MANUALE

DEL SERVIZIO DI CONSERVAZIONE

0365.690019
info@edok.it
www.edok.it
Via dei Traversi 25 - 25079 **Vobarno** (BS)
Via Cacciamali 67 - 25125 **Brescia** (BS)
P.IVA / C.F 02663950984
CAP.SOC. € 205.000 int.ver

Sommario

1. SCOPO E AMBITO DEL DOCUMENTO 4
2. TERMINOLOGIA (GLOSSARIO E ACRONIMI) 5
3. NORMATIVA E STANDARD DI RIFERIMENTO 13
3.1 Normativa di riferimento 13
3.2 Standard di riferimento 14
3.3 Certificazioni del Conservatore 14
4. RUOLI E RESPONSABILITA' 16
5. STRUTTURA ORGANIZZATIVA PER IL SERVIZIO DI CONSERVAZIONE 17
5.1 Organigramma 17
5.2 Strutture organizzative 18
5.3 Cessazione dei servizi di conservazione 20
6. OGGETTI SOTTOPOSTI A CONSERVAZIONE 21
6.1 Classificazione 21
6.2 Tipologie documentali 21
6.3 Formato dei file 22
6.4 Pacchetto di Versamento 22
6.4.1 Versamento PdV via FTP in formato zip 22
6.4.2 Versamento automatico FE 23
6.5 Pacchetto di Archiviazione 24
6.6 Pacchetto di Distribuzione 25
7. IL PROCESSO DI CONSERVAZIONE 26
7.1 Modalità di acquisizione dei pacchetti di versamento per la loro presa in carico 26
7.2 Verifiche effettuate sui pacchetti di versamento e sugli oggetti in essi contenuti 28
7.3 Accettazione dei pacchetti di versamento e generazione rapporto di versamento 28
7.4 Formazione del Pacchetto di Archiviazione 28
7.5 Richiesta e gestione del pacchetto di distribuzione ai fini dell'esibizione 29
7.6 Predisposizione di misure a garanzia dell'interoperabilità e trasferibilità ad altri conservatori 29
7.7 Cancellazione dei documenti 29
8. IL SISTEMA DI CONSERVAZIONE 31
8.1 Componenti Logiche 31
8.2 Componenti Tecnologiche 33
8.3 Componenti Fisiche 33
8.3.1 Infrastruttura 35
8.3.2 Cablaggio 35
8.3.3 Alimentazione 36
8.3.4 Condizionamento 36

8.3.5 Antincendio 37
8.3.6 Fattore di rischio acqua 38
8.3.7 Sicurezza 38
8.3.8 Accesso alla rete dati 39
8.4 Procedure di gestione e di evoluzione 40
9. MONITORAGGIO E CONTROLLI 42
9.1 Procedure di monitoraggio 42
9.2 Verifica dell'integrità degli archivi 42
9.3 Soluzioni adottate in caso di anomalie 42
9.4 Registro delle anomalie 46

Manuale di Conservazione

EDOK SRL

EMISSIONE DEL DOCUMENTO

Azione	Data	Nominativo	Funzione
Redazione	04/07/2022	Chiara De Angeli	Consulente interna Servizio di conservazione
Verifica	01/09/2022	Studio Legale Lisi	Consulente esterno Legale
Approvazione	30/09/2022	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"
Versione 2.0	31/01/2020	Adeguamento al nuovo software di conservazione Modifica dei capitoli: 1 SCOPO E AMBITO DEL DOCUMENTO 3.1 Normativa di riferimento 5 STRUTTURA ORGANIZZATIVA 6.2 tipologie documentali 6.4 pacchetti di versamento 7 PROCESSO DI CONSERVAZIONE 8 SISTEMA DI CONSERVAZIONE 9. MONITORAGGI E CONTROLLI	
Versione 2.1	01/08/2020	Paragrafi 4 e 5.1 aggiornato nominativo Responsabile dei sistemi informativi per la conservazione	
Versione 3.0	03/10/2022	Adeguamento del Manuale alle nuove Linee Guida AgID su formazione, gestione e conservazione dei documenti informatici	

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.

Con l'introduzione della fatturazione elettronica obbligatoria anche tra privati e il conseguente aumento esponenziale dei volumi di conservazione, Edok ha implementato una nuova soluzione software in grado di automatizzare numerosi passaggi e restituire al cliente/utente una nuova interfaccia di versamento/esibizione più agevole e intuitiva. Il presente manuale riporta nel dettaglio il processo e la nuova architettura fisica e logica alla base del nuovo sistema di conservazione Edok.

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 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.

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 *Linee guida su Formazione, Gestione e Conservazione dei documenti informatici* adottate da AgID per la prima volta nel settembre 2020.

Di seguito le definizioni contenute nel documento su menzionato.

TERMINE	DEFINIZIONE
Accesso	operazione che consente di prendere visione dei documenti informatici
Affidabilità	Caratteristica che, con riferimento a un sistema di gestione documentale o conservazione, esprime il livello di fiducia che l'utente ripone nel sistema stesso, mentre con riferimento al documento informatico esprime la credibilità e l'accuratezza della rappresentazione di atti e fatti in esso contenuta.
Aggregazione documentale informatica	Insieme di documenti informatici o insieme 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 dei documenti prodotti o acquisiti da un soggetto pubblico o privato durante lo svolgimento della propria attività.
Archivio informatico	archivio costituito da documenti informatici, organizzati in aggregazioni documentali informatiche
Area organizzativa omogenea	Un insieme di funzioni e di uffici individuati dall'ente al fine di gestire i documenti in modo unitario e coordinato, secondo quanto disposto dall'art. 50 comma 4 del D.P.R. 28 dicembre 2000, n. 445. Essa rappresenta il canale ufficiale per l'invio di istanze e l'avvio di procedimenti amministrativi.
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 in virtù della quale un oggetto deve considerarsi come corrispondente a ciò che era nel momento originario della sua produzione. Pertanto un oggetto è autentico se nel contempo è integro e completo, non avendo subito nel corso del tempo o dello spazio alcuna modifica non autorizzata. L'autenticità è valutata sulla base di precise evidenze.
Certificazione	Attestazione di terza parte relativa alla conformità ai requisiti specificati di prodotti, processi, persone e sistemi.
Classificazione	Attività di organizzazione di tutti i documenti secondo uno schema costituito da un insieme di voci articolate in modo gerarchico e che individuano, in astratto, le funzioni, competenze, attività e/o materie del soggetto produttore.

Cloud della PA	Ambiente virtuale che consente alle Pubbliche Amministrazioni di erogare servizi digitali ai cittadini e alle imprese nel rispetto di requisiti minimi di sicurezza e affidabilità.
Codec	Algoritmo di codifica e decodifica che consente di generare flussi binari, eventualmente imbustarli in un file o in un wrapper (codifica), così come di estrarli da esso (decodifica).
Conservatore	soggetto, pubblico o privato, che svolge attività di conservazione dei documenti informatici
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, garantendo nel tempo le caratteristiche di autenticità, integrità, leggibilità, reperibilità dei documenti
Convenzioni di denominazione del file	le Insieme di regole sintattiche che definisce il nome dei file all'interno di un filesystem o pacchetto.
Coordinatore della Gestione Documentale	Soggetto 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 AOO.
Destinatario	Soggetto o sistema al quale il documento informatico è indirizzato
Digest	Vedi impronta crittografica
Documento amministrativo informatico	Ogni rappresentazione, grafica, fotocinematografica, elettromagnetica o di qualunque altra specie, del contenuto di atti, anche interni, formati dalle pubbliche amministrazioni, o, comunque, da queste ultime utilizzati ai fini dell'attività amministrativa
Documento elettronico	Qualsiasi contenuto conservato in forma elettronica, in particolare testo o registrazione sonora, visiva o audiovisiva
Documento informatico	Documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti
Duplicato informatico	il documento informatico ottenuto mediante la memorizzazione, sullo stesso dispositivo o su dispositivi diversi, della medesima sequenza di valori binari del documento originario
eSeal	Vedi sigillo elettronico.
Esibizione	operazione che consente di visualizzare un documento conservato
eSignature	Vedi firma elettronica.
Estratto di documento informatico	Parte del documento tratto dal documento originale
Estratto per riassunto di documento informatico	Documento nel quale si attestano in maniera sintetica fatti, stati o qualità desunti da documenti informatici

Estrazione statica dei dati	Estrazione di informazioni utili da grandi quantità di dati (es. database, datawarehouse ecc.), attraverso metodi automatici o semi-automatici
Evidenza informatica	Sequenza finita di bit che può essere elaborata da una procedura informatica.
Fascicolo informatico	Aggregazione documentale informatica strutturata e univocamente identificata contenente atti, documenti o dati informatici prodotti e funzionali all'esercizio di una attività o allo svolgimento di uno specifico procedimento.
File	Insieme di informazioni, dati o comandi logicamente correlati, raccolti sotto un unico nome e registrati, per mezzo di un programma di elaborazione o discrittura, nella memoria di un computer.
File Container	Vedi Formato contenitore
File wrapper	Vedi Formato contenitore
File-manifesto	File che contiene metadati riferiti ad un file o ad un pacchetto di file.
Filesystem	Sistema di gestione dei file, strutturato mediante una o più gerarchie ad albero, che determina le modalità di assegnazione dei nomi, memorizzazione e organizzazione all'interno di uno storage.
Firma elettronica	Vedi articolo 3 del Regolamento eIDAS.
Firma elettronica avanzata	Vedi articoli 3 e 26 del Regolamento eIDAS.
Firma elettronica qualificata	Vedi articolo 3 del Regolamento eIDAS.
Flusso (binario)	Sequenza di bit prodotta in un intervallo temporale finito e continuativo che ha un'origine precisa ma di cui potrebbe non essere predeterminato il suo istante di interruzione
Formato contenitore	Formato di file progettato per consentire l'inclusione ("imbustamento" o wrapping), in uno stesso file, di una o più evidenze informatiche soggette a differenti tipi di codifica e al quale possono essere associati specifici metadati.
Formato del documento informatico	Modalità di rappresentazione della sequenza di bit che costituiscono il documento informatico; comunemente è identificato attraverso l'estensione del file.
Formato "deprecato"	Formato in passato considerato ufficiale il cui uso è attualmente sconsigliato a favore di una versione più recente.
Funzionalità aggiuntive del protocollo informatico	Nel sistema di protocollo informatico, componenti supplementari rispetto a quelle minime, necessarie alla gestione dei flussi documentali, alla conservazione dei documenti nonché alla accessibilità delle informazioni.
Funzioni minime del protocollo informatico	Componenti del sistema di protocollo informatico che rispettano i requisiti di operazioni ed informazioni minime di cui all'articolo 56 del D.P.R. 28 dicembre 2000, n. 445.
Funzione di *hash* crittografica	Funzione matematica che genera, a partire da una evidenza

	informatica, una impronta crittografica o digest (vedi) in modo tale che risulti computazionalmente difficile (di fatto impossibile), a partire da questa, ricostruire l'evidenza informatica originaria e generare impronte uguali a partire da evidenze informatiche differenti.
Gestione documentale	Processo finalizzato al controllo efficiente e sistematico della produzione, ricezione, tenuta, uso, selezione e conservazione dei documenti.
Hash	Termine inglese usato, impropriamente, come sinonimo d'uso di "impronta crittografica" o "digest" (vedi).
Identificativo univoco	Sequenza di numeri o caratteri alfanumerici associata in modo univoco e persistente ad un'entità all'interno di uno specifico ambito di applicazione.
Impronta crittografica	Sequenza di bit di lunghezza predefinita, risultato dell'applicazione di una funzione di hash crittografica a un'evidenza informatica.
Integrità	Caratteristica di un documento informatico o di un'aggregazione documentale in virtù della quale risulta che essi non hanno subito nel tempo e nello spazio alcuna alterazione non autorizzata. La caratteristica dell'integrità, insieme a quella della completezza, concorre a determinare la caratteristica dell'autenticità.
Interoperabilità	Caratteristica di un sistema informativo, le cui interfacce sono pubbliche e aperte, e capaci di interagire in maniera automatica con altri sistemi informativi per lo scambio di informazioni e l'erogazione di servizi.
Leggibilità	Caratteristica di un documento informatico che garantisce la qualità di poter essere decodificato e interpretato da un'applicazione informatica.
Manuale di conservazione	Documento informatico che descrive il sistema di conservazione e illustra dettagliatamente l'organizzazione, i soggetti coinvolti e i ruoli svolti dagli stessi, il modello di funzionamento, la descrizione del processo, la descrizione delle architetture e delle infrastrutture.
Manuale di gestione	Documento informatico che descrive il sistema di gestione, anche ai fini della conservazione, dei documenti informatici e fornisce le istruzioni peril corretto funzionamento del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi.
Metadati	Dati associati a un o documento informatico, a un fascicolo informatico o a un'aggregazione documentale per identificarli, descrivendone il contesto, il contenuto e la struttura - così da permetterne la gestione del tempo - in conformità a quanto definito nella norma ISO 15489-1:2016 e più nello specifico

	dalla norma ISO 23081-1:2017.
Naming convention	Vedi Convenzioni di denominazione
Oggetto di conservazione	Oggetto digitale versato in un sistema di conservazione.
Oggetto digitale	Oggetto informativo digitale, che può assumere varie forme tra le quali quelle di documento informatico, fascicolo informatico, aggregazione documentale informatica o archivio informatico.
Pacchetto di archiviazione	Pacchetto informativo generato dalla trasformazione di uno o più pacchetti di versamento coerentemente con 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 di accesso a oggetti di conservazione.
Pacchetto di file (*file package*)	Insieme finito di più file (possibilmente organizzati in una struttura di sottoalbero all'interno di un filesystem) che costituiscono, collettivamente oltre che individualmente, un contenuto informativo unitario e auto-consistente.
Pacchetto di versamento	Pacchetto informativo inviato dal produttore al sistema di conservazione secondo il formato descritto nel manuale di conservazione.
Path	Percorso (vedi).
Pathname	Concatenazione ordinata del percorso di un file e del suo nome.
Percorso	Informazioni relative alla localizzazione virtuale del file all'interno del filesystem espressa come concatenazione ordinata del nome dei nodi del percorso
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.
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.
Piano di classificazione (Titolario)	Struttura logica che permette di organizzare documenti e oggetti digitali secondo uno schema desunto dalle funzioni e dalle attività dell'amministrazione interessata.
Piano di conservazione	Documento, allegato al manuale di gestione e integrato con il sistema di classificazione, in cui sono definiti i 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 di organizzazione delle aggregazioni documentali	Strumento integrato con il sistema di classificazione a partire dai livelli gerarchici inferiori di quest'ultimo e finalizzato a individuare le tipologie di aggregazioni documentali (tipologie di serie e tipologie di fascicoli) che devono essere prodotte e

	gestite in rapporto ai procedimenti e attività in cui si declinano le funzioni svolte dall'ente
Piano generale della sicurezza	Documento che pianifica le 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 e, in caso di affidamento del servizio all'esterno, dagli accordi stipulati tra il titolare dell'oggetto di conservazione e il responsabile del servizio di conservazione.
Processo	Insieme di attività correlate o interagenti che trasformano elementi in ingresso in elementi in uscita.
qSeal	Sigillo elettronico qualificato, come da art. 35 del Regolamento eIDAS.
qSignature	Firma elettronica qualificata, come da art. 25 del Regolamento eIDAS.
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.
Registro di protocollo	Registro informatico ove sono memorizzate le informazioni prescritte dalla normativa per tutti i documenti ricevuti e spediti da un ente e per tutti i documenti informatici dell'ente stesso.
Registro particolare	Registro informatico individuato da una pubblica amministrazione per la memorizzazione delle informazioni relative a documenti soggetti a registrazione particolare.
Regolamento eIDAS	Electronic IDentification Authentication and Signature, Regolamento (UE) № 910/2014 del Parlamento Europeo e del Consiglio, del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari perle transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE.
Repertorio	Registro su cui vengono annotati con un numero progressivo i fascicoli secondo l'ordine cronologico in cui si costituiscono all'interno delle suddivisioni del piano di classificazione
Responsabile del servizio di conservazione	soggetto che coordina il processo di conservazione all'interno del conservatore, in possesso dei requisiti professionali individuati da AGID
Responsabile della conservazione	Soggetto che definisce e attua le politiche complessive del sistema di conservazione e ne governa la gestione con piena responsabilità ed autonomia.
Responsabile della gestione documentale	Soggetto responsabile della gestione del sistema documentale o responsabile del 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.
Responsabile della protezione dei dati	Persona con conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, in grado di assolvere i compiti di cui all'articolo 39 del Regolamento (UE) 2016/679.
Riferimento temporale	Insieme di dati che rappresenta una data e un'ora con riferimento al Tempo Universale Coordinato (UTC).
Riversamento	Procedura mediante la quale uno o più documenti informatici sono convertiti da un formato di file (ovvero di busta, ovvero di pacchetto di file) ad un altro, lasciandone invariato il contenuto per quanto possibilmente permesso dalle caratteristiche tecniche del formato (ovvero dei formati) dei file e delle codifiche di destinazione.
Scarto	Operazione con cui si eliminano definitivamente, secondo quanto previsto dalla normativa vigente, i documenti ritenuti non più rilevanti ai fini giuridico-amministrativo e storicoculturale.
Serie	Raggruppamento di documenti con caratteristiche omogenee (vedi anche aggregazione documentale informatica).
Sidecar (file)	File-manifesto (vedi).
Sigillo elettronico	Dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati in forma elettronica, per garantire l'origine e l'integrità di questi ultimi.
Sistema di conservazione	Insieme di regole, procedure e tecnologie che assicurano la conservazione dei documenti informatici in attuazione a quanto previsto dall'art. 44, comma 1, del CAD.
Sistema di gestione informatica dei documenti	Insieme delle risorse di calcolo, degli apparati, delle reti di comunicazione e delle procedure informatiche utilizzati dalle organizzazioni per la gestione dei documenti. Nell'ambito della pubblica amministrazione è il sistema di cui all'articolo 52 del D.P.R. 28 dicembre 2000, n. 445
Timeline	Linea temporale virtuale su cui sono disposti degli eventi relativi ad un sistema informativo o a un documento informatico. Costituiscono esempi molto diversi di timeline un file di log di sistema, un flusso multimediale contenente essenze audio\video sincronizzate.
Titolare dell'oggetto di conservazione	Soggetto produttore degli oggetti di conservazione.
Trasferimento	Passaggio di custodia dei documenti da una persona o un ente ad un'altra persona o un altro ente
TUDA	Testo Unico della Documentazione Amministrativa, Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, e successive modificazioni e integrazioni.
Ufficio	riferito ad un'area organizzativa omogenea, un ufficio dell'area

