ENTAKSISOLUTIONS

SISTEMA DI GESTIONE CERTIFICATO
ISO 9001 | ISO 20000-1 | ISO 22301
ISO 27001 | ISO 27017 | ISO 27018 | ISO 27035
SERVIZIO DI CONSERVAZIONE CERTIFICATO
ETSI 319-401 | ETSI 119-511
PER LA CONSERVAZIONE A LUNGO TERMINE

Manuale

MAN eCON 20210628 Preservation Service Policy

Entaksi Solutions SpA

Indice

Informazioni sul documento

Progetto	Sistema Integrato di Gestione
Tipo	Manuale
Nome documento	MAN eCON 20210628 Preservation Service Policy
Versione	1.0.0
Data creazione	28/06/2021
Ultima revisione	01/12/2021
Autore	Alessia Soccio
Stato	Rilasciato
Classificazione	Pubblico

Riproduzioni cartacee di questo documento sono da considerarsi copie di lavoro non censite dal SIG.

Revisioni e relative distribuzioni

Data	Versione	Nome	Mansione	Azione	Distribuzione
28/06/2021	0.0.1	Alessia Soccio	RARC	Creazione bozza.	Pubblico
01/12/2021	1.0.0	Alessia Soccio	RARC	Revisione e rilascio.	Pubblico

Approvazione del documento

Data	Addetto	Mansione	Firma
01/12/2021	Alessandro Geri	Responsabile del Servizio di Conservazione	*Firmato digitalmente*

1. Introduzione

Il presente documento costituisce la Preservation Service Policy riferita al Servizio di Conservazione eCON erogato da Entaksi Solutions Spa, con sede legale in via la Piana 76, fraz. Pontepetri, 51028 San Marcello Piteglio (PT) (sito web: http://www.entaksi.eu).

Il Servizio di Conservazione eCON è un servizio di conservazione qualificato a lungo termine delle firme elettroniche qualificate e sigilli elettronici, così come definito dal Regolamento UE 910/2014 del Parlamento europeo e del Consiglio del 23 luglio 2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno eIDAS.

Il documento illustra i seguenti argomenti:

- la descrizione di tutte le politiche riguardanti il Servizio di Conservazione eCON;
- l'insieme delle norme applicabili al Servizio di Conservazione qualificato eCON, e la comunità di riferimento alla quale sono indirizzate;
- i requisiti di sicurezza applicati.

1.1. Identificativo del documento

Questo documento è identificato dal seguente OID:

OID	Descrizione
1.3.6.1.4.1.57823.1.1	MAN eCON 20210628 Preservation Service Policy 1.0.0

Gli OID che identificano le specifiche policy di conservazione sono indicati all'interno del documento.

Il seguente URI è l'identificativo digitale del servizio di conservazione eCON:
`https://r.entaksi.eu/oids/1.3.6.1.4.1.57823.3.1`

1.2. Aggiornamento del documento

Entaksi ha definito un processo di revisione di tutti i documenti interni, comprese le politiche e i documenti di pratica.

I documenti sono periodicamente rivisti sotto la responsabilità del management di Entaksi, al fine di valutarne la conformità ai requisiti nazionali e internazionali, agli standard, alla legislazione cogente, ai regolamenti vigenti, alle particolari esigenze imposte dall'evoluzione tecnica e tecnologica, all'evoluzione del contesto aziendale.

Il riesame e l'eventuale aggiornamento avvengono almeno una volta all'anno, oppure ogni qualvolta si verifichi una delle seguenti circostanze:

- cambiamenti organizzativi interni che impattano sul sistema;
- modifiche rilevanti dell'architettura hardware o software;
- aggiornamenti normativi;
- cambiamenti nelle procedure, nelle metodologie o nel contesto aziendale.

1.3. Approvazione e pubblicazione

Il presente documento e tutte le politiche e pratiche interne in esso menzionate sono state approvate dalla Direzione di Entaksi, pubblicate e comunicate ai dipendenti e, per quanto riguarda quelle classificate come "pubbliche", pubblicate sul sito web aziendale.

