Manuale di Conservazione

EDOK SRL

EMISSIONE DEL DOCUMENTO

Azione	Data	Nominativo	Funzione
Redazione	10/01/2018	Fabio Zanni	Responsabile Servizio di conservazione
Verifica	16/01/2018	Studio Legale Lisi	Consulente esterno
Approvazione	30/01/2018	Fabio Zanni	Responsabile Servizio di conservazione

REGISTRO DELLE VERSIONI

N°Ver/Rev/Bozza	Data emissione	Modifiche apportate	Osservazioni
Versione 1	10/11/2014	Prima redazione	
Versione 1.1	09/08/2017	Revisioni per modifica del responsabile sicurezza dei sistemi e responsabile del trattamento dati. Migrazione su VPC B.com	
Versione 1.2	30/01/2018	Revisione per modifica dei capitoli: 3. NORMATIVA E STANDARD DI RIFERIMENTO 5. STRUTTURA ORGANIZZATIVA PER IL SERVIZIO DI CONSERVAZIONE 6. OGGETTI SOTTOPOSTI A CONSERVAZIONE 7. IL PROCESSO DI CONSERVAZIONE 8. IL SISTEMA DI CONSERVAZIONE	Aggiunto allegato: “Metadati Minimi Conservazione.xlsx”

INDICE DEL DOCUMENTO

Sommario

1 SCOPO E AMBITO DEL DOCUMENTO

Il presente manuale illustra dettagliatamente l'organizzazione, i soggetti coinvolti e i ruoli svolti dagli stessi, il modello di funzionamento, la descrizione del processo, la descrizione dell'architettura e dell'infrastruttura utilizzata, le misure di sicurezza adottate e ogni altra informazione utile alla gestione e alla verifica del funzionamento, nel tempo, del sistema di conservazione realizzato dal conservatore Edok srl.

Edok srl opera dal 2005, anno della sua fondazione, nel settore della gestione elettronica documentale ed è specializzata nella progettazione, sviluppo e distribuzione di piattaforme software e fornitura di servizi per la l'archiviazione digitale, la gestione elettronica dei documenti, la gestione dei processi documentali e la conservazione digitale a norma di legge.

Grazie all'esperienza maturata e ad una piattaforma documentale sviluppata in casa, Edok srl riesce a costruire progetti documentali su misura. Partendo da un'approfondita fase di analisi, durante la quale vengono ascoltate e raccolte le esigenze, viene disegnato il progetto in house, in outsourcing o ibrido che viene poi implementato dai tecnici con particolare cura alla fase di configurazione e integrazione con i sistemi informatici già presenti e alla formazione degli operatori.

Data la natura dei servizi erogati, Edok srl considera l'implementazione e il mantenimento di un sistema di gestione integrato qualità e sicurezza delle informazioni un fattore determinate per migliorare il livello di efficienza dei processi aziendali e per la tutela del proprio patrimonio informativo. Per tale ragione la direzione si è impegnata affinché venissero mantenute le certificazioni ISO 9001 e ISO 27001, certificazioni ottenute con il tramite dell'ente accreditato Accredia RINA SERVICE Spa.

Il processo di conservazione vede coinvolte, a vario titolo, differenti figure e differenti professionalità. Tutte le figure coinvolte sono coordinate dal responsabile del servizio di conservazione che è il punto di riferimento per le attività del conservatore.

Il responsabile del servizio di conservazione

Il responsabile del servizio di conservazione è colui che si occupa di definire e attuare le politiche complessive del sistema di conservazione, nonché di governare la gestione del sistema di conservazione; inoltre a lui spetta la definizione delle caratteristiche e dei requisiti del sistema di conservazione in conformità alla normativa vigente. È il garante della corretta erogazione del servizio di conservazione all'ente produttore, gestisce tutte le convenzioni, definisce gli aspetti tecnico-operativi e valida i disciplinari tecnici che specificano gli aspetti di dettaglio e le modalità operative di erogazione dei servizi di conservazione.

Il responsabile della funzione archivistica

Il responsabile della funzione archivistica è colui che definisce e gestisce il processo di conservazione, incluse le modalità di trasferimento da parte dell'ente produttore, di acquisizione, verifica di integrità e descrizione archivistica dei documenti e delle aggregazioni documentali trasferiti, di esibizione, di accesso e fruizione del patrimonio documentario e informativo conservato;

Il responsabile del trattamento dati personali

Il responsabile del trattamento dei dati personali è il garante del rispetto delle vigenti disposizioni in materia di trattamento dei dati personali; garantisce che il trattamento dei dati affidati dai Clienti avvenga nel rispetto delle istruzioni impartite dal titolare del trattamento dei dati personali, con garanzia di sicurezza e di riservatezza.

Il responsabile della sicurezza dei sistemi per la conservazione

Il responsabile della sicurezza dei sistemi per la conservazione si occupa del monitoraggio continuo e del rispetto dei requisiti di sicurezza del sistema di conservazione stabiliti dagli standard, dalle normative e dalle politiche e procedure interne di sicurezza; è suo dovere segnalare ogni eventuale difformità al' responsabile del servizio di conservazione" e individuare e pianificare le necessarie azioni correttive.

Il responsabile dei sistemi informativi per la conservazione

Il responsabile dei sistemi informativi per la conservazione gestisce il corretto funzionamento di tutte le componenti hardware e software del sistema di conservazione. Tiene monitorati i livelli di servizio (SLA) concordati con il Cliente e segnala eventuali difformità degli SLA al Responsabile del servizio di conservazione individuando e pianificando le necessarie azioni correttive.

Controlla e verifica anche i livelli di servizio erogati da terzi segnalando le eventuali difformità al Responsabile del servizio di conservazione. Infine pianifica lo sviluppo delle infrastrutture tecnologiche del sistema di conservazione.

Il Responsabile dello sviluppo e della manutenzione del sistema di conservazione

A tale responsabile compete il coordinamento dello sviluppo e della manutenzione delle componenti hardware e software del sistema di conservazione. Pianifica e tiene monitorati i progetti di sviluppo del sistema di conservazione oltre agli SLA relativi alla manutenzione del sistema di conservazione. Si interfaccia, inoltre, con il Cliente relativamente alle modalità di trasferimento dei documenti e fascicoli informatici in merito ai formati elettronici da utilizzare, all'evoluzione tecnologica hardware e software, alle eventuali migrazioni verso nuove piattaforme tecnologiche. A lui, infine, compete la gestione dello sviluppo di siti web e portali connessi al servizio di conservazione.

Torna al sommario

2 TERMINOLOGIA (GLOSSARIO E ACRONIMI)

Relativamente alla terminologia utilizzata all'interno del presente manuale si fa riferimento al Glossario contenuto nell'Allegato 1 alle regole tecniche in materia di sistemi di conservazione approvate con DPCM 3 dicembre 2013.

Di seguito le definizioni contenute nel documento su menzionato.

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 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
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
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	complesso dei metadati, la cui struttura è descritta nell'allegato 5 del presente decreto, da associare al

informatico	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
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 presente decreto
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
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
transazione informatica	particolare evento caratterizzato dall'atomicità, consistenza, 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

3 NORMATIVA E STANDARD DI RIFERIMENTO

3.1 Normativa di riferimento

Il presente paragrafo riporta la principale normativa di riferimento per l'attività di conservazione a livello nazionale, eventualmente quella a livello locale in vigore nei luoghi dove sono conservati i documenti e quella specifica relativa alle diverse tipologie di documenti riguardanti il contratto di erogazione del servizio di conservazione.

Alla data attuale l'elenco dei principali riferimenti normativi italiani in materia, ordinati secondo il criterio della gerarchia delle fonti, è costituito da:

- Codice Civile [Libro Quinto Del lavoro, Titolo II Del lavoro nell'impresa, Capo III Delle imprese commerciali e delle altre imprese soggette a registrazione, Sezione III Disposizioni particolari per le imprese commerciali, Paragrafo 2 Delle scritture contabili], articolo 2215 bis - Documentazione informatica;
- Legge 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;
- Regolamento UE n° 910/2014 eIDAS in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE: art. 24 (Requisiti per i prestatori di servizi fiduciari qualificati)
- Decreto del Ministero dell'Economia e delle Finanze del 17 giugno 2014 - Modalità di assolvimento degli obblighi fiscali relativi ai documenti informatici ed alla loro riproduzione su diversi tipi di supporto
- Decreto del Presidente del Consiglio dei Ministri del 13 novembre 2014 - Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti

informatici nonché di formazione e conservazione dei documenti informatici delle pubbliche amministrazioni

- Circolare AGID 10 aprile 2014, n. 65 - Modalità per l'accreditamento e la vigilanza sui soggetti pubblici e privati che svolgono attività di conservazione dei documenti informatici di cui all'articolo 44-bis, comma 1, del decreto legislativo 7 marzo 2005, n. 82.
- Deliberazione Cnipa del 21 maggio 2009, n. 45 (come modificata dalla determinazione dirigenziale DigitPA n. 69/2010). Regole per la creazione dei certificati di firma e di marca che quelle per il loro utilizzo, riconoscimento e verifica;
- Direttiva 2010/45/UE del 13 luglio 2010 recante modifica della direttiva 2006/112/CE relativa al sistema comune d'imposta sul valore aggiunto per quanto riguarda le norme in materie di fatturazione. Recepita in Italia dalla Legge 228/2012, legge di stabilità 2013 del 24 dicembre 2012.
- Circolare dell'Agenzia delle Entrate n. 45/E del 19 ottobre 2005;
- Circolare dell'Agenzia delle Entrate n. 36/E del 06 dicembre 2006;
- Risoluzione Agenzia delle Entrate nr. 161E del 9 luglio 2007;
- Risoluzioni Agenzia delle Entrate nr. 158E del 15 giugno e nr. 196E del 30 luglio 2009;

Torna al sommario

3.2 Standard di riferimento

Riportiamo gli standard a cui l'attività di conservazione si riferisce e che sono elencati nell'allegato 3 delle Regole Tecniche in materia di Sistema di conservazione con indicazione delle versioni aggiornate al 1° ottobre 2014. Si precisa che la coerenza del sistema di conservazione a tali standard è obbligatoria per i soggetti accreditandi e accreditati.

- ISO 14721:2012 OAIS (Open Archival Information System), Sistema informativo aperto per l'archiviazione;
- ISO/IEC 27001, 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.

- ISO 9001 Sistemi di gestione per la qualità

Torna al sommario

4 RUOLI E RESPONSABILITA'

Di seguito sono indicate le attività svolte e i nominativi delle persone che ricoprono i ruoli elencati nella tabella seguente, cosi come individuati nel documento "Profili professionali". Nel caso di deleghe, per ciascuna delega sono indicate le attività delegate, i dati identificativi del soggetto delegato e il periodo di validità della delega.

La tabella mantiene traccia dei dati delle persone che nel tempo hanno ricoperto i suddetti ruoli.

ruoli	nominativo	attività di competenza	periodo nel ruolo	eventuali deleghe
Responsabile del servizio di conservazione	Fabio Zanni	- Definizione e attuazione delle politiche complessive del sistema di conservazione, nonché del governo della gestione del sistema di conservazione; - definizione delle caratteristiche e dei requisiti del sistema di conservazione in conformità alla normativa vigente; - corretta erogazione del servizio di conservazione esperienza in all'ente produttore; - gestione delle convenzioni, definizione degli aspetti tecnico-operativi e validazione dei disciplinari tecnici che specificano gli aspetti di dettaglio e le modalità operative di erogazione dei servizi di conservazione.	Dal 2005	
Responsabile Sicurezza dei sistemi per la conservazione	Stefano Zani	- Rispetto e monitoraggio dei requisiti di sicurezza del sistema di conservazione stabiliti dagli standard, dalle normative e dalle politiche e procedure interne di sicurezza; - segnalazione delle eventuali difformità al Responsabile del servizio di conservazione e individuazione e pianificazione delle necessarie azioni correttive.	Dal 10/01/14	

Responsabile funzione archivistica di conservazione	A.R.C.A. Scarl	- Definizione e gestione del processo di conservazione, incluse le modalità di trasferimento da parte dell'ente produttore, di acquisizione, verifica di integrità e descrizione archivistica dei documenti e delle aggregazioni documentali trasferiti, di esibizione, di accesso e fruizione del patrimonio documentario e informativo conservato; - definizione del set di metadati di conservazione dei documenti e dei fascicoli informatici; - monitoraggio del processo di conservazione e analisi archivistica per lo sviluppo di nuove funzionalità del sistema di conservazione; - collaborazione con l'ente produttore ai fini del trasferimento in conservazione, della selezione e della gestione dei rapporti con il Ministero dei beni e delle attività culturali per quanto di competenza.	Dal 1/08/14	Daniela Bregoli
Responsabile trattamento dati personali	Studio legale Lisi	- Garanzia del rispetto delle vigenti disposizioni in materia di trattamento dei dati personali; - garanzia che il trattamento dei dati affidati dai Clienti avverrà nel rispetto delle istruzioni impartite dal titolare del trattamento dei dati personali, con garanzia di sicurezza e di riservatezza.	Da agosto 2017	Andrea Lisi
Responsabile sistemi informativi per la conservazione	TILAK Srl	- Gestione dell'esercizio delle componenti hardware e software del sistema di conservazione; - monitoraggio del mantenimento dei livelli di servizio (SLA) concordati con l'ente produttore; - segnalazione delle eventuali difformità degli SLA al	Da agosto 2017	Vittorio Taglietti

		Responsabile del servizio di conservazione e individuazione e pianificazione delle necessarie azioni correttive; - pianificazione dello sviluppo delle infrastrutture tecnologiche del sistema di conservazione; - controllo e verifica dei livelli di servizio erogati da terzi con segnalazione delle eventuali difformità al Responsabile del servizio di conservazione.		
Responsabile sviluppo e manutenzione del sistema di conservazione	Fulvio Gabana	- Coordinamento dello sviluppo e manutenzione delle componenti hardware e software del sistema di conservazione; - pianificazione e monitoraggio dei progetti di sviluppo del sistema di conservazione; - monitoraggio degli SLA relativi alla manutenzione del sistema di conservazione; - interfaccia con l'ente produttore relativamente alle modalità di trasferimento dei documenti e fascicoli informatici in merito ai formati elettronici da utilizzare, all'evoluzione tecnologica hardware e software, alle eventuali migrazioni verso nuove piattaforme tecnologiche; - gestione dello sviluppo di siti web e portali connessi al servizio di conservazione.	Dal 2005	

Torna al sommario

5 STRUTTURA ORGANIZZATIVA PER IL SERVIZIO DI CONSERVAZIONE

5.1 Organigramma

Le strutture organizzative coinvolte nel servizio di conservazione sono:

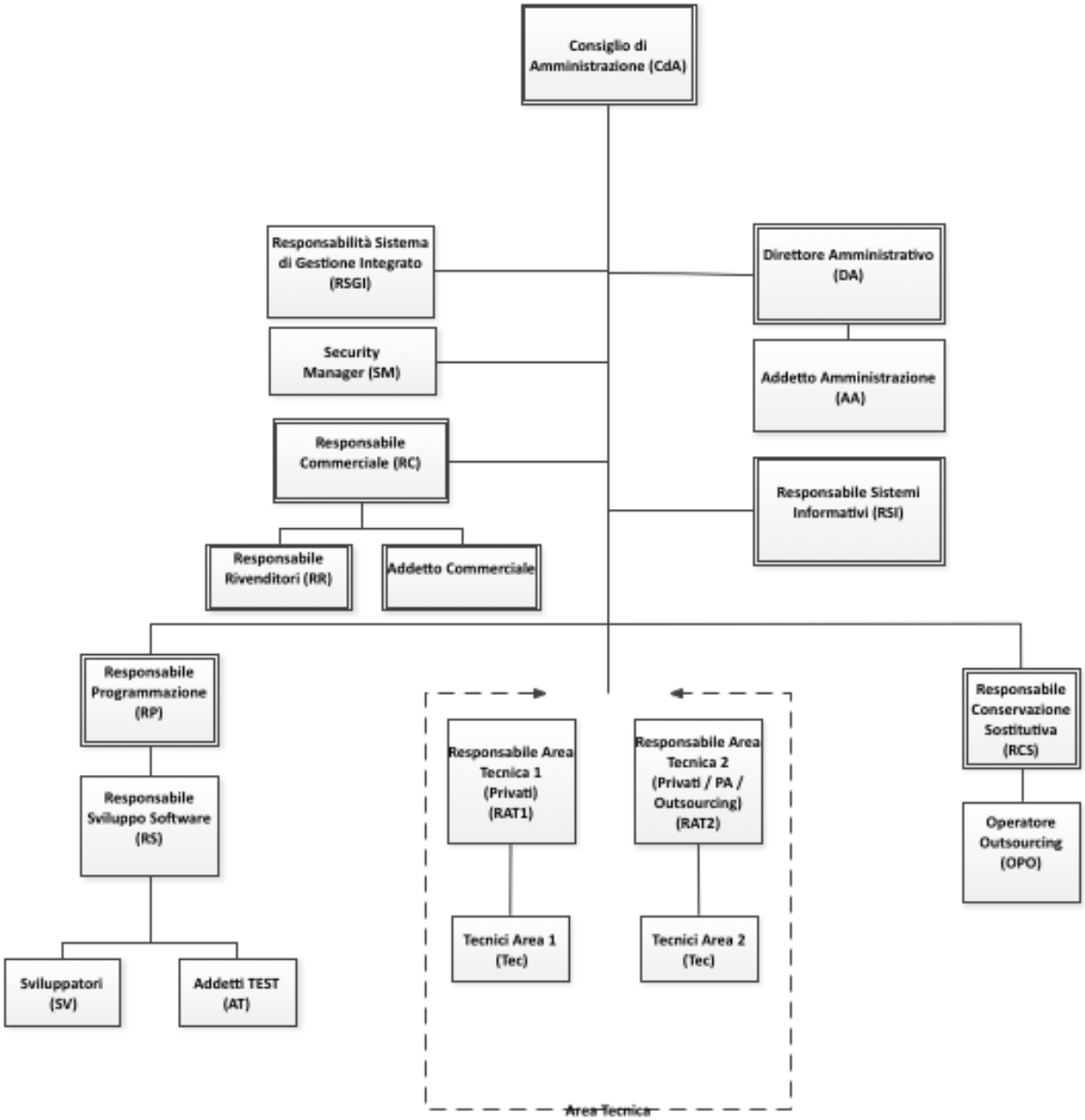

Figura 1 Strutture organizzative coinvolte nel servizio di conservazione

Torna al sommario

5.2 Strutture organizzative

Nelle varie fasi caratterizzanti il ciclo di vita del processo di conservazione digitale intervengono numerosi soggetti, i principali dei quali indicati e descritti nei precedenti capitoli, ciascuno dei quali è coinvolto a differenti livelli e responsabilità.

Nella seguente tabella sono riepilogate le principali attività che caratterizzano il servizio di conservazione poste in relazione ai ruoli e responsabilità costituenti la struttura organizzativa:

Descrizione Fase	Responsabile del servizio di conservazione	Responsabile della funzione archivistica di conservazione	Responsabile del trattamento dei dati personali	Responsabile della sicurezza dei sistemi di conservazione	Responsabile dei sistemi informativi di conservazione	Responsabile sviluppo e manutenzione dei sistemi di conservazione
Attivazione del servizio di conservazione (a seguito della sottoscrizione di un contratto)	X					
Acquisizione, verifica e gestione dei pacchetti di versamento presi in carico	X				X	X
Generazione del rapporto di versamento	X					X
Preparazione e gestione del pacchetto di archiviazione	X					X
Preparazione e gestione del pacchetto di distribuzione ai fini dell'esibizione e della produzione di duplicati e copie informatiche su richiesta	X	X				
Scarto dei pacchetti di archiviazione		X			X	
Chiusura del servizio di conservazione (al termine di un contratto)	X					

Conduzione e manutenzione del sistema di conservazione					X	X
Monitoraggio del sistema di conservazione				X	X	
Change management	X	X	X			X
Verifica periodica di conformità a normativa e standard di riferimento	X	X	X	X		
Aggiornamento del manuale di conservazione	X	X				
Verifica della conformità alle vigenti disposizioni in materia di trattamento dei dati personali			X			

Torna al sommario

5.3 Cessazione dei servizi di conservazione

Edok ha sviluppato un apposito piano di cessazione contenente le procedure con le quali, in caso di cessazione delle proprie attività, intende garantire la corretta migrazione dei documenti conservati verso un nuovo conservatore e, in ogni caso, la restituzione al produttore degli archivi di conservazione realizzati. Il piano, reso disponibile su richiesta del produttore, prevede anche la creazione di un'utenza di emergenza con diritti di accesso in sola lettura al sistema così da garantire, anche in caso di completa indisponibilità di personale Edok, l'accessibilità agli archivi di conservazione realizzati: tale chiave è stata depositata presso lo studio dell'Avv. Andrea Lisi, via V.M. Stampacchia 21, Lecce e sarà rilasciata solo su ordine di un'autorità giudiziaria.

Torna al sommario

6 OGGETTI SOTTOPOSTI A CONSERVAZIONE

6.1 Catalogazione

Ogni pacchetto di versamento sottoposto al Sistema di Conservazione deve essere catalogato in base alle anagrafiche del Sistema in relazione al Cliente produttore. La catalogazione è così strutturata:

- Codice della Società.

- Codice della Tipologia documentale.
- Eventuale codice della Sotto Tipologia.

Ogni Cliente fruitore del Servizio di Conservazione potrà, in base agli accordi contrattuali, avere associate una o più Società nonché una o più Tipologie documentali. Una Tipologia documentale può essere ulteriormente suddivisa in più Sotto Tipologie.

Torna al sommario

6.2 Tipologie documentali

Le Tipologie Documentali determinano la categoria di un insieme omogeneo di documenti e ne stabiliscono le caratteristiche:

- Schema dei metadati.
- Formati dei file.
- Tempistiche.

Le Tempistiche sono definite in base agli accordi stipulati con il Cliente e in relazione alle Tipologie considerate.

Per le Tipologie definite nel Sistema di Conservazione si faccia riferimento all'allegato "Metadati Minimi Conservazione.xlsx" che riporta, suddivise per le seguenti marco classi, l'elenco delle Tipologie e le relative proprietà:

LUL
CICLO ATTIVO
CICLO PASSIVO
REGISTRI
DICHIARATIVI
PEC
PA
CONTRATTI

Torna al sommario

6.3 Formato dei file

I formati accettati dal sistema di conservazione sono i seguenti:

- File testuali TXT
- Documenti PDF

- Documenti PDF firmati PADES e CADES (P7M)
- File XML
- Messaggi di Posta EML
- Formati grafici TIFF e JPEG

Torna al sommario

6.4 Pacchetto di versamento

Il PdV è il pacchetto informativo inviato dal produttore al sistema di conservazione secondo un formato predefinito e concordato così come descritto nel presente manuale.

L'assetto ed il contenuto dei pacchetti di versamento sono delineati in accordo con il produttore.

I pacchetti di versamento contengono gli oggetti da sottoporre a conservazione

Edok srl ha predisposto una procedura in grado di supportare il Produttore nella creazione del Pacchetto di Versamento e nell'automatizzare la fase di caricamento, in un'apposita area SFTP/FTPS (in base agli accordi contrattuali esistenti con il cliente).

Il PdV viene ricevuto compresso secondo il formato .zip e contiene sia la documentazione da archiviare (nel formato concordato con il cliente tra quelli gestiti dal sistema) sia i relativi metadati minimi (così come previsti dall'Allegato 5 delle regole tecniche in materia di sistemi di conservazione) sia quelli ulteriori concordati con il singolo cliente.

I contratti di servizio regolano tutte le componenti informative utili per procedere ad una conservazione corretta ed adeguata. Il sistema di conservazione supporterà, compatibilmente con la normativa vigente, tutti i pacchetti di versamento previsti negli specifici contratti di servizio.

Torna al sommario

6.5 Pacchetto di archiviazione

Il PdA è il pacchetto informativo composto dalla trasformazione di uno o più pacchetti di versamento secondo quanto indicato dal DPCM 3 dicembre 2013 e secondo le modalità riportate nel seguente manuale.

Il PdA viene creato al termine della procedura di acquisizione del pacchetto di versamento e sarà univocamente identificato all'interno del sistema di conservazione.

I metadati presenti all'interno del o dei PdV da cui origina il PdA verranno inseriti all'interno del IPdA secondo quanto previsto dai singoli contratti di servizio. Il sistema di conservazione verifica in ogni caso almeno la presenza del nucleo minimo di metadati previsti dallo standard UniSincro e dall'allegato 5 alle Regole tecniche in materia di sistemi di conservazione nonché dalle ulteriori normative aventi ad oggetto specifiche tipologie documentali (Es. DMEF 17 giugno 2014 in relazione ai documenti fiscalmente rilevanti).

Torna al sommario

6.6 Pacchetto di distribuzione

Il pacchetto di distribuzione è il pacchetto informativo inviato dal sistema di conservazione all'utente in risposta ad una sua richiesta.

Il pacchetto di distribuzione, che viene generato dal sistema di conservazione, deriva dal pacchetto di archiviazione ed è strutturato come quest'ultimo. Nel Pacchetto di Versamento la peculiare diversità risiede

nella sua destinazione, in quanto esso viene creato con il fine di mettere a disposizione degli utenti, per le finalità per cui essi ne hanno fatto richiesta, gli oggetti sottoposti a conservazione. A seconda di quanto previsto da ogni singolo contratto di servizio i PdD verranno sottoscritti digitalmente o meno da parte del responsabile del servizio di conservazione su delega del Conservatore.

Torna al sommario

7 IL PROCESSO DI CONSERVAZIONE

Di seguito viene descritto in maniera generale il processo di conservazione corredandolo di schemi e rappresentazioni grafiche, delle diverse funzioni relative al processo di conservazione.

Il riferimento del processo realizzato è lo standard ISO:14721:2003 meglio conosciuto come Open Archival Information System.

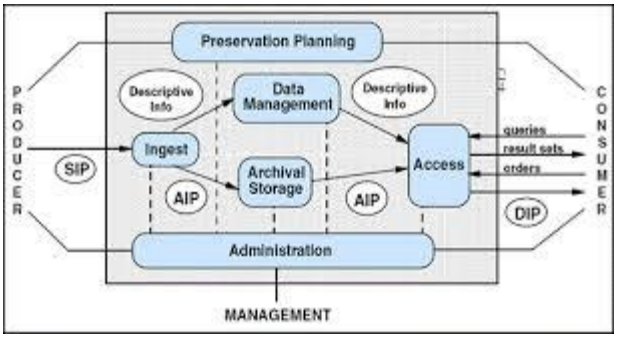

Figura 2 Processo di conservazione

Torna al sommario

7.1 Importazione di pacchetti ricevuti esternamente

Il sistema prevede la ricezione di pacchetti di versamento generati da applicativi esterni tramite la gestione di una struttura a cartelle in cui ad ogni cliente viene associata una e una sola cartella il cui nome corrisponde al codice del cliente.

Il processo di conservazione viene scatenato dalla ricezione tramite SFTP/FTPS (in base agli accordi contrattuali esistenti con il cliente) di un archivio in formato compresso contenente i file da archiviare nel formato concordato secondo cui le procedure sono state già create e configurate.

Ogni cliente può accedere univocamente alla propria cartella con un utente specifico rilasciato secondo le procedure di autenticazione/autorizzazione previste. Il file ricevuto viene preso in carico dal modulo di ricezione il prima possibile per liberare la cartella di ricezione e evitare conflitti nel caso in cui due pacchetti abbiano lo stesso nome.

I pacchetti ricevuti vengono aggiunti alla coda di importazione: il file ricevuto viene tracciato nel registro dei pacchetti ricevuti disponibili agli utenti autorizzati (amministratore, responsabili e operatori delegati dai responsabili):

Figura 3 Registro pacchetti di versamento

I dati tracciati riguardano la data, il nome, la dimensione, la hash e l'eventuale presenza della firma del pacchetto.

Periodicamente la coda di importazione viene elaborata considerando un insieme di file, secondo logiche che garantiscono l'elaborazione bilanciata di tutti i clienti indipendente dalla quantità di pacchetti versati.

Per ogni file viene eseguito il seguente processo:

- Verifica nel nome del pacchetto, che deve includere il formato del pacchetto, il codice della società (che deve essere associata al cliente corrente), il codice della tipologia e il codice del periodo di riferimento,
- Analisi del contenuto del pacchetto in base al formato e verifica dei metadati e dei relativi file (documenti e allegati). Eventuale verifica della firma per i pacchetti firmati.
- Importazione effettiva del pacchetto: creazione della registrazione nel catalogo dei PdV e importazione dei documenti nel Sistema di Conservazione.
- Creazione, registrazione e invio del rapporto di versamento al cliente (sia in caso di verifica fallita, quindi di rifiuto del pacchetto, sia in caso di importazione completata con successo e quindi di accettazione).

Le fasi descritte precedentemente vengono tracciate nel registro dei pacchetti ricevuti in cui gli operatori possono seguire le diverse fasi di importazione (che possono richiedere diverso tempo). I passaggi eseguiti vengono dettagli in un log di importazione disponibile alla fine del processo e mantenuto dal registro dei pacchetti ricevuti:

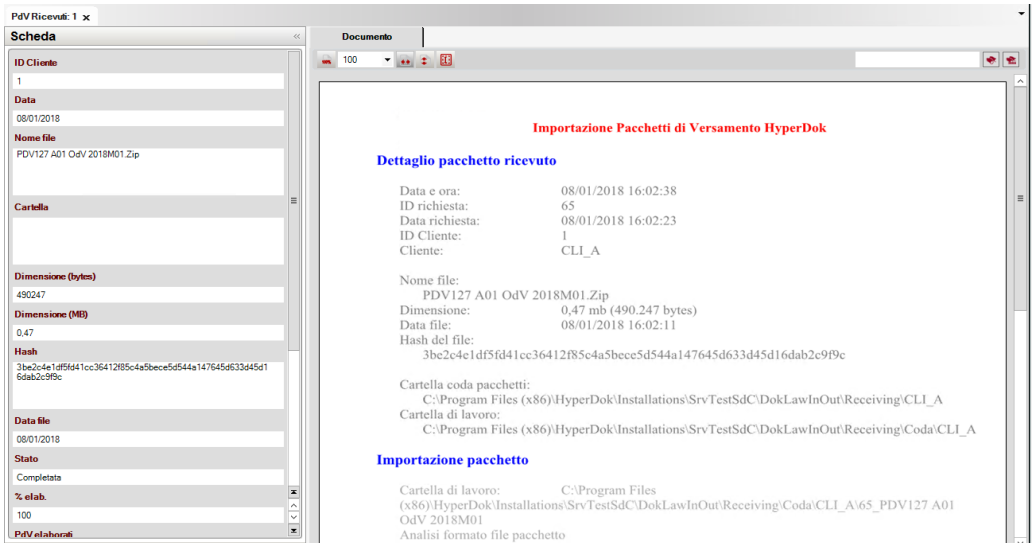

Figura 4 Log pacchetto di versamento

Il rapporto di versamento include il nome del file elaborato e la sua hash, nonché gli eventuali errori che ne hanno determinato il rifiuto (ad esempio per il riferimento ad una tipologia non definita per la società corrente) ed eventuali segnalazioni che non compromettono l'accettazione (ad esempio per i PdV classici la differenza, a parità di codice, del nome di una tipologia).

Il prodotto dell'importazione è visibile da client nel catalogo dei PdV, in cui ad un pacchetto è legato il relativo rapporto di versamento:

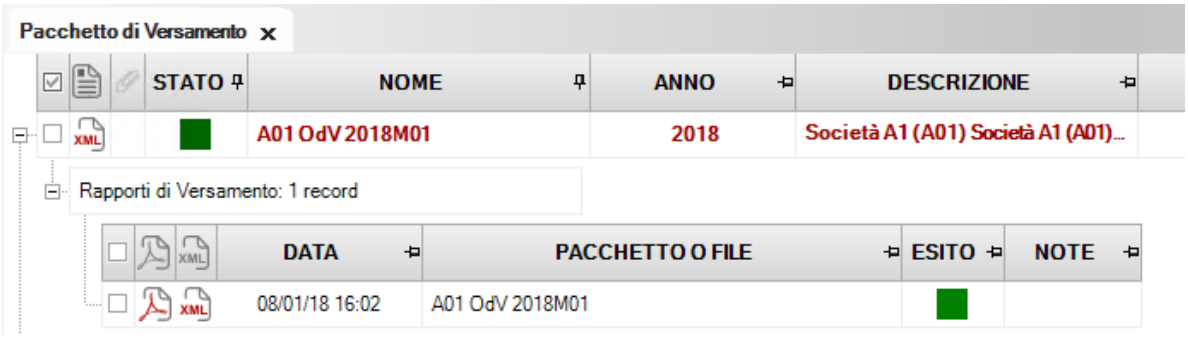

Figura 5 Visualizzazione PdV e rapporto di versamento

Tale processo è descritto in dettaglio nel manuale tecnico: "Ricezione Pacchetti di Versamento Outsourcing" in cui vengono descritti i formati accettati e le regole che ne determinano il rifiuto o l'accettazione.

In caso di fallimento dell'importazione viene sempre generato un rapporto di versamento che dettaglia i dati del pacchetto e le ragioni del rifiuto. Tra le possibili cause di rifiuto si hanno ad esempio:

- Il riferimento ad una catalogazione errata, quindi di un codice Società e Tipologia non definite per il cliente produttore.
- La mancanza di uno o più file indicati dal file indice.
- La differenza tra le hash dei file del pacchetto e quelli riportati nel file indice.
- La non validità della firma (per i pacchetti firmati).
- La presenza di formati file non supportati per Tipologia del Pacchetto.
- La mancanza dei metadati minimi definiti per la Tipologia del Pacchetto.

Torna al sommario

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

Ogni versamento da parte dell'utente contiene pacchetti uniformi per tipologia documentale e produttore.

La verifica relativa all'identificazione del produttore avviene mediante il controllo incrociato delle credenziali di accesso dell'utente che effettua il versamento al sistema di conservazione mediante l'utilizzo dell'apposito client fornitogli, con le informazioni relative al codice tipologia documentale e al codice Azienda contenute all'interno del pacchetto di versamento e alla configurazione dei Pacchetti di

Versamento generati attraverso appositi canali cifrati così da garantire sempre la coincidenza tra utente e produttore.

Se da tali verifiche non emergesse la piena congruenza di questi elementi, allora il pacchetto di versamento non verrebbe accettato. Tramite questa procedura si possono controllare tutti gli eventuali errori o problemi rispetto alla provenienza dei documenti.

Le verifiche effettuate in fase di importazione dei pacchetti di versamento prevedono:

- L'analisi della catalogazione del pacchetto a partire dal nome del file: il codice cliente, il codice società e il codice tipologia devono essere congruenti alla configurazione del Cliente.
- Verifica dell'integrità del pacchetto e della presenza del relativo file indice e dei file da inviare in conservazione.
- Verifica dell'esistenza e dell'hash di tutti i file presenti nel pacchetto rispetto a quanto riportato dal file indice.
- Verifica del formato dei file inclusi nel pacchetto e definiti dalla tipologia documentale.
- Verifica della sussistenza di tutti i metadati attesi e quantomeno quelli obbligatori peculiari della tipologia documentale in oggetto.
- In caso di pacchetti di versamento firmati verifica della validità delle sottoscrizioni digitali apposte ai documenti portati in conservazione.

In caso di fallimento di uno dei passaggi di verifica le motivazioni vengono riportate nel Rapporto di Versamento inviato al cliente.

Torna al sommario

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

A seguito dell'esito positivo delle attività di verifica del pacchetto di versamento, quest'ultimo viene accettato e il sistema ne esegue l'importazione.

Così come previsto dall'art. 9, comma 1, lett. d) del DPCM 3 dicembre 2013, il Rapporto di versamento conterrà un riferimento al momento di accettazione del PdV (in formato UTC) e l'impronta del PdV ricevuto.

Il singolo rapporto viene univocamente individuato dal sistema di conservazione mediante l'hash del documento generato e ad un ID univoco registrato. Il Rapporto di Versamento e verrà conservato nel sistema di conservazione per lo stesso tempo previsto per i PdA generati dai PdV ai quali si riferisce.

I rapporti di versamento così prodotti e conservati sono resi disponibili al produttore. I singoli contratti di servizio potranno prevedere anche la sottoscrizione del singolo rapporto di versamento.

Torna al sommario

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

Quando le verifiche descritte nel paragrafo precedente non vengono superate, il pacchetto di versamento viene rifiutato.

Le anomalie riscontrate, riferite alle verifiche effettuate sul pacchetto di versamento riguardano:

- Mancata identificazione dell'utente tramite il riscontro delle credenziali
- Incompatibilità del formato con quelli attesi
- Presenza di almeno tutti i metadati minimi necessari

I singoli contratti di servizio potranno prevedere anche il rifiuto dei PdV nei casi in cui non siano presenti anche gli ulteriori metadati concordati o nel caso di esito negativo della verifica delle firme apposte ai documenti versati.

In tale caso verrà generato un avviso di versamento non corretto che sarà inoltrato al produttore e al Reparto interno delegato dal conservatore per avviare tutti i controlli necessari a giungere ad un corretto versamento. L'avviso, inoltrato tramite mail, riporterà in allegato il log della procedura per poter consentire agli operatori di meglio analizzare l'accaduto e risalire il prima possibile all'errore.

Tutti le anomalie riscontrate verranno riportate in un apposito "registro delle anomalie" tenuto informaticamente e conservato a cura del conservatore.

Torna al sommario

7.5 Preparazione e gestione del pacchetto di archiviazione

La preparazione del Pacchetto di Archiviazione (PdA) avviene attraverso una procedura che agisce sulla base di parametri prefissati (quali il periodo di riferimento dei documenti, il termine legale e i criteri di raggruppamento) che consentono al Sistema ed alla procedura di conservazione di individuare automaticamente i documenti costituenti il Pacchetto di Archiviazione.

La relativa codifica è costituita dai seguenti elementi:

- tipologia di documento;
- azienda che opera la conservazione;
- anno relativo alla conservazione;
- periodo di riferimento dei documenti;

Operativamente gli utenti abilitati del sistema di conservazione potranno visualizzare i Pacchetti di Versamento generati dai rispettivi produttori e potranno operare effettuando una selezione dei Pacchetti di Versamento che desideriamo portare in archiviazione. Per far ciò dall'apposita icona nel menu in alto dovranno selezionare il menu "Archiviazione pacchetti" come indicato nella figura sottostante:

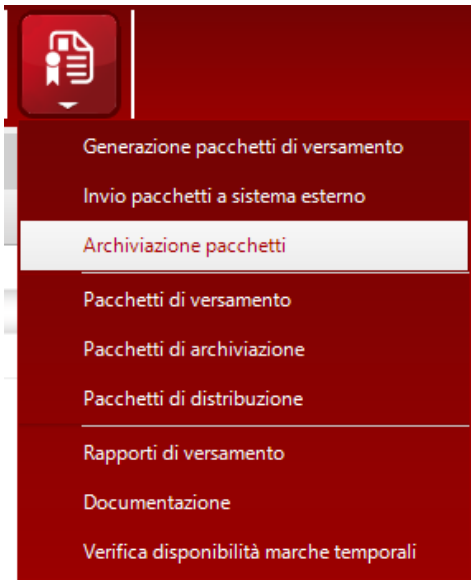

Figura 6 Dettaglio comandi software HyperDok

A questo punto il software HyperDok presenterà sarà la seguente maschera:

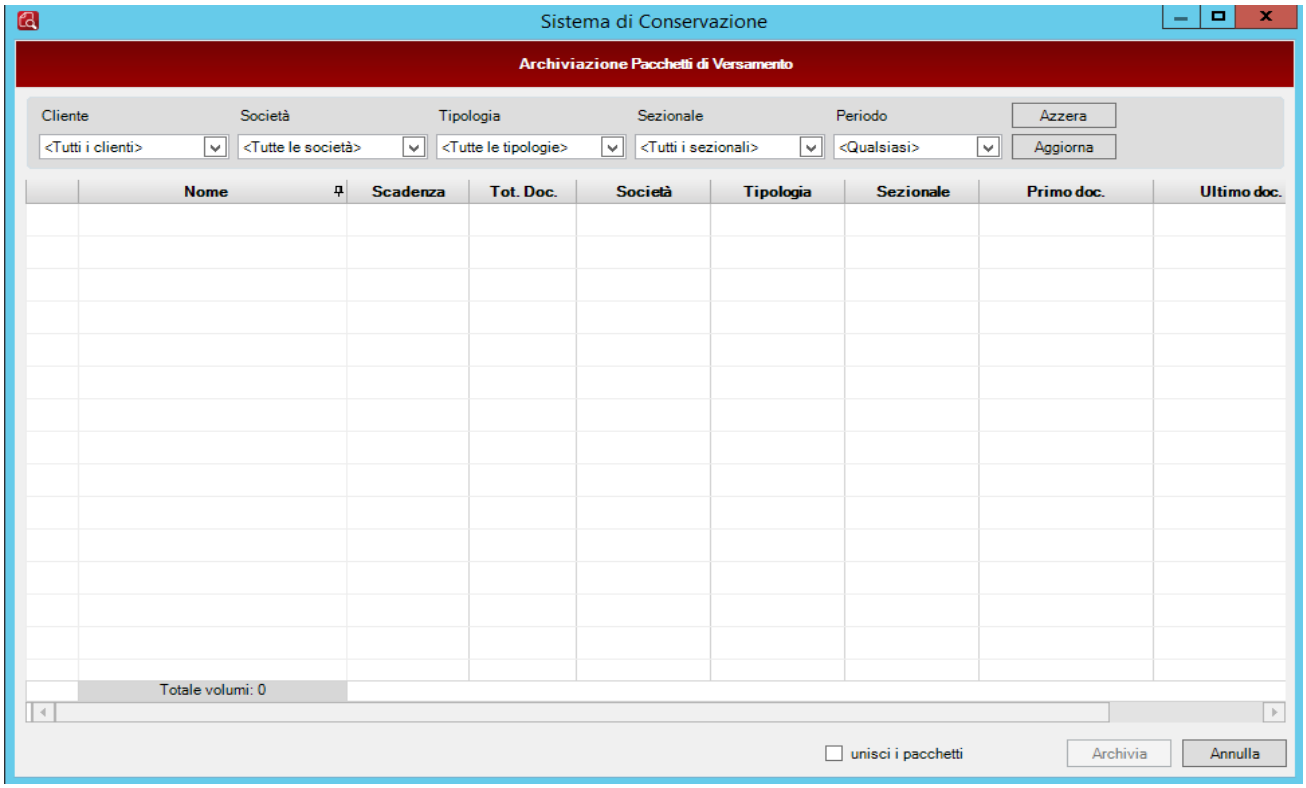

Figura 7 Dettaglio maschera software HyperDok

Prima di cliccare sul bottone “Aggiorna” in alto a destra, che ci consente di visualizzare tutti i Pacchetti di Versamento accettati in attesa della generazione del Pacchetto di Archiviazione è bene sapere che è possibile effettuare un filtro sui campi: Cliente o Produttore, Società, Tipologia, Sezionale o Periodo per

permettere all'operatore di lavorare solo su parte dei Pacchetti di Versamento oppure per procedere con la generazione di un Pacchetto di Archiviazione per ciascun Pacchetto di Versamento Prodotto.

In base ai filtri impostati, cliccando sul tasto "Aggiorna", verranno visualizzati solo i Pacchetti di Versamento interessati e sarà possibile procedere alla generazione dei Pacchetti di Archiviazione mediante il bottone "Archivia" in basso a destra. È possibile unire più pacchetti di Versamento in un unico Pacchetto di Archiviazione. In questo caso il software tiene traccia nel Pacchetto di Archiviazione di ciascun Pacchetto di Versamento di cui è composto.

Come dall'immagine sotto riportata, sarà possibile inserire una nota opzionale che sarà inserita all'interno del campo "Note" del Pacchetto di Archiviazione.

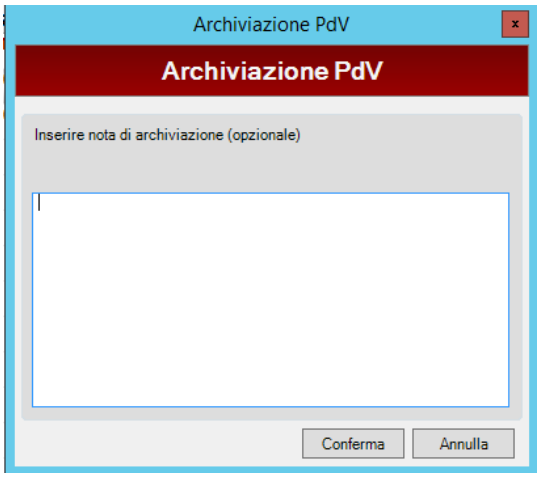

Figura 8 Dettaglio gestione note PdA software HyperDok

Quindi apparirà una nuova finestra dove verrà richiesto il PIN del dispositivo di firma digitale configurato all'interno dell'applicativo per quello specifico utente, operazione che consentirà di apporre la firma digitale direttamente da parte del Responsabile della Conservazione del Cliente o da un suo delegato (o anche dal Responsabile del servizio di conservazione dietro opportuno affidamento) al Pacchetto di Archiviazione e successivamente effettuerà l'apposizione di una marca temporale.

Inserito il PIN cliccare sul bottone "Firma" per eseguire la procedura di creazione del PDA:

Figura 9 Dettaglio firma digitale software HyperDok

Tutti i Pacchetti di Archiviazione generati saranno depositati in un archivio consultabile e ognuno di essi sarà collegato al o ai rispettivi Pacchetti di Versamento

Torna al sommario

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

Secondo quanto stabilito dall'articolo 10 del DPCM 3 dicembre 2013, ai fini dell'esibizione dei documenti, il sistema di conservazione permette ai soggetti autorizzati l'accesso diretto, anche da remoto, al documento informatico conservato, attraverso la produzione di un pacchetto di distribuzione selettiva secondo le modalità descritte nel manuale di conservazione.

Il sistema di conservazione di Edok srl permette di produrre i pacchetti di distribuzione partendo da una richiesta che può essere generata da un utente abilitato in due diversi modi:

- Richiesta semplice, ovvero una richiesta che viene generata scegliendo uno o più documenti specifici di una Società di cui si richiede la distribuzione.

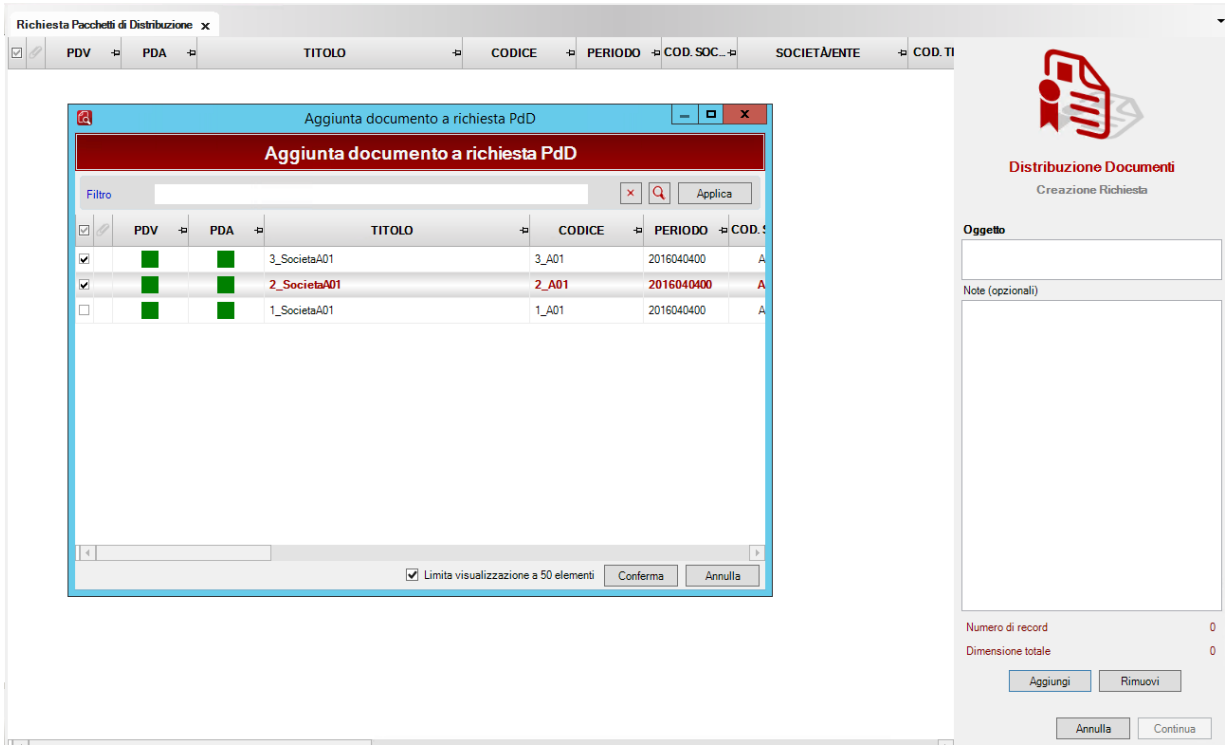

Figura 10. Dettaglio richiesta PdD software HyperDok opzione 1

- Richiesta da PdA, ovvero viene richiesta la distribuzione di un intero pacchetto di archiviazione

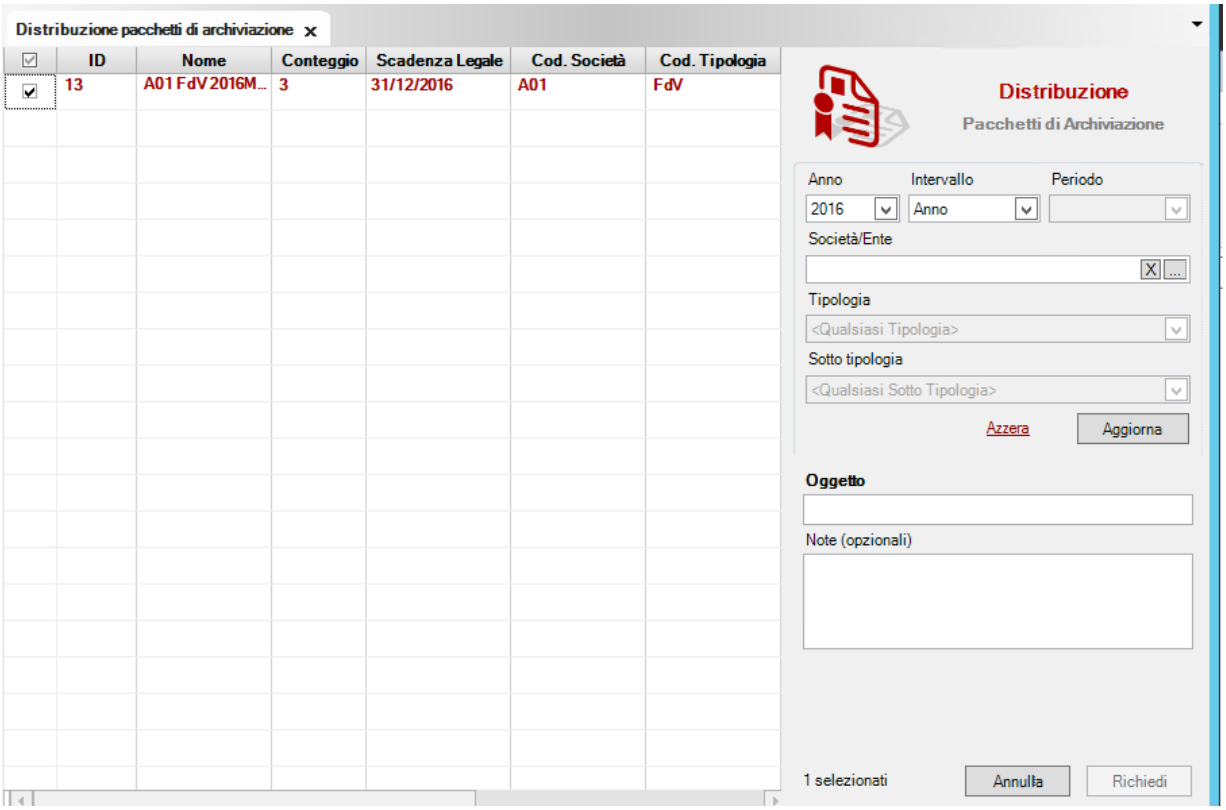

Figura 11 Dettaglio richiesta PdD software HyperDok opzione 2

Queste richieste vengono inviate al responsabile della conservazione della società che le prende in carico e decide se approvarle o rifiutarle

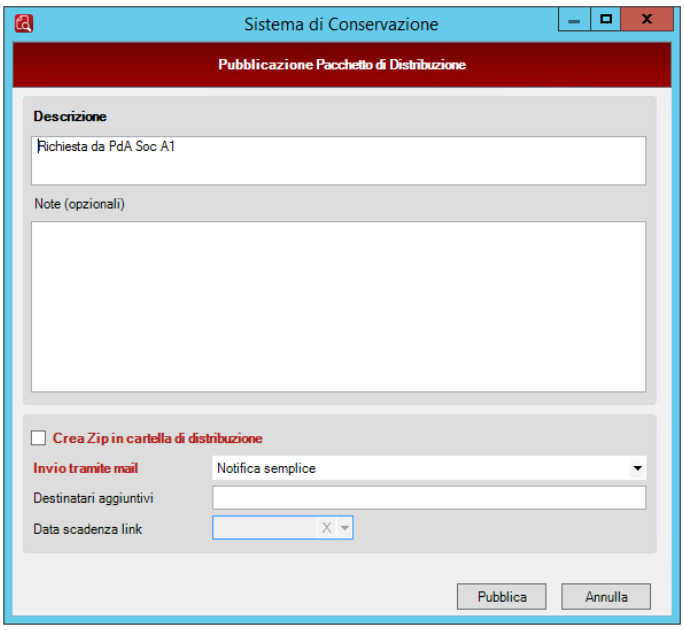

Figura 12 Dettaglio pubblicazione PdD software HyperDok

A questo punto il pacchetto viene pubblicato e l'accesso alla modalità di consultazione è consentito solamente agli utenti adeguatamente autorizzati, secondo gli specifici accordi contrattuali raggiunti.

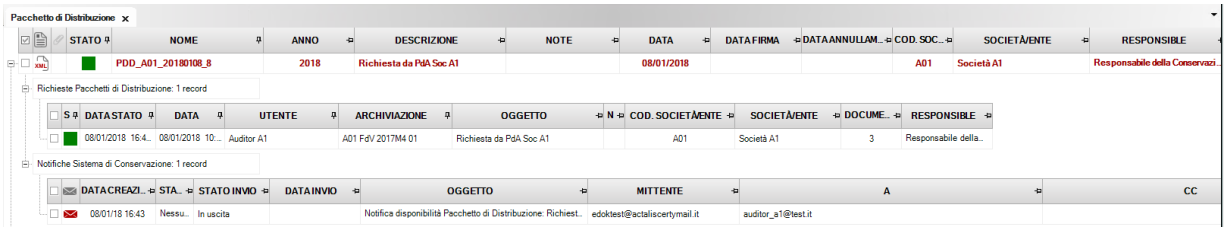

Figura 13 Dettaglio visualizzazione PdD software HyperDok

L'utente avrà quindi la possibilità di richiedere la generazione di un pacchetto di distribuzione contenente un singolo documento digitale o uno specifico insieme dei documenti digitali, corredati da tutti i relativi metadati presenti nel pacchetto o nei pacchetti di archiviazione da cui derivano. Il pacchetto di distribuzione sarà per quanto possibile strutturato nello stesso modo in cui è strutturato il pacchetto di archiviazione seppure con la diversa finalità di rispondere alla richiesta di accesso inoltrata dall'utente.

Torna al sommario

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

Finalità del processo è quella di consentire la creazione di duplicati o copie di uno o più documenti sottoposti a conservazione:

- la duplicazione permetterà di ottenere documenti informatici aventi la stessa rappresentazione informatica egli originali da cui sono tratti;
- la copia permetterà, invece, di ottenere documenti informativi aventi lo stesso contenuto informativo degli originali da cui sono tratti ma differente rappresentazione informatica.

La creazione di copie informatiche o duplicati informatici dei documenti sottoposti a conservazione avviene o su decisione del Responsabile della conservazione in relazione all'evolversi del contesto tecnologico o su richieste degli utenti secondo quanto previsto dalle regole tecniche in materia di formazione del documento informatico di cui al DPCM 13 novembre 2014.

Quando il sistema riceve una richiesta da un utente procede, preliminarmente, alla ricerca del documento o documenti informatici di cui occorre il duplicato o la copia tramite le apposite funzionalità di ricerca messe a disposizione del sistema.

Una volta avuta conferma dell'avvenuta corretta individuazione del documento richiamato sarà possibile procedere al download dello stesso, mediante l'utilizzo della funzione di sistema a tale scopo dedicata.

Nel momento in cui si renda necessario, magari per problemi associati all'obsolescenza del formato utilizzato per la conservazione dei documenti, modificare la rappresentazione informatica degli stessi il sistema offrirà al responsabile della conservazione la possibilità di utilizzare un differente processo.

Per mezzo di tale processo il sistema sarà in grado di creare un nuovo documento informatico, in un formato diverso da quello d'origine, versandolo nel sistema con le medesime modalità che erano state utilizzate per il documento originario.

Nell'espletamento di tale operazioni, ai sensi di quanto previsto dal Codice dell'amministrazione digitale e dalle regole tecniche in materia di formazione del documento informatico ivi richiamate, il Responsabile della conservazione richiederà l'intervento di un Pubblico ufficiale che certificherà la conformità del

documento copiato al suo originale o, nei casi ove sia possibile, certificherà l'intero processo che porta alla formazione delle copie.

Torna al sommario

7.8 Scarto dei pacchetti di archiviazione

L'art. 9 comma 1, lett. K del DPCM 3 dicembre 2013 stabilisce che deve essere effettuato lo scarto dal sistema di conservazione, alla scadenza dei termini di conservazione previsti dalla norma, dandone informativa al soggetto produttore.

Il Sistema di conservazione implementato da Edok srl permette di gestire agevolmente lo scarto del materiale documentario non destinato alla conservazione permanente, ma caratterizzato invece da tempi di conservazione limitati e diversificati. Le attività di scarto si baseranno sulle tempistiche indicate, per ciascuna tipologia di documento o fascicolo, in un apposito piano di conservazione definito con il produttore. Sarà dunque il sistema ad avvisare il responsabile del servizio di conservazione attraverso una o più notifiche impostabili, circa la scadenza dei tempi di conservazione dei documenti. Ricevuta la notifica il responsabile del servizio di conservazione comunicherà al produttore la scadenza dei termini previsti e solo dietro autorizzazione del produttore procederà allo scarto.

Eventuali procedure specifiche potranno essere concordate con il produttore.

Torna al sommario

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

Il sistema lavora utilizzando pacchetti strutturati in accordo con quanto definito nell'Allegato 4 delle regole tecniche contenute nel DPCM 3 dicembre 2013. Conformemente a quanto previsto, la struttura dell'Indice del Pacchetto di Archiviazione, infatti, fa riferimento allo standard SInCRO – Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali (UNI 11386:2010) ossia l'attuale standard internazionale riguardante la struttura dell'insieme dei dati a supporto del processo di conservazione.

Il sistema è quindi in grado di accettare pacchetti strutturati secondo lo standard SInCRO provenienti da altri sistemi di conservazione. Ugualmente i pacchetti creati dal sistema Edok srl potranno essere versati ad altri sistemi di conservazione che utilizzano lo standard medesimo.

La definizione e la struttura degli ulteriori metadati non previsti dallo standard UniSincro ma inseriti nel campo *moreinfo* è stata dettagliata nei singoli contratti di servizio.

A titolo esemplificativo riportiamo un esempio di un Pacchetto di Versamento:

```
<?xml version="1.0" encoding="utf-8"?>
<sincro:IdC sincro:url="http://www.uni.com/U3011/sincro/" sincro:version="1.0"
xmlns:sincro="
http://www.uni.com/U3011/sincro/" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance"
xsi:schemaLocation="http://www.uni.com/U3011/sincro/IdC.xsd">
```

<sincro:SelfDescription>
<sincro:ID sincro:scheme="Hyperdok">
0313_01878290129UNISPI_A2013_V01_80a1ee79-beb0-4020-beca-0d2c8c4ae34b</sincro:ID>
<sincro:CreatingApplication>
<sincro:Name>Hyperdok</sincro:Name>
<sincro:Version>4.0.1.52</sincro:Version>
<sincro:Producer>edok s.r.l</sincro:Producer>
</sincro:CreatingApplication>
</sincro:SelfDescription>
<sincro:VdC>
<sincro:ID sincro:scheme="Hyperdok">0000000140</sincro:ID>
<sincro:MoreInfo sincro:XMLScheme="file:///edokPdvMetadata.xsd">
<sincro:EmbeddedMetadata>
<extra:PdvMetadata xmlns:extra="file:///edokPdvMetadata.xsd">
<extra:Name>0313_01878290129UNISPI_A2013_V01</extra:Name>
<extra:Description>C.A.F. XXXXX s.r.l. (01878290129) Modello unico società di persone (UNISP) Integrativo (I) Annuale 2013
</extra:Description>
<extra:GUID>80a1ee79-beb0-4020-beca-0d2c8c4ae34b</extra:GUID>
<extra:Year>2014</extra:Year>
<extra:Date>20141222153840</extra:Date>
<extra:Operator>MICHELA, XXXXX</extra:Operator>
<extra:OperCode>IT:XXXXXX71D53L6888B</extra:OperCode>
<extra:CustomerCode>0313</extra:CustomerCode>
<extra:CompanyCode>01870000000</extra:CompanyCode>
<extra:Company>C.A.F. XXXXXX s.r.l.</extra:Company>
<extra:TypologyCode>UNISP</extra:TypologyCode>
<extra:Typology>Modello unico società di persone</extra:Typology>
<extra:TypologyAreaCode>I</extra:TypologyAreaCode>
<extra:TypologyArea>Integrativo</extra:TypologyArea>
<extra:Volume>UNISP</extra:Volume>
<extra:Columns>
<extra:Column>Anno|String|-|4||Anno</extra:Column>
<extra:Column>Rag_Soc|String|-|40||Rag_Soc</extra:Column>
<extra:Column>Cod_Dic|String|-|10||Cod_Dic</extra:Column>
<extra:Column>Tipo_Doc|String|-|20||Tipo_Doc</extra:Column>

<extra:Column>D_CodSogg|String|-|8||D_CodSogg</extra:Column>
<extra:Column>D_CodParcel|String|-|6||D_CodParcel</extra:Column>
<extra:Column>D_CodContabilita|String|-|7||D_CodContabilita
</extra:Column>
<extra:Column>D_CodDichiarazione|String|-|7||D_CodDichiarazione
</extra:Column>
<extra:Column>D_RagioneSociale|String|-|50||D_RagioneSociale
</extra:Column>
<extra:Column>D_Cognome|String|-|25||D_Cognome</extra:Column>
<extra:Column>D_Nome|String|-|25||D_Nome</extra:Column>
<extra:Column>D_IND_Comune|String|-|50||D_IND_Comune</extra:Column>
<extra:Column>D_IND_IndirizzoSede|String|-|100||D_IND_IndirizzoSede
</extra:Column>
<extra:Column>D_IND_Provincia|String|-|2||D_IND_Provincia
</extra:Column>
<extra:Column>D_Delegazione|String|-|50||D_Delegazione</extra:Column>
<extra:Column>D_CodSiglaPaghe|String|-|3||D_CodSiglaPaghe
</extra:Column>
<extra:Column>D_CodSiglaContabilita|String|-|3||D_CodSiglaContabilita
</extra:Column>
<extra:Column>D_CodSiglaClienti|String|-|3||D_CodSiglaClienti
</extra:Column>
<extra:Column>D_CodGrappPaghe|String|-|3||D_CodGrappPaghe
</extra:Column>
<extra:Column>D_CodGrappContabilita|String|-|3||D_CodGrappContabilita
</extra:Column>
<extra:Column>D_CodSigla3|String|-|3||D_CodSigla3</extra:Column>
<extra:Column>D_CodiceFiscale|String|-|16||D_CodiceFiscale
</extra:Column>
<extra:Column>D_PartitaIVA|String|-|11||D_PartitaIVA</extra:Column>
<extra:Column>D_CodREA|String|-|6||D_CodREA</extra:Column>
<extra:Column>D_CodMandGeuni|String|-|3||D_CodMandGeuni</extra:Column>
<extra:Column>D_CodFornitore|String|-|10||D_CodFornitore
</extra:Column>
<extra:Column>D_NumDitta|String|-|2||D_NumDitta</extra:Column>
<extra:Column>D_flDittaPrivato|String|-|10||D_flDittaPrivato
</extra:Column>

```
<extra:Column>D_flSocietaDittaInd|String|-|10||D_flSocietaDittaInd
</extra:Column>
<extra:Column>D_flCessata|String|-|1||D_flCessata</extra:Column>
<extra:Column>D_flSocio|String|-|1||D_flSocio</extra:Column>
<extra:Column>D_flFiscale|String|-|1||D_flFiscale</extra:Column>
<extra:Column>D_flPaghe|String|-|1||D_flPaghe</extra:Column>
<extra:Column>D_flMdl|String|-|1||D_flMdl</extra:Column>
<extra:Column>D_fl1|String|-|1||D_fl1</extra:Column>
<extra:Column>D_fl2|String|-|1||D_fl2</extra:Column>
<extra:Column>D_fl3|String|-|1||D_fl3</extra:Column>
<extra:Column>D_DataRecord|DateTime|-|-||D_DataRecord</extra:Column>
<extra:Column>Doppi|String|-|1||Doppi</extra:Column>
<extra:Column>Integrative|String|-|1||Integrative</extra:Column>
<extra:Column>Cod_Soc|String|-|3||Cod_Soc</extra:Column>
<extra:Column>Cod_Soc_Desc|String|-|100||Cod_Soc_Desc</extra:Column>
<extra:Column>RecordID|Int32|-|-||RecordID</extra:Column>
<extra:Column>Note|String|-|-||Note</extra:Column>
<extra:Column>ModPiuRicOK|String|-|1||ModPiuRicOK</extra:Column>
<extra:Column>ModNoRicOK|String|-|1||Modello no CS</extra:Column>
<extra:Column>Cod_Tipo_Doc_CS|String|-|1||Cod_Tipo_Doc_CS
</extra:Column>
<extra:Column>Anno_Fiscale|Int32|-|-||Anno_Fiscale</extra:Column>
</extra:Columns>
<extra:DocTypes>
<extra:DocType>Doc|PDF</extra:DocType>
</extra:DocTypes>
<extra:FirstDocDate>01/01/2013 00:00:00</extra:FirstDocDate>
<extra:LastDocDate>01/01/2013 00:00:00</extra:LastDocDate>
<extra:StoringDueDate>31/12/2014 00:00:00</extra:StoringDueDate>
<extra:LegalDeadline>31/12/2014 00:00:00</extra:LegalDeadline>
<extra:Note />
</extra:PdvMetadata>
</sincro:EmbeddedMetadata>
</sincro:VdC>
```

Torna al sommario

8 IL SISTEMA DI CONSERVAZIONE

Il Sistema di Conservazione si fonda sulle seguenti componenti:

- Un insieme di servizi e applicativi software che attraverso tutte le sue componenti permette di rendere disponibile le funzioni a supporto del processo di conservazione, dalla ricezione alla distribuzione dei documenti passando per l'archiviazione;
- Il supporto di memorizzazione, che rappresenta il sistema fisico su cui vengono conservati nel tempo i documenti sottoposti al processo di conservazione;
- Il dispositivo di firma o HSM per la gestione della procedura di firma dei documenti;
- I server di storage, in pratica il sistema dove vengono fisicamente memorizzati tutti i documenti sottoposti a processo di conservazione;
- Responsabile della conservazione, per le attività di amministrazione e monitoraggio;
- Gli Utenti che accedono al sistema di conservazione attraverso credenziali di accesso e in virtù di un profilo funzionale a cui sono associati al fine di effettuare operazioni di versamento e/o consultazione;
- Servizi di Certification Authority e Time Stamp Authority per apporre firme digitali, marche temporali e verifica dei certificati;

Tutti i componenti del Sistema sono protetti da adeguate misure di sicurezza, descritte all'interno del Piano di Sicurezza.

Con il termine "moduli" si intendono varie tipologie di applicativi informatici che compongo il Sistema. Essenzialmente i moduli si dividono in quattro tipologie:

- Servizi: servizi NT, rappresentano la parte server dell'applicativo.
- Manager: applicativo che permette di configurare e gestire un servizio.
- Client: applicativi che si connette ad uno o più servizi.

I moduli software che compongono l'infrastruttura base del Sistema rappresentano il cuore operativo dell'intera soluzione: organizzano, temporizzano e controllano le interazioni tra il database installato lato server e gli altri moduli che si occupano di funzioni specifiche nella gestione elettronica documentale e nella conservazione.

Torna al sommario

8.1 Componenti Logiche

L'insieme dei Servizi e Client che costituiscono lo strato software del Sistema di Conservazione sono stati ideati e sviluppati interamente da Edok srl utilizzando le più recente tecnologie di sviluppo.

L'architettura si articolo su più componenti logici:

- *Autenticazione a autorizzazione:* l'accesso alle diverse aree è limitato dalle autorizzazioni di ogni utente e dai ruoli che ricoprono (amministratore, responsabile, operatore, utente e auditor).

- *Ricezione e importazione:* servizi scalabili dedicati alla ricezione, verifica e importazione dei Pacchetti di Versamento;
- *Archiviazione:* moduli e client dedicati all'Archiviazione dei Pacchetti di Versamento;
- *Consultazione:* applicativi client per la consultazione del Sistema di Conservazione e la richiesta dei Pacchetti di Distribuzione;
- *Distribuzione:* moduli dedicati alla gestione del processo di Distribuzione che prevede la richiesta formale da parte di un utente accreditato e la successiva approvazione del Responsabile, con conseguente generazione di un Pacchetto di Distribuzione.
- *Analisi integrità:* moduli dedicati alla verifica e all'analisi degli oggetti del Sistema di Conservazione, sia in modalità manuale sia automatica.
- *Gestione:* client di configurazione e controllo del Sistema.

Questo lo schema logico ad alto livello del Sistema, che può coinvolgere più server applicativi:

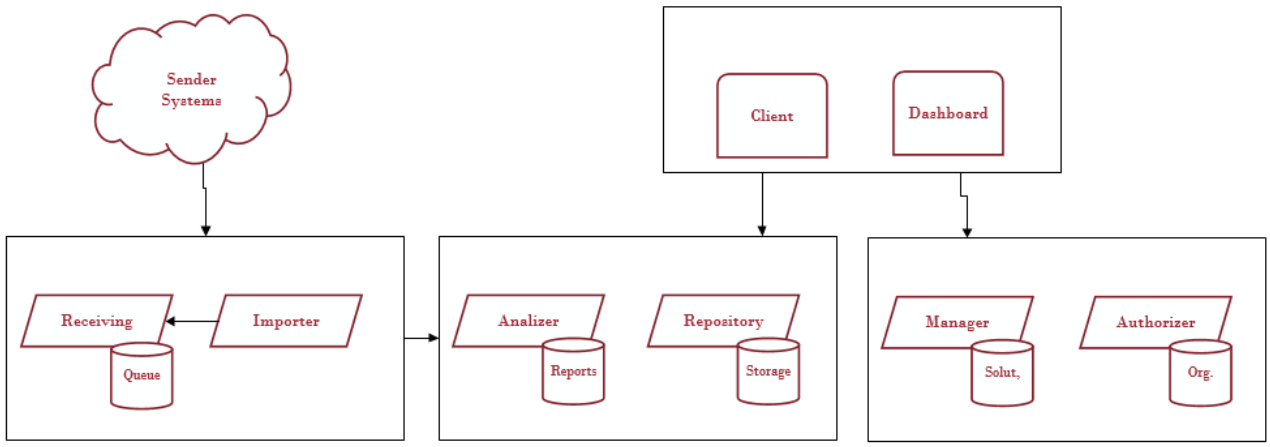

Figura 14 Schema logico Sistema di conservazione

- **Receiving** si occupa di gestire la ricezione dei pacchetti di versamento inviati dai clienti nelle apposite aree FTP. Il modulo analizza ogni file ricevuto e se valido ne esegue l'importazione. In entrambi i casi invia una notifica al cliente. Il modulo può avere più istanze, anche su server distinti, per garantire la scalabilità di una delle fasi più onerose del sistema.
- **Importer:** esegue l'effettiva importazione del pacchetto di versamento nel Sistema, generando la registrazione del pacchetto e il relativo Rapporto di Versamento.
- **Repository:** Il sistema di conservazione è centralizzato in un unico storage dei documenti per evitare inutili duplicazioni dei dati e su tali storage è costruita la gestione delle tre tipologie di pacchetti previste dalla normativa: versamento (PdV), archiviazione (PdA) e distribuzione (PdD). Interagisce direttamente con i database e il file system.
- **Manager:** componente di gestione della configurazione del sistema.
- **Authorizer:** componente per la gestione dell'autenticazione e dell'autorizzazione degli utenti.

- **Analizer:** componente per la verifica dell'integrità degli oggetti del sistema sia su richiesta manuale sia automatica. La consistenza dei dati è garantita dal confronto incrociato degli hash dei file coinvolti, memorizzati negli appositi cataloghi del sistema.

- **Client e Dashboard:** applicativi web e Windows per la consultazione (client HyperView e HyperWeb) e un insieme di tool e dashboard per la configurazione

Torna al sommario

8.2 Componenti Tecnologiche

L'Architettura logica descritta nel capitolo precedente è realizzata dall'iterazione di più componenti software realizzati interamente da Edok srl con molteplici tecnologiche, in particolare nell'ambito dell'eco-sistema Microsoft .NET.

I componenti software del Sistema di Conservazione sono una parte della soluzione HyperDok© fornita da Edok a innumerevoli e prestigiosi clienti e come tali sotto posti ad un ciclo di produzione di certificato.

In particolare, per il Servizio di Conservazione outsourcing, i diversi moduli sono stati pensati per garantirne la scalabilità in base al carico di lavoro e l'unificazione centralizzata della gestione e del monitoraggio.

8.3 Componenti Fisiche

Edok Srl, per l'erogazione dei servizi di conservazione, utilizza propri sistemi allocati presso il Data Center di Brennercom. Si tratta di un Data Center tecnologicamente avanzato, che ha sede a Bolzano ed è collegato direttamente alla rete Highspeed in fibra ottica di Brennercom offrendo quindi un collegamento sicuro e performante alle reti dati mondiali. Grazie a ridondanza multipla e scalabilità di tutte le componenti dell'infrastruttura, rispetta pienamente tutte le richieste di disponibilità, sicurezza e performance.

CUBE dispone di gruppi di continuità statici (UPS) modulari, che offrono un servizio continuo in termini di alimentazione elettrica. La temperatura dell'ambiente è fissata a 23°C +/- 2°C, controllata in modo ridondante da un impianto di condizionamento. L´accesso ai locali è sorvegliato 24 ore su 24 ed è consentito solo a persone autorizzate.

Il Data Center "CUBE" è stato progettato e realizzato seguendo rigidamente le norme costruttive previste da ANSI/TIA/EIA 942, lo standard internazionale rilasciato dalla TIA (Telecommunications Industry Association). Tale standard indica i requisiti minimi da rispettare, suddividendo i vari settori, come ad esempio il condizionamento e l'alimentazione elettrica, in 4 diversi livelli (TIER), secondo la qualità della struttura. Il TIER 1 individua i requisiti minimi necessari per rispettare lo standard, mentre il TIER 4 determina le caratteristiche di un data center all'avanguardia.

La tabella seguente riassume le caratteristiche dei vari settori; le parti colorate rappresentano i requisiti rispettati da CUBE, il data center di Brennercom:

	TIER 1 Basic	**TIER 2** Redundant Components	**TIER 3** Concurrently Maintainable	**TIER 4** Fault Tolerant
Site Availability Disponibilità del sito	99.671%	99.749%	99.982 %	99.995%
Downtown(Hours/Year)	28.8	22.0	1.6	0.4

Ore di disservizio annue				
Operations Center Centro operativo	Not Required	Not Required	Required	Required
Redundant Backbone Pathways Collegamenti ridondanti alla rete dorsale	No	No	Yes	Yes
Redundant Horizontal Cabling Cablaggio orizzontale ridondante	No	No	No	Optional
UPS Redundancy Ridondanza UPS	N	N+1	N+1	2N
Gaseous Suppression System Sistema di spegnimento a gas inerte	No	No	Clean Agents FM200/Intergen	Clean Agents FM200/Intergen
Redundant Access Provider Services Accesso ridondante ai servizi provider	Not Required	Not Required	Required	Required

Particolare riferimento allo standard internazionale è stato fatto in merito a condizionamento, alimentazione elettrica, impianto antincendio e sicurezza. Sono soprattutto questi i settori in cui CUBE soddisfa richieste di livelli (TIER) elevati. CUBE si colloca tra il livello 3 e il livello 4 dello standard sopra menzionato, che è diventato un riferimento internazionale per i costruttori e gestori di Data Center.

L'alimentazione elettrica è assolutamente ridondante, scalabile e può contare su una struttura di emergenza. L'impianto di condizionamento è realizzato nel rispetto della più ampia ridondanza e scalabilità, basandosi sul principio dei "corridoi caldi e dei corridoi freddi". L'innovativo impianto antincendio si fonda su un gas inerte, l'HFC-227ea, un prodotto in grado di assicurare risultati eccellenti in modo sicuro (senza rischio alcuno). Inoltre, CUBE soddisfa tutte le richieste nel campo della sicurezza. Oltre a un sistema di videosorveglianza 24 ore su 24, un sistema di badge e rilevamento delle impronte digitali controlla l'accesso fisico al Data Center (Single point of entry).

Brennercom, oltre ad altri riconoscimenti e certificazioni, nell'ottobre 2003 ha ottenuto l'importante CIS - Certification Information Security-Management System – ISO/IEC 27001. Si tratta di una norma internazionale che fornisce i requisiti di un Sistema di Gestione della Sicurezza nelle Tecnologie dell'Informazione (Information Security Management System - ISMS).

Poiché l'informazione è un bene che aggiunge valore all'impresa e ormai la maggior parte delle informazioni sono custodite su supporti informatici, ogni azienda deve essere in grado di garantire la sicurezza dei propri dati in un contesto in cui i rischi informatici causati dalle violazioni dei sistemi di sicurezza sono in continuo aumento.

L'obiettivo dello standard ISO/IEC 27001 è proprio quello di proteggere i dati e le informazioni da ogni tipo di minaccia, al fine di assicurarne l'integrità, la riservatezza e la disponibilità e di fornire i requisiti per adottare un adeguato sistema di gestione della sicurezza delle informazioni (SGSI) finalizzato ad una corretta gestione dei dati sensibili dell'azienda.

8.3.1 Infrastruttura

CUBE, il Data Center di Brennercom, si trova a 700 m. dall'uscita Autostradale di Bolzano Sud al 2° piano del palazzo Brennercom. CUBE è dotato di un'infrastruttura all'avanguardia.

Il CUbE di Bolzano è stato strutturato secondo lo Standard ANSI/TIA/EIA come segue:

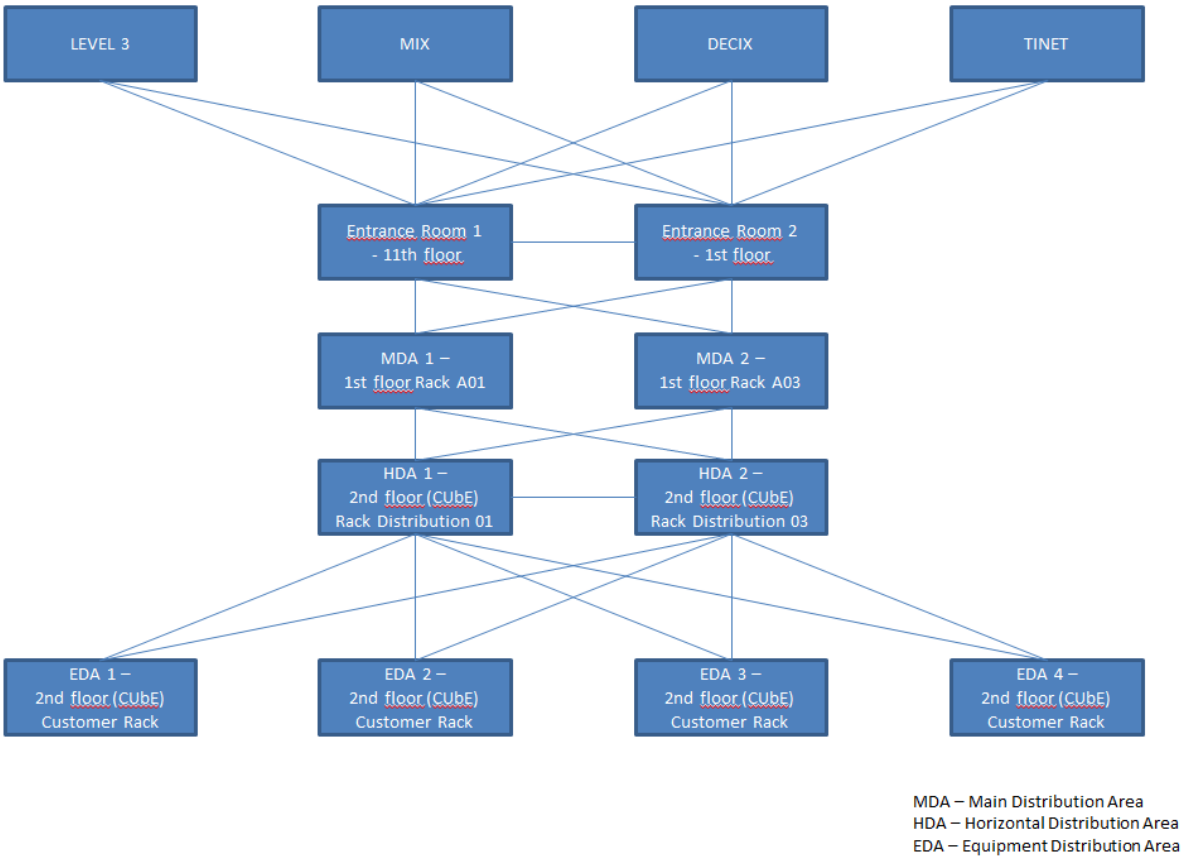

Figura 15 Struttura Data Center

8.3.2 Cablaggio

Per garantire l'integrità dei dati trasportati, è fondamentale schermare i cablaggi, evitando di esporli a interferenze elettriche. Questo significa soprattutto creare due percorsi distinti: uno per il cablaggio dati e l'altro per il cablaggio elettrico, perché campi elettrici e magnetici possono influenzare le proprietà trasmissive. Inoltre, è necessario mantenere una divisione anche per evitare eventuali surriscaldamenti.

Secondo quanto previsto dallo standard ANSI/TIA/EIA 942, sono i cablaggi sono stati realizzati nel rispetto delle seguenti regole:

- i cavi di alimentazione elettrica sono stati posati nel pavimento flottante raffreddato, sistemandoli in canalizzazioni separate dai cavi dati in rame

- i cavi dati in rame sono stati posati in canalizzazioni separate da cavi dati in fibra ottica, che si trovano in canaline in PVC predisposti lungo il soffitto

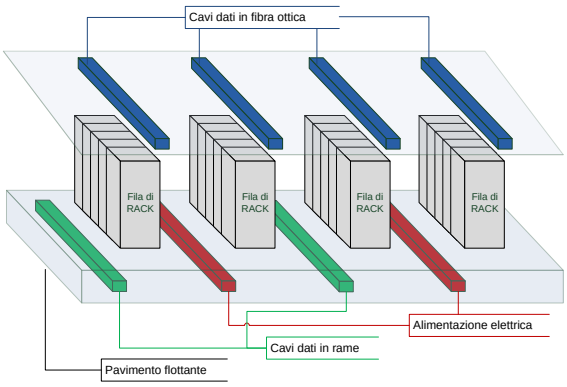

Figura 16 Cablaggi

8.3.3 Alimentazione

I server hanno bisogno di essere alimentati ininterrottamente, senza cali o picchi di tensione, per evitare lo spegnimento o addirittura danni alle apparecchiature. È quindi necessaria un'alimentazione elettrica costante e continua. CUBE è dotato di un sistema di alimentazione elettrica che soddisfa appieno tali requisiti. L'alimentazione elettrica primaria fino alla cabina di trasformazione è garantita da un collegamento ridondante alla rete dell'Azienda Energetica S.p.A.. Oltre la metà dell'energia che l'Azienda Energetica mette a disposizione è corrente autoprodotta, mentre la parte restante è fornita dal gestore nazionale. L'energie elettrica autoprodotta e acquistata permettono di raggiungere un altissimo livello di affidabilità in termini di continuità del servizio. In occasione del blackout del 2003 l'azienda elettrica ha ristabilito il servizio in soli 20 minuti – come primo fornitore nazionale (Fonte: Azienda Energetica S.p.A.).

L'alimentazione elettrica diretta è gestita da 2 UPS (BENNING – ENERTRONIC modular) con potenzialità di 480kVA ciascuno, scalabili con moduli in parallelo da 40kVA ciascuno (ridondanza n+1 per UPS). L'alimentazione elettrica è doppia (linea A+B), mentre la distribuzione attualmente è dimensionata per ogni armadio per un potenziale di 12 kW.

In mancanza dell'alimentazione elettrica primaria, la continuità è garantita dagli UPS. Questi si appoggiano a gruppi di batterie fintanto che non viene fornita energia di soccorso da un gruppo elettrogeno a gasolio (EUROGEN©), che è in grado di erogare 810kVA e di garantire una completa autonomia fino al ripristino della rete di alimentazione primaria. Questo motore Diesel ha una cilindrata pari a 20.000cc con una potenza di 1.000cv.

I gruppi di continuità statici (UPS) sono del tipo electronic modular; sono composti da singoli moduli UPS in parallelo, dove ogni modulo UPS può essere sostituito senza interrompere l'alimentazione al carico (hot-plug) e senza dover ricorrere al by-pass.

Questa configurazione garantisce la massima affidabilità al sistema di continuità (MTBF: mean time between failure) e la massima facilità di manutenzione (MTTR: mean time to repair), garantendo una disponibilità (D = MTBF/(MTBF+MTTR) = 0.9999991) (Fonte: BENNING) unica nel campo degli UPS.

Queste caratteristiche, unite al rendimento del 94%, bassa distorsione d'ingresso (<5%), ridotte dimensioni d'ingombro, facile espansibilità nel tempo, bassi costi di manutenzione, garantiscono un sistema con ottime performance.

Per garantire la massima affidabilità del sistema, periodicamente si effettuano test e attività di manutenzione.

I Server-Rack (RITTAL) del Data Center dispongono di due alimentazioni elettriche fisicamente separate. Ciascun armadio dispone di 3 kW. Su richiesta è possibile aumentare l'alimentazione fino a un'energia massima assorbita di 12 kW per armadio, senza alcuna modifica di tipo impiantistico. Il superamento di questa soglia è naturalmente possibile, ma trattandosi di una soluzione "a progetto", implica una modifica delle protezioni elettriche. L´alimentazione elettrica viene fornita tramite attacchi del tipo C13/SHUKO.

Grazie a un modernissimo sistema di supervisione delle prese di distribuzione è possibile monitorare i parametri e i consumi elettrici.

Torna al sommario

8.3.4 Condizionamento

Il condizionamento è una componente fondamentale di tutte le infrastrutture IT. I più importanti produttori di server come ad esempio HP, Intel, Dell e Compaq, garantiscono un funzionamento dei sistemi fino a una temperatura ambientale di 30°C – 35°C. Superate tali soglie, i sistemi eseguono uno shut down automatico, con conseguente interruzione del servizio da loro erogato.

CUBE, il Data Center di Brennercom, presenta elevati standard di condizionamento. Attraverso il principio dei "corridoi caldi/corridoi freddi" è garantita una temperatura di 23°C +/- 2°C anche a pieno regime di tutti i sistemi. Il controllo della temperatura è effettuato anche nei locali tecnici che contengono infrastrutture vitali per il corretto funzionamento del Data Center come ad esempio il locale UPS. I locali tecnici sono controllati da un elevato numero di sonde, che segnalano l'eventuale superamento di soglie impostate. Queste sonde sono installate soprattutto sulle porte frontali dei Rack, ad altezze diverse.

Per ottimizzare la circolazione dell'aria, viene applicato il principio dei "corridoi caldi/corridoi freddi". In un corridoio freddo l'aria refrigerata è rilasciata dagli armadi condizionatori attraverso il pavimento flottante. Dal lato dei corridoi freddi si trova la parte frontale dei server, che aspira l'aria fredda. L'aria riscaldata dai server è invece rilasciata sul retro (corridoi caldi), sale verso l'alto ed è aspirata dalle unità di trattamento aria (UTA).

Gli armadi condizionatori sono inoltre dotati di un AFPS (Automatic Floor Pressurization System). Questo mantiene una pressione costante pari a 20mPa all´interno del pavimento flottante. Appena viene aperta una plotta del pavimento per fare lavori di manutenzione e aria fredda defluisce quindi nella sala, questo viene registrato dagli armadi condizionatori, che aumentano il flusso di aria rilasciata, finché non viene ristabilita la pressione iniziale.

In alcune aree della Server Farm il condizionamento avviene secondo il modello ICS (Inside Cooling System). In questi casi l´aria fredda viene rilasciata direttamente all´interno dell´armadio. Non avviene più un raffreddamento dell´intero corridoio, ma l´aria fredde viene rilasciata in modo mirato e dedicato per ogni singolo armadio.

Per realizzare tutto ciò è stato installato un impianto ad acqua refrigerata (Chiller + UTA). Nel Data Center sono attualmente installate 4 UTA da 180 kW frigoriferi ciascuna, che possono crescere di numero a seconda dell'incremento del numero di rack installati. Inoltre sono state installate 3 unitá Chiller da 200 kW ciascuno.

Le unità perimetrali UNIFLAIR si distinguono per una serie di plus innovativi quali:

- ventilazione ottimizzata a commutazione elettronica (EC), elevata efficienza energetica e possibilità di variazione continua della portata d'aria
- controllo della pressione sotto il pavimento in modo da garantire una corretta distribuzione dell'aria nell'ambiente grazie all'innovativo sistema AFPS (Automatic Floor Pressurization System)
- controllo della temperatura in mandata

- sistema di regolazione integrato che ottimizza il funzionamento delle diversi componenti del sistema attraverso il monitoraggio continuo dei parametri operativi
- integrazione con i chiller esterni dotati di intelligent free cooling
- ampia connettività ai sistemi di supervisione grazie alla possibilità di dialogare con i più diffusi protocolli di comunicazione.

Torna al sommario

8.3.5 Antincendio

Per custodire i propri server in un ambiente sicuro, è necessario poter contare anche sulla presenza di un'adeguata struttura antincendio. Questa è costituita sia da un impianto di rilevazione che di estinzione incendi.

CUBE è dotato di un innovativo sistema di rilevamento ed estinzione incendi in grado di individuare immediatamente un principio d'incendio grazie a 66 rilevatori ottici installati sia nel soffitto che nel pavimento flottante del data center. Il sistema di spegnimento è a saturazione totale HFC 227 EA (eptafluoropano), un gas puro che non contiene particolati né residui oleosi, ha un minimo effetto di deterioramento e permette uno spegnimento rapido e ad alta efficacia, senza danneggiare le apparecchiature presenti nel locale. Il gas chimico HFC-227ea è innocuo dal punto di vista tossicologico ed estingue senza lasciare tracce.

L'estinguente HFC-227ea: Gli impianti di spegnimento a gas chimico HFC-227ea (FM200 ®) - Eptafluoropropano (CF^3CHFCF^3) sono da considerarsi dei sistemi a clean agent. A differenza dell'Halon 1301, che interveniva sull'incendio per via chimica, l'estinguente HFC-227ea agisce soprattutto per raffreddamento fisico, rimuovendo il calore dalla fiamma. Per la sua volatilità e ridottissima tossicità, questo tipo di estinguente è molto diffuso negli ambienti a saturazione totale. Risulta essere il gas chimico in commercio meno dannoso per l'uomo e l'ambiente. Il principio di funzionamento del gas HFC-227ea è quello della saturazione dell'ambiente (total flooding); questo sistema di funzionamento ha il grande vantaggio di non dover preoccuparsi dell'ubicazione dei materiali a rischio, né della loro conformazione, perché crea condizioni omogenee in tutto l'ambiente.

Quando i rilevatori all'interno della sala o del pavimento captano un incendio, scatta l'allarme antincendio. Dopo una breve pausa, necessaria all'evacuazione del locale tecnologico, si aprono le valvole da cui fuoriesce il gas contenuto in apposite bombole. L'estinguente arriva alle valvole allo stato liquido e si diffonde poi nella stanza in forma gassosa.

Contemporaneamente viene avvisato sia il personale specializzato Brennercom che i vigili del fuoco di Bolzano, la cui sede è vicina al Data Center, in via Druso 116, 39100 Bolzano.

Nel pieno rispetto della norma UNI ISO 14520 Clean agent extinguishing system, in fase di collaudo del Data Center è stato effettuato un test di integrità volumetrica dell'ambiente. Si tratta di una procedura che permette di determinare il tempo minimo di permanenza del gas all'interno del locale. La norma UNI ISO prevede che il tempo minimo di permanenza del gas all'interno del locale debba essere pari a 10 minuti, per permettere lo spegnimento assoluto e definitivo di qualsiasi fonte di calore. Durante le prove, dopo 22 minuti, su varie altezze del locale protetto venivano misurate ancora concentrazioni di sostanza estinguente superiori all'85% della concentrazione di progetto (7,86%). Questo indica che il locale è schermato molto bene, permettendo quindi uno spegnimento sicuro e completo. Il test d'integrità effettuato è stato pertanto ampiamente superato.

Torna al sommario

8.3.6 Fattore di rischio acqua

L'acqua può causare danni gravissimi a un'infrastruttura IT e rappresenta pertanto un fattore di rischio molto alto. Di conseguenza, in CUBE è stata realizzata una vasca raccogli acqua che segue i tubi del condizionamento. È leggermente inclinata, è dotata di uno scarico e di rilevatori all'interno. Questo permette di rilevare il prima possibile eventuali perdite d'acqua e di evitare danni irreparabili alla struttura.

Torna al sommario

8.3.7 Sicurezza

Oltre a garantire massima affidabilità in termini di performance in quanto a alimentazione elettrica, condizionamento e impianto antincendio, è necessario potersi affidare anche a un locale sicuro in termini di accesso ai server e quindi ai dati in esso depositati. Al riguardo, CUBE dispone di sistema di sicurezza all'avanguardia.

In principio è stata effettuata un'analisi del rischio. L'analisi del rischio è richiesta dalla normativa sulla sicurezza dell'informazione (ISO 27001). Nello specifico si tratta di una procedura sistematica che consente di valutare i rischi in modo ampio e completo, rendere trasparenti contesti complessi e affrontare ambiti che potrebbero presentare lacune o non essere del tutto sicuri. Il processo di analisi è suddiviso in tre parti:

- Identificazione del rischio – a quali rischi è esposta la mia azienda
- Stima del rischio – quali rischi si verificano e con quale probabilità; analisi dei rischi nel senso più stretto del termine
- Gestione del rischio – identificazione delle cause e pianificazione dei provvedimenti.

Sulla base di questa analisi sono stati definiti i seguenti provvedimenti:

L'accesso autonomo è controllato con sistema a passaggio individuale e autenticazione biometrica. E' attivo un sistema di video-sorveglianza dei locali, 24 ore su 24, sette giorni su sette, con impianto di *alerting* e registrazione. Inoltre, ogni armadio (rack, ½ rack, ¼ rack) è chiuso a chiave.

Modalità di accesso

Il sistema di controllo degli accessi a più livelli assicura che solo persone autorizzate accedano al Data Center. Per permettere l'accesso di una persona è necessaria l'autorizzazione del rappresentante legale dell'azienda e un copia della carta d'identità. Dopo aver esaminato i documenti, il collaboratore riceverà diritti di accesso specifici (sala visitatori, sala Co-Location). I collaboratori, ai quali è stato autorizzato l'accesso alla sala Co-Location, dovranno depositare la propria impronta digitale elettronica. Brennercom garantisce il trattamento dei dati personali nel pieno rispetto delle normative in vigore sulla privacy. La sala visitatori e la sala Co-Location sono video-sorvegliate e l'accesso avviene sotto stretta osservazione del personale di sicurezza Brennercom.

L'accesso alla sala Co-location del Data Center avviene esclusivamente attraverso una bussola di entrata (Single Point of Entry), che controlla sia la validità del badge sia quella delle impronte digitali. Tutti gli ingressi sono registrati da un software di accesso.

Anche l'accesso al locale avviene nel rispetto delle norme di riferimento per servizi di Sicurezza delle Informazioni (ISO 27001).

Videosorveglianza

Il Data Center è sottoposto a videosorveglianza 24 ore al giorno, 365 giorni l'anno. Questo consente di sorvegliare tutto ciò che avviene all'interno dei locali tecnologici e di impedire l'accesso alle persone non autorizzate. Il sistema attiva direttamente un allarme grazie alla funzione Video-Motion-Detection (VMD) e inizializza l'intervento del personale specializzato.

Le videocamere registrano 25 frame / sec.

Torna al sommario

8.3.8 Accesso alla rete dati

È fondamentale fornire a server, ovunque siano collocati, una connettività adeguata al loro uso. Questo è necessario in prima linea per permettere un accesso alle strutture e consentire una gestione delle stesse, anche da remoto. Installare i propri server in CUBE offre anche la possibilità di avere una connettività adatta a ogni singolo server e al suo utilizzo.

Il server o i server collocati nel Data Center Brennercom, affinché possano scambiare dati con il mondo esterno devono necessariamente avere attivato almeno una delle seguenti connettività:

- Connettività Internet: intesa come collegamento Internet pubblico fino all'interfaccia Edok, ovvero la porta a cui Edok è collegato con i suoi server.
- Connettività Intranet: intesa come collegamento dati interaziendale e limitato da una parte dalla consegna in Brennercom del circuito o dei circuiti provenienti dalla/e sede/i e dall'altra dalla porta a cui Edok è collegato con i suoi server.

Per questo tipo di connettività, Brennercom è in grado di garantire livelli di servizio ben superiori a quanto sia possibile offrire presso la sede di Edok Srl, dove il collegamento di accesso risulta più vulnerabile a eventuali disservizi. Infatti, la connettività Internet presso CUBE è completamente ridondata, di apparato, e attraverso anello ottico raggiunge il MIX (Milan Internet Exchange). Per quanto riguarda l'Intranet, invece, la LAN interna è completamente "in doppio" fino allo switch di consegna, virtual router compreso.

Il collegamento del Data Center alle reti dati mondiali è ad alta affidabilità, ridondante al 100% e avviene attraverso un allacciamento alla rete IP/MPLS di Brennercom, come mostrato nella seguente immagine.

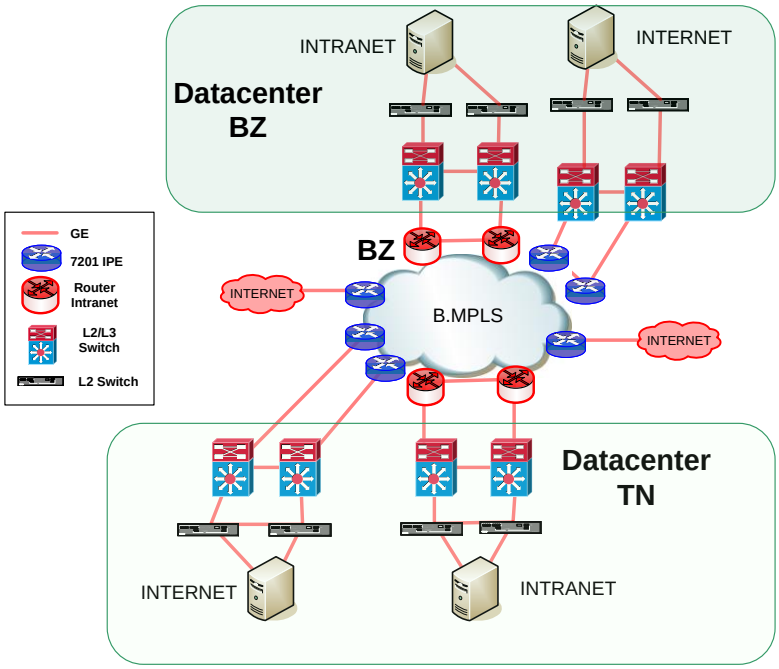

Figura 17 Collegamento del centro di calcolo alla rete IP/MPLS

Tecniche innovative di switching e virtualizzazione nei Data Center di Bolzano e Trento permettono l'allacciamento dei sistemi dei Clienti alla rete IP/MPLS. L'accesso alla rete MPLS avviene solitamente attraverso una porta di raccolta dello Switch di aggregazione di livello 3 e può avvenire su richiesta anche in modo ridondante (accesso anche attraverso un secondo Switch di aggregazione). Durante la pianificazione dell'accesso alla rete è stata riservata particolare attenzione alla riduzione del numero di apparati Livello 2 e Livello 3. Questo permette di evitare inutili e fastidiosi ritardi di rete, garantendo l'accesso più veloce alla rete aziendale e/o ai vari Internet Service Provider.

Tutti gli Switch di CORE hanno alimentatori e processori ridondati, mentre gli Switch dedicati al CUbE sono alimentati in modo ridondato tramite interruttori di trasferimento statici. Tutta la topologia di rete è stata progettata in modo ridondante.

„No connectivity – no security issue" – Secondo questo principio, non è ammissibile che Clienti possano avere accesso ad Internet attraverso collegamenti non sicuri. L'accesso a Internet avviene quindi attraverso un Firewall centrale (Managed Firewall).

Torna al sommario

8.4 Procedure di gestione e di evoluzione

Il progetto di evoluzione del sistema di conservazione prende il via con la redazione di un documento di sviluppo interno all'azienda che viene valutato dal Responsabile del servizio di Conservazione di concerto con i consulenti legali, di sicurezza ed archivistici

Per ogni evoluzione del sistema di conservazione definitivamente adottata, saranno conseguentemente aggiornate le procedure per la gestione delle varie componenti (logiche, fisiche e tecnologiche), il piano della sicurezza ed il manuale della conservazione.

L'aggiornamento del Sistema o parti di esso è preventivamente richiesta al Responsabile Software e se necessario al Responsabile della Conservazione in base ad un processo di approvazione che prevede di indicare le motivazioni che spingono all'aggiornamento e le parti interessate.

L'aggiornamento effettivo deve seguire apposite procedere che partono dalla verifica del piano di test (manuali e automatici) fino alle necessarie operazioni di backup, interruzione, aggiornamento, verifica e rimessa online delle parti modificate.

Qualsiasi attività diretta all'evoluzione del sistema di conservazione sarà effettuata nel rispetto degli SLA (Service Level Agreement) concordati con i clienti.

Torna al sommario

9 MONITORAGGIO E CONTROLLI

Il sistema è sottoposto ad una attività di monitoraggio costante al fine di garantire la piena funzionalità di ogni componente del sistema, a partire dall'inizio dell'attività di conservazione.

Torna al sommario

9.1 Procedure di monitoraggio

L'attività di monitoraggio può essere distinto in monitoraggio applicativo e monitoraggio infrastrutturale.

Monitoraggio applicativo

Rispetto al versamento e alla verifica dei PdV, il sistema produce e restituisce un log sia nel caso di esito positivo della procedura che nel caso di errore. Nel caso di errore il file log viene inoltrato per email al produttore del pacchetto specifico. Ogni file log creato dal sistema, sia esso di errore o di successo, viene conservato nel sistema per un periodo di 30 giorni.

Nella fase di esibizione, il monitoraggio viene eseguito tramite la verifica quotidiana della corretta operatività delle componenti che garantiscono l'accesso, la ricerca, la consultazione e l'esibizione dei documenti sottoposti a conservazione.

Monitoraggio infrastrutturale

È il monitoraggio della totalità dei dispositivi hardware che costituisce il sistema di conservazione di Edok srl (elaboratori, storage e dispositivi di networking)

Edok srl prevede la possibilità di farsi assistere nell'attività di monitoraggio e controllo anche da parti terze adeguatamente selezionate, delle quali verrà di volta in volta data comunicazione nel singolo contratto di sevizio.

Torna al sommario

9.2 Verifica dell'integrità degli archivi

Edok srl ha previsto un'attività periodica (mensile) di verifica dell'integrità egli archivi e della leggibilità dei medesimi.

Il sistema consente di gestire in maniera flessibile tale attività, ad esempio mediante la possibilità di rendere automatico il controllo, mediante l'apposita configurazione prevista.

Il controllo dell'integrità si realizza mediante il confronto dell'hash ricalcolato per ciascuno dei documenti sottoposti a conservazione con il primo hash, dello stesso documento, che era stato originariamente memorizzato nel sistema.

Il controllo della leggibilità consente di verificare che tutti i singoli bit siano correttamente leggibili.

Al termine di ogni verifica effettuata è prodotto un report che è portato a conoscenza del Responsabile del servizio della conservazione al fine di constatare la corretta esecuzione della verifica o evidenziare le anomalie riscontrate.

Torna al sommario

9.3 Soluzioni adottate in caso di anomalie

Le anomalie del sistema di conservazione, che vengono evidenziate al termine della fase di controllo, possono essere di diversa tipologia. Esse possono differenziarsi molto avendo riguardo alla collocazione nel processo di conservazione dell'evento che le ha causate. Le soluzioni di volta in volta adottate per risolvere le eventuali anomalie possono, quindi, essere sostanzialmente eterogenee in ragione della natura e della gravità rilevate.

I rischi principali identificati nell'ambito della gestione del Sistema Informatico sono:

- Malfunzionamento del Sistema software;
- Guasto al dispositivo di firma;
- Indisponibilità del sito della Certification Authority.

- Guasto all'Hardware o ai sistemi di connettività

Di seguito vengono riportate le principali contromisure individuate:

Malfunzionamento del Sistema Software

Il Sistema Informatico utilizzato per la conservazione è governato e gestito dal Conservatore, sotto il controllo del Responsabile dei Sistemi Informativi.

La struttura hardware del Sistema Informatico in esercizio risponde ai requisiti di alta affidabilità e di ridondanza in modo da garantire un esercizio continuo. In caso di compromissione di tale struttura, la versione in esercizio può essere ripristinata in tempo reale utilizzando gli apparati ridondanti del Sistema. Qualora ciò non fosse possibile si dovrà ricorrere alla copia originale del Software e provvedere alla relativa installazione su un nuovo apparato.

Guasto al dispositivo di firma

In caso di guasto al dispositivo di firma occorre procedere alla individuazione della tipologia di guasto e provvedere immediatamente alla sua riparazione. Nel caso di smart card o token-USB, il problema può essere risolto utilizzando il dispositivo sicuro di un altro Delegato.

Indisponibilità del sito della TSA

La compromissione del sito della Time Stamping Authority per il rilascio della marca temporale da apporre sull'evidenza informatica a chiusura del processo di conservazione, è un evento particolarmente remoto, in quanto implementa politiche di continuità di erogazione del servizio con SLA di altissimo livello.

Guasto del Server Network Time Protocol

I server NTP sono due, un primario e un secondario. Il server secondario entra in funzione nel caso in cui il primario si guasti.

Guasto all'hardaware o ai sistemi di connettività

Con il supporto di Brennercom, EDOK ha sviluppato un sistema di prevenzione e gestione dei guasti all'hardware e ai sistemi di connettività denominato *Assurance*. *Assurance* è l'insieme delle attività finalizzate al ripristino dell'erogazione ottimale del servizio in caso di interruzione o degrado dello stesso, dovuto a guasti o altri eventi. Il principale obiettivo perseguito dal processo di *Assurance* è il ripristino del servizio nel minor tempo possibile.

In breve, il processo di assurance è suddiviso nei sottoprocessi di seguito elencati:

- Incident Management
    - Incident Request Registration
        - notifica e registrazione della richiesta d'intervento
        - tentativo di diagnosi e di problem solving di livello 0
    - Incindent Request Assignment
        - assegnazione per competenza del ticket
    - Incident Request Tracking
        - diagnosi di livello 1 e/o 2
        - individuazione della causa di disservizio/malfunzionamento
        - definizione delle attività inerenti la rimozione del disservizio/malfunzionamento

- Incident Request Resolution
  - rimozione del guasto o malfunzionamento
  - chiusura del ticket.

- Request Reporting
- Problem Management

I singoli punti vengono di seguito descritti così come concordati con Brennercom.

Incident Management

Incident Request Registration

L'Incident Request Registration consiste nell'attività effettuata dalla struttura di HD/NOC di ricezione e registrazione di una segnalazione di un guasto (malfunzionamento) o di una interruzione del servizio (definiti secondo lo standard ITIL come incident). La notifica di un guasto o di un'interruzione di servizio avviene attraverso una segnalazione dell'allarme del sistema di monitoraggio o da parte di personale autorizzato di Edok Srl attraverso una chiamata al numero gratuito dedicato. Se la segnalazione viene effettuata da Edok Srl, la chiamata è seguita da un'e-mail alla struttura di HD/NOC contenente il relativo "ticket".

Se la segnalazione viene invece fatta dalla struttura di HD/NOC, quest'ultima informerà Edok, chiamandolo al numero da lui stesso comunicato.

La chiamata viene registrata nel sistema di "Trouble Ticketing" di Brennercom che inoltra la richiesta di intervento alle strutture di Brennercom preposte per la diagnosi e la rimozione delle anomalie.

A livello di Incident Request Registration è prevista, contestualmente alla ricezione, l'attività di identificazione della fonte di segnalazione nonché dell'autorizzazione ad effettuare la segnalazione prima di accettarla. Dopo questa fase, è previsto che venga effettuato un tentativo di diagnosi e problem solving di Livello 0, possibilmente rimanendo ancora in contatto con il segnalatore (personale Edok). L'operatore della struttura di HD/NOC a tal fine interroga il TTS di Brennercom, al fine di verificare se per il tipo di segnalazione effettuata da Edok esiste un piano di elaborazione e soluzione. In caso di esito positivo, l'operatore della struttura di HD/NOC raccoglie le informazioni richieste ed esegue le attività previste dal workflow proposto.

Incident Request Assignment

Qualora il TTS Brennercom non suggerisca un modello di soluzione per la rimozione del guasto o dell'interruzione del servizio e il tentativo di diagnosi e di problem solving di Livello 0 non abbia chiuso l'istanza segnalata (anche se la soluzione del guasto è conosciuta), il ticket verrà trasferito per competenza agli specialisti di rete o alla struttura tecnica territoriale con tutte le informazioni tracciate nello stato precedente:

- identificativo del ticket (numero progressivo ed univoco corrispondente al trouble ticket)
- data ed ora dell'apertura del ticket
- data ed ora del guasto dichiarato da Edok Srl
- nome dell'operatore di HD/NOC che ha preso in carico la segnalazione
- dati di colui che ha effettuato la segnalazione (nome, numero da richiamare, e-mail,…)

- tipologia della segnalazione (guasto, informazione, …)
- sede di erogazione del servizio interessato dal guasto
- caratteristiche del guasto riscontrato (livello di gravità)
- esito dell'attività di diagnosi di livello 0
- gruppo tecnico specialistico o squadra tecnica territoriale a cui viene inoltrato il ticket per l'ulteriore diagnosi (di livello 1 e 2) o per la rimozione del guasto o dell'interruzione del servizio
- altre informazioni.

L'inoltro del ticket agli specialisti di rete o alla struttura tecnica territoriale viene tracciata aggiornando i sistemi di Trouble Ticketing di Brennercom e di Edok Srl.

Incident Request Tracking

Quest'attività comprende le attività di diagnosi, individuazione e determinazione della causa del guasto o dell'interruzione di servizio ed il ripristino del corretto funzionamento dello stesso. In un'ottica di escalation di competenza delle istanze assegnate, il ripristino del servizio può coinvolgere anche i fornitori di tecnologie o terzi. Ove necessario sono previste attività di "problem determination and solving" che coinvolgono o delegano le attività di risoluzione a strutture (in particolare le squadre della Struttura Tecnica Territoriale) che intervengono direttamente nei luoghi interessati dal disservizio. Rientrano in queste attività gli interventi sugli apparati presso i locali di Edok e/o la localizzazione di guasti su apparati di rete. Qualora si renda necessario un intervento in loco presso i locali di Edok, tale intervento è effettuato secondo lo specifico Service Level Agreement relativo al servizio in oggetto. Edok si impegna a rendere accessibili i locali in caso di necessità di intervento in loco da parte di Brennercom.

Tali interventi continueranno ad essere tracciati sul sistema informativo di Brennercom e di Edok, evidenziando i cambiamenti di stato ed eventualmente le caratteristiche del Ticket.

Incident Request Resolution

È l'attività conclusiva della "problem determination" di qualunque livello e consiste nel ripristino, in caso di guasto o interruzione di servizio, delle normali funzionalità. La risoluzione del guasto o dell'interruzione del servizio è documentata dal costante aggiornamento del ticket sul sistema TTS di Brennercom. L'aggiornamento riguarda un insieme di informazioni fra cui le azioni intraprese dagli operatori del Centro Servizi e dai tecnici di rete o della struttura tecnica territoriale per risolvere la criticità.

Una volta aggiornato il ticket, la struttura di HD/NOC effettua gli aggiornamenti sul Sistema di Trouble Ticketing e provvederà a fare le verifiche del caso e a chiudere l'istanza.

Dalla data e dall'ora di risoluzione del guasto o dell'interruzione del servizio indicato nel rapporto finale, il Centro Servizi di Brennercom continuerà a monitorare il servizio ed in particolare il collegamento di rete interessato per ulteriori 48 ore.

Request Reporting

Ad intervalli di tempo concordati o ad ogni cambio di stato di un ticket/incident, Brennercom provvede a contattare Edok, informandolo sullo stato di avanzamento della procedura di soluzione del guasto o interruzione di servizio.

- Primo rapporto: entro 30 minuti dall'apertura dell'istanza in orario d'ufficio e entro 60 minuti al di fuori di questo orario, i tecnici contatteranno Edok per fornire una prima diagnosi del problema. Il numero chiamato può essere stabilito di volta in volta. Contestualmente viene aggiornato il ticket aperto sul sistema di Trouble Ticketing di Edok Srl.
- Rapporti successivi: in seguito al primo rapporto, il HD/NOC di Brennercom contatterà Edok Srl ogni 60 minuti per informarlo sullo stato dell'istanza aperta e aggiornerà contestualmente il ticket aperto sul sistema.

Problem management

Il compito principale dell'incident management è il ripristino del servizio per Edok Srl in tempi rapidi, implementando anche soluzioni work-around per garantire i livelli di servizio concordati. Il problem management, coinvolgendo operatori tecnici specializzati di 3° livello, analizza invece più a fondo le cause dei vari guasti e interruzioni di servizio, attivandosi per elaborare soluzioni in grado di risolvere definitivamente le anomalie riscontrate.

Torna al sommario

9.4 Registro delle anomalie

Tutte le anomalie riscontrate, unitamente alle azioni intraprese per contrastarle e impedire il loro ripresentarsi, sono dettagliate in un registro dei verbali delle anomalie mantenuto costantemente aggiornato e reso disponibile presso il sistema di conservazione.

Il registro viene tenuto dai vari responsabili (ciascuno in relazione alle proprie competente) e viene costantemente supervisionato dal Responsabile del servizio di conservazione.

Torna al sommario