	stessa che utilizza i servizi messi a disposizione dal sistema di protocollo informatico
Utente abilitato	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	Passaggio di custodia, di proprietà e/o di responsabilità dei documenti. Nel caso di un organo giudiziario e amministrativo dello Stato operazione con la quale il responsabile della conservazione trasferisce 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:

- Regolamento UE 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
- Regolamento UE 679/2016 – Regolamento generale sulla protezione dei dati (GDPR) relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE
- 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 Ministero Economia e Finanze del 3 aprile 2013, n. 55 - Regolamento in materia di emissione, trasmissione e ricevimento della fattura elettronica da applicarsi alle amministrazioni pubbliche;
- 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 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;
- Linee Guida su formazione, gestione e conservazione dei documenti informatici, emanate dall'Agenzia per l'Italia Digitale ai sensi dell'art. 71 del D.Lgs. 82 2005
- Circolare dell'Agenzia delle Entrate n. 45/E del 19 ottobre 2005;
- Circolare dell'Agenzia delle Entrate n. 36/E del 06 dicembre 2006;
- Circolare 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;
- 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

3.2 Standard di riferimento

- Riportiamo i principali standard adottati da Safety 21 SpA e ritenuti coerenti con le Linee guida AgID su formazione, gestione e conservazione dei documenti informatici (allegato 4) e ricompresi tra i requisiti per la fornitura di servizi di conservazione previsti dal relativo Regolamento AgID sui criteri per la fornitura di servizi di conservazione del maggio 2021.
- ISO 14721 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);
- ISO/IEC 22313 Sicurezza e resilienza - Sistemi di gestione per la continuità operativa
- 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;
- ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers
- ETSI TS 119 511 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers providing long-term preservation of digital signatures or general data using digital signature techniques
- UNI 11386:2020 Standard SInCRO - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali;
- ISO/UNI 37001 Sistemi di gestione per la prevenzione della corruzione
- ISO 15836 Information and documentation - The Dublin Core metadata element set, Sistema di metadata del Dublin Core.
- ISO 9001 Sistemi di gestione per la qualità

3.3 Certificazioni del Conservatore

- **ISO 9001:2015**

Certificato	Prima emissione	Scadenza	Rilasciato da
N. 30863/14/S	02.07.2014	10.07.2023	RINA SERVICES S.P.A.

Attività di progettazione, sviluppo e distribuzione di software e servizi informatici; erogazione servizi di conservazione digitale a norma di legge, di fatturazione elettronica e di gestione elettronica di documenti per enti pubblici e privati; erogazione servizi di spedizione multicanale.

- **ISO/IEC 27001:2013 - UNI CEI EN ISO/IEC 27001:2017**

Certificato	Prima emissione	Scadenza	Rilasciato da
N. 278/14	17.07.2014	16.07.2023	RINA SERVICES S.P.A.

Attività di progettazione, sviluppo e distribuzione di software e servizi informatici; erogazione servizi di conservazione digitale a norma di legge, di fatturazione elettronica e di gestione elettronica di documenti per enti pubblici e privati; erogazione servizi di spedizione multicanale.

- **ISO/IEC 27017:2015 E ISO/IEC 27018:2019**

Certificato	Prima emissione	Scadenza	Rilasciato da
N. 278/14	17.07.2014	16.07.2023	RINA SERVICES S.P.A.

Attività di progettazione, sviluppo e distribuzione di software e servizi informatici; erogazione in modalità cloud e on premises di servizi di conservazione digitale a norma di legge, di fatturazione elettronica e di gestione elettronica di documenti per enti pubblici e privati; erogazione servizi di spedizione multicanale.
Le attività di erogazione di servizi di conservazione digitale a norma di legge, di fatturazione elettronica e di gestione elettronica di documenti per enti pubblici e privati verificate con l'utilizzo dei controlli previsti dalle linee guida ISO/IEC 27017:2015 e ISO/IEC 27018:2019.

- **Conformità all'art.24 del Regolamento (UE) 910/2014 eIDAS - Circolare di Accreditamento di ACCREDIA**

Certificato	Prima emissione	Scadenza	Rilasciato da
CONS-18/7	08.02.2018	07.02.2022	RINA SERVICES S.P.A.

È conforme ai requisiti individuati all'art. 24 del Regolamento (UE) 910/2014 EIDAS come definito nella Circolare di Accreditamento di ACCREDIA e valutati sulla base della Lista di Riscontro di AgID "Conservatore di documenti informatici ai sensi dell'art. 29, comma 1, del D.lgs. 7 marzo 2005, n. 82".

- **Iscrizione al Marketplace dei servizi di conservazione**

ai sensi dell'articolo 34 comma 1-bis lettera b) del decreto legislativo 7 marzo 2005, n. 82 e s.m.i., recante il Codice dell'amministrazione digitale (CAD).
Verificata la conformità formale della documentazione presentata rispetto agli Allegati A e B del "Regolamento sui criteri per la fornitura dei servizi di conservazione dei documenti informatici e relativi allegati, ai sensi dell'art. 34, comma 1bis, lettera b)", da parte del "Servizio Qualificazione servizi fiduciari, infrastrutture e servizi cloud".
Iscrizione (agli atti con protocollo AgID n. 11514 del 07/06/2022) accolta in data 05/07/2022.

- **ISO 37001: Certificazione del Sistema di Gestione Anti-Corruzione**

Prima emissione	Certificatore
Prevista entro la fine del 2022	RINA SERVICES S.P.A.

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	Attività di competenza	Nominativo	periodo nel ruolo	eventuali deleghe
Responsabile del servizio di conservazione	- 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.	Fabio Zanni	Dal 2005	
Responsabile trattamento dati personali	- 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.	Studio legale Lisi	Da agosto 2017	Andrea Lisi

Torna al sommario

5. STRUTTURA ORGANIZZATIVA PER IL SERVIZIO DI CONSERVAZIONE

5.1 Organigramma

Le strutture organizzative coinvolte nel servizio di conservazione sono:

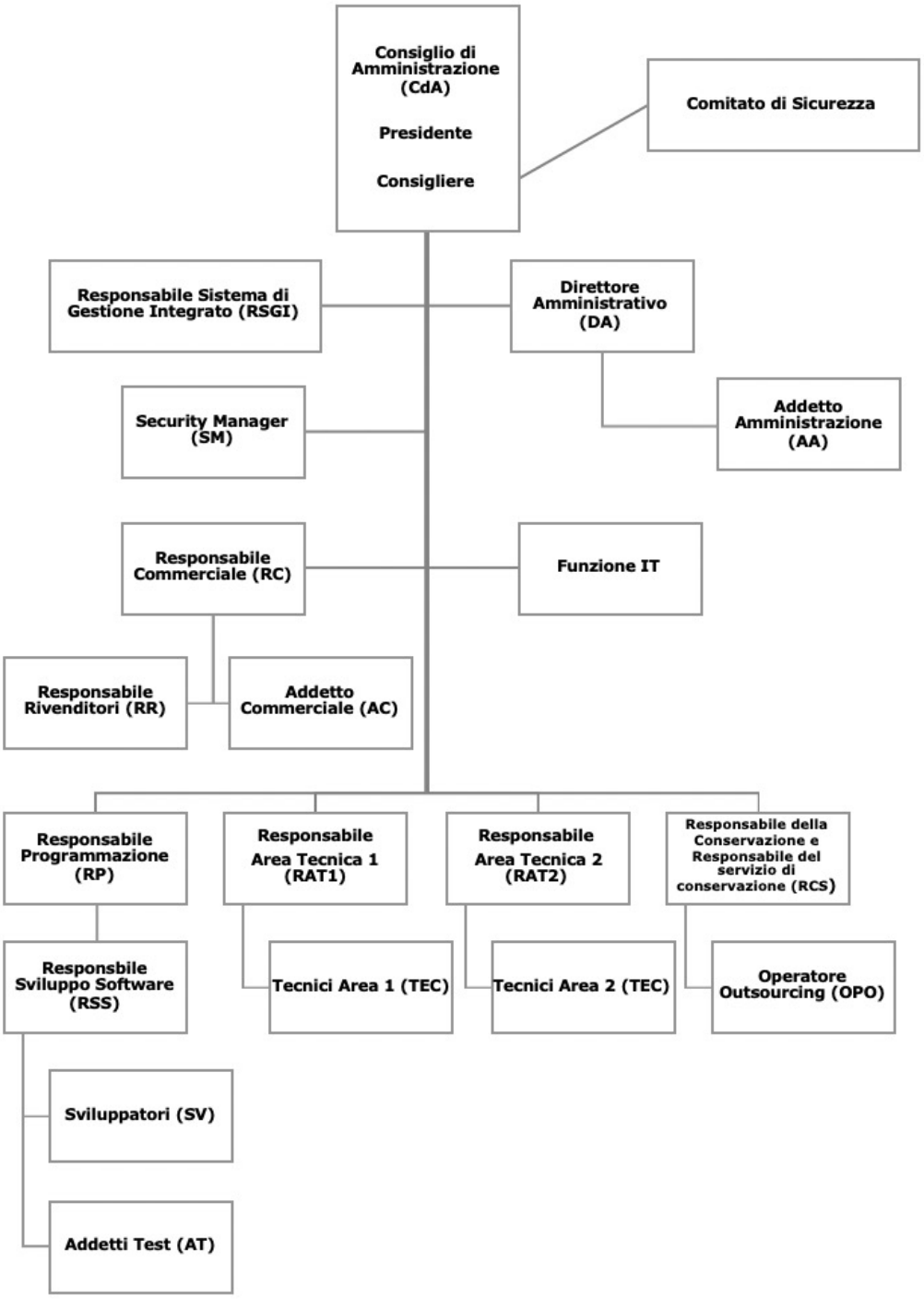

Figura 1 Organigramma aziendale

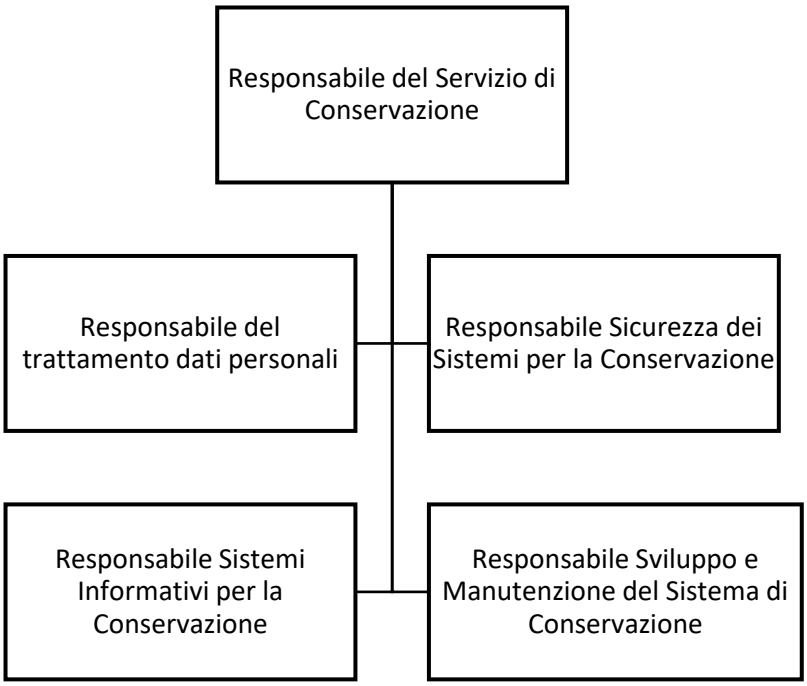

Figura 2 Strutture organizzative coinvolte nel servizio di conservazione

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**			

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

Nel capitolo sono elencati gli oggetti digitali sottoposti a conservazione, specificandone le tipologie, i formati gestiti e i metadati associati. Per "oggetti digitali" ci si riferisce a documenti che possono assumere varie forme, tra le quali quelle di documento informatico, fascicolo informatico, aggregazione documentale informatica o archivio informatico.

I documenti sono riposti nel Sistema di Conservazione con i propri metadati minimi elencati nell'Allegato 5 – "Metadati" delle Linee Guida AGID e così come chiarito nel documento esplicativo redatto dal Tavolo tecnico inter istituzionale coordinato da AGID (hanno partecipato inoltre alcuni rappresentanti dell'Agenzia delle Entrate e Sogei, del Consiglio Nazionale dei dottori commercialisti, dell'Osservatorio Digital B2b della School of Management del Politecnico di Milano). Il documento spiega inoltre che questi metadati dovrebbero essere generati e associati permanentemente al documento al momento della sua formazione; qualora tali informazioni siano invece già incluse nel documento informatico, la loro generazione e associazione può essere eseguita anche in fase successiva ma sempre sotto la responsabilità esclusiva del Soggetto Produttore.

Nel caso in cui un documento fosse inviato al Sistema di Conservazione senza i metadati obbligatori previsti dall'allegato sopra citato, il Conservatore è autorizzato dal Titolare a valorizzare i metadati utilizzando le informazioni estraibili dal documento stesso. Nell'impossibilità di apporre tutti metadati mancanti, il Conservatore è comunque autorizzato a conservare il documento.

In fase di analisi iniziale con il Titolare, Edok definisce le caratteristiche del servizio tenendo in considerazione le seguenti caratteristiche:

- Le tipologie documentali;
- I formati documentali in termini di leggibilità e portabilità;
- I metadati da associare;
- Eventuali modalità di sottoscrizione;
- Tempistiche di conservazione e scarto;
- Service Level Agreement;
- Altre eventuali indicazioni dei clienti.

I documenti informatici sono poi conservati come previsto dal contratto e dalle condizioni generali del servizio (Allegato contrattuale A "Condizioni generali di contratto").

6.1 Classificazione

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

- Codice della Società
- Codice della Tipologia documentale

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.

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

Per le Tipologie definite nel Sistema di Conservazione si faccia riferimento all'allegato "Mod. 13 - Metadati Minimi Conservazione.xlsx" che riporta, suddivise per le seguenti macro classi, l'elenco delle Tipologie e le relative proprietà.

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

I formati devono essere scelti e valutati in funzione delle seguenti caratteristiche:

- Diffusione: deve essere ampiamente utilizzato;
- Portabilità: deve rispondere a standard documentati e open source;
- Apertura: definito da standard e specifiche pubbliche;
- Funzionalità: possibilità di essere gestito da più prodotti informatici;
- Sicurezza: livello di modificabilità e difesa da eventuali attacchi;
- Supporto allo sviluppo: eventuale manutenzione.

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. I pacchetti di versamento contengono gli oggetti da sottoporre a conservazione.

L'assetto e il contenuto dei pacchetti di versamento sono delineati in accordo con il Produttore, sviluppando adattatori ad-hoc, con la possibilità di importare come allegati i file di chiusura di PdA da migrare.

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). Tutte le modalità di Versamento sono dettagliate nei paragrafi successivi.

Con l'acquisizione del Pacchetto, Edok può rilevare le informazioni seguenti:

- Produttore;
- Tipologia documentale;
- Documenti e relativi metadati;
- Data/ora di creazione;
- Ruoli coinvolti nel processo;
- Riferimenti normativi.

6.4.1 Versamento PdV via FTP in formato zip

Il pacchetto di versamento è rappresentato da un file in formato zip strutturato in base alle specifiche definite dall'apposita documentazione.

Indipendente dal formato il processo di acquisizione di questi file è il seguente:

- Il file viene caricato nell'area cliente tramite FTP sicuro;

- Il file viene analizzato per escludere minacce come malware e virus. In caso di infezione il file viene bloccato e inviato dal sistema nella zona di quarantena e il cliente avvisato del problema;
- Se il file è valido viene spostato dall'area FTP ed inserito in una coda di elaborazione;
- Il cliente riceve via mail un documento di Presa in Carico che riporta i dati del file e la sua hash.
    - Il documento di Presa in Carico viene salvato nella stessa area FTP, con il nome del PdV originale.
- La registrazione del PdV ricevuto e della presa in carico saranno consultabili dal Portale CS nell'area del cliente mittente;
- I file ricevuti in coda di elaborazione vengono progressivamente elaborati;
    - Il file zip viene analizzato in base ad uno dei formati supportati (CSV, PEC, FE).
    - Si verifica la validità del file compresso e la presenza degli elementi, in base al formato scelto.
    - Si verifica che la società e la tipologia documentale siano definite e attive nel sistema.
    - Per ogni documento si verifica la disponibilità di tutti i metadata della tipologia scelta e la presenza dei file richiesti e nel formato previsto.
- Se tutte le regole sono state rispettate i documenti vengono importati nel sistema e legati al PdV ricevuto;
    - Viene generato un Rapporto di Versamento di accettazione che riporta gli estremi del PdV creato e il suo codice univoco.
- Se vi sono problemi di convalida il PdV viene rifiutato;
    - In questo caso viene generato un Rapporto di Versamento di rifiuto che riporta gli estremi del file ricevuto e l'elenco delle difformità rilevate, quali ad esempio:
        - Tipologia non disponibile
        - Metadata mancante per il documento F00001
        - File del documento F00001 mancante o vuoto
- Il Rapporto di Versamento viene inviato al cliente e salvato nell'area FTP, dove è stato depositato il file da parte del cliente. Il Rapporto di Versamento avrà sarà denominato con il nome del PdV originale con suffisso "_RdV" per differenziarlo dalla presa in carico inziale;
- Il PdV e i Documenti collegati saranno disponibili nel Portale CS nell'area del cliente mittente.

6.4.2 Versamento automatico FE

Per i clienti che hanno sottoscritto i servizi di Fatturazione Elettronica con Edok, ai fini di rendere efficiente e trasparente il versamento di un gran numero di documenti, è stato creato apposito modulo di versamento automatico.

Il processo è schematizzato come segue:

- Mensilmente viene generato il PdV dei documenti di un mese precedente definito dal decalage determinato (attualmente 3 mesi).
- Il PdV generato è associato soltanto ad una società e può essere di tre tipologie:
    - FEdV: Fatture Elettroniche di Vendita
    - FEdA: Fatture Elettroniche di Acquisto
    - DF: Dati Fattura
    - LI: Liquidazione IVA
- I metadati richiesti da ogni tipologia, come riportato nell'apposito documento, vengono estratti dai file dei documenti perché in formato standard.
- Il Rapporto di Versamento generato non viene inviato al cliente direttamente ma è disponibile, assieme al PdV e ai Documenti collegati, sul Portale CS.

Le condizioni di versamento delle fatture elettroniche sono indicate nel contratto dedicato al servizio FE.

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.

6.5 Pacchetto di Archiviazione

Il PdA è il pacchetto informativo composto dalla trasformazione di uno o più pacchetti di versamento secondo quanto indicato dalle Linee Guida AgID e secondo le modalità riportate nel seguente manuale. I pacchetti di Archiviazione sono generati aggregando i documenti per Ragione Sociale e per Tipologia, come definito inizialmente durante l'organizzazione del Sistema di Conservazione. Questo tipo di attività viene fatta automaticamente.

Il PdA viene generato periodicamente in base alle tempistiche indicate per la tipologia (generalmente entro un anno), in base alle dimensioni o in base a particolari accordi contrattuali. Le informazioni riportare nel PdA sono le stesse caricate/inviate dal Produttore per la creazione del PdV.

I metadati presenti all'interno del o dei PdV da cui origina il PdA verranno inseriti all'interno del PdA 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 UNI SinCRO e dall'allegato 5 alle Linee Guida AgID su formazione, gestione e conservazione dei documenti informatici nonché dalle ulteriori normative aventi ad oggetto specifiche tipologie documentali (Es. DMEF 17 giugno 2014 in relazione ai documenti fiscalmente rilevanti).

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

```
<?xml version="1.0" encoding="utf-8"?>
<s:PIndex xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
 xsi:schemaLocation="http://www.uni.com/U3011/sincro-v2/ XSD/PIndex.xsd http://www.edok.it/sincro/AttachMetadata.xsd XSD/Atta
 s:language="it" s:uri="http://www.uni.com/U3011/sincro-v2/PIndex.xsd" s:sincroVersion="2.0"
 xmlns:s="http://www.uni.com/U3011/sincro-v2/">
  <s:SelfDescription>
    <s:ID s:scheme="PDA">00228060166__Lul__2022M08__A001::87a1c071-a151-45bf-b838-f9f9d66f5361</s:ID>
    <s:CreatingApplication>
      <s:Name>DokLaw</s:Name>
      <s:Version>2.15.1.0</s:Version>
      <s:Producer>edok s.r.l</s:Producer>
    </s:CreatingApplication>
  </s:SelfDescription>
  <s:PVolume>
    <s:ID s:scheme="PDA">87a1c071-a151-45bf-b838-f9f9d66f5361</s:ID>
    <s:Label>87a1c071-a151-45bf-b838-f9f9d66f5361</s:Label>
    <s:Description>T[redacted] S.P.A. (0022[redacted]) Libro Unico Lavoro (Lul) Agosto 2022 (2022M08) A001</s:Description>
    <s:MoreInfo s:xmlSchema="file://XSD/LegalPackageMetadata.xsd">
      <s:EmbeddedMetadata>
        <LegalPackageMetadata xmlns="http://www.edok.it/sincro/LegalPackageMetadata.xsd">
          <Nome>00228060166 Lul 2022M08 A001</Nome>
          <Descrizione>T[redacted] S.P.A. (0022[redacted]) Libro Unico Lavoro (Lul) Agosto 2022 (2022M08) A001</Descrizione>
          <Guid>87a1c071-a151-45bf-b838-f9f9d66f5361</Guid>
          <Società>T[redacted] S.P.A. (00228060166)</Società>
          <Tipologia>Libro Unico Lavoro (Lul)</Tipologia>
          <Note />
          <Versamenti>
            <Versamento>
              <Indice>1</Indice>
              <Nome>00228[redacted]Lul 2022M08 ID0001</Nome>
              <Descrizione>[redacted]R S.P.A. (00228060166) Libro Unico Lavoro (Lul) Agosto 2022 (2022M08) ID0001</Descrizione>
              <Guid>d7e6904c-c49e-42e4-7a86-08da921fc5a3</Guid>
              <Data>2022-09-09T06:57:18.3813327</Data>
            </Versamento>
          </Versamenti>
        </LegalPackageMetadata>
      </s:EmbeddedMetadata>
    </s:MoreInfo>
  </s:PVolume>
  <s:FileGroup>
```

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 Distribuzione 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. Indipendentemente da quanto previsto da ogni singolo contratto di servizio i PdD si è scelto di firmare digitalmente tutti i PdD generati (il file indice).

Per ricevere un PdD, l'utente deve fare la richiesta tramite apposito carrello e con le funzionalità di aggiunta presenti negli archivi Documenti oppure PdA. Deve poi inviare la richiesta con una motivazione e la scelta del formato (scelta suggerita). Un operatore - o il responsabile - deve valutare la richiesta, confermandola con la scelta del formato oppure rifiutandola. Si passa poi alla generazione e alla messa a disposizione del PdD sul Portale. Tutte le richieste e i PdD prodotti vengono opportunamente registrate a sistema e consultabili dagli utenti con gli appositi diritti.

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 14721:2012 meglio conosciuto come OAIS - Open Archival Information System.

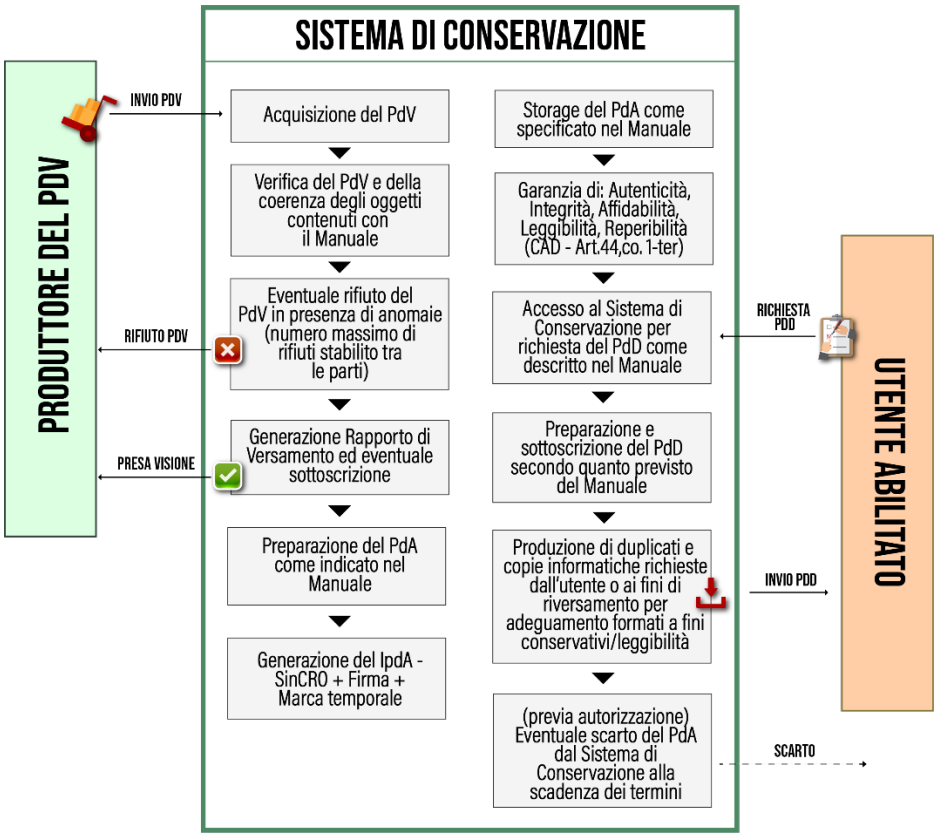

Figura 3 Schema processo di conservazione

Come specificato nel successivo par. 9.1, tutte le attività svolte dalle singole componenti del Sistema di conservazione (versamento, controllo, formazione e sottoscrizione Pda, produzione e rilascio Pdd, etc..) sono tracciate in specifici log testuali disponibili per ogni portale, API o servizio sui server in cui il componente viene eseguito. I log sono suddivisi per giorno e dimensione tracciano tutti gli eventi che coinvolgono il componente con in evidenza la data e l'esito dell'operazione.

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

Il sistema di conservazione prevede la ricezione di pacchetti di versamento generati da applicativi esterni al sistema stesso tramite la gestione di una struttura a cartelle che prevede due possibilità:

1) Cartella capo gruppo C{codice}_{nome}
2) Cartella società {codice}_{nome}

Il codice alfanumerico è assegnato da Edok al cliente nel proprio gestionale e registrato in anagrafica. Il parametro {nome} viene ignorato dal sistema e serve per facilitare controlli manuali.

Il processo di conservazione inizia con la 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 la stessa nomenclatura. Per evitare questa casistica è data possibilità al cliente di gestire una parte del nome con un riferimento univoco.
I pacchetti ricevuti vengono aggiunti alla coda di importazione: il file ricevuto è disponibile sia al cliente tramite Portale (allo scopo di monitorare il flusso dei suoi versamenti) sia agli "operatori" tramite Dashboard:

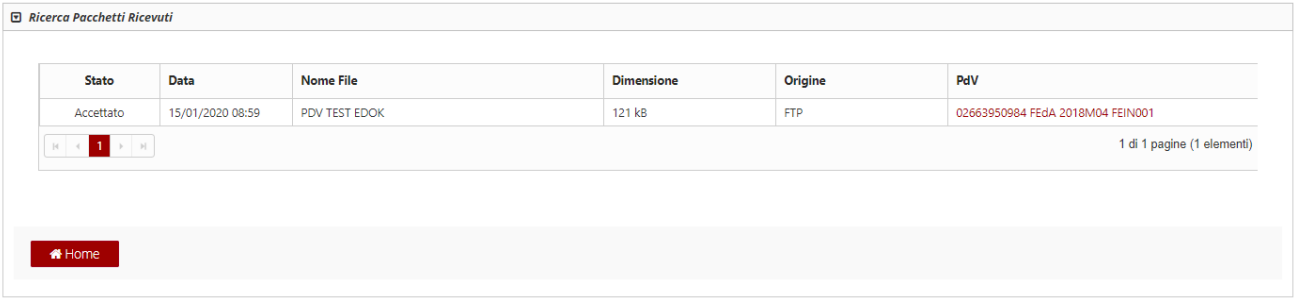

Figura 4 Esempio di pacchetto visualizzato dall'operatore

I dati tracciati riguardano lo stato del pacchetto, la data, il nome del file originale, la dimensione, origine e il link al PdV creato automaticamente.
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 (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).
- 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).

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).
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 a 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;

Per ulteriori dettagli fare riferimento alla documentazione specifica.

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 in base alla cartella SFTP dove viene ricevuto il pacchetto.
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.
- Verifica dell'esistenza e dell'hash di tutti i file presenti nel pacchetto a seconda del tipo di pacchetto e dall'indicazione o meno da parte del cliente.
- 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 fallimento di uno dei passaggi di verifica le motivazioni vengono riportate nel Rapporto di Versamento inviato al cliente.

7.3 Accettazione dei pacchetti di versamento e generazione rapporto di versamento

In primo luogo c'è una presa in carico che riporta l'hash del file ricevuto e quindi il RdV che contiene l'hash del file indice generato da noi.
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 dalla lett. d) del par. 4.7 delle Linee Guida AgID su formazione, gestione e conservazione dei documenti informatici, 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.

7.4 Formazione del Pacchetto di Archiviazione

La formazione del Pacchetto di Archiviazione avviene manualmente attraverso l'utilizzo di una firma digitale e una marca temporale (per pacchetto), secondo le modalità previste dalla normativa vigente, apposti su uno o più Pacchetti di Versamento creati precedentemente. Nello specifico, il Pacchetto di Archiviazione è gestito come spiegato di seguito.

- I PdV creati e accettati sono analizzati rapidamente per individuare eventuali anomalie;
- I Pacchetti di Archiviazione sono prodotti, tramite procedura singola o massiva;
- Ai PdA è apposta una firma digitale;
- I PdA ricevono una marca temporale;
- I PdA sono inseriti nel database;
- Contestualmente è generato un rapporto di archiviazione (RdA) per ogni PdA.

A seconda degli accordi intrapresi con il Produttore, i Pacchetti di Archiviazione possono essere creati automaticamente secondo le tempistiche predefinite.

Figura 5 Rappresentazione grafica creazione pacchetti

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

Secondo quanto stabilito dal par. 4.9 delle Linee Guida AgID su formazione, gestione e conservazione dei documenti informatici, 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 per uno specifico/i documento/i o per uno specifico pacchetto di archiviazione. Per dettagli sull'operatività della richiesta di PdD consultare il manuale "Istruzioni portale SOS CS".

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

Il sistema lavora utilizzando pacchetti strutturati in accordo con quanto definito dalle regole tecniche contenute nelle LLGG AgID. 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 11386:2020) 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 generare file indici strutturati secondo lo standard SInCRO per quanto riguarda i PdA e i PdD, garantendo la possibilità di interoperabilità con altri sistemi. In entrambi i casi si è reso necessario utilizzare le strutture MoreInfo per ampliare le informazioni esposte. Ad esempio:

- L'elenco dei PdV inclusi in un PdA.
- Il dettaglio dei metadata per ogni Documento (FileGroup) e il tipo dei file associati al Documento.
- L'elenco dei PdA associati ai documenti inclusi in un PdD.

Qualora il Produttore abbia richiesto la memorizzazione di ulteriori metadati non previsti dallo standard UNI SinCRO ma inseriti nel campo *moreinfo*, la loro definizione e la loro struttura verrà dettagliata nei singoli contratti di servizio.

7.7 Cancellazione dei documenti

L'operazione con cui si eliminano, osservando la normativa vigente, i documenti privi di valore prende il nome di scarto. Il tempo di conservazione dei documenti viene accordato col Produttore e, talvolta, previa autorizzazione di terzi. I

documenti con un significativo valore storico, ad esempio, possono essere eliminati solamente con l'autorizzazione del Ministero che si occupa di questa materia.

Il Titolare dei documenti può avanzare una richiesta di annullamento in qualsiasi momento. Nel caso di annullamento la richieste deve essere fatta tramite applicativo e deve essere approvata. In questo caso rimane registrata nel sistema. Edok manda una PEC al Titolare per dargli X giorni di tempo per annullare la propria richiesta prima della cancellazione definitiva. Non è possibile annullare i singoli documenti, ma solamente uno o più Pacchetti.
È inoltre possibile, senza approvazione, annullare o eliminare PdV non ancora archiviati.

Torna al sommario

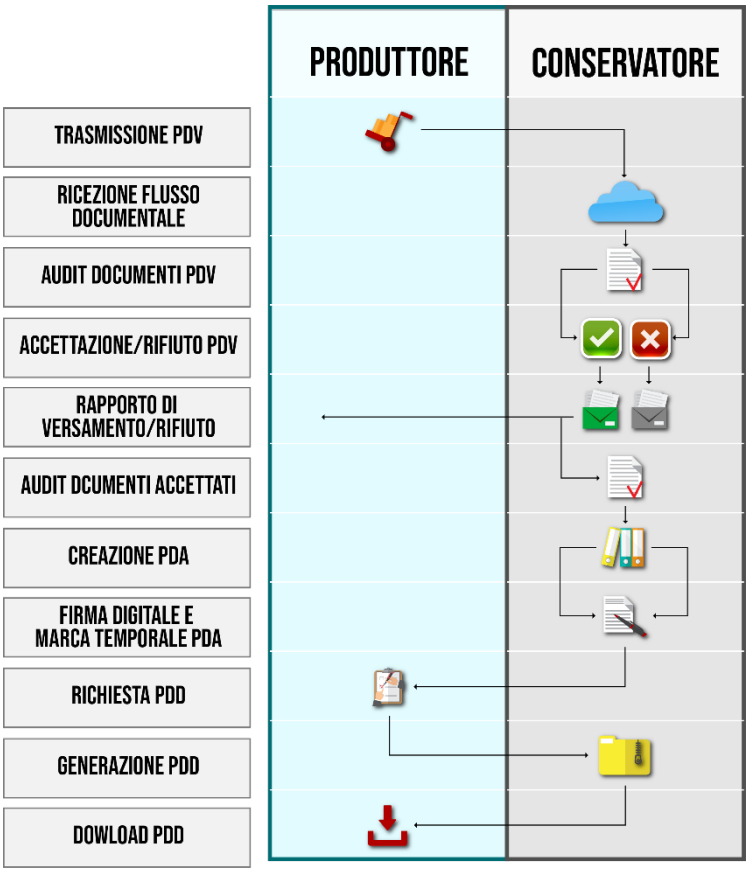

Figura 6 Rappresentazione grafica del processo

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 compongono il Sistema. Essenzialmente i moduli si dividono in quattro tipologie:

- Servizi: servizi NT, rappresentano la parte server dell'applicativo.
- Dashboard: 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.

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 recenti tecnologie di sviluppo.
L'architettura si articola 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 automatici per l'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.
- *Dashboard:* sistema centralizzato di configurazione e di controllo.

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

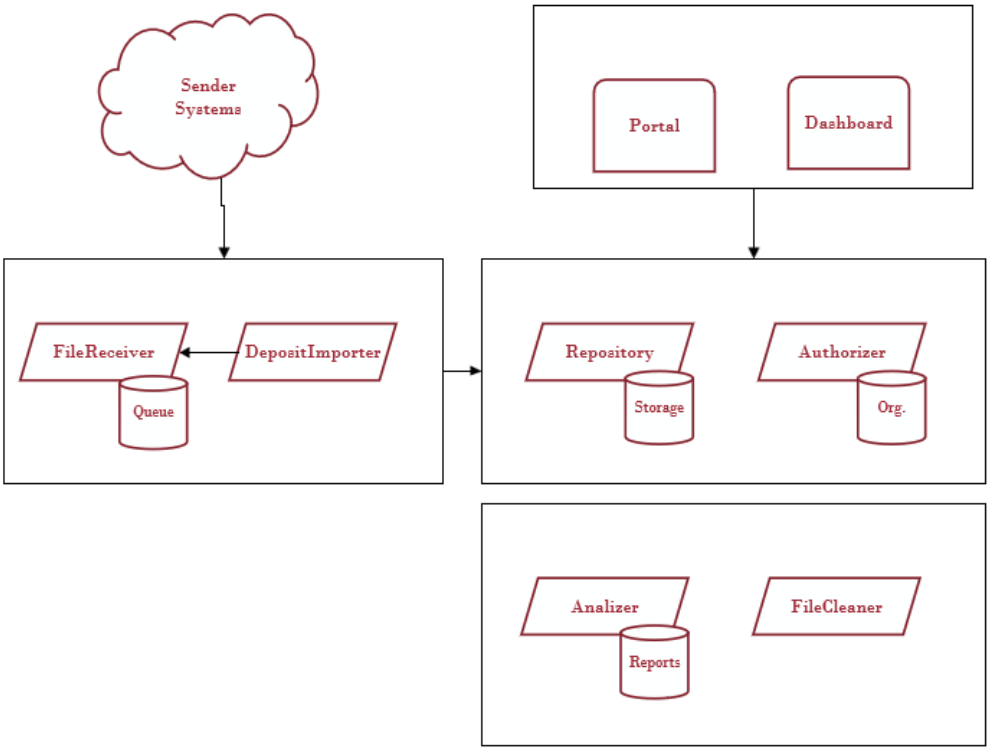

Figura 7 Schema Sistema di conservazione

- **FileReceiver:** si occupa di gestire la coda di ricezione dei pacchetti di versamento inviati dai clienti nelle apposite aree FTP. Il modulo esegue lo spostamento del file ricevuto e l'accodamento per la successiva elaborazione. Tramite apposito servizio invia notifica di Presa in Carico al cliente.
- **DepositImporter:** esegue l'effettiva importazione del pacchetto di versamento nel Sistema, generando la registrazione del pacchetto e il relativo Rapporto di Versamento. Tramite apposito modulo invia il rapporto di versamento al cliente e lo salva nella stessa cartella FTP del file originale.
- **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.
- **Dashboard:** componente di gestione della configurazione del sistema e di monitoraggio da parte degli operatori e del RdC..
- **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.
- **Portale:** client web per la consultazione dell'archivio SdC e per la richiesta da parte dei clienti di PdD.
- **FileCleaner:** modulo di pulizia delle cartelle e della cosa FTP per le rimozione di file elaborati dopo un certo periodo di tempo.

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. Core
I componenti software del Sistema di Conservazione sono una parte della soluzione HyperDok© fornita da Edok a innumerevoli e prestigiosi clienti e come tali sottoposti 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

Per l'erogazione dei servizi di conservazione Edok Srl 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 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.
Il Data Center "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.
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) Ore di disservizio annue	28.8	22.0	1.6	0.4
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, ha la certificazione ISO/IEC 27001 Information Security-Management System. Questa norma internazionale 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.

Inoltre, Brennercom compare nel registro pubblico come Cloud Service Provider certificato per l'erogazione di tutte le tipologie di servizi in cloud previste per la Pubblica Amministrazione. Infine, Brennercom ha ottenuto la certificazione CSP di tipo C, che la abilita all'erogazione di servizi Infrastructure as a Service (IaaS), Platform as a Service (PaaS) e Software as a Service (SaaS).

8.3.1 Infrastruttura

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

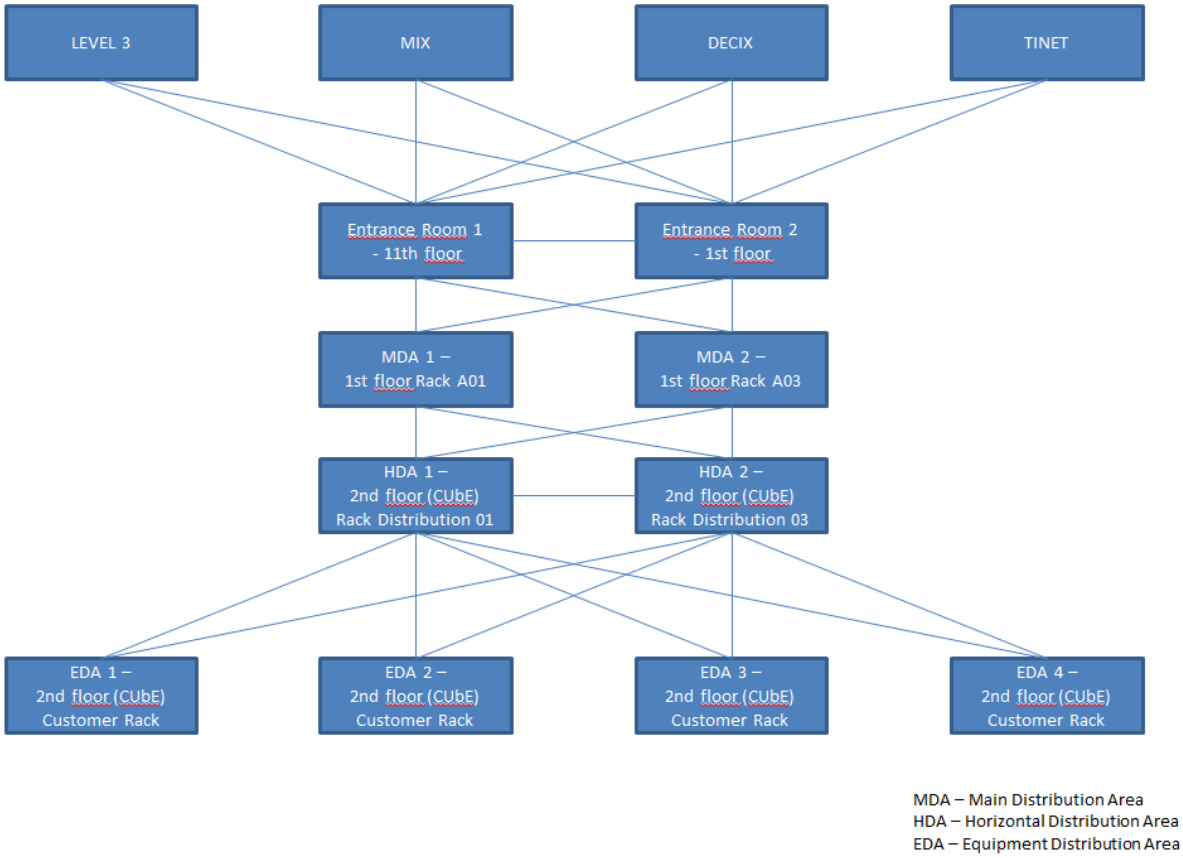

Figura 8 Struttura Data Center

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

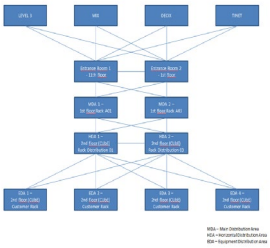

Figura 9 Cablaggi

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'energia elettrica autoprodotta e acquistata permette di raggiungere un altissimo livello di affidabilità in termini di continuità del servizio.

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.

8.3.4 Condizionamento

Il condizionamento è una componente fondamentale di tutte le infrastrutture IT. 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 diverse 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.

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.

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.

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.

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.

<u>Modalità di accesso</u>

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 una 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.
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.

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.

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.

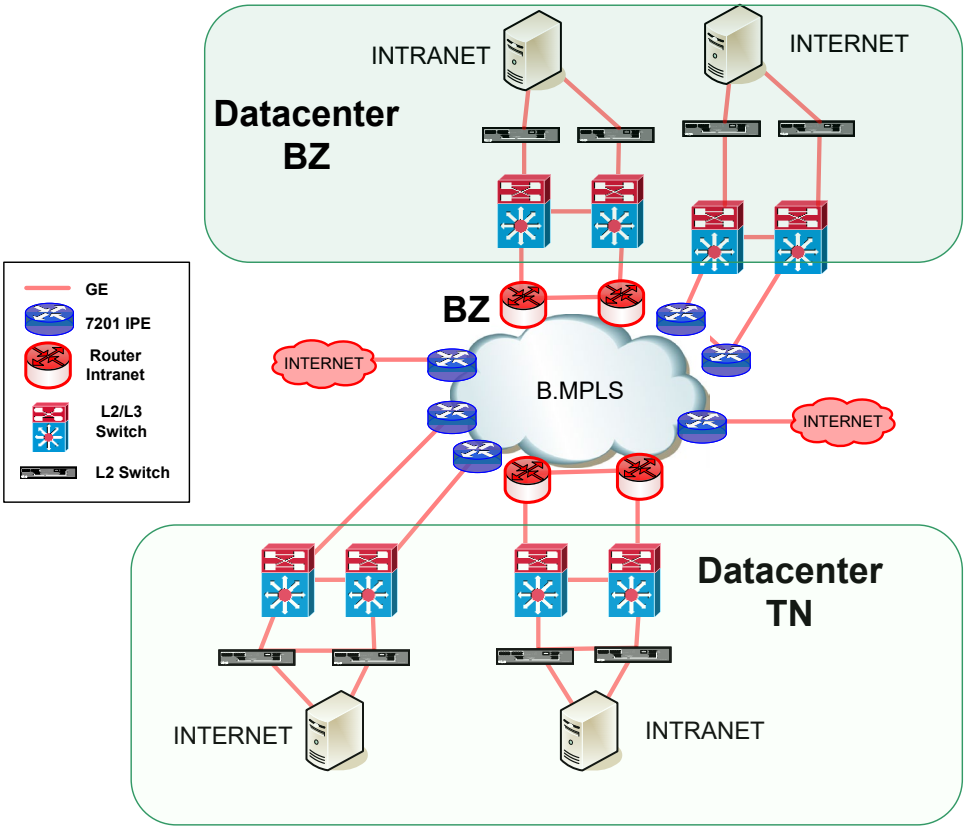

Figura 10 Collegamento del centro di calcolo alla rete IP/MPLS

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).

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 del servizio di conservazione 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.

9.1 Procedure di monitoraggio

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

Monitoraggio applicativo

Tutte le attività svolte dai componenti del SdC sono tracciate in specifici log testuali disponibili per ogni portale, API o servizio sui server in cui il componente viene eseguito. I log sono suddivisi per giorno e dimensione tracciano tutti gli eventi che coinvolgono il componente con in evidenza la data e l'esito dell'operazione.

Per il Portale e le Api è tracciato inoltre l'utente da cui è nato l'evento tracciato. Per quanto riguarda le attività utenti è inoltre disponibile un log applicativo centralizzo esposto nella Dashboad di gestione dedicata al RdC e agli Operatori incaricati.

Vengono inoltre verificate periodicamente:

- gli esisti delle chiamate verso i server Portal e API per valutare gli indici di errore o di fallimento della richiesta;
- l'esito dei e versamenti e delle archiviazione: ogni elaborazione geneta degli stati ed eventualmente dei messaggi di errore
- il numero di accessi ripetuti da parte di un utente considerati sospetti perché frequenti.

Monitoraggio infrastrutturale

È il monitoraggio della totalità dell'infrastruttura 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.

Il monitoraggio viene effettuato tramite l'applicativo Easysuite che oltra alla registrazione dei log permette il monitoraggio di tutte le componenti infrastrutturali del Sistema di Conservazione. I monitoraggi attivi permettono una verifica in real time della disponibilità dei servizi e delle performance degli stessi. Sono inoltre stati configurati degli allarmi che avvertono tempestivamente i referenti dell'area tecnica in caso di problematiche.

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 verrà salvato nel sistema e reso disponibile nella Dashboard. In caso di errori o avvisi il report sarà portato a conoscenza del Responsabile del servizio della conservazione al fine di constatare la corretta esecuzione della verifica o evidenziare le anomalie riscontrate.

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.
- Indisponibilità della base dati, dello storage FS/S3 dei file.

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 del servizio di conservazione.

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'hardware o ai sistemi di connettività

Edok ha definito e attuato un processo di incident management che garantisce un approccio coerente ed efficace per la gestione degli incidenti relativa alla sicurezza delle informazioni, incluse le comunicazioni relative gli eventuali eventi di sicurezza ed i punti di debolezza (vulnerabilità). Nello specifico il processo permette:

- la corretta gestione degli eventi di sicurezza e delle debolezze associate ai sistemi utilizzati per il processo di conservazione;
- la definizione delle modalità di segnalazione relative all'utilizzo improprio delle credenziali di accesso e dei relativi diritti;
- la corretta rilevazione, valutazione e gestione delle violazioni dei dati personali (data breach) e delle eventuali comunicazioni al Garante della Privacy e agli Interessati;

- la corretta rilevazione, valutazione e gestione di incidenti ha comportato interruzioni di servizio o violazioni di sicurezza sul SdC.

Tale processo si integra al processo di gestione dell'incidente attivato dal fornitore Brennercom e di seguito dettagliato.

Grazie al supporto di Brennercom, è attivo 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 alla 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,etc)
- 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.

9.4 Registro delle anomalie

È stato predisposto un modello di registro da utilizzare in caso di anomalie.
Eventuali irregolarità riscontrate, unitamente alle azioni intraprese per contrastarle e impedire il loro ripresentarsi, saranno dettagliate in questo documento, in modo da mantenerlo costantemente aggiornato e reso disponibile presso il sistema di conservazione.
Il registro può essere utilizzato dai vari responsabili (ciascuno in relazione alle proprie competente) ed è supervisionato dal Responsabile del servizio di conservazione.

Torna al sommario