Entaksi mette a disposizione di tutti i clienti dei servizi di conservazione e delle parti interessate qualsiasi aggiornamento di questo documento e di altra documentazione pertinente non appena l'aggiornamento viene approvato e rivisto sulla base della procedura di revisione.

Qualsiasi modifica che possa influire sull'accettazione del servizio da parte del soggetto, dell'abbonato o degli affidatari, sarà comunicata da Entaksi attraverso il canale di comunicazione stabilito nei termini e nelle condizioni del servizio.

2. Definizioni e abbreviazioni

2.1. Definizioni

certificate status authority

authority providing certificate status information.

container

data object, which contains a set of data objects and optional additional information, which describes the contained data objects and optionally its content and its interrelationships.

data object

actual binary/octet data being operated on (e.g. transformed, digested, or signed) by an application and which may be associated with additional information like an identifier, the encoding, size or type.

delta preservation object container

special preservation object container describing the difference to an already existing preservation object container.

EU qualified preservation service

preservation service that meets the requirements for qualified preservation service for qualified electronic signatures and/or for qualified electronic seals as laid down in Regulation (EU) 910/2014.

evidence record

unit of data, which can be used to prove the existence of an archived data object or an archived data object group at a certain time.

expected evidence duration

for a preservation service with temporary storage or without storage, duration during which the preservation service expects that the preservation evidence can be used to achieve the preservation goal long-term: time period during which technological changes may be a concern.

metadata

data about other data.

notification interface

interface provided by the preservation client supporting the notification protocol.

notification protocol

protocol used by a preservation service to notify the preservation client.

preservation client

component or a piece of software which interacts with a preservation service via the preservation protocol.

preservation evidence

evidence produced by the preservation service which can be used to demonstrate that one or more preservation goals are met for a given preservation object.

preservation evidence policy

set of rules that specify the requirements and the internal process to generate or how to validate a preservation evidence.

preservation evidence retention period

for a preservation service With Temporary Storage (WTS) the time period during which the evidences that are produced asynchronously can be retrieved from the preservation service.

preservation goal

one of the following objectives achieved during the preservation time frame: extending over long periods of time the validity status of digital signatures, providing proofs of existence of data over long periods of time, or augmentation of externally provided preservation evidences.

preservation interface

component implementing the preservation protocol on the side of the preservation service preservation manifest: data object in a preservation object container referring to the preservation data objects or additional information and metadata in the preservation object container.

preservation mechanism

mechanism used to preserve preservation objects and to maintain the validity of preservation evidences.

preservation object

typed data object, which is submitted to, processed by or retrieved from a preservation service.

preservation object container

container which contains a set of data objects and optionally related metadata providing information about the data objects and optionally preservation manifest(s) specifying its content and relationships.

preservation object identifier

unique identifier of a (set of) preservation object(s) submitted to a preservation service.

preservation planning

monitoring changes and risks e.g. concerning innovations in storage, access and preservation technologies, new design strategies, etc.

preservation period

for a preservation service with storage, duration during which the preservation service preserves the submitted preservation objects and the associated evidences.

preservation profile

uniquely identified set of implementation details pertinent to a preservation storage model and one or more preservation goals which specifies how preservation evidences are generated and validated.

preservation protocol

protocol to communicate between the preservation service and a preservation client.

preservation scheme

generic set of procedures and rules pertinent to a preservation storage model and one or more preservation goals which outlines how preservation evidences are created and validated.

preservation service

service capable of extending the validity status of a digital signature over long periods of time and/or of providing proofs of existence of data over long periods of time.

preservation storage model

one of the following ways of implementing a preservation service: with storage, with temporary storage, without storage.

preservation submitter

legal or natural person using the preservation client to submit the submission data object.

preservation subscriber

legal or natural person bound by agreement with a preservation trust service provider to any subscriber obligations.

proof of existence

evidence that proves that an object existed at a specific date/time.

proof of integrity

evidence that data has not been altered since it was protected.

signer

entity being the creator of a digital signature.

submission data object

original data object provided by the client.

time-stamp

data in electronic form which binds other electronic data to a particular time establishing evidence that these data existed at that time.

time-stamping authority

trust service provider which issues time-stamps using one or more time-stamping units.

time-stamping service

trust service for issuing time-stamps.

time-stamping unit

set of hardware and software which is managed as a unit and has a single time-stamp signing key active at a time.

trusted list

list that provides information about the status and the status history of the trust services from trust service providers regarding compliance with the applicable requirements and the relevant provisions of the applicable legislation.

validation data

data that is used to validate a digital signature.

2.2. Abbreviazioni

CA

Certification Authority

IP

Internet Protocol

IT

Information Technology

TSP

Trust Service Provider

UTC

Coordinated Universal Time

AUG

Augmentation goal

CSA

Certificate Status Authority

EUMS

European Union Member State

PDS

Preservation of Digital Signatures

PGD

Preservation of General Data

PO

Preservation Object

POC

Preservation Object Container

PRP

Preservation service Protocol

PSP

Preservation Service Provider

QES

Qualified Electronic Signature or Qualified Electronic Seal

SigS

digital Signature creation Service

SubDO

Submission Data Object

TS

Trust Service

TSA

Time-Stamping Authority

TSP

Trust Service Provider

ValS

Validation Service

WOS

Without Storage

WST

With Storage

WTS

With Temporary Storage

3. Riferimenti

Per garantire la gestione a norma del Servizio di Conservazione eCON, Entaksi definisce i criteri e i processi del Servizio in base alla normativa italiana ed europea in materia, oltre ad implementare standard internazionali che definiscono la gestione teorica, operativa e funzionale del sistema. Vengono qui di seguito riportati le norme e gli standard di riferimento per l'azienda.

Questo documento di policy è conforme ai riferimenti normativi elencati di seguito, come richiesto dal regolamento eIDAS e dalla normativa italiana sulla conservazione digitale.

3.1. Riferimenti normativi e standard

3.1.1. Certificazioni

Entaksi ha ottenuto le seguenti certificazioni:

UNI ISO 9001:2015

Sistemi di Gestione per la Qualità – Requisiti.

ISO/IEC 20000-1:2018

Tecnologie informatiche – Erogazione di servizi informatici.

ISO/IEC 27001:2013

Tecnologia delle informazioni - Tecniche di sicurezza - Sistemi di gestione della sicurezza delle informazioni - Requisiti.

ISO/IEC 27017:2015

Tecnologia delle informazioni - Tecniche di sicurezza - Codice di condotta per i controlli di sicurezza delle informazioni basato su ISO / IEC 27002 per i servizi cloud.

ISO/IEC 27018:2019

Tecnologia delle informazioni - Tecniche di sicurezza - Codice di condotta per la protezione delle informazioni di identificazione personale (PII) nei cloud pubblici che fungono da processori PII.

ISO/IEC 27035:2016

Tecnologia delle informazioni - Tecniche di sicurezza - Gestione degli incidenti di sicurezza delle informazioni.

ISO/IEC 22301:2019

Tecnologia delle informazioni - Sicurezza e resilienza - Sistemi di gestione della continuità operativa aziendale.

Sistema di conservazione dei documenti digitali

Tecnologia delle informazioni - Conservazione digitale - art. 24 Regolamento UE n° 910/2014 sull'identità digitale.

eIDAS

Regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE.

ETSI EN 319 401 V2.3.1 (2021-05)

Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers, policy e requisiti per i fornitori di servizi fiduciari.

ETSI TS 119 511 v1.1.1 (2019-06)

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, policy e requisiti di sicurezza per servizi fiduciari di conservazione di firme digitali e la conservazione di dati mediante tecniche basate sulla firma digitale.

3.1.2. Long-Term Preservation

eIDAS

Regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE.

ETSI TS 119 512 V1.1.2 (2020-10)

Electronic Signatures and Infrastructures (ESI); Protocols for trust service providers providing long-term data preservation services, protocolli per fornitori di servizi fiduciari che forniscono servizi di conservazione dei dati a lungo termine.

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 319 102-1 V1.1.1 (2016-5)

Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation

3.1.3. Normativa italiana sulla conservazione digitale

CAD

Decreto legislativo N° 82/2005, "Codice dell'Amministrazione Digitale".

Linee Guida sulla formazione, gestione e conservazione dei documenti informatici

Linee guida ufficiali sulla creazione, gestione e conservazione dei documenti informatici, pubblicate da AgID in data 11/09/2020 alle quali vengono aggiunte le modifiche con la relativa proroga contenute nella Determinazione 371/2021 del 17/05/2021.

Determinazione AgID 25 giugno 2021 n.455

Concernente l'adozione del "Regolamento sui criteri per la fornitura dei servizi di conservazione dei documenti informatici".

3.1.4. Protezione dei dati personali

Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio

Regolamento UE del 27 aprile 2016, 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 (regolamento generale sulla protezione dei dati).

Decreto Legislativo 10 agosto 2018, n. 101

Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, 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 (regolamento generale sulla protezione dei dati).

3.1.5. Altre disposizioni

ISO/IEC 14721:2012

Space data and information transfer systems — Open archival information system (OAIS) — Reference model.

ETSI TS 119 312 V1.4.1 (2021-08)

Electronic Signatures and Infrastructures (ESI) - Cryptographic Suites.

3.2. Riferimenti informativi

Il servizio qualificato di conservazione a lungo termine di Entaksi è supportato dalle seguenti policy:

Tabella 1. Policy Servizio di Conservazione eCON

Nome del documento	Versione del documento	Valido da
MAN SIG 20210708 Preservation Service Policy	1.0.0	01/12/2021
MAN eCON 20200628 Signature Validation Policy	1.0.0	01/12/2021
MAN eCON 20200628 Preservation Evidence Policy	1.0.0	01/12/2021
MAN SIG 20200511 Politica per la sicurezza delle informazioni	1.1.0	01/12/2021

Inoltre, il Servizio di conservazione eCON è descritto nelle seguenti dichiarazioni di pratica e manuali:

Tabella 2. Documenti Servizio di Conservazione eCON

Nome del documento	Versione del documento	Valido da
MAN SIG 20210708 Preservation Service Practice Statement	1.0.0	01/12/2021
MAN eCON 20151222 Conservazione	1.7.0	01/12/2021

Tutti i documenti elencati in precedenza sono classificati come "pubblici" e divulgati alle parti interessate tramite il sito web della società.

Oltre a questi, i documenti successivi illustrano alcuni argomenti confidenziali sul Servizio di Conservazione eCON, per lo più legati alle procedure di sicurezza del sistema e alle questioni tecniche.

Tabella 3. Documenti riservati Servizio di Conservazione eCON

Nome del documento	Versione del documento	Valido da
MAN eCON 20190918 Piano di cessazione	1.3.0	01/12/2021
MAN eCON 20151222 Piano della sicurezza	1.4.0	01/12/2021

Entaksi, a causa del loro contenuto confidenziale, non divulga questi documenti e nessun altro dei suoi manuali interni, procedure e documenti di sicurezza. Tuttavia, secondo la disponibilità e l'impegno dell'azienda, è disponibile a sottoporsi a audit di verifica da parte dei suoi clienti o di altre parti interessate, previa firma di un accordo di non divulgazione.

4. Ruoli e responsabilità

La **comunità di riferimento del Servizio di Conservazione eCON**, così come richiesta in riferimento allo Standard ISO/IEC 14721:2012 OAIS (Open Archival Information System), è descritta nei manuali utente eCON, e per quanto riguarda il personale Entaksi vengono riportati anche i ruoli e le attività per ogni responsabile del servizio.

Entaksi è nominato Trust Service Provider per il servizio di conservazione a lungo termine eCON.

Il servizio di conservazione eCON è amministrato da vari "**Responsabili**", ognuno dei quali ricopre un ruolo specifico nell'azienda e in particolare nel servizio, al fine di garantire meglio l'affidabilità del sistema senza sovrapposizioni di attività e seguendo una compartimentazione dei ruoli:

- **Responsabile del Servizio di Conservazione**.
- **Vice Responsabile del Servