Manuale di Conservazione
Comune di Rovetta

1 *Introduzione al documento*

1.1 Scopo e campo di applicazione del documento

Il presente documento è il Manuale di Conservazione come previsto dalle Linee Guida sulla formazione, gestione e conservazione dei documenti informatici di Agid in vigore dal 10 settembre 2020 (di seguito indicate come Linee Guida di Agid) e dal Codice dell'Amministrazione digitale D.Lgs. 82/2005.

Come richiesto dalle Linee Guida di Agid, il presente documento "deve illustrare dettagliatamente l'Amministrazione, i soggetti coinvolti e i ruoli svolti dagli stessi, il modello di funzionamento, la descrizione del processo, la descrizione delle architetture e delle infrastrutture utilizzate, le misure di sicurezza adottate e ogni altra informazione utile alla gestione e alla verifica del funzionamento, nel tempo, del sistema di conservazione".
In caso di ispezione da parte delle autorità di vigilanza preposte, il Manuale di Conservazione permette un agevole svolgimento di tutte le attività di controllo.
Il Manuale di Conservazione integra e dettaglia i Manuali del sistema di conservazione dei conservatori esterni Credemtel e TopConsult.

Si rimanda ai Manuali del sistema di conservazione dei Conservatori per indicazioni dettagliate circa:

- struttura organizzativa e ruoli di responsabilità del Conservatore
- formati e metadati associati agli oggetti conservati
- processo di conservazione e trattazione dei pacchetti di versamento, archiviazione e distribuzione
- dettaglio tecnico del sistema di conservazione
- monitoraggio e controlli effettuati dal Conservatore
- disposizioni in vigore nei luoghi dove sono conservati i documenti

1.2 Principi del Manuale

Il Manuale di Conservazione mira a:

- fornire una chiara presentazione del sistema di conservazione e dei processi erogati
- descrivere l'insieme delle fasi del processo
- includere le informazioni rilevanti, con un livello di dettaglio sufficiente ad agevolare le ispezioni, evitando informazioni tecniche articolate e non necessarie

Il Manuale di Conservazione è adottato dall'Amministrazione con provvedimento formale ed è pubblicato sul sito istituzionale, nella Sezione Amministrazione trasparente.

1.3 Normativa e standard di riferimento, terminologia

I principali riferimenti normativi relativi alla conservazione sono:

- Codice dell'Amministrazione digitale D.Lgs. 82/2005
- Linee Guida sulla formazione, gestione e conservazione dei documenti informatici di Agid, adottate con determinazione 407/2020 e in vigore dal 10 settembre 2020

Per ulteriori indicazioni e per quanto riguarda la terminologia (glossario e acronimi) e gli standard in uso si rimanda ai Manuali del sistema di conservazione dei Conservatori.

2 *Modello organizzativo, ruoli e responsabilità*

2.1 Modello organizzativo

Il modello organizzativo adottato è in *outsourcing*: l'Amministrazione affida il servizio di conservazione a conservatore esterno, ai sensi dall'art. 34, c. 1-bis del Codice dell'Amministrazione digitale D.Lgs. 82/2005, fatte salve le competenze del Ministero della cultura, ai sensi del Codice dei beni culturali e del paesaggio D.Lgs. 42/2004.

2.2 Amministrazione, Titolare dell'oggetto della conservazione

L'Amministrazione è il Titolare dei documenti informatici posti in conservazione e, in relazione al modello organizzativo adottato, affida ai Conservatori, Credemtel e TopConsult, la gestione del servizio di conservazione secondo quanto previsto dalla normativa in materia e specificato nel contratto di servizio.

Amministrazione: Comune di Rovetta
Indirizzo: Piazza Ferrari, 24 24020 Rovetta (BG)
Codice fiscale: 00338710163
Partita IVA: 00338710163
Sito web: https://www.comune.rovetta.bg.it/

2.3 Responsabile della conservazione

Il Responsabile della conservazione opera secondo quanto previsto dall'art. 44, c. 1-quater, del Codice dell'Amministrazione digitale D.Lgs. 82/2005.
Il Responsabile della conservazione:

- è un ruolo previsto dall'organigramma del Titolare dell'oggetto di conservazione
- è un dirigente o un funzionario interno formalmente designato e in possesso di idonee competenze giuridiche, informatiche e archivistiche
- può essere svolto dal responsabile della gestione documentale o dal coordinatore della gestione documentale, ove nominato

Il Responsabile della conservazione dell'Amministrazione definisce e attua le politiche complessive del sistema di conservazione e ne governa la gestione con piena responsabilità e autonomia, in relazione al modello organizzativo adottato.
Il Responsabile della conservazione è persona fisica inserita stabilmente nell'organico dell'Amministrazione titolare dell'oggetto della conservazione; la normativa gli attribuisce compiti riguardanti le funzioni, gli adempimenti, le attività e le responsabilità del processo di conservazione. L'obiettivo principale del Responsabile della conservazione è definire e impostare le modalità di trattamento della documentazione soggetta a conservazione.
Le Linee guida di Agid enfatizzano il ruolo del Responsabile della conservazione che diviene fondamentale all'interno del processo di conservazione, insieme ai suoi delegati o ai terzi affidatari.
Il Responsabile della conservazione provvede a predisporre il manuale di conservazione e ne cura l'aggiornamento periodico in presenza di cambiamenti normativi, organizzativi, procedurali o tecnologici rilevanti.

Le attività attribuite dalle Linee guida di Agid al Responsabile della conservazione ed eventualmente affidate al Conservatore sono:

- definire le politiche di conservazione e i requisiti funzionali del sistema di conservazione, in conformità alla normativa vigente e tenuto conto degli standard internazionali, in ragione delle specificità degli oggetti digitali da conservare (documenti informatici e aggregazioni informatiche), della natura delle attività che il Titolare dell'oggetto di conservazione svolge e delle caratteristiche del sistema di gestione informatica dei documenti adottato
- gestire il processo di conservazione e garantire nel tempo la conformità alla normativa vigente
- generare e sottoscrivere il rapporto di versamento
- generare e sottoscrivere il pacchetto di distribuzione con firma digitale o firma elettronica qualificata
- effettuare il monitoraggio della corretta funzionalità del sistema di conservazione
- effettuare la verifica periodica, con cadenza non superiore ai cinque anni, dell'integrità e della leggibilità dei documenti informatici e delle aggregazioni documentarie degli archivi
- al fine di garantire la conservazione e l'accesso ai documenti informatici, adottare misure per rilevare tempestivamente l'eventuale degrado dei sistemi di memorizzazione e delle registrazioni e, ove necessario, per ripristinare la corretta funzionalità, adottare analoghe misure con riguardo all'obsolescenza dei formati
- provvedere alla duplicazione o copia dei documenti informatici in relazione all'evolversi del contesto tecnologico

- predisporre le misure necessarie per la sicurezza fisica e logica del sistema di conservazione
- assicurare la presenza di un pubblico ufficiale, nei casi in cui sia richiesto il suo intervento, garantendo allo stesso l'assistenza e le risorse necessarie per l'espletamento delle attività al medesimo attribuite
- assicurare agli organismi competenti previsti dalle norme vigenti l'assistenza e le risorse necessarie per l'espletamento delle attività di verifica e di vigilanza.

Il Responsabile della conservazione affida ai Conservatori le attività definite dalle Linee guida di Agid sopra elencate, rimanendo in ogni caso inteso che la responsabilità giuridica generale sui processi di conservazione, in quanto non delegabile, rimane in capo al Responsabile della conservazione.

Responsabile della conservazione: Simona Fausti
Amministrazione: Comune di Rovetta
Atto/disposizione di nomina: decreto sindacale n. 5 del 01/06/2022

Il Responsabile della conservazione, sotto la propria responsabilità, può delegare lo svolgimento delle proprie attività o parte di esse a uno o più soggetti, che all'interno dell'Amministrazione, abbiano specifiche competenze ed esperienze.

2.4 Conservatore

L'Amministrazione, avvalendosi di quanto previsto dal Codice dell'Amministrazione digitale D.Lgs. 82/2005 e dalle Linee guida di Agid, ha affidato lo svolgimento delle attività di conservazione a Credemtel e a TopConsult.

Credemtel
Denominazione sociale: Credemtel S.p.A.
Sede legale: via Togliatti, 36/1, 42020 Montecavolo di Quattro Castella (RE)
Sito web: https://credemtel.it/
E-mail: credemtel@credemtel.it
Pec: credemtel@pec.gruppocredem.it
Telefono: 0522.203040
Codice Fiscale: 01378570350
Partita IVA: 02823390352
Numero REA: 181067

TopConsult
Denominazione sociale: TopConsult S.r.l.
Sede legale: Via Valeggio, 22/E, 10128 Torino TO
Sito web: https://www.topconsult.it/it/
E-mail: marketing@topconsult.it
Pec: credemtel@pec.gruppocredem.it
Telefono: +39 011 5805994
Codice Fiscale: 05370340019
Partita IVA: 05370340019

Gli obiettivi dei Conservatori tramite il servizio conservazione sono:
- garantire conservazione, archiviazione e gestione dei documenti informatici e dei fascicoli informatici
- erogare servizi di accesso basati sui contenuti digitali conservati
- fornire supporto, formazione e consulenza al Titolare dell'oggetto di conservazione per i processi di dematerializzazione

I Conservatori assumono l'incarico di svolgere le attività affidate dal Responsabile della conservazione dell'Amministrazione in accordo con quanto previsto dal contratto, dagli allegati tecnici contrattuali e dalle disposizioni delle Linee guida di Agid.
I Conservatori provvedono ad attribuire lo svolgimento delle attività al responsabile del servizio della conservazione e a più persone che, per competenza ed esperienza, garantiscano la corretta esecuzione dei processi di conservazione definiti dalle norme, dal contratto e dal Manuale del sistema di conservazione. Per il dettaglio delle figure di responsabilità interne ai Conservatori, si rimanda ai Manuali del sistema di conservazione dei Conservatori.
Gli estremi identificativi del responsabile del servizio di conservazione dei Conservatori (cognome, nome, codice fiscale) sono riportati anche nelle informazioni associate ai documenti conservati.
L'affidamento dello svolgimento delle attività del Responsabile della conservazione è stato conferito

dall'Amministrazione ai Conservatori alla sottoscrizione del contratto di adesione al servizio di conservazione. La conservazione è svolta affidando a Credemtel e TopConsult il ruolo e i compiti fissati nel documento di nomina a Responsabile del servizio di conservazione.

2.5 Produttore dei pacchetti di versamento

Il responsabile della gestione documentale svolge il ruolo di Produttore dei pacchetti di versamento e provvede a trasmettere i pacchetti al sistema di conservazione dei Conservatori.
Per pacchetto di versamento si intende: insieme finito di più file (organizzati in una struttura di sottoalbero all'interno di un filesystem) che costituiscono collettivamente oltre che individualmente un contenuto informativo unitario e auto-consistente e che viene inviato dall'ente Produttore ai sistemi di conservazione.
L'Amministrazione provvede a:

- generare e trasmettere al sistema di conservazione i pacchetti di versamento nelle modalità e con i formati concordati con i Conservatori e descritti nei Manuali dei loro sistemi di conservazione
- verificare il buon esito della operazione di trasferimento al sistema di conservazione tramite la presa visione del rapporto di versamento prodotto dal sistema di conservazione stesso.

2.6 Utente

L'utente è il soggetto che può richiedere al sistema di conservazione l'accesso per acquisire le informazioni di interesse nei limiti previsti dalla legge. Tali informazioni vengono fornite dal sistema di conservazione secondo le modalità definite nei Manuali del sistema di conservazione dei Conservatori.
Il sistema di conservazione permette ai soggetti autorizzati l'accesso diretto, anche da remoto, ai documenti informatici conservati e consente la produzione di un pacchetto di distribuzione direttamente acquisibile dai soggetti autorizzati.
Per pacchetto di distribuzione si intende: insieme finito di più file (organizzati in una struttura di sottoalbero all'interno di un filesystem) che costituiscono collettivamente oltre che individualmente un contenuto informativo unitario e auto-consistente e che è inviato dal sistema di conservazione all'Utente in risposta a una sua richiesta di accesso a oggetti di conservazione.
Il Responsabile della conservazione è identificato come Utente del Sistema di conservazione. L'Amministrazione può definire nel ruolo di Utente ulteriori operatori a tal fine abilitati.
L'abilitazione e l'autenticazione degli utenti avviene in base alle procedure di gestione utenze indicate nel Piano della sicurezza del sistema di conservazione, e nel rispetto delle misure di sicurezza previste dal Codice in materia di protezione dei dati personali D.Lgs. 196/2003 agg. 2018.

3 Formazione e gestione dei documenti e dei fascicoli informatici

3.1 Formazione e gestione dei documenti e dei fascicoli informatici da conservare

L'Amministrazione forma e gestisce i documenti e i fascicoli informatici seguendo le disposizioni del Codice dell'Amministrazione digitale D.Lgs. 82/2005 e delle Linee guida di Agid, utilizzando gli strumenti informatici a disposizione.

3.2 Controlli

L'Amministrazione assicura che i documenti inviati in conservazione siano statici e non modificabili, in modo tale che il contenuto non possa essere alterabile durante le fasi di conservazione e accesso e sia quindi immutabile nel tempo.

3.3 Gestione delle anomalie

I sistemi di conservazione sono configurati per accettare documenti in formati prestabiliti e con metadati definiti. Al venir meno di una di queste condizioni, sopraggiungendo l'impossibilità di accettare il documento, i sistemi lasciano in attesa il documento in entrata senza immetterlo nel sistema di conservazione e contestualmente segnalano l'anomalia all'Amministrazione.
Il trattamento delle anomalie avviene mediante l'utilizzo di un'interfaccia web disponibile e accessibile alle risorse preposte al monitoraggio degli invii in conservazione.

3.4 Formato dei documenti informatici

L'Amministrazione utilizza per creare i documenti destinati alla conservazione i formati idonei per la conservazione a lungo termine (DPCM 3/12/2013 Regole tecniche per il protocollo informatico, Allegato 2 Formati sino al 1° gennaio 2022 e successivamente Linee guida di Agid, Allegato 2 Formati di file e riversamento) e definiti nei Manuali del sistema di conservazione dei Conservatori.

3.5 Metadati dei documenti informatici

L'Amministrazione associa ai documenti i metadati previsti per il Documento amministrativo informatico (DPCM 3/12/2013 Regole tecniche per il protocollo informatico, Allegato 5 Metadati sino al 1° gennaio 2022 e successivamente Linee guida di Agid, Allegato 5 I metadati) e descritti nei Manuali del sistema di conservazione dei Conservatori.

3.6 Metadati dei fascicoli informatici

L'Amministrazione associa ai fascicoli i metadati previsti per le Aggregazioni documentali informatiche (DPCM 3/12/2013 Regole tecniche per il protocollo informatico, Allegato 5 Metadati sino al 1° gennaio 2022 e successivamente Linee guida di Agid, Allegato 5 I metadati) e descritti nei Manuali del sistema di conservazione dei Conservatori.

4 Sistema di conservazione

4.1 Sistema di conservazione di Credemtel

Il servizio di conservazione permette di mantenere e garantire nel tempo le caratteristiche di autenticità, integrità, affidabilità, leggibilità, reperibilità e la validità legale dei documenti informatici, nel rispetto della normativa vigente.
Il servizio è erogato in modalità SaaS (*Software as a Service*) tramite interfaccia web disponibile e accessibile alle risorse preposte individuate dall'Amministrazione.
Il sistema di conservazione integra i sistemi e gli strumenti di produzione e gestione documentale in uso presso l'Amministrazione, intervenendo solamente nella fase di conservazione per i documenti e i fascicoli che l'Amministrazione sceglie di conservare.

Il processo di conservazione si articola nelle seguenti fasi:

1. Acquisizione da parte del sistema di conservazione del pacchetto di versamento per la sua presa in carico
2. Verifica che il pacchetto di versamento e gli oggetti contenuti siano coerenti con le modalità previste nel Manuale del sistema di conservazione, con i formati di conservazione e con le eventuali personalizzazioni specifiche realizzate per l'Amministrazione
3. Preparazione del rapporto di conferma
4. Eventuale rifiuto del pacchetto di versamento, nel caso in cui le verifiche di cui alla fase 2 abbiano evidenziato anomalie e/o non conformità
5. Ricezione degli oggetti da conservare
6. Verifica degli oggetti da conservare
7. Generazione automatica del rapporto di versamento relativo a ciascun pacchetto di versamento, univocamente identificato dal sistema di conservazione e contenente un riferimento temporale, specificato con riferimento al Tempo Universale Coordinato (UTC), e una o più impronte, calcolate sull'intero contenuto del pacchetto di versamento
8. Sottoscrizione del rapporto di versamento con firma digitale apposta da Credemtel
9. Preparazione e gestione del pacchetto di archiviazione
10. Sottoscrizione del pacchetto di archiviazione con firma digitale apposta da Credemtel e apposizione di una validazione temporale con marca temporale alla relativa impronta (Chiusura del pacchetto di archiviazione)
11. Quando richiesto, preparazione e sottoscrizione con firma digitale di Credemtel del pacchetto di distribuzione ai fini dell'esibizione richiesta dall'Utente
12. Quando richiesto, produzione di duplicati informatici effettuati su richiesta dell'Amministrazione, in conformità a quanto previsto dalla normativa vigente
13. Quando richiesto, eventuale scarto del pacchetto di archiviazione dal sistema di conservazione

Per la descrizione dettagliata del servizio di conservazione si rimanda al Manuale del sistema di conservazione di Credemtel.

Il sistema di conservazione di Credemtel poggia sulle seguenti tre componenti:

1. Applicativa, consistente nell'insieme di tutte le componenti funzionali a supporto del processo di conservazione;
2. Fisica, rappresentata dai *server* di *front-end*, di *back-end*, di *database* e di *storage* su cui vengono conservati nel tempo i metadati relativi agli oggetti di conservazione;
3. Di sicurezza, assicurata da un dispositivo HSM che fornisce servizi di firma digitale ed evidenza temporale qualificata utilizzati dal servizio di conservazione

Il sistema di conservazione e l'applicazione web sono erogate dalle infrastrutture tecnologiche fornite in modalità *cloud* da Microsoft Azure. I servizi di *file transfer* sono erogati in *Facility Management* su infrastrutture tecnologiche fornite da Accenture Financial Advanced Solutions & Technology. Il dispositivo HSM e i servizi di verifica e apposizione delle firme digitali sono forniti in *full outsourcing* da Aruba PEC, una *Certification Authority* erogante servizi fiduciari accreditata presso AgID e raggiungibile da remoto in modalità protetta. Tutti i sopraelencati componenti del servizio di conservazione sono protetti da adeguate misure di sicurezza.
Gli ambienti di sviluppo, di test e di produzione sono tenuti rigorosamente separati.

Il sistema di conservazione e l'applicazione web di consultazione sono costruiti su un'architettura a tre livelli:

- Livello di presentazione (*presentation layer*)
- Livello di business logic (*business layer*)
- Livello dati (*data access layer, database, storage*)

Il Conservatore ha concordato con i citati fornitori un piano di *back-up* dei dati con *retention* differenziata a seconda della loro tipologia e delle loro specifiche peculiarità. Anche i servizi di firma digitale e il dispositivo HSM sono stati realizzati con i massimi livelli di sicurezza richiesti per una *Certification Authority* accreditata presso AgID.

Tutte le componenti fisiche del servizio di conservazione sono state realizzate su più data center aggregati in "zone" in grado di erogare servizi in Alta Affidabilità:

- Il sistema di conservazione e l'applicazione web di consultazione sono erogati in modalità *cloud* tramite tre zone di disponibilità, tutte contemporaneamente attive, dislocate nell'Italia settentrionale, tra loro replicate e bilanciate in tempo reale. In caso di fault di zona, le altre sopperiscono al carico e garantiscono la resilienza operativa dei servizi erogati;
- I servizi di *file transfer* sono erogati da due che costituiscono il sito primario in provincia di Milano, con un sito secondario di *disaster recovery* posto in provincia di Roma per la continuità dei servizi;
- I servizi di firma digitale e il dispositivi HSM sono forniti da una zona costituente il sito primario di Arezzo, con un sito secondario di *disaster recovery* in provincia di Bergamo per la continuità dei servizi.

Credemtel è collegata tramite rete MPLS del gruppo CREDEM, che garantisce tutti i collegamenti verso i citati fornitori e verso internet.

Tutte le procedure di gestione ed evoluzione del servizio di conservazione (escluse quelle relative ai controlli e al monitoraggio, per cui si rimanda al Manuale del sistema di conservazione di Credemtel) e dei corrispondenti sistemi che lo supportano sono descritti nelle seguenti procedure del sistema di gestione:

- P01 Gestione normativa: verifiche periodiche di conformità relativa alla normativa e agli standard di riferimento;
- P06 Progettazione: l'evoluzione delle componenti logiche, tecnologiche e fisiche del sistema di conservazione prevede l'apertura di un progetto o intervento minore che analizzi, sviluppi e tesi le attività di cambiamento del sistema di conservazione stesso o dei sistemi di base hardware e software che lo supportano;
- P09 Approvvigionamento: questa procedura descrive le modalità di approvvigionamento di beni e servizi e di manutenzione e gestione delle infrastrutture e degli strumenti informatici di proprietà di Credemtel o nella sua disponibilità per altro titolo giuridico;
- P17 Erogazione dei servizi: questa procedure descrive le modalità di:

  gestione dei cambiamenti: rilasci di applicazioni software, modifica di sistemi e dati;

  back-up dei dati: il sistema informativo effettua in automatico una copia giornaliera di *back-up* di tutti gli oggetti di conservazione; tali copie vengono mantenute con *retention policy* conforme al contratto con l'Amministrazione, alla normativa applicabile e alla *best practice* di settore;

  presidio dei servizi e del sistema di conservazione;

  monitoraggio degli SLA dei servizi erogati;

  gestione del *capacity management* del sistema informativo.
- P18 Gestione incidenti: questa procedura descrive le modalità da adottare per gestire i vari scenari di incidente che possono occorrere: incidente IT, incidente di sicurezza fisica o informatica compresi eventuali data breach, incidente alle sedi o al personale che erogano servizi critici di Credemtel. La procedura descrive gli scenari e le modalità di gestione della crisi fino alla possibile attivazione del DS13 Piano di Resilienza Operativa;
- P20 Gestione della sicurezza logica: la procedura stabilisce le modalità utilizzate per implementare le misure di sicurezza logica e fisica necessarie a garantire la conformità dei servizi e dei sistemi alla norma ISO 27001 vigente.

Il sistema di conservazione dispone inoltre di un log di sistema delle attività eseguite, sia manuali che automatizzate, accessibile in consultazione dalla consolle di conservazione. Tale log viene periodicamente inserito in un documento informatico dotato di evidenza temporale qualificata, sottoscritto digitalmente e conservato in un apposito registro del sistema di conservazione di Credemtel. Il log traccia tutti i dati e le informazioni occorrenti per la ricostruzione delle operazioni compiute.

4.2 Sistema di conservazione di TopConsult

L'architettura del sistema di conservazione di TopConsult è basata sul prodotto TopMedia Social NED, piattaforma pensata per la gestione documentale, la collaborazione aziendale e la conservazione di lungo periodo. Il sistema risulta potente e robusto anche in condizioni di carico elevate; scalabile al bisogno (più piattaforme su più server, più archivi documentali collegati ad una piattaforma, archivi centralizzati o distribuiti) e affidabile.

I documenti conservati sono gestiti in modo che:

- i metadati utili per archiviare, classificare e ricercare risiedano all'interno di database sql standard di mercato;
- i contenuti (cioè i file abbinati ai metadati) risiedano su appositi dischi/aree tipicamente (ma non necessariamente) magnetiche.

Tutte le applicazioni e i diversi tipi di client colloquiano con l'ambiente di conservazione utilizzando il protocollo standard per la comunicazione sicura HTTPS.

Le componenti logiche del sistema di conservazione risultano così articolate:

Front end di versamento: riceve i pacchetti di versamento da parte del Produttore. I documenti ed i metadati sono ricevuti con le modalità concordate e descritte nell'Allegato A (Specificità di Contratto). Si espone tramite HTTPS e Web services che consentono, attraverso metodi SOAP, al Produttore la definizione di processi di versamento.

Back end: effettua i controlli; segnala eventuali anomalie; provvede all'archiviazione sui sistemi di storage generando i pacchetti di archiviazione, apponendo la firma digitale e la marca temporale; provvede alle attività di controllo e mantenimento. Si compone di:

- *Orchestration*: area di elaborazione e controllo dei pacchetti di versamento. In questa area protetta del sistema i dati vengono sottoposti a controlli e verifiche di integrità;
- *Application*: costituisce il livello di business del sistema di conservazione in cui i pacchetti di versamento vengono elaborati generando i pacchetti di archiviazione, i metadati memorizzati della base dati ed i relativi documenti memorizzati nel sistema di storage;
- *Storage*: costituisce il *data store* del sistema di conservazione. Si articola su più livelli localizzati presso il *data center*: il primo utilizza sistemi di *storage array* ridondanti in tecnologia SSD; il secondo, con funzioni di *backup*, utilizza sistemi di *storage* in tecnologia HDD.

Front end di consultazione: consente agli utenti autorizzati l'accesso ai documenti conservati. Si espone tramite HTTPS e web services e gestisce il livello di presentazione tramite una applicazione web, strumento di consultazione utilizzato dagli utenti e eventualmente dalle autorità di controllo, per accedere ai documenti conservati.

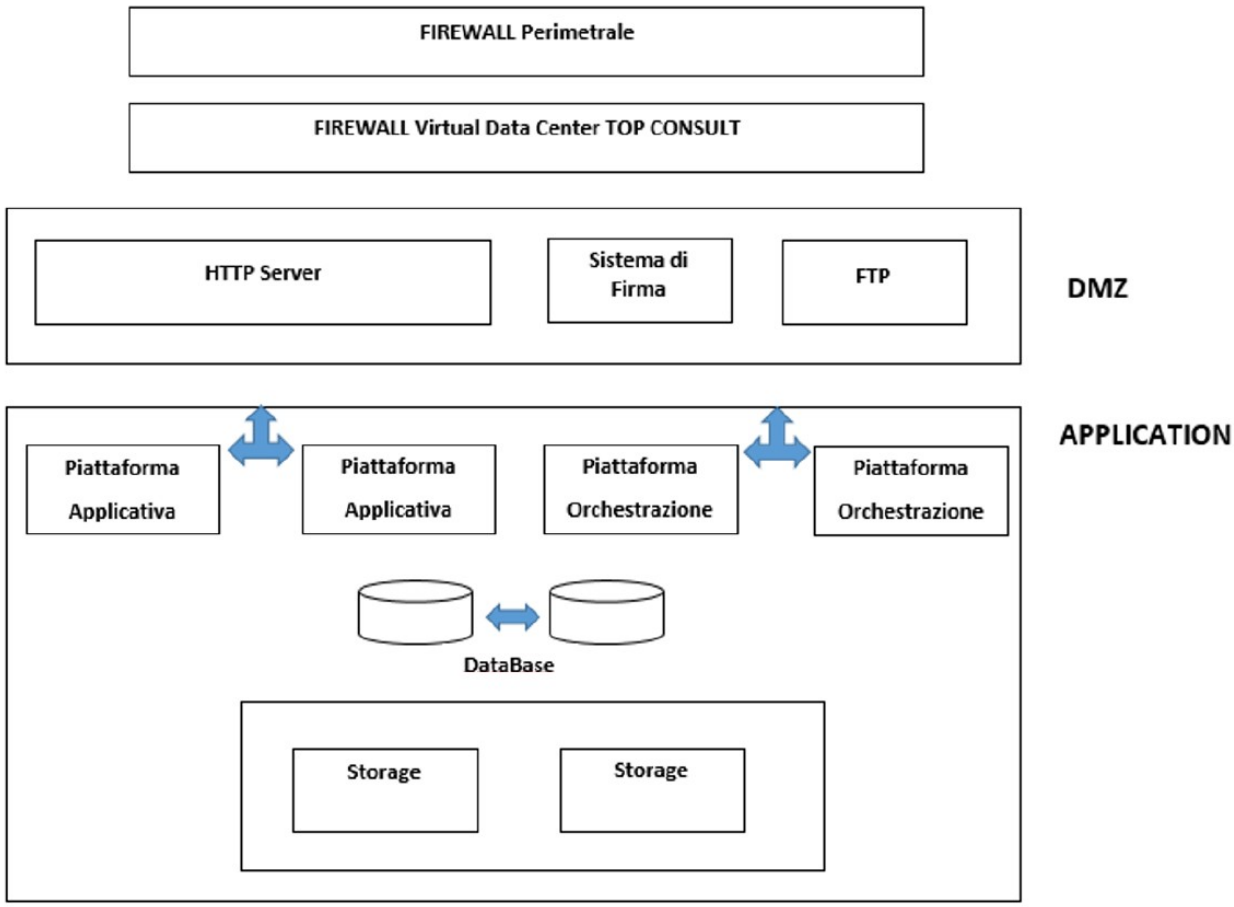
Per quanto riguarda le componenti tecnologiche del sistema di conservazione di TopConsult, esse risultano così articolate:

- Connettività: il sistema di conservazione utilizza accessi di rete ridondanti e POP in loco, incluso il Mix;
- Sistema di virtualizzazione: piattaforma di virtualizzazione VMware vSphere, host fisici in cluster, tutti multiprocessore e multicore, doppiamente alimentati, connessi da un'infrastruttura di rete commutata 10GbE;
- Supporti magnetici: *storage* di *array* fisici forniscono le capacità di storage ai server del sistema di virtualizzazione. Il sistema garantisce requisiti di sicurezza in termini di protezione autonoma dal ransomware, accesso admin multifattore, *multitenant* sicuro, crittografia *in-flight* e dei dati a riposo;
- Sistema di firma: sistema di firma remota per la gestione delle operazioni di firma digitale a norma di legge, in grado di gestire elevati volumi di transazioni con la flessibilità e affidabilità indispensabili ai processi di conservazione;
- Application

Nome	Descrizione
Application Server	Applicazioni proprietarie sviluppate in .NET Framework 4.8 gestiscono le funzioni di: • ORCHESTRATION • ARCHIVIAZIONE • CONSERVAZIONE • ESIBIZIONE
Database Server	MS SQLServer 2019 Enterprise ridondati, configurati in modalità HA, dedicati alla memorizzazione dei metadati dei documenti sottoposti a conservazione.
File Server	Insieme di server WINDOWS 2016 FS di diverse tecnologie che gestiscono lo spazio disco su più file system.
Firewall	Insieme di appliance, configurate in modalità HA, dedicate alla difesa della rete informatica, garantiscono una protezione in termini di sicurezza informatica della rete stessa.
Failover Service	Filosofia architetturale utilizzata dal Sistema di Conservazione nella configurazione di tutti i server Single Point of Failure: FIREWALL, DB Server, APPLICATION Server. L'uso di sistemi di Load Balancing, configurazioni di tipo CARP e DB Clustering, consentono di superare improvvise situazioni di failure.

L'infrastruttura fisica del Servizio di conservazione è stata creata con l'intento di rispettare i principi di modularità e ridondanza. Da questi principi nasce la decisione di gestire tutti i moduli logici e tecnologici come server virtuali. A tal fine, la ridondanza è realizzata unicamente mediante la copia dei *server* virtuali su più *host* fisici.

Il *data center* usato per fornire il servizio di conservazione è di livello Rating 4 (former Tier 4) di ANSI/TIA 942-A, progettato per i massimi livelli possibili di affidabilità e ridondanza, atto a garantire la costante disponibilità del sistema ed è localizzato fisicamente sul territorio italiano. In particolare, Top Consult eroga il proprio servizio di Conservazione utilizzando la *server farm* Aruba di Ponte San Pietro (BG). Attraverso un collegamento *peer to peer* in fibra (*dark fibre*) tutti i *server* virtuali sono replicati in tempo reale nel sito di Disaster Recovery. Quest'ultimo è realizzato da un host fisico ospitato presso il Data Center IT1 di Arezzo. La procedura di *switch* tra il sito primario ed il secondario è realizzata tramite il cambio dei puntamenti a livello di DNS.


FIREWALL Perimetrale
FIREWALL Virtual Data Center TOP CONSULT
HTTP Server
Sistema di Firma
FTP
DMZ
Piattaforma Applicativa
Piattaforma Applicativa
Piattaforma Orchestrazione
Piattaforma Orchestrazione
APPLICATION
DataBase
Storage
Storage

5 Documenti conservati

5.1 Tipologie di documenti conservati da Credemtel

L'Amministrazione concorda con Credemtel le tipologie di documenti (classi documentali) da conservare. Sono inclusi anche i fascicoli informatici, conservati come file in formato xml.
Le tipologie di documenti gestite dal sistema di conservazione sono descritte nella documentazione tecnica parte integrante e sostanziale del contratto per l'affidamento del servizio di conservazione. L'allegato tecnico per ciascuna tipologia di documento conservato definisce formati, metadati, sottoscrizione digitale, frequenza di versamento e software/altre informazioni per la visualizzazione dei documenti.

L'Amministrazione conserva tramite il servizio di conservazione di Credemtel le seguenti tipologie di documenti:

- Atti amministrativi – Allegato Atto generico
- Atti amministrativi – Allegato Atto interno
- Atti amministrativi – Allegato Deliberazione
- Atti amministrativi – Allegato Determinazione-Liquidazione
- Atti amministrativi – Allegato Ordinanza-Decreto
- Atti amministrativi – Allegato Verbale di adunanza
- Atti amministrativi – Atto generico
- Atti amministrativi – Atto interno
- Atti amministrativi – Deliberazione
- Atti amministrativi – Determinazione-Liquidazione
- Atti amministrativi – Ordinanza-Decreto
- Atti amministrativi – Registro atti amministrativi
- Atti amministrativi – Verbale di adunanza
- Contratti – Allegato del contratto
- Contratti – Contratto
- Messi notificatori – Allegato pubblicazione
- Messi notificatori – Documento di notifica
- Messi notificatori – Documento pubblicazione
- Messi notificatori – Registro depositi
- Messi notificatori – Registro notifiche
- Messi notificatori – Registro pubblicazioni
- Personale – CU Ordinario
- Personale – CUD
- Personale – Cedolino
- Protocollo – Fascicolo
- Protocollo – Protocollo e-mail in arrivo
- Protocollo – Protocollo e-mail in partenza
- Protocollo – Protocollo fattura
- Protocollo – Protocollo ricevuta PEC
- Protocollo – Registro di protocollo
- Tributi – Ricevuta pagamento WEB

Per la descrizione e le caratteristiche delle tipologie di documenti conservati nel sistema di conservazione, si rimanda al Manuale del sistema di conservazione di Credemtel.

5.1 Tipologie di documenti conservati da TopConsult

L'Amministrazione concorda con TopConsult le tipologie di documenti (classi documentali) da conservare.
Le tipologie di documenti gestite dal sistema di conservazione sono descritte nella documentazione tecnica parte integrante e sostanziale del contratto per l'affidamento del servizio di conservazione. L'allegato tecnico per ciascuna tipologia di documento conservato definisce formati, metadati, sottoscrizione digitale, frequenza di versamento e software/altre informazioni per la visualizzazione dei documenti.

L'Amministrazione conserva tramite il servizio di conservazione di TopConsult le seguenti tipologie di documenti:

- Ricevute telematiche

Si segnala che delle categorie documentarie qui sopra elencate si trovano in conservazione presso TopConsult solo i documenti prodotti fino al 2025. Per mandati e reversali successivi al 1° gennaio 2026, si ricerchi l'ambiente di conservazione di Credemtel. Per la descrizione e le caratteristiche delle tipologie di documenti conservati nel sistema di conservazione di TopConsult si rimanda al Manuale del sistema di conservazione.

6 Misure di sicurezza

6.1 Misure di sicurezza dell'Amministrazione

L'Amministrazione provvede alle misure di sicurezza nelle fasi di trattamento, formazione e gestione dei documenti e dei fascicoli informatici definiti come da conservare.
All'interfaccia web per la gestione dei documenti inviati in conservazione (dedicata alle operazioni di verifica stato dei documenti, esibizione, ecc.) accedono solo gli utenti individuati dall'Amministrazione e che possiedono i privilegi di accesso.
L'Amministrazione si assicura preventivamente all'invio in conservazione che i documenti siano privi di qualsiasi agente di alterazione, pertanto i documenti da conservare non devono contenere virus, macroistruzioni corrispondenti in comandi interni che, al verificarsi di determinati eventi, possono generare automaticamente modifiche o variazione dei dati contenuti nel documento, né codici eseguibili corrispondenti in istruzioni, non sempre visibili all'operatore, che consentono all'elaboratore di modificare il contenuto del documento informatico.
I Conservatori declinano ogni responsabilità nel caso non sia rispettata la reciproca salvaguardia.

7.2 Misure di sicurezza del sistema di conservazione

I sistemi di conservazione sono conforme ai requisiti di sicurezza prescritti dalla normativa.
Come previsto dalle norme vigenti in materia, i Conservatori adottano idonee e preventive misure di sicurezza al fine di ridurre al minimo i rischi di:

- distruzione o perdita, anche accidentale, dei documenti informatici
- danneggiamento delle risorse hardware su cui i documenti informatici sono registrati e dei locali ove i medesimi vengono custoditi
- accesso non autorizzato
- trattamenti non consentiti dalla legge o dai regolamenti aziendali

Le misure di sicurezza adottate assicurano:

- l'integrità dei documenti informatici, da intendersi come salvaguardia dell'esattezza dei dati, difesa da manomissioni o modifiche da parte di soggetti non autorizzati
- la disponibilità dei dati e dei documenti informatici da intendersi come la certezza che l'accesso sia sempre possibile quando necessario; indica quindi la garanzia di fruibilità dei documenti informatici, evitando la perdita o la riduzione dei dati anche accidentale utilizzando un sistema di backup
- la riservatezza dei documenti informatici da intendersi come garanzia che le informazioni siano accessibili solo da persone autorizzate e come protezione delle trasmissioni e controllo degli accessi stessi

Per la descrizione delle misure di sicurezza e delle infrastrutture si rimanda ai Manuali del sistema di conservazione dei Conservatori.

8 Trattamento dei dati personali

8.1 Misure per la protezione e il trattamento dei dati personali di Credemtel

Nelle fasi di creazione, digitalizzazione, trattamento e invio in conservazione dei documenti e dei fascicoli informatici, l'Amministrazione pone massima cura nel rispetto delle disposizioni previste dal Codice in materia di protezione dei dati personali D.Lgs. 196/2003 agg. 2018.

In materia di trattamento dei dati personali, Credemtel garantisce la tutela degli interessati in ottemperanza a quanto disposto dal Regolamento UE 2016/679, disciplinato in Italia dal D.Lgs. 101/2018. In particolare, agli interessati sono fornite le informative di cui agli artt. 13 e 14 del richiamato provvedimento. Nella suddetta informativa l'Amministrazione è informata sui diritti di accesso ai dati personali e altri diritti (art. 15 del Regolamento UE 2016/679).
La titolarità del trattamento di dati personali contenuti nei documenti oggetto di conservazione è in capo all'Amministrazione, in quanto produttore e titolare dei documenti oggetto di conservazione.
Credemtel è nominata quale "responsabile esterno" del trattamento dei dati personali necessari allo svolgimento del processo di conservazione. Credemtel si impegna, nel trattamento dei suddetti dati, ad attenersi alle istruzioni e a svolgere i compiti indicati dall'Amministrazione.
Il Responsabile del trattamento dei dati personali all'interno di Credemtel assume la responsabilità sulla garanzia del rispetto delle vigenti disposizioni in materia di trattamento dei dati personali e sulla garanzia che il trattamento dei dati affidati dall'Amministrazione avvenga nel rispetto delle istruzioni impartite dal titolare del trattamento dei dati personali, con garanzia di sicurezza e di riservatezza.

Credemtel, nel ruolo di Conservatore, tratta i dati personali con strumenti automatizzati per il tempo strettamente necessario a conseguire gli scopi per cui sono stati raccolti. Specifiche misure di sicurezza sono osservate per prevenire la perdita dei dati, usi illeciti o non corretti e accessi non autorizzati. In relazione ai trattamenti appena indicati, Credemtel garantisce agli interessati, alle condizioni previste dal GDPR, di esercitare i diritti sanciti dagli articoli da 15 a 21 dello stesso GDPR e, in particolare, il diritto di:

- ottenere conferma che sia o meno in corso un trattamento di dati personali che li riguardano e, in tal caso, ottenere l'accesso ai loro dati personali – compresa una copia degli stessi – e la comunicazione, tra le altre, delle seguenti informazioni: finalità del trattamento, categorie di dati personali trattati, destinatari cui questi sono stati o saranno comunicati, periodo di conservazione dei dati, diritti dell'interessato (diritto di accesso – articolo 15 GDPR);
- ottenere, senza ingiustificato ritardo, la rettifica dei dati personali inesatti che li riguardano e/o l'integrazione dei dati personali incompleti (diritto di rettifica – articolo 16 GDPR);
- ottenere, senza ingiustificato ritardo, la cancellazione dei dati personali che li riguardano (diritto alla cancellazione – articolo 17 GDPR);
- ottenere la limitazione del trattamento (diritto di limitazione di trattamento – articolo 18 GDPR);
- ricevere in un formato strutturato, di uso comune e leggibile da un dispositivo automatico, i dati personali che li riguardano, trasmetterli a un altro titolare senza impedimenti e, ove tecnicamente fattibile, ottenere che i loro dati personali siano trasmessi direttamente dalla Società ad altro titolare, qualora il trattamento si basi sul consenso e sia effettuato con mezzi automatizzati (diritto alla portabilità dei dati – articolo 20 GDPR);
- opporsi al trattamento dei dati personali che li riguardano, salvo che sussistano motivi legittimi per il Titolare di continuare il trattamento (diritto di opposizione – articolo 21 GDPR);
- proporre reclamo all'Autorità Garante per la protezione dei dati personali, Piazza di Montecitorio n. 121, 00186, Roma (RM).

L'esercizio dei diritti in qualità di interessato è gratuito ai sensi dell'articolo 12 GDPR. Tuttavia, nel caso di richieste manifestamente infondate o eccessive, anche per la loro ripetitività, Credemtel potrebbe addebitare un contributo spese ragionevole, alla luce dei costi amministrativi sostenuti per gestire le richieste, o negare la soddisfazione di richieste.

8.2 Misure per la protezione e il trattamento dei dati personali di TopConsult

TopConsult si è posta l'obiettivo di preservare gli interessi propri e dei propri clienti ponendo particolare attenzione agli aspetti di:

- Requisiti legali
- Livello di servizio
- Continuità operativa
- Riservatezza, integrità e disponibilità delle informazioni

A tale scopo, TopConsult si adopera a perseguire la sicurezza delle informazioni:

- utilizzando buone pratiche per proteggere le risorse informative dell'organizzazione da minacce alla sicurezza di informazioni interne o esterne, intenzionali o accidentali

- allineando gestione della sicurezza delle informazioni con il contesto di gestione del rischio strategico dell'organizzazione
- fissando obiettivi di sicurezza delle informazioni e stabilendo direzione e principi per l'azione
- stabilendo criteri per la valutazione dei rischi e l'accettazione del rischio
- controllando l'accesso alle risorse informative in base alle esigenze di business e di sicurezza
- proteggendo le informazioni e i supporti fisici in transito
- proteggendo le informazioni associate con l'interconnessione dei sistemi informativi aziendali
- applicando garanzie per la condivisione delle informazioni
- osservando la politica della scrivania pulita per documenti e supporti di memorizzazione rimovibili
- osservando la politica dello schermo pulito per servizi di elaborazione delle informazioni
- implementando adeguate misure di sicurezza al mobile computing e alle comunicazioni
- utilizzando adeguati controlli crittografici per la protezione delle informazioni
- garantendo protezione, durata e un uso corretto delle chiavi crittografiche attraverso il loro ciclo di vita
- stabilendo regole per lo sviluppo di software e sistemi e l'applicazione di tali norme agli sviluppi all'interno dell'organizzazione
- garantendo la protezione dei beni dell'organizzazione che sono accessibili dai fornitori
- proibendo l'uso di software non autorizzato e rispettando le leggi sui diritti di proprietà intellettuale
- proteggendo dati organizzativi e di tutela della privacy
- predisponendo copie di backup delle informazioni, del software e delle immagini di sistema e testandole regolarmente
- mantenendo registrazioni per un periodo adeguato prima di smaltirle con cura
- applicando azioni disciplinari e scoraggiando l'uso improprio dei servizi di informazione da parte del personale
- rispettando i requisiti applicabili relativi alla sicurezza delle informazioni, compresi i requisiti enunciati nella norma ISO/IEC 27001:2013
- riesaminando l'efficacia del SGSI a intervalli regolari
- migliorando continuamente il SGSI.

Il Sistema di Gestione per la Sicurezza delle Informazioni assicura che la gestione della continuità operativa, le procedure di backup, la protezione da malware, la gestione degli accessi ai sistemi e all'informazione e la gestione degli incidenti siano effettivamente implementati e adeguatamente supportati da specifiche policy e procedure documentate.

I requisiti della sicurezza delle informazioni sono continuamente allineati agli obiettivi strategici di business aziendale e garantiscono che l'informazione sia condivisa e fruibile mantenendo il rischio, che questo comporta, ad un livello accettabile.

La Direzione sostiene la sicurezza delle informazioni tramite un chiaro indirizzo, un impegno evidente, incarichi espliciti e riconoscimento delle responsabilità.

Tutto il personale contribuisce, ognuno con la propria competenza e professionalità, all'effettiva efficacia del Sistema di Gestione per la Sicurezza delle Informazioni e al rispetto della presente politica. Il Sistema di Gestione per la Sicurezza delle Informazioni è soggetto a sistematico riesame e miglioramento.