quanto previsto dal manuale di conservazione;
- adotta le misure necessarie per la sicurezza fisica e logica del sistema di conservazione ai sensi dell'art. 12 del DPCM 3 dicembre 2013 (nuove regole tecniche in materia di sistema di conservazione);
- predispone il manuale di conservazione di cui all'art. 8 del DPCM 3 dicembre 2013 (nuove regole tecniche in materia di sistema di conservazione) e ne cura l'aggiornamento periodico in presenza di cambiamenti normativi, organizzativi, procedurali o tecnologici rilevanti.

Avvalendosi della struttura organizzativa specifica (descritta nei paragrafi seguenti) assicura che tutte le componenti erogate dal servizio vengano evase secondo gli SLA concordati e i requirement specifici dei documenti mandati in conservazione.
All'interno di supporto applicativo è stato incarico un referente per le seguenti funzioni operative:

1. gestisce il processo di conservazione

2. genera il rapporto di versamento, secondo le modalità previste dal manuale di conservazione;
3. effettua il monitoraggio della corretta funzionalità del sistema di conservazione;

torna al sommario

4.4 Il Responsabile della Funzione archivistica

Definisce, in accordo con l'ente produttore, le modalità di trasferimento dei documenti informatici verso il sistema di conservazione.
Si occupa di stabilire:

- Modalità di acquisizione
- Modalità di aggregazione (se necessari)
- Set di metadati associati ai flussi documentali

Svolge le attività specifica per assicurare la:

- definizione e gestione del processo di conservazione, incluse le modalità di trasferimento da parte dell'ente produttore, di acquisizione, verifica di integrità e descrizione archivistica dei documenti e delle aggregazioni documentali trasferite, di esibizione, di accesso e fruizione del patrimonio documentario e informativo conservato;
- definizione del set di metadati di conservazione dei documenti e dei fascicoli informatici;
- monitoraggio del processo di conservazione e analisi archivistica per lo sviluppo di nuove funzionalità del sistema di conservazione;
- collaborazione con l'ente produttore ai fini del trasferimento in conservazione, della selezione e della gestione dei rapporti con il Ministero dei beni e delle attività culturali per quanto di competenza.

torna al sommario

4.5 Responsabile Applicativo

E' la persona di riferimento la quale assicura che tutte le nuove richieste di evoluzione funzionale e/o di integrazione con altre applicazioni vengano ricevute, valutate e applicate al sistema di conservazione secondo i tempi e i requisiti concordati con il cliente e in accordo con le indicazioni del Responsabile del Servizio di Conservazione. Ha in carico la manutenzione dell'applicazione a supporto del servizio di Conservazione a Norma.
E' colui che adegua il servizio alle evoluzioni richieste dai clienti e imposte dai cambiamenti normativi adottando le soluzioni appositamente predisposte sul sistema di conservazione. Inoltre è responsabile della pronta segnalazione al Responsabile del Servizio di Conservazione degli incidenti con livello di gravità massimo.

torna al sommario

4.6 Responsabile dei Sistemi Informativi

E' la persona che gestisce l'esercizio delle componenti hardware e software del sistema di conservazione, garantendone l'adeguatezza nel tempo. Si occupa del monitoraggio dei livelli

di servizio dell'infrastruttura e segnala eventuali difformità degli SLA al Responsabile del Servizio, pianificando eventuali azioni correttive.

torna al sommario

4.7 Responsabile della Sicurezza

E' la persona che stabilisce e manutiene le policy di sicurezza relative al sistema di conservazione, le condivide con il Responsabile del Servizio di Conservazione e ne verifica l'applicazione nel tempo. Individua eventuali difformità, le comunica al Responsabile del servizio e pianifica le azioni correttive individuate.

torna al sommario

4.8 Responsabile del trattamento dati personali

Garantisce il rispetto della normativa vigente in materia del trattamento dei dati personali e del rispetto delle istruzioni impartite dal Titolare del trattamento.

Il responsabile del trattamento dei dati personali nominato per il servizio di Conservazione a Norma, al fine di garantire il rispetto della normativa vigente (GDPR e AgID), opera in armonia con quanto previsto dalla procedura di Gruppo *PGT01_0_Gestione Privacy Gdpr,* redatta dalla funzione Coordinamento Privacy (DPO) ed autorizzata dalla Direzione Aziendale. Essa individua la figura del "Privacy Manager" come garante del rispetto delle misure di sicurezza tecniche e/o organizzative previste dagli accordi siglati con il Cliente. Per il servizio di Conservazione a Norma, la figura identificata come Privacy Manager nella procedura citata, corrisponde al Responsabile del trattamento dati personali.

torna al sommario

5 Struttura Organizzativa

5.1 *Organigramma*

Si riporta di seguito l'organigramma di Engineering Ingegneria Informatica S.p.A., estratto dal documento MGP02 Manuale Organizzazione Gruppo Engineering.

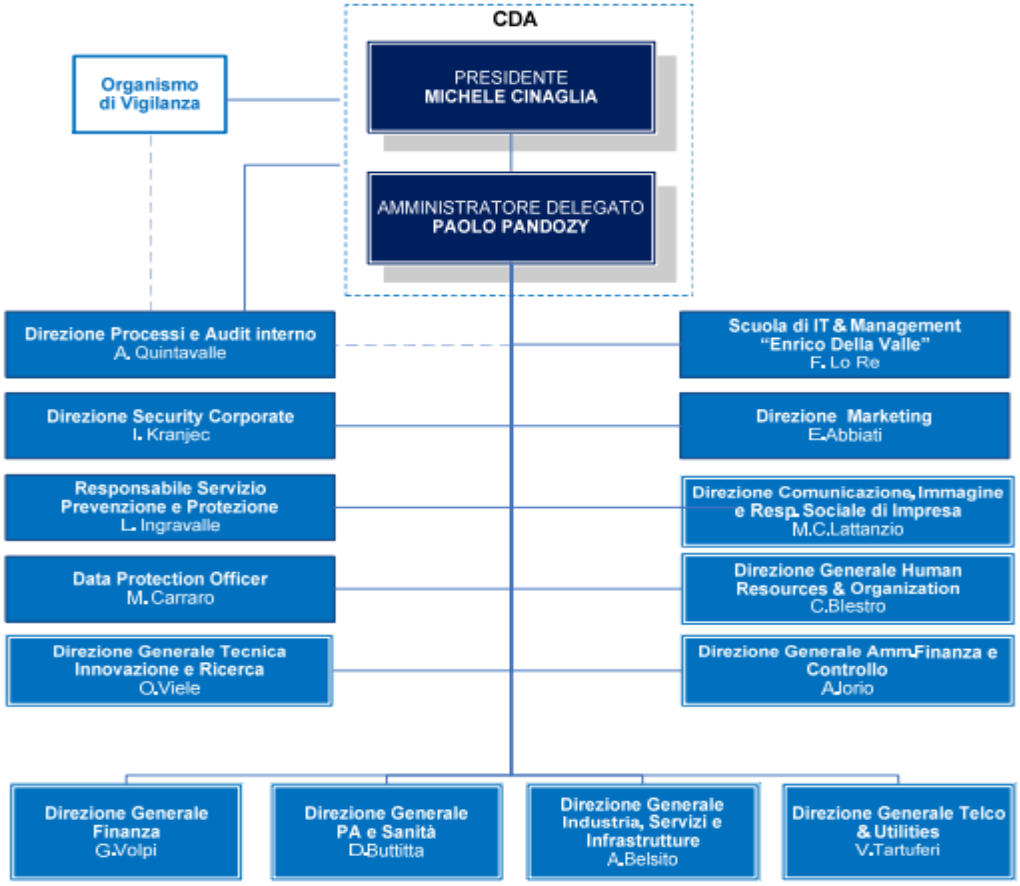

Figura 1 – Organigramma Engineering Ingegneria Informatica

Nella figura che segue sono riportate le strutture organizzative di Engineering Ingegneria Informatica S.p.A. coinvolte nel processo di conservazione

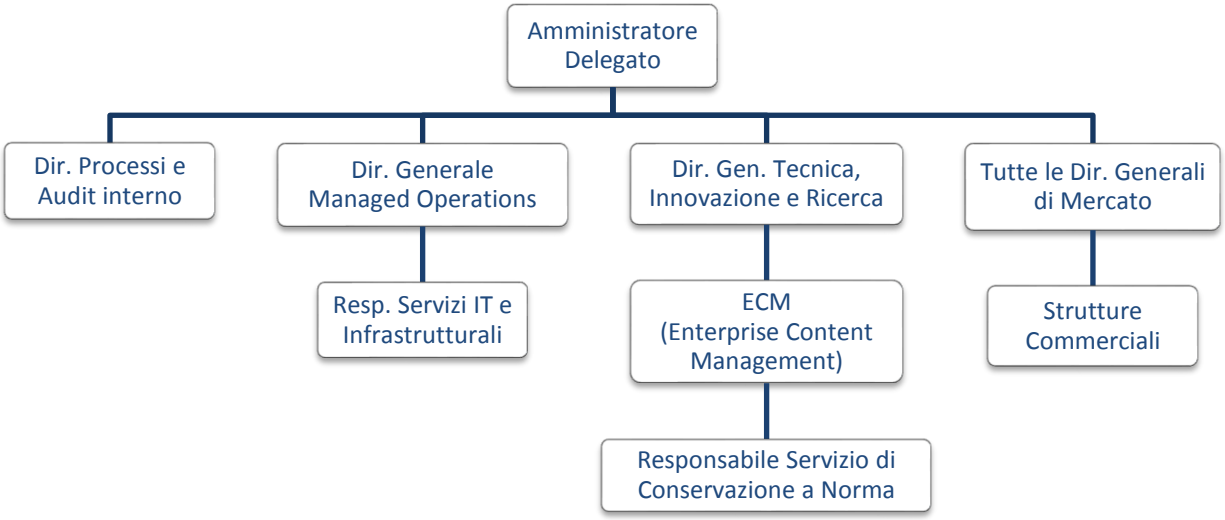

Figura 2 – strutture coinvolte nell'erogazione del servizio

Per l'erogazione del servizio di Conservazione a norma sono state definite specifiche figure interne all'organizzazione dell'Azienda in grado di garantire la corretta erogazione e adeguati supporti nei confronti del Produttore e dell'Utente.
Queste figure sono coordinate dal Responsabile di Erogazione del Servizio.

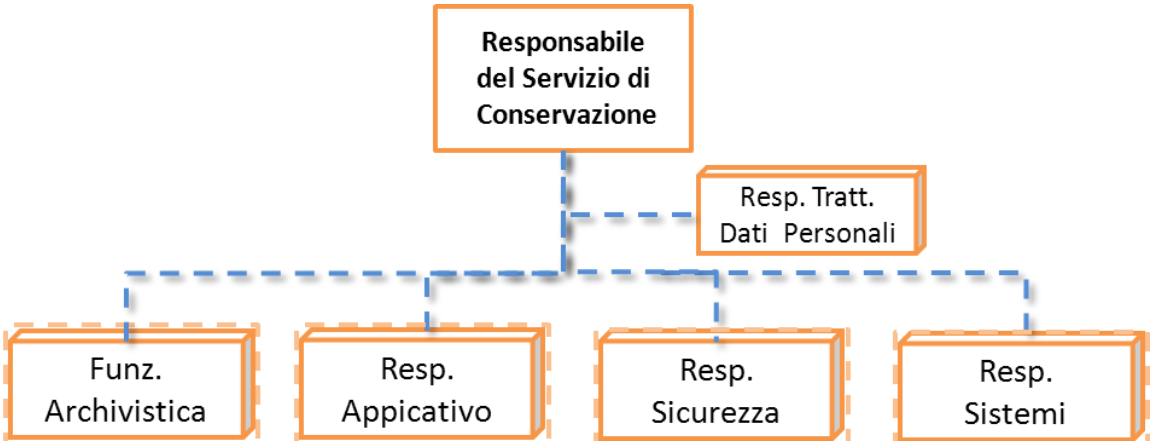

Figura 3 – Organizzazione specifica del servizio

torna al sommario

5.2 Strutture Organizzative

5.2.1 Supporto operativo

Il Supporto operativo rappresenta il principale punto di contatto Single Point of Contact relativo alle segnalazioni provenienti dai clienti (Produttore e Utente) e strutture interne che possono accedere al servizio di Supporto operativo attraverso l'invio di una e-mail all'l'indirizzo Servizio_CN@Eng.it .

Il Supporto operativo, prende in carico la segnalazione tracciando opportunamente la richiesta nel Sistema di Trouble Ticketing Eng, catalogando la segnalazione per tipologia e livello di gravità.
Sotto vengono riportate le tipologie selezionabili e i livelli di gravità gestiti:

Tipologie di Segnalazione:
- Incident;
- Change Request;
- Service Request.

Per la tipologia Incident vengono riportati sotto i livelli di Gravità, in ordine decrescente:
- Livello 4;
- Livello 3;
- Livello 2;
- Livello 1.

I livelli di Gravità sono definiti in base all'impatto dell'incidente:

Descrizione	criticità	Caratteristiche per la classificazione
Incidente	4	Evento che provoca (o può provocare) una interruzione di attività, un guasto, una perdita o una riduzione del servizio. L'evento è gestito.
Malfunzionamento	3	Evento che compromette l'asset ma in modo discontinuo
Incidente non bloccante	2	Evento dannoso che non ha impatti significativi rispetto al sistema di produzione, che continua, quindi a funzionare correttamente e completamente
Anomalia	1	Evento sporadico che non compromette gli asset e l'operatività dei processi.

Sulla base dei contenuti della segnalazione, il Supporto operativo prende in carico la richiesta ed esegue quanto necessario per chiuderla autonomamente oppure la indirizza verso il livello specialistico competente per la sua risoluzione:
- Supporto Applicativo;
- Supporto Sistemistico.

In ogni caso è il Supporto operativo che comunica all'entità interessata la chiusura del ticket.

Le tipologie di **Change Request** scalabili al Supporto operativo sono:
- richiesta configurazione nuovi Clienti;
- richiesta configurazione nuove famiglie documentali;
- richiesta creazione nuovi report di servizio;
- modifica configurazione Clienti/famiglie documentali esistenti;

- modifica alla reportistica già esistente.

Le tipologie di **Service Request** scalabili al Supporto operativo sono:
- chiarimenti funzionali relativi all'utilizzo dell'interfaccia Web del sistema di conservazione;
- verifiche relative alla configurazione del servizio;
- richiesta produzione supporti.

Inoltre nel caso in cui il sistema di Conservazione a Norma rilevi situazioni anomale dovute alla presenza di dati errati forniti dal Produttore (metadati non coerenti, problemi sui flussi, sequenze di numerazione non rispettate, ecc.), il Supporto operativo prende in carico l'anomalia, e può contattare il Produttore tramite i canali e le modalità concordate per la notifica e per eventuali azioni da intraprendere per la chiusura del ticket.

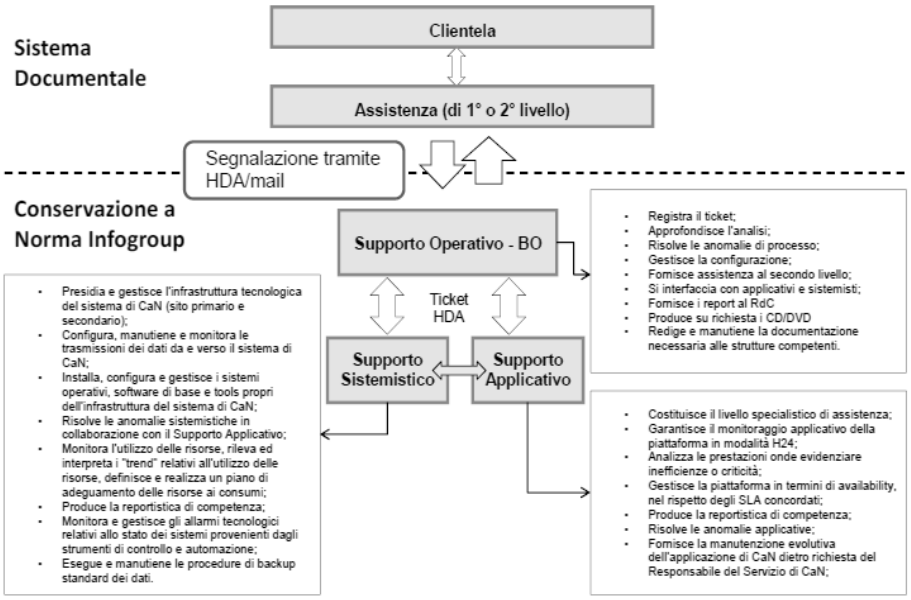

Figura 4 - workflow di lavorazione delle segnalazioni

torna al sommario

5.2.2 Servizio di Supporto Applicativo

Il servizio è gestito dal Responsabile Applicativo e ha lo scopo di assicurare il corretto funzionamento dell'applicativo di Conservazione a Norma e opera di concerto con il Supporto Operativo per la gestione delle eventuali segnalazioni di malfunzionamento.
Il servizio di Supporto Applicativo, dietro indicazione del Responsabile del Servizio di Conservazione, mantiene aggiornata l'applicazione secondo le esigenze dei Clienti e secondo le evoluzioni della normativa vigente che regola la Conservazione a Norma.

Il Supporto Applicativo ha i seguenti compiti:
- monitoraggio applicativo in modalità H24;
- supporto specialistico di Assistenza Applicativa;
- produzione della reportistica di competenza;
- Presa in carico delle Change Request provenienti dal Supporto Operativo;
- gestione delle Service Request provenienti dal Supporto Operativo.

Le principali tipologie di segnalazione gestite dal Supporto Applicativo sono:

- segnalazioni di malfunzionamenti generati dalla piattaforma di Conservazione;
- segnalazioni di malfunzionamenti dovuti ad un'errata formattazione dei PdV/documenti ricevuti del Produttore;
- Problematiche relative ad aspetti funzionali sul processo che alimenta la piattaforma di Conservazione a Norma.

torna al sommario

5.2.3 Servizio Sistemistico

Il servizio è gestito dal Responsabile dei Sistemi Informativi e ha lo scopo di assicurare il corretto funzionamento dell'infrastruttura tecnologica del servizio di Conservazione a Norma e opera di concerto con il Supporto Operativo e il Supporto Applicativo per la gestione delle eventuali segnalazioni di malfunzionamento.
Di seguito sono elencate in sintesi le principali attività svolte dal Servizio Sistemistico:

- Presidia e gestisce l'infrastruttura tecnologica del sistema di Conservazione a Norma (sito primario e secondario);
- Configura, manutiene e monitora le trasmissioni dei dati da e verso il sistema di Conservazione a Norma;
- Installa, configura e gestisce i sistemi operativi, software di base e tools propri dell'infrastruttura del sistema di Conservazione a Norma;
- Risolve le anomalie sistemistiche in collaborazione con il Supporto Applicativo;
- Monitora l'utilizzo delle risorse, rileva ed interpreta i "trend" relativi all'utilizzo delle risorse, definisce e realizza un piano di adeguamento delle risorse ai consumi;
- Produce la reportistica di competenza;
- Monitora e gestisce gli allarmi tecnologici relativi allo stato dei sistemi provenienti dagli strumenti di controllo e automazione;
- Esegue e manutiene le procedure di backup standard dei dati.

Per maggiori dettagli delle attività svolte si rimanda all'allegato specifico (descrizione infrastruttura)

Matrice	Responsabile del Servizio di Conservazione	Responsabile della funzione **archivistica** di conservazione	Responsabile della **sicurezza** dei sistemi per la conservazione	Responsabile del **trattamento dei dati personali**	Responsabile dei **sistemi** informativi per la conservazione	Responsabile dello sviluppo e della manutenzione del sistema di conservazione (Resp. **Applicativo**)
attivazione del servizio di conservazione (a seguito della sottoscrizione di un contratto)	**R**	**C**	**C**	**I**		**A**
acquisizione, verifica e gestione dei pacchetti di versamento presi in carico e generazione del rapporto di versamento	**R**	**A**			**C**	
preparazione e gestione del pacchetto di archiviazione	**R**	**C**				**A**
preparazione e gestione del pacchetto di distribuzione ai fini dell'esibizione e della produzione di duplicati e copie informatiche su richiesta	**R**	**C**		**I**	**C**	**A**
scarto dei pacchetti di archiviazione		**R**		**I**	**C**	**A**
chiusura del servizio di conservazione (al termine di un contratto)	**R**	**I**		**I**	**C**	**C**
conduzione e manutenzione del sistema di conservazione				**C**	**C**	**R**
monitoraggio del sistema di conservazione	**I**	**I**			**R**	**A**
change management				**C**	**C**	**R**
verifica periodica di conformità a normativa e standard di riferimento	**R**	**C**				

- R: Responsabile
- A: Agisce
- C: Collabora
- I: Informato

torna al sommario

6 Oggetti sottoposti a Conservazione

6.1 *Oggetti sottoposti a conservazione*

Sono oggetti del sistema di conservazione:

a) i **documenti informatici** e i **documenti amministrativi informatici** prodotti dal Cliente e acquisiti da Eng, con i metadati ad essi associati di cui all'allegato 5 delle Regole Tecniche;
b) i **fascicoli informatici** ovvero le aggregazioni documentali informatiche con i metadati ad essi associati, contenenti i riferimenti che univocamente identificano i singoli oggetti documentali che appartengono al fascicolo o all'aggregazione documentale.

Segue un esempio di tabella dei formati gestiti.

visualizzatore	Tipo documento	formato del file
Acrobat	Contabili di sportello	Pdf, p7m
Acrobat	Contratti clientela	Pdf, p7m
Acrobat	Documenti Fiscali	Xml, Pdf, p7m, tsd
Acrobat	Dichiarazioni varie	Pdf, p7m
Acrobat	Documenti con apposizione Data certa	Pdf, tsr
Immagini	Immagini con apposizione Data certa	Tiff, tsr

Integrazioni alla presente tabella possono essere presenti nell'allegato "specificità del contratto".

In occasione degli Audit interni, condotti annualmente viene effettuata un'analisi circa l'obsolescenza dei formati presenti in Conservazione.

Gli oggetti della conservazione sono trattati dal sistema di conservazione in pacchetti informativi come descritto nel presente documento e conformemente all'art. 4 delle Regole Tecniche:

- Pacchetti di Versamento
- Pacchetti di Archiviazione
- Pacchetti di Distribuzione

torna al sommario

6.2 *Formati e metadati*

Le tipologie documentali afferenti agli oggetti descritti nel precedente paragrafo sono individuate dal Responsabile del servizio di Conservazione d'intesa con il la funzione archivistica ed applicativa, in fase di attivazione del servizio e conformemente a quanto stipulato in sede contrattuale, tenendo conto delle:

a) peculiarità delle classi documentali;
b) dei formati dei file accettabili in conservazione.

Ai sensi della normativa vigente sono conservati solo i formati di file idonei ad essere correttamente conservati, individuati dall'allegato 2 alle Regole Tecniche, a cui integralmente si rinvia, rispettando i requisiti ivi previsti di "standard aperti", in modo da garantire a

chiunque in futuro la possibilità tecnica di avere accesso ai dati conservati, corredati da una struttura di dati per la memorizzazione nel sistema di conservazione in grado di assicurare l'interoperabilità tra sistemi.

Tutti i documenti versati sul sistema di conservazione Eng sono contraddistinti da un set di metadati obbligatori per il sistema, che li identificano univocamente, e che sono descritti nel capitolo relativo al PDV.

torna al sommario

6.3 Pacchetto di Versamento (PdV)

Il servizio di Conservazione riceve i documenti inviati dal Produttore attraverso canali di comunicazione sicuri concordati col Cliente in sede di attivazione del servizio.
I documenti da sottoporre a conservazione devono essere predisposti secondo quanto previsto contrattualmente per quanto attiene la presenza della firma digitale, dei metadati e la correttezza del formato.
I documenti contenuti nel PdV confluiscono, nelle modalità di seguito descritte, in uno o più PDA.

Il prodotto offre una completa personalizzazione riguardo alla configurazione dei metadati ed alla loro obbligatorietà, consentendo totale piena libertà rispetto alla scelta di quali includere, e di conseguenza la piena adesione allo standard Dublin Core Metadata ISO 15836:2009.

A livello di documento è possibile definire un set di metadati minimi che il documento deve possedere per poter essere versato nel sistema di conservazione (il set di metadati minimi è condiviso con il Cliente/produttore e viene dettagliato nel documento Specificità di Contratto)

Di default il set di metadati minimo è il seguente:

- Id documento
- Soggetto produttore (codifica definita con il cliente; es. nome, cognome, piva, cod fiscale,….)
- Data documento
- Tipo documento/oggetto

A livello di PdV si sono definiti dei parametri (collocati nella testata del flusso) che identificano univocamente il produttore del PdV stesso.

A livello di documento si sono definiti i seguenti metadati (es. di uno specifico servizio):

Nome metadato	Note
CHIAVE/NUMERO	Obbligatorio. Questo dato deve essere sempre presente all'interno
ANNO	Concorre a formare l'univocità della chiave
REGISTRO	Concorre a formare l'univocità della chiave

Non tutti i seguenti sono obbligatori:

Nome metadato	Note
COD_SOC	Indica la società o ente produttore
COD_UO	Unità Organizzativa
COD_SPORTELLO	Sportello operante (dettaglio applicazione/sezione della UO)

Nome metadato	Note
WORKSTATION	ID della workstation dell'operatore
OPERATORE	Matricola dell'operatore (del produttore)
COD_RAPPORTO	Rapporto del Cliente (per documento Clientela)
NDG	NDG del Cliente
NOME	Nome del Cliente
COGNOME	Cognome del Cliente
IMPORTO	Importo dell'operazione
COD_ADESIONE	Specifico per Fascicolo
FG_ANNULLO	flag
EMAIL_CLIENTE	e-mail del Cliente
TRANSAZIONE	Tipo di transazione (es. BONIF)
DATA_CONTABILE	Se operazioni contabile
DATA_CREAZIONE	Obbligatoria
DATA_FIRMA	Se documento firmato
VERSIONE	Dettaglio del viewer/applicativo generatore

Le strutture dati di colloquio tra Cliente e Conservatore sono dettagliate nell'allegato Specificità del Contratto e concordate con il cliente.

torna al sommario

6.4 Pacchetto di Archiviazione

Il PdA contiene un numero variabile di documenti ed un indice.
L'indice del PDA è un file in formato XML che riporta, per ognuno dei file inclusi nel blocco, alcune informazioni tra cui un "urn" (unified resource name) e un "hash".
L'urn è una stringa univoca che identifica l'oggetto digitale, mentre l'hash è un'impronta del documento, ovvero una sequenza di bit che può essere ricavata dal file in modo ripetibile e standardizzato e che garantisce una corrispondenza esatta col contenuto originale.

La modalità di conservazione mediante indice permette di **verificare l'integrità** di ogni singolo file, a prescindere da tutti gli altri file conservati nello stesso blocco. Infatti sarà sufficiente essere in possesso di un file "candidato" e conoscere il suo urn identificativo per poter eseguire la funzione di hash e confrontare l'impronta ricalcolata con la stringa riportata nell'indice.

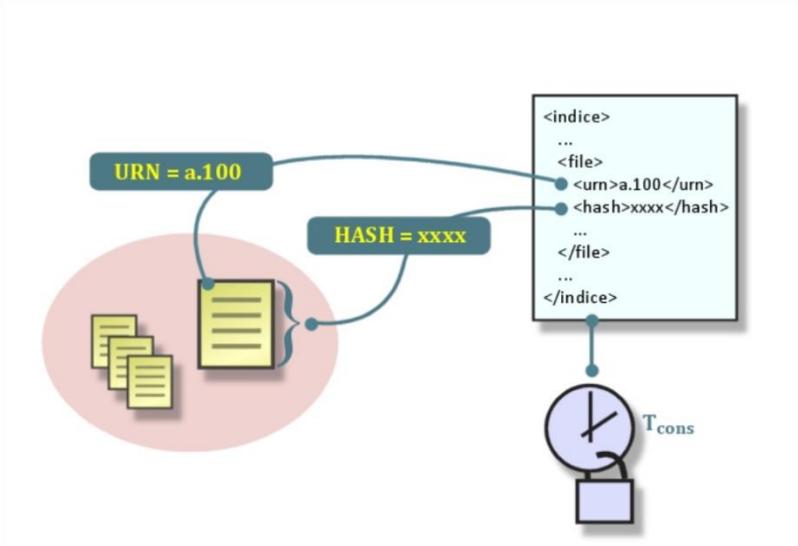

Figura 5 struttura dell'indice del PdA

Il Pacchetto di Archiviazione viene composto a partire da uno o più PDV ed è un'entità logica nella quale sono contenuti uno o più documenti, in base a criteri che possono essere definiti con il Produttore/Committente o Responsabile della Conservazione.

torna al sommario

6.4.1 Contenuti dell'indice del PdA (SinCRO)

La soluzione Digibox adottata da Eng è compliant con lo standard UNI 11386 [UNI 11386:2010 - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali (SinCRO)].
All'interno della sottocommissione DIAM/SC11 (Gestione dei documenti archivistici) dell'Ente nazionale italiano di unificazione (UNI), un apposito gruppo di lavoro denominato SInCRO, ha definito la struttura dell'insieme dei dati a supporto del processo di conservazione individuando gli elementi informativi necessari alla creazione di un Indice di Conservazione.
L'implementazione di tale indice, del quale SInCRO ha descritto sia la semantica sia l'articolazione, permette di utilizzare una struttura-dati condivisa e raggiungere un soddisfacente grado d'interoperabilità nei processi di migrazione, mediante l'adozione di uno Schema XML appositamente elaborato. Di seguito lo schema SinCRO implementato.
In aggiunta a quanto previsto dalla normativa, il software prevede alcuni metadati aggiuntivi (non obbligatori) sfruttando il tag MoreInfo.
A livello generale:

- CRL al momento dell'avvenuto versamento
- CRL al momento della chiusura del RdV relativo al documento specifico (come specificato al par. "Costruzione e conservazione del Pacchetto di Archiviazione")
- Certificati-Trusted: vengono inseriti i nomi dei certificati Trusted relativi alle firme presenti nei documenti contenuti nel PdA

A livello di singolo file:

- Informazioni sulle verifiche di firma effettuate (Forza Accettazione / Forza Conservazione)
- Nome e cognome del firmatario (se le verifiche sono attivate e la firma è presente)
- Esiti di verifica firma. Informazioni sulla validità della firma, verifica crittografica, controllo certificato stato della revoca, con riferimento alle CRL reperite nella sezione "Generale", sopra menzionata

Si allega un Indice di esempio:

SInCRO-2472_ITOD
24721510906201131

Si descrive nel capitolo successivo il processo di generazione e la struttura definitiva del PDA .

torna al sommario

6.5 Pacchetto di Distribuzione

Il sistema permette all'utente la ricerca e la visualizzazione degli oggetti conservati.
La visualizzazione avviene tramite un sistema di autenticazione e autorizzazione anche da remoto. L'oggetto che il sistema genera per la consultazione è il Pacchetto di Distribuzione che viene confezionato dal Servizio di Conservazione secondo quanto previsto dalla normativa vigente.
L'accesso ai documenti avviene tramite una serie di servizi webservice esposti dall'applicazione (in modalità sicura) che restituiscono:

- il documento conservato all'interno dell'archivio a norma;
- le prove di conservazione (idPdA);

in particolare il pacchetto di distribuzione relativo ad uno o più documenti è composto da:

- idPdA.xml.p7m (firmato dal RdC)
- idPdA.xml.tsr (marca temporale)
- RdV del (o dei) PdV relativi ai documenti presenti nel PdD
- dati e metadati (collocati su file XML)
- documento o documenti richiesti

Se il Cliente lo richiede può essere effettuata una ricerca massiva con produzione di specifico PDD veicolato al cliente o sotto forma di supporto o tramite canali precedentemente definiti dal Responsabile del Servizio di Conservazione.

torna al sommario

7 Processo di Conservazione

7.1 Descrizione del servizio

Nel seguito una breve descrizione delle caratteristiche principali del servizio di Conservazione a Norma erogato da Eng:

- **Conservazione a Norma dei documenti**: memorizzazione dei documenti informatici inviati dal Cliente su un supporto di cui sia garantita l'integrità e la leggibilità nel tempo secondo le prescrizioni stabilite dalla normativa vigente in materia, con le modalità, nei tempi e limiti definiti contrattualmente. Il servizio comprende la verifica periodica dell'integrità dei documenti, l'eventuale riversamento diretto e le attività necessarie per le ottemperanze fiscali, ove richiesto.
- **Consultazione dei documenti conservati a Norma**: ricerca e visualizzazione dei documenti inviati in conservazione. Tale servizio ed il relativo software di visualizzazione è garantito per il tempo definito contrattualmente per la conservazione a Norma dei documenti.
- **Produzione di supporti dei documenti conservati a Norma**: il servizio consiste nella generazione e invio di supporti fisici a Norma contenenti i Pacchetti di Distribuzione, a seguito di una specifica richiesta del Cliente.
- **Riversamento dei documenti**, su richiesta esplicita del Cliente, secondo quanto stabilito contrattualmente e definito successivamente.

Eng eroga il servizio di Conservazione a Norma (Digibox) utilizzando infrastrutture tecnologiche che soddisfano i requisiti di alta affidabilità richiesti dalla normativa.
Il servizio è erogato su due siti per garantirne la continuità:

Primario: Settimo Torinese (TO) presso il Data Center sito in Viale della Costituzione, 3 – 10036 Settimo Torinese (TO) **Secondario**: Firenze presso il Data Center sito in Via della Toscana, 31 – 50127 Firenze (FI)

Si descrive di seguito il processo di Conservazione. Il processo è in linea con quanto richiesto dalla normativa:

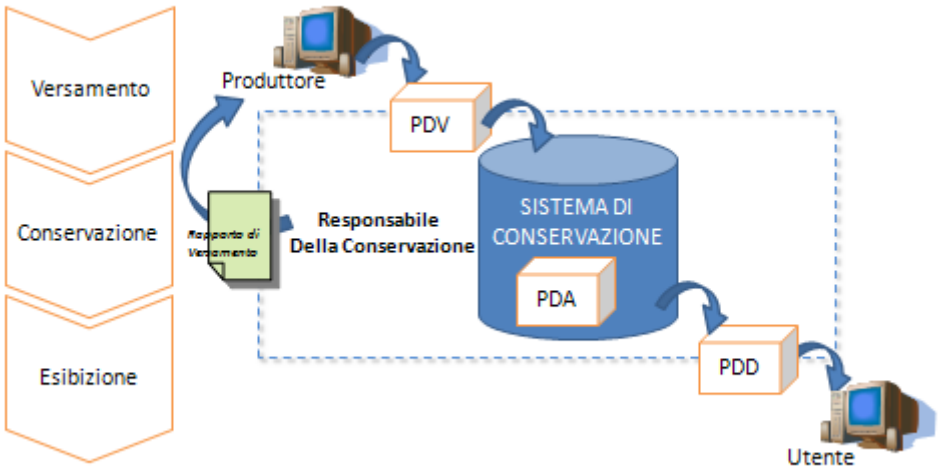

Figura 6 - Processo di Conservazione

torna al sommario

7.2 Attivazione e chiusura del Servizio

Il servizio di Conservazione dei documenti Informatici per ogni Cliente/Famiglia Documentale viene attivato al termine di un processo di configurazione che segue questi fasi fondamentali:

a) condivisione informazioni tecniche di richiesta configurazione PDV: questa fase comprende la definizione di dettaglio dei PDV che il produttore (o Cliente) andrà a produrre ed i controlli che verranno attivati sul sistema di conservazione.
b) consolidamento delle informazioni tecniche propedeutiche all'attivazione del servizio (famiglia documentale, metadati);
c) validazione delle configurazioni da parte del Responsabile del Servizio di Conservazione e del Responsabile sicurezza del Servizio di Conservazione;
d) configurazione ambiente di test;
e) ricezione ed elaborazione Pacchetti di Versamento da conservare in ambiente di Test;
f) configurazione ambiente di produzione e start-up del servizio;
g) canali di comunicazione per la ricezione dei Pacchetti di Versamento e ricezione reportistica periodica.

Ognuna delle fasi sopra indicate viene eseguita per ogni tipologia di configurazione e tipologia documentale richiesta.
Nella fase di attivazione del sevizio vengono definiti canali utilizzati per lo scambio informativo tra Produttore e Conservatore. Tali canali avranno caratteristiche di sicurezza ed identificazione del mittente:

- SFTP
- https
- Certificato lato Client
- Etc etc

Il canale utilizzato e relativi livelli di servizio andranno definiti nell'allegato Specificità del Contratto

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

a) condivisione informazioni tecniche di richiesta cessazione;
b) consolidamento delle informazioni tecniche propedeutiche alla cessazione del servizio, definizione della data formale di Cessazione;
c) notifica della chiusura e delle sue modalità al Responsabile del Servizio di Conservazione;
d) cessazione tecnica;
e) attivazione di un piano di riversamento su richiesta del cliente.

Le modalità di riversamento previste, sono riportate a chiusura del presente capitolo del Manuale.

Nel caso di **dismissione** definitiva dell'erogazione del servizio di Conservazione da parte di Engineering sarà attuato quanto previsto dal "Piano di Cessazione del Servizio di Conservazione a Norma" predisposto dall'ente conservatore.

torna al sommario

7.3 Controlli sulla ricezione dei PdV

La corretta ricezione dei PdV, proveniente dal Produttore/Cliente, è monitorata dal Servizio Sistemistico tramite presidio del canale di comunicazione concordato.
In caso di anomalie il Supporto Operativo prende in carico la segnalazione proveniente dal Servizio Sistemistico, identificando la soluzione ed eventualmente contattando i riferimenti tecnici del cliente.

torna al sommario

7.4 Verifica del Pacchetto di Versamento

Il processo di conservazione dei documenti prevede il mantenimento nel tempo di un insieme di evidenze informatiche (documenti e metadati) contenute nel pacchetto di versamento oltre a quelle generate dal sistema di conservazione (prove di conservazione).
Queste evidenze comprovano l'integrità dei dati e l'autenticità dei documenti firmati digitalmente dal Produttore.
All'atto della ricezione dei documenti contenuti all'interno del PdV, il sistema esegue le seguenti operazioni :

- Controlli pregiudiziali:
  - Verifica presenza dei metadati minimi e di quelli concordati
  - Verifica della correttezza dell'impronta hash del documento ricevuto
  - Verifica che il formato dichiarato dal Produttore sia corrispondente a quanto concordato
  - Verifica della firma digitale su ogni documento.
- Altri controlli:

- specifici relativi alla tipologia di documento da inviare in conservazione.
- possibilità di definire ulteriori controlli che sono concordati con il Cliente in sede contrattuale e definiti nella fase di attivazione del servizio.

Nel caso che uno di questi controlli abbia un esito negativo si genera un'eccezione che può essere gestita come:

- warning: si segnala che c'è una difformità rispetto a quanto atteso ma il processo prosegue nella conservazione.
- error: l'esito ha generato uno blocco del processo per lo specifico pacchetto/documento e necessità di un intervento da parte del Supporto Operativo (p.e. il controllo dell'hash è bloccante).

Eseguiti i controlli pregiudiziali ha inizio la fase di versamento.

Le operazioni di versamento, come tutte le operazioni di rilievo normativo, vengono tracciate in specifici log applicativi, su tabelle del database ovvero su file system, a seconda della tipologia delle informazioni ivi contenute.
I log memorizzati su database vengono mantenuti online per tutta la durata del periodo di conservazione, mentre quelli su file system vengono opportunamente suddivisi per mese / anno per una maggior facilità di consultazione (come descritto nel piano di sicurezza).

Esempio di log delle operazioni riguardanti le interazioni con l'esterno (con documenti esito negativo per doppia chiave primaria):

ID	Data	Operazione	User	Ruolo	ID oggetto	Cliente	Chiave logica	Esito
713308	13/07/2017 22:16	CENSIMENTO	usr_vers	Versatore	450451	Cliente 1	CONS201707120151000	OK
768392	13/07/2017 23:11	VERSAMENTO	usr_vers	Versatore	238737049	Cliente 2	3960620170712CAMVA111145330	OK
1107672	30/06/2017 17:18	RECUPERO	usr_recupero	Versatore				KO
1107660	30/06/2017 11:46	RECUPERO	usr_recupero	Recuperatore	231196691	Cliente 3	15_2016_File79	OK

torna al sommario

7.5 Accettazione o Rifiuto del PdV

Qualora i controlli precedentemente descritti sui documenti ricevuti abbiano dato **esito positivo**, il sistema:

- memorizza i documenti nella propria base dati di lavoro e sono disponibili per essere inseriti in un PdA.
- predispone i dati per produzione degli esiti di avvenuta presa in carico del PDV e dei singoli documento (Rapporto di Versamento).
- procede alla costruzione del PdA conformemente alle regole specifiche per la tipologia di documento e Cliente.

Nel caso in cui venga rilevato un **esito negativo** di uno dei controlli sui documenti ricevuti, il sistema può procedere un tre differenti modalità:

1. Accettazione parziale del PdV: se "esito negativo" ha gravita "ERRORE" si rifiuta il documento e si segnala nel RdV l'impossibilità di conservare il documento e se ne tiene traccia nel RdV.

2. Accettazione dell'intero PdV: se "esito negativo" ha gravita "WARNING" si accetta l'intero contenuto del PdV e si tiene traccia del warning nei log Applicativi.
3. Rifiuto del PdV: se tutti i records contenuti nel PdV generano errore, oppure il PdV non risulta elaborabile (p.e. problemi di integrità) si rifiuta l'intero PdV e si genera un esito di ricezione con stato KO.

Nel terzo caso il mittente/cliente concorda con il Responsabile del Servizio di Conservazione una modalità per sanare l'errore. Le verifiche e controlli eseguiti vengono tracciati nel log applicativi che per loro natura conservano un riferimento temporale.

torna al sommario

7.6 Rapporto di Versamento (RdV)

E' un file XML generato in modo automatico alla chiusura della fase di controllo ed è relativo ad uno o più pacchetti di versamento, univocamente identificato dal sistema di conservazione e contenente un riferimento temporale, specificato con riferimento al Tempo universale coordinato (UTC) e l' impronta relativa al PdV (o ai PdV) oltre alle chiavi univoche dei documenti eventualmente rifiutati.

Su tale XML si appone firma e marca temporale che avviene contestualmente alla sua creazione ed attesta il contenuto del PdV e l'istante in cui vengono terminate le attività di verifica.

Esempio di rapporto di versamento

```
<RDV id="351">
 <DataGenerazione>06072017</DataGenerazione>
 <PacchettiDiVersamento>
  <PDV>
   <NomePacchetto>CONS201706222xxxx.zip</NomePacchetto>
   <DataVersamento>06072017</DataVersamento>
   <Canale>FLUSSO</Canale>
   <DocumentiVersati>887</DocumentiVersati>
   <ElementiPDV>
    <ElementoPDV id="8276158" tipo="IDX_STD">
     <URN>AziendaCliente:Paperless:2500:448530:INDICE.xml</URN>
     <Hash algoritmo="SHA-256" codifica="B64">kS09eBJW5HMuYzqJCLQbVO/v5PMBfUW/yYcVA2s61dI=</Hash>
     <Path>
      S3://000001/2500/001/PDV/CONS201706222500000-INDICE.xml
     </Path>
    </ElementoPDV>
    <ElementoPDV id="8276160" tipo="IDX_CLI">
     <URN>
      AziendaCliente:Paperless:2500:448530:INDICE-CLIENTE.xml
     </URN>
     <Hash algoritmo="SHA-256" codifica="B64">RwgkIZ3FltYAyhxyCQBiAwji0nEnIBfa2oykX29Pbkg=</Hash>
     <Path>
      S3://000001/2500/001/PDV/CONS201706222500000-INDICE-CLIENTE.xml
     </Path>
    </ElementoPDV>
   </ElementiPDV>
   <Motivazione/>
  </PDV>
 </PacchettiDiVersamento>
</RDV>
```

Il Rapporto di Versamento viene conservato, memorizzato su DB e legato ai documenti che sono oggetto dei PDV a cui si riferisce. Sarà possibile risalire al RdV dal singolo documento ricercato.

Il sistema provvede ad un primo reperimento delle CRL di tutti i certificati TRUSTED corrispondenti ai certificati di firma al momento dei controlli che vengono eseguiti sul pacchetto di versamento. Avremo quindi tante CRL quanti sono le autorità di certificazione riconducibili alle firme presenti sui documenti.

Le seconde CRL vengono invece reperita per consolidare la fase di costruzione del Rapporto di Versamento con l'assoluta certezza della validità dei certificati delle firme dei documenti ricevuti.

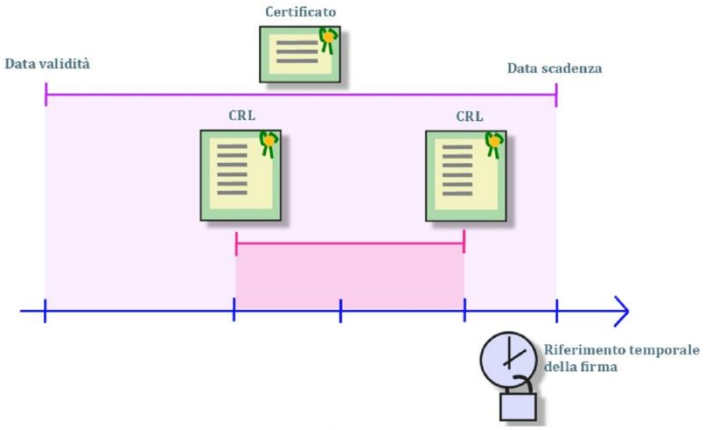

Figura 7 - Controllo CRL

torna al sommario

7.7 Costruzione e conservazione del Pacchetto di Archiviazione

Superate le fasi di controllo sui PDV e generazione del RdV il sistema abilita l'esecuzione di una serie di regola che permettono la formazione del PDA; tali regole sono completamente configurabili e riguardano ad esempio:

- Dimensione del semilavorato (che formerà il pacchetto)
- Anzianità del documento (dal tempo si ingresso nel sistema)
- Firmato o non firmato (o certificato di firma in scadenza)
- Regole basate su specifici metadati (codice fiscale, mittente,… altro)
- PdA coincidenti con un PdV ricevuto

Opportuni allarmi segnalano la presenza di documenti che sono in attesa di conservazione e non vengono inclusi in nessuna regola di costruzione PdA.

Definendo, eventualmente nuove regole di costruzione del PdA viene attivato un nuovo processo di costruzione del PDA, per eventuali documenti che precedentemente non sono stati inclusi in nessun range di regole, L'inserimento di nuove regole è tracciato nei file di log del sistema.
I documenti così lavorati e che hanno superato le fasi precedenti, concorrono a formare il Pacchetto di Archiviazione, che è assemblato dal sistema nei tempi e con i criteri di raggruppamento scelti e concordati in fase di attivazione del servizio di conservazione.

Il Pacchetto di Archiviazione si forma contestualmente alla creazione del suo indice; il processo è descritto nei punti seguenti:

a) Creazione di dell'indice xml (in formato Sincro) relativo al blocco di documenti da inviare in conservazione.
b) Reperimento delle prove di conservazione (certificati trusted delle firme dei documenti, CRL dei certificati scaricate per costruzione RdV) per la totalità dei documenti firmati presenti nel Pacchetto, che verranno inserite nel "more info" dell'indice.
c) Sottoscrizione dell'indice xml (in formato Sincro) con firma digitale del Responsabile del servizio di Conservazione e successiva apposizione di una marca temporale per fornire data certa al Pacchetto di Archiviazione.

Al termine di queste fasi è formato il PdA che è costituito da un insieme di file comprovanti la autenticità dei documenti in conservazione (vedi schema riportato nel paragrafo specifico).
L'indice del PDA è strutturato secondo lo standard e contiene:

- Info varie previste dallo standard Sincro
- Per ogni documento:
  - Hash
  - Urn
  - Nel campo "more info": le CRL relative al documento e l'esito dei controlli effettuati.
  - Riferimento al RdV

La conservazione dei documenti digitali vera e propria ha inizio con la formazione del PdA e la costruzione dell'indice.
Una volta terminata la raccolta delle prove, queste vengono associate ai documenti conservati. A questo punto il sistema provvede a creare l'indice Sincro, sottoscriverlo ed apporre il timestamp definitivo di conservazione

Parte integrante di questo processo è la sottoscrizione digitale dell'Indice (Sincro) da parte del Responsabile del servizio di Conservazione. In questa fase è inclusa anche l'apposizione di un "time-stamp", ovvero un riferimento temporale certificato che costituisce evidenza dell'esistenza e dell'esatta composizione del file collegato all'istante indicato.
Apponendo un time stamp all'indice lo si "sigilla" e contemporaneamente si fissa il riferimento temporale.
Con questo procedimento, dunque, si viene a costituire un riferimento temporale certificato per ognuno dei file inclusi nel PdA.

In conclusione di tale processo abbiamo il PDA così costituito:

- idPdA.xml.p7m (firmato dal RdC)
- idPdA.xml.tsr (marca temporale)
- dati e metadati
- documento o documenti di cui l'indice idPdA

torna al sommario

7.8 Processo di Esibizione tramite Pacchetto di Distribuzione

L'esibizione dei documenti avviene tramite autenticazione.
L'utente può richiedere al sistema di conservazione l'accesso ai documenti per acquisire le informazioni di interesse nei limiti previsti dalla legge. Tali informazioni vengono fornite ai soggetti autorizzati tramite l'accesso diretto, anche da remoto, al documento informatico conservato, attraverso la produzione di un pacchetto di distribuzione selettivo tramite specifica ricerca nel sistema di Conservazione a Norma.
Per quanto riguarda l'attività di ricerca e l'esibizione a norma dei documenti conservati (anche a fronte di una verifica ispettiva da parte delle Autorità competenti) lo strumento di accesso all'archivio documentale a norma del Cliente è consentito dal servizio webservice esposto dall'applicazione e sottoposto ad autenticazione ed autorizzazione. Il Cliente, autenticato ed autorizzato, tramite l'interfaccia messa a disposizione, può pertanto richiedere la visualizzazione di tutti i documenti conservati al fine di :

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

Il sistema di Conservazione a Norma può essere anche integrato con il sistema Documentale o altra applicazione del cliente per facilitare la fruizione del servizio di consultazione.
Se il Cliente lo richiede può essere effettuata una ricerca massiva con produzione di specifico PDD veicolato al cliente o sotto forma di supporto o tramite canali precedentemente definiti.

Il Pacchetto di distribuzione relativo ad un PdA risulta quindi composto da:

- idPdA.xml.p7m (formato dal RdC)
- idPdA.xml.tsr (marca temporale)
- dati e metadati (collocati su file di testo)
- documento o documenti di cui l'indice idPdA (in sequenza)
- RdV (relativo ai documenti contenuti nel PdA)

Il sistema di conservazione documentale è soggetto a meccanismi di protezione dei dati che transitano in rete, in modo da impedire accessi fraudolenti o non autorizzati. Tale protezione è realizzata mediante apparati di sicurezza che analizzano il traffico e su base di specifiche regole di abilitazione viene consentito il flusso di dati strettamente necessario al funzionamento dell'applicazione.

torna al sommario

7.9 Veicolazione dei PdD e Gestione dei supporti rimovibili

Il servizio di conservazione è organizzato per conservare i blocchi o PDA completi su repository informatici on-line disponibili nel centro dati di Eng. L'applicazione Digibox consente la produzione di PDD che possono essere forniti al Cliente tramite opportuni canali sicuri.
Può essere anche definita una modalità sicura di scambio di supporti removibili a partire da uno o più PDD e le modalità vengono concordate con il cliente e riportate negli allegati contrattuali; il supporto viene generato su richiesta del cliente e sotto la supervisione del Responsabile del servizio di Conservazione.

Se necessario, può essere applicato un meccanismo di crittografia per mettere in sicurezza la delivery del supporto removibile.
In ogni supporto vengono riversati dei pacchetti di distribuzione (PdD), uno per ogni PDA e contenenti sia gli oggetti che l'insieme delle evidenze di conservazione.

torna al sommario

7.10 Interoperabilità: cessione o acquisizione documenti da altro conservatore

Per interoperabilità si intende la capacità di cedere o acquisire copie o duplicati dei documenti conservati, da un supporto ad un altro senza che ciò comporti una alterazione del contenuto digitale dei medesimi e del valore degli stessi.
Tale procedimento verrà eseguito sotto la responsabilità del responsabile del servizio e verrà concordato con il Responsabile della Conservazione (del Cliente) dei documenti oggetto di "travaso".

Viene eseguita normalmente su richiesta del Cliente e si effettua mediante generazione dell'ISO oppure altro metodo da definire con il Cliente (ed eventualmente con l'altro Conservatore).

Se nel processo di acquisizione risultasse necessario una "trasformazione" dei documenti o dei PdA forniti, sarà necessario effettuare una copia dei documenti conservati da un supporto ad un altro con una alterazione del contenuto digitale dei medesimi. Questa è una attività ammessa dalla normativa, nel caso in cui si voglia ad esempio aggiornare tecnologicamente l'archivio sostitutivo per garantire la possibilità di esibizione della documentazione a fronte di innovazioni tecnologiche. In questo caso potrebbe essere necessaria l'apposizione di una ulteriore firma digitale, o l'attestazione di conformità all'archivio esistente da parte di Pubblico Ufficiale che viene coinvolto dal Responsabile della Conservazione (del Cliente) o del Servizio di Conservazione.

Il coinvolgimento di un Pubblico Ufficiale esperto in processi di conservazione può essere richiesto al fine di:

a) validare il piano di acquisizione o cessione
b) verificare che il processo di trasformazione del formato dei documenti non alteri il contenuto e la forma dei documenti stessi;
c) validare il processo di apposizione delle firme digitali sui documenti acquisiti in conformità con le normative vigenti;

Per procedere all'acquisizione di documenti che risiedono presso altro conservatore, tramite un "travaso massivo" sia di copie che di duplicati informatici sarà necessario definire una mappatura dei dati o metadati forniti dal conservatore cedente ed acquisiti dal nuovo conservatore.
La procedura di import prevede:

- la costruzione di nuovi PdA a partire dai PdD forniti dal cedente
- il popolamento della base dati dei metadati a partire dal db export dati del cedente.

La procedura prevede una fase di quadratura pre e post migrazione, sotto la supervisione del Responsabile del servizio.

torna al sommario

7.11 Scarto del pacchetto di Archiviazione

Alla scadenza dei termini di conservazione relativi alla specifica tipologia documentale e comunque definiti in sede contrattuale con il Cliente, avviene lo scarto del Pacchetto di Archiviazione dal sistema di conservazione a norma.
Per dare la possibilità di poter prolungare i termini di conservazione prima dello scarto, verrà data informativa al produttore con congruo anticipo (almeno 6 mesi) al fine di confermare la cancellazione ovvero mantenere in conservazione i PdA per un ulteriore anno.
Il Responsabile delle Conservazione del produttore ha la possibilità di richiedere lo scarto di tutti o alcuni i PdA segnalati dal sistema, tramite approvazione con propria firma digitale.

La cancellazione avverrà soltanto dopo che sono state eseguite le fasi di approvazione esplicita da parte del RdC.

torna al sommario

7.12 Conservazione documenti Pregressi

Il sistema permette la gestione di archivi di documenti conservati secondo la normativa precedente al DPCM del 3 Dicembre 2013.
In questo caso sarà possibile eseguire su tutti questi documenti le analoghe funzioni sopra descritte con l'eccezione del fatto che l'indice del PdA (indice del blocco) non avrà un formato Sincro ma conterrà comunque le evidenze di conservazione previste dalla normativa pre 2013.

torna al sommario

8 Il Sistema di Conservazione

8.1 Applicativo di Conservazione

Il sistema software utilizzato per la gestione del processo di conservazione legale dei documenti digitali è costituito da un prodotto SW (Digibox) di Eng, interamente (ed internamente) realizzato e manutenuto.
E' un sistema integrato e completo per la conservazione a norma dei documenti informatici ed è realizzato per "lavorare" su un sistema di storage ad oggetti, una tecnologia appositamente introdotta per questa tipologia di servizio.

Il pacchetto software esegue la conservazione nel tempo dei documenti informatici e presenta le seguenti caratteristiche generali:

- Completezza - presenza di qualsiasi documento emesso
- Robustezza - garanzia di consistenza dei dati inseriti
- Sicurezza - protezione dalla manipolazione non autorizzata dei dati
- Affidabilità - indipendenza dai guasti dell'hardware
- Chiarezza - facilità di consultazione secondo diversi criteri di ricerca

garantendo:

- la completezza e l'inalterabilità dei documenti inviati in conservazione
- la possibilità di verifica dell'integrità dei documenti conservati
- i riferimenti temporali certi.

Inoltre è in grado di gestire diverse tipologie di documenti, relativi a diversi ambiti applicativi, e diversi formati, per esempio:

- Documenti di sportello bancario
- Contratti ed allegati
- Fatture attive e Fatture passive
- Libri e registri sociali
- Libri e registri contabili
- Libri e registri assicurativi
- Assegni
- Mandati di pagamento e Reversali d'incasso
- Ricevute e quietanze di pagamento
- Delibere, determine, atti e provvedimenti
- Altro..

Ognuna di queste tipologie è caratterizzata da specifici metadati e apposite regole, definibili in modo parametrico, che consentono di gestire insiemi di documenti omogenei.

Il sistema è progettato per partizionare in maniera opportuna i dati gestiti al fine di garantire la separazione per contesto organizzativo o utente.
Il partizionamento opera tra i dati di Aziende diverse o di diversi dipartimenti o uffici afferenti ad una stessa Azienda I fascicoli e documenti, provenienti anche da flussi diversi di conservazione, identificati univocamente tramite una chiave primaria, fin dal loro ingresso in conservazione.

Il sistema di partizionamento è direttamente collegato al sistema di controllo degli accessi e tracciatura, viene quindi garantita la riservatezza dei dati presenti in archivio.

Tutti i documenti sono disponibili on-line, congiuntamente alle rispettive prove di conservazione, per le funzioni di ricerca ed esibizione, così come previsto dalla normativa vigente. La struttura architetturale del prodotto consente di definire diversi livelli operativi e garantisce che ciascuna Azienda/Ente, Area Organizzativa, Agenzia, Ufficio, Dipartimento, ecc. possa accedere solo ed esclusivamente ai suoi documenti, in base alle credenziali e alle politiche di accesso attivate.
Il pacchetto software prevede la conservazione singola e/o cumulativa, dei documenti elettronici firmati ed implementa un formato di composizione delle marche tale da permettere l'esibizione probatoria di un singolo documento.
Ogni singolo file può essere esibito insieme ai suoi metadati, registrati nel data base, e alle sue prove di conservazione in maniera assolutamente INDIPENDENTE dagli altri documenti. Infatti, nei file contenenti le prove di conservazione l'unico riferimento ai file originali è l'hash del documento stesso, che non ha quindi nessun vincolo di riservatezza.

torna al sommario

8.2 Componenti Logiche

L'applicazione è logicamente divisibile in 3 principali gruppi:

- Versamento
- Conservazione
- Verifiche e allarmi
- Esibizione
- Console di Gestione

Versamento

La parte di versamento è in grado di ricevere i documenti tramite 2 principali modalità :

- Versamento massivo tramite flussi di documenti
- Versamento singolo, tramite WebService

Si occupa di effettuare le verifiche iniziali e la creazione del RdV (verifica del formato, firma etc) e di recupero da internet delle CRL.

Conservazione

E' la parte che si occupa di tutti i processi di conservazione, in particolare

- Verifica dei documenti ai fini della conservazione: ricalcolo e confronto hash, verifiche di firma, etc.
- Reperimento e verifica delle prove di conservazione: controllo catena trusted, CRL, etc.
- Creazione PdA
- Firma del RdC
- Apposizione marche temporali

Verifiche e allarmi

Tramite questa componente si rende possibile l'assoluta coerenza del sistema e di tutti i suoi processi. Un sistema di allarmi provvede infatti ad informare tempestivamente il personale

addetto al presidio dell'eventuale presenza di un problema, o più semplicemente di un ritardo nelle fasi elaborative. Gli allarmi sono configurabili in base a diversi parametri e per ciascuna fase elaborativa. Gli allarmi arrivano per e-mail e contengono:

- Nel Subject: una breve descrizione del problema e della sua gravità
- Nel body: possono contenere il dettaglio del problema rilevato

Alcuni esempi di allarmi

- Presenza di documenti non conservati ad una certa ora. Questo allarme scatta nel caso in cui, ad una certa ora, almeno un documento non abbia raggiunto lo stato di "conservato". Nel subject della mail è presente una sintesi del problema (ad esempio: presenza di 2 documenti non conservati). Nel body della mail troviamo l'elenco di tutti i documenti, per un veloce riscontro
- Documenti di un determinato Cliente non pervenuti. Ad esempio, nel caso in cui un Cliente spedisca i suoi documenti sempre ad una determinata ora oppure entro un cut-off, questo allarme è utile ad individuare un eventuale problema nella spedizione dei documenti e induce il personale di presidio a verificare eventuali problemi di connettività o di file transfer

Esibizione

La parte di esibizione di occupa di garantire il reperimento dei documenti conservati e delle prove della loro conservazione nel tempo. L'esibizione può essere richiesta in 3 diverse modalità:

- WebService; tipicamente tramite un applicativo, che fa richiesta del documento e/o delle sue prove di conservazione
- Interfaccia WEB. L'utente può direttamente ricercare e scaricare file e prove di conservazione
- Supporti. Su richiesta del Cliente, è possibile la creazione di supporti digitali contenenti una selezione di documenti con le relative prove di conservazione

Console di Gestione

La console di gestione è l'applicativo web che consente di supervisionare tutte le funzionalità dell'applicazione ed è suddivisa in due grandi filoni

- Gestione applicativo
- Interrogazione contenuti

Gestione applicativo

La gestione dell'applicativo consente la configurazione e la gestione dei task, ovvero:

- Censimento e manutenzione delle tipologie documentali, metadati etc.
- Configurazione utenti, Clienti e loro abilitazioni e personalizzazioni
- Configurazione parametri generali dell'applicazione
- Gestione dei task, monitoraggio del sistema, stop / start dei servizi e dei singoli task

Interrogazione contenuti

La parte di interrogazione contenuti consente una piena navigabilità, con parametri di ricerca predefiniti e rende possibile la ricerca di documenti e files conservati, l'interrogazione ed il download dei documenti e delle loro prove di conservazione.

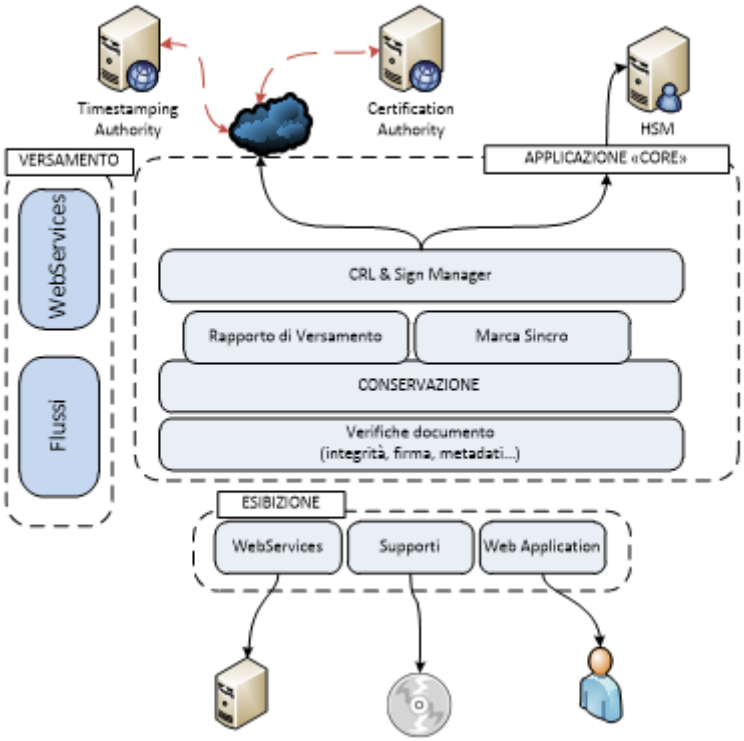

Figura 8: schema logico applicazione

torna al sommario

8.3 Componenti Tecnologiche

L'applicazione di conservazione è una applicazione Web a tre livelli (desktop, application e database) e utilizzabile da posti di lavoro dotati di sistema operativo Windows (XP, Vista o 7) o Linux, per mezzo di browser standard quali ad esempio Internet Explorer, Mozilla Firefox, Google Chrome, Apple Safari. Per le postazioni che dovranno operare sulle funzionalità di firma è necessario che localmente siano attivi i driver del dispositivo di firma (lettore, smart card o token USB di firma, tablet per la firma grafometrica, ecc.), oppure che sia utilizzato un dispositivo HSM (Hardware Security Module) raggiungibile via rete.

Tutte le componenti applicative del sistema poggiano su una piattaforma architetturale uniforme:

- Java J2EE
- Framework ORM Hibernate
- Architettura SOA
- RDBMS

- Application server Wildfly 10+
- HCP (Hitachi Content Platform)

La base dati utilizzata è un data base relazionale interfacciata attraverso Hibernate e supporta Oracle RAC 11g Enterprise Edition.

Il bilanciamento applicativo è effettuato tramite Message Queue JMS (Active MQ).

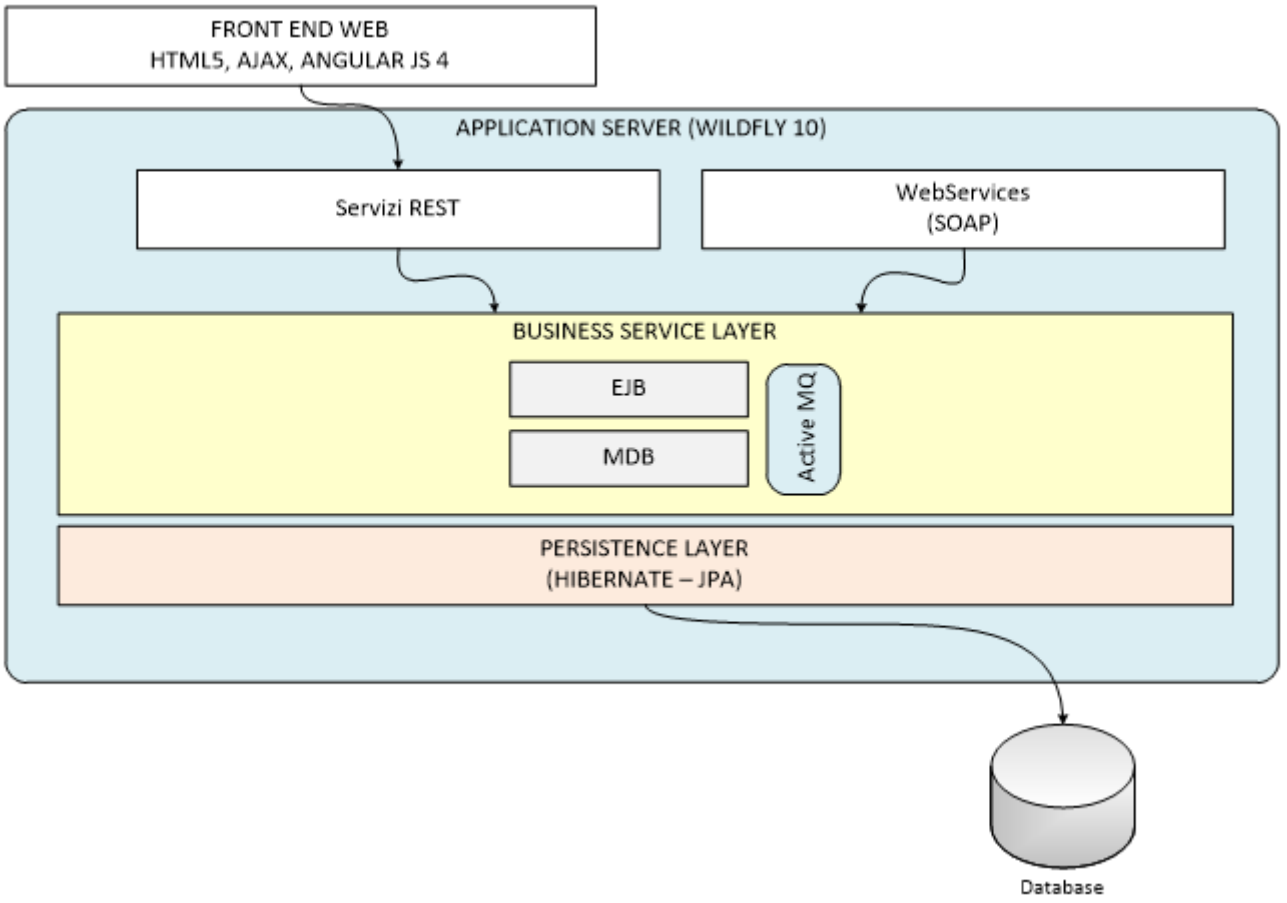

Figura 9: framework applicativo

torna al sommario

8.4 Componenti Fisiche

Eng eroga i servizi all'interno dei propri Data Center primario e secondario, attraverso i quali è in grado di offrire un servizio di alta qualità in termini di continuità ed affidabilità. Tale qualità è ottenuta grazie alle caratteristiche progettuali che hanno contraddistinto la realizzazione dei Data Center, con criteri focalizzati sempre sull'obiettivo di fornire ad ogni livello le massime garanzie di sicurezza e continuità, sia per quanto riguarda l'erogazione di energia elettrica, sia attraverso un opportuno condizionamento climatico, sia attraverso un adeguato meccanismo di sicurezza fisica (impianto antincendio e sorveglianza con allarmi 24x7), sia attraverso la ridondanza architetturale dei sistemi, delle infrastrutture di rete e delle connessioni verso l'esterno.

I criteri progettuali e realizzativi dei Datacenter Eng rispondono ai requisiti imposti ai datacenter di livello T4, livello massimo previsto dallo standard Uptime Institute Tier Standard.
Di seguito si riportano le principali caratteristiche dei Data Center Eng:

- Ambiente protetto con accesso garantito solo al personale autorizzato;
- Linee elettriche doppie provenienti da rami diversi (doppia cabina elettrica, doppio G.E., doppi UPS);
- Sistema di raffreddamento ridondato;
- UPS ridondati e monitorati;
- Sistema per la rilevazione fumi e lo spegnimento incendi automatico;
- Pavimento flottante e canalizzazioni separate per l'impianto elettrico e cablaggio dati;

Le principali caratteristiche delle architetture deputate alla erogazione dei servizi sono riportate, invece, qui sotto:

- Architettura di switching layer 3 completamente ridondata con connessioni a 1Gbit/s o superiori;
- Sistemi Firewall ridondati, in diverse tecnologie;
- Storage Area Network centralizzata e ridondata con doppio fabric;
- Storage di classe Enterprise;
- Sistemi di RDBMS ridondati (principali fornitori di mercato);
- Backup Centralizzato attraverso LAN dedicata ad 1Gbit/s e via SAN;
- Sistema di Monitoring dello stato della rete, dei sistemi e dei servizi;
- Connessioni ad Internet tramite linee di differenti Carrier;
- Completa remotizzazione dei sistemi di amministrazione.

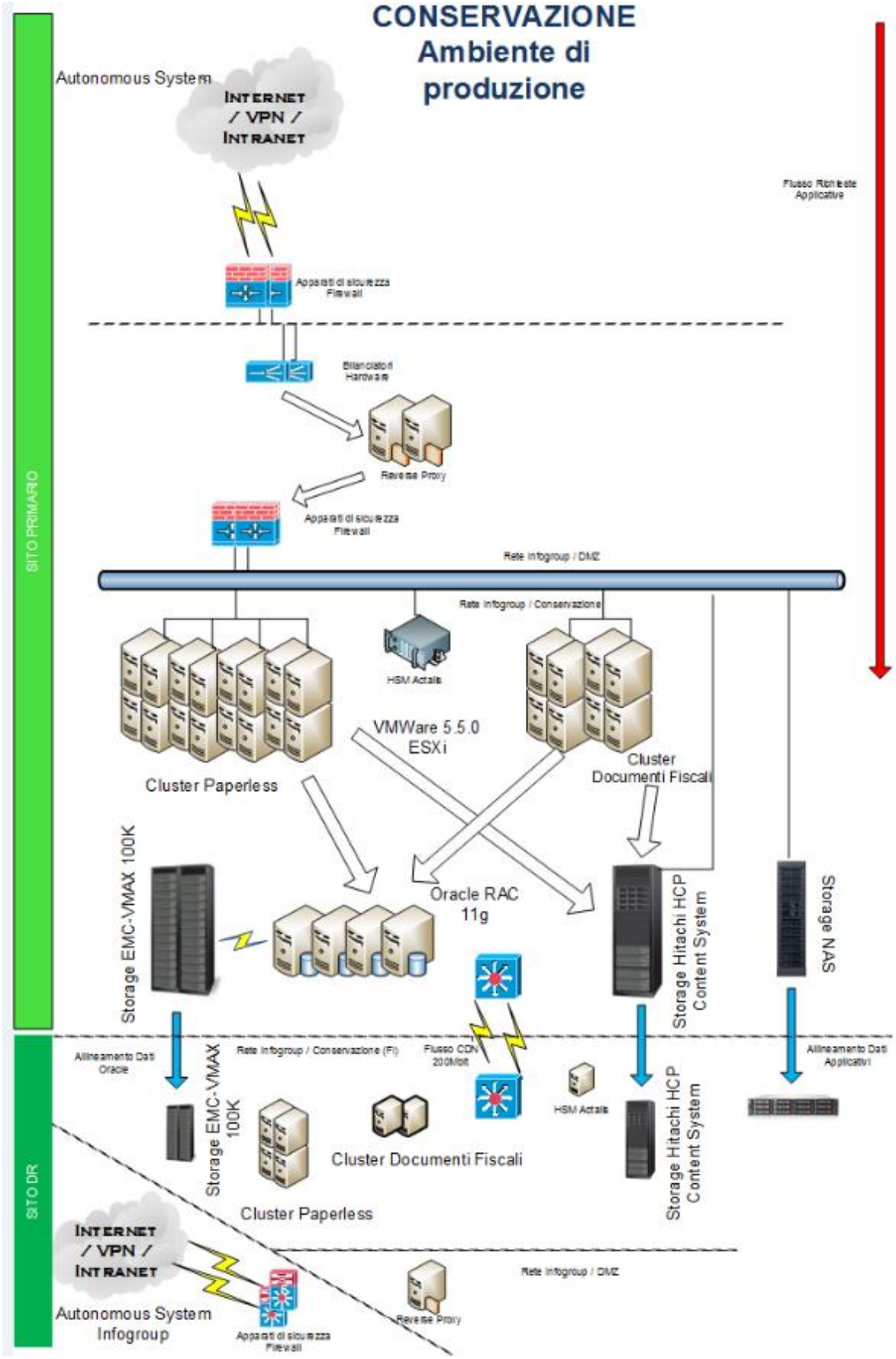

Figura 10 Schema infrastruttura

8.5 Procedure di Gestione e di Evoluzione

L'erogazione del servizio è regolata dalle procedure di "ciclo di vita di una infrastruttura" e "ciclo di vita del SW".

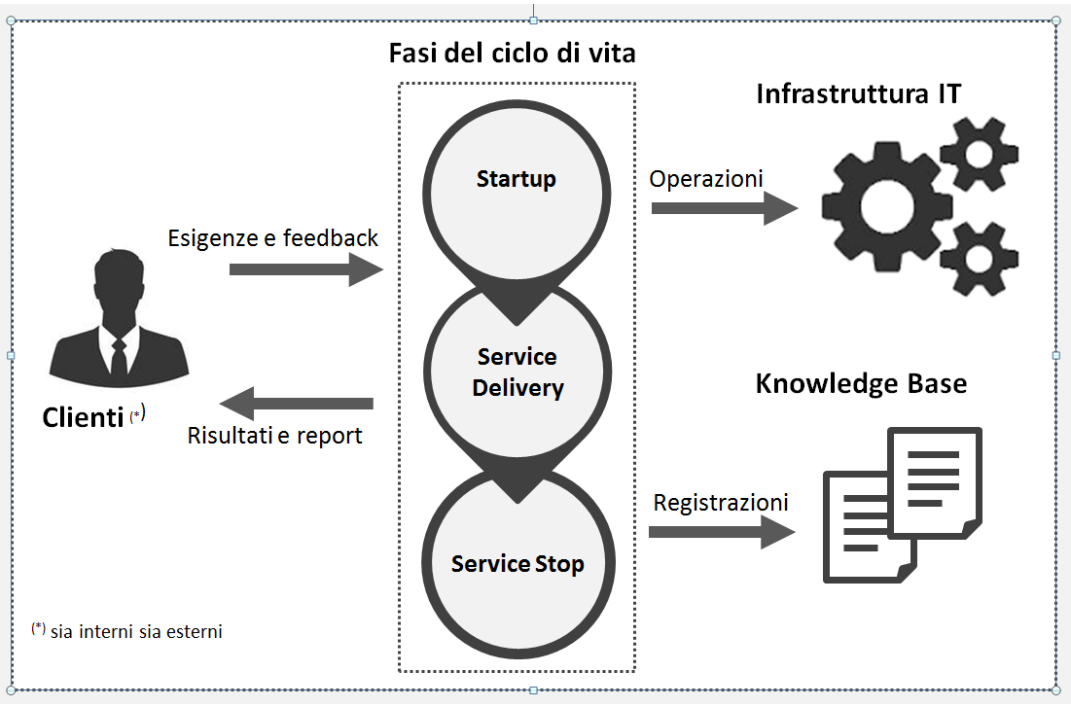

Figura 11 - ciclo di vita del Servizio

Le procedure che regolano la gestione e l'evoluzione sono legate alla fase di Service delivery.
Nella fase Service Delivery:

- è assicurato il funzionamento del software, seguendo quanto dettato nei processi Incident Management, Change Management e Request Management,
- il software è allineato alle variazioni delle esigenze dei Clienti, seguendo quanto dettato nei processi Customer Relation Management e Change Management,
- sono individuate e messe in atto le azioni preventive e migliorative pertinenti il software, seguendo quanto dettato dai processi Review Management e Change Management.

La procedura centrale del processo di gestione è quella di Change management; queste richieste di change possono scaturire:

- da nuove esigenze dei Clienti,
- da una azione, migliorativa o preventiva, decisa in sede di review del software,
- per un workaround o per eliminarne le cause di un difetto del software.

Le richieste di change possono essere attivate dal Service Manager. Maggiori dettagli si trovano nelle procedure aziendali.

torna al sommario

9 MONITORAGGIO E CONTROLLI

La normativa che disciplina il processo di conservazione dei documenti informatici prevede un alto livello di sicurezza per quanto riguarda le policy di archiviazione e accessibilità dei documenti conservati. I Dettagli sono riportati nel Piano di Sicurezza.

torna al sommario

9.1 Tracciabilità delle operazioni

Un apposito servizio centralizza i files di log di tutte le componenti HW e applicative; La sincronizzazione di tutti i sistemi sul tempo campione proveniente dalla fonte esterna prevista dalla legge consente la ricostruzione della corretta sequenzialità di accadimento delle operazioni registrate nei file di log.
Eng implementa un SIEM (Security Information and Event Management) basato su tecnologia McAfee per la gestione dei log provenienti da sistemi, apparati di rete e Firewall. Il sistema si compone di numero tre elementi: Event Receiver Collector, LogManager, Enterprise Security Manager.
I tre moduli svolgono compiti distinti, in particolare:

- Event Receiver Collector (ERC): McAfee Event Receiver raccoglie eventi e log di terze parti più velocemente e con maggiore affidabilità di ogni altra soluzione, utilizzando un sistema integrato di raccolta dei flussi di rete.
- LogManager (ELM): McAfee Enterprise Log Manager consente la gestione automatizzata e l'analisi di log di tutti i tipi, come i log degli eventi di Windows, dei database, delle applicazioni e di sistema. I log sono firmati e convalidati per garantire autenticità e integrità: un requisito per la conformità alla normativa e di valore legale. I set predefiniti di regole per la conformità e la reportistica semplificano la dimostrazione del rispetto della conformità e dell'esecuzione delle policy da parte dell'azienda.
- Enterprise Security Manager (ESM) : McAfee Enterprise Security Manager fornisce i contesti in modo veloce e approfondito per identificare le minacce critiche, agire rapidamente e rispondere in modo semplice ai requisiti di conformità. L'aggiornamento continuo sulle minacce globali e sui rischi aziendali consente una gestione dei rischi adattiva e autonoma, rendendo disponibili le risposte alle minacce e la reportistica per le questioni di conformità nell'ordine di minuti anziché di ore.

L'azione sinergica delle tre componenti permette di procedere alla raccolta dei log, la loro correlazione e analisi nonché la storicizzazione e la retention nel rispetto delle normative attuali.
Questo servizio permette anche l'identificazione di condizioni di allarme in corrispondenza delle quali si attivano specifiche azioni fra cui anche l'apertura di trouble ticket gestiti dalla piattaforma o tramite mail verso l'ufficio sicurezza Eng e l'ufficio Sistemi Eng.

torna al sommario

9.2 Monitoraggio dell'applicazione

Tutte le componenti hardware, i sistemi operativi e le applicazioni sono sottoposte a continuo monitoraggio da parte del personale sistemistico Eng. Questo monitoraggio permette di rilevare componenti non funzionanti, degradate o sature.

Il monitoraggio di queste due ultime condizioni (degradazione e saturazione delle risorse) consente di prevenire fenomeni bloccanti e limitare i disservizi derivanti. Inoltre monitorare queste condizioni consente di pianificare eventuali upgrade o modifiche dell'architettura.

La struttura di monitoraggio ha due tipologie di controlli:

- Sistemistici (utilizzo risorse, controllo accessi, ……)
- Applicativi (sonde su servizi dummy, quadrature, monitoraggio picchi elaborativi, ….)

I livelli di servizio sono regolati da SLA definite con il cliente i cui KPI sono monitorati e verificati periodicamente.

torna al sommario

9.3 Controlli periodici di integrità

I controlli periodici di integrità dei documenti conservati sono pianificati dal Responsabile del servizio di Conservazione, tenendo conto dello stato e dell'importanza dei processi e delle aree oggetto di verifica, nonché dei risultati delle precedenti verifiche. La frequenza con la quale vengono disposti i controlli di integrità è almeno biennale. Periodicamente viene predisposto il relativo report di verifica.
La scelta del personale verificatore viene fatta in modo da garantire obiettività ed imparzialità nel processo di verifica.
Di seguito le tipologie di verifiche attuate nel processo di controllo di integrità:

- verifiche periodiche sullo stato di conservazione dei supporti di memorizzazione, tendenti a verificare con l'ausilio di software appropriati, lo stato di conservazione dei supporti di memorizzazione e a ricercare eventuali difetti, provvedendo, se necessario, al riversamento diretto o sostitutivo del contenuto dei supporti.
- verifiche periodiche sui documenti conservati, tendenti a verificare periodicamente, con cadenza non superiore a cinque anni, l'effettiva integrità dei documenti stessi, provvedendo, se necessario, al loro riversamento. La procedura che gestisce il processo di conservazione presenta delle funzionalità di controllo massivo dei dati conservati: questi controlli consistono nell'impostare a livello informatico la periodicità dei controlli da effettuare; attualmente, il sistema è configurato per verificare giornalmente un milione di documenti, eseguendo ogni giorno i controlli a rotazione su documenti diversi. L'applicazione che gestisce il processo di conservazione, effettua un check automatico registrando per ogni PdA/documento conservato, la data e ora in cui è stata eseguita l'ultima verifica di integrità. Nel caso siano verificate delle anomalie viene aperto un incident al fine di recuperare il dato dalle copie di sicurezza.

verifiche di leggibilità dei documenti in conservazione da parte di operatori (human readability) possono essere eseguite a richiesta del Committente, tramite apertura di un campione pseudocasuale statistico dei documenti. I dati rilevati, relativamente al numero di documenti verificati ed agli eventuali risultati negativi, saranno inseriti in apposito report inviato al committente. La cadenza dei controlli e le dimensioni del campione da considerare sono da definire a livello contrattuale

torna al sommario

9.4 Soluzioni adottate in caso di Anomalie

Il presentarsi di un evento anomalo viene gestito con la creazione di un ticket verso la struttura preposta a manutenere il servizio. E' prevista, in caso di anomalia l'apertura di un incident.
Si distinguono due tipi di incident del software: l'incident normale e l'incident grave. Gli incident gravi sono quelli che causano un impatto sul Cliente. È prerogativa del Service Manager decidere che un incident è grave perché è il soggetto designato a valutare i danni ai Clienti.
In generale l'incident viene sempre generato se l'anomalia causa un non rispetto delle SLA contrattualizzate con un qualsiasi Cliente.
Una volta che l'anomalia viene rilevata, verrà:

- analizzata
- si procederà alle azioni di ripristino del servizio
- e di determineranno e documenteranno le azioni di correzione.

Per ripristinare, tempestivamente, il corretto funzionamento il Team deve individuare ed eseguire, anche con la collaborazione degli utenti e dei Clienti, le operazioni per lo workaround di ogni incident, documentando le operazioni eseguite come workaround dell'incident, quando dette operazioni sono state eseguite ed i risultati ottenuti con l'esecuzione di dette operazioni.

Se lo workaround di un incident ha ripristinato il corretto funzionamento del software, il Team deve documentare quando il software ha ripreso a funzionare correttamente.

Se invece lo workaround di un incident non ha sortito effetti: il Service Manager (o responsabile del servizio) deve attivare un change in emergenza per ripristinare, tempestivamente, il corretto funzionamento del servizio.

Maggiori dettagli sono descritti nelle procedure Aziendali di gestione incident.

torna al sommario

9.5 Procedure di Continuità Operativa e Disaster Recovery

Qualora si verifichi un evento che comporti l'indisponibilità del sistema di conservazione Primario, viene proposta l'attivazione delle misure di Continuità Operativa in funzione dell'effettiva gravità ed estensione dell'emergenza.

La soluzione di Continuità Operativa definita per gestire questa tipologia di emergenza prevede che **le risorse critiche che supportano il servizio di Conservazione (Team di Emergenza) si trasferiscano presso uno o più siti alternativi** per la prosecuzione delle proprie attività. Il trasferimento riguarda risorse preventivamente identificate in numero sufficiente a garantire
la **sopravvivenza delle sole attività critiche** per il tempo necessario all'organizzazione di contromisure durature nel tempo.

L'architettura del Disaster Recovery a supporto della Continuità Operativa prevede il Sito Primario presso l'infrastruttura tecnologica di Settimo Torinese (TO), mentre il sito

Secondario è implementato presso il Data Center di Firenze, distante oltre 300 Km dal sito primario.
Il sito secondario permette di usufruire dei servizi in Produzione in caso di indisponibilità del Data Center Primario, nel rispetto dei requisiti (RTO e RPO) riportati negli SLA definiti contrattualmente ed in sede di attivazione del servizio.

9.6 Verifica della Compliance del Servizio

Il Servizio di Conservazione a Norma è sottoposto a periodici Audit Interni svolti dalla Direzione Processi e Auditing Interno (DPAI), secondo le modalità descritte nella procedura del Sistema di Gestione per la qualità del Gruppo Engineering *MS01P01_Procedura Gestione Audit Interni*.
Essa prevede l'emissione di un programma annuale di audit interni, che comprende anche il servizio di Conservazione a Norma.

torna al sommario

----- fine documento ----

Firmato digitalmente da:PAOLO PANDOZY
Data:15/07/2019 08:52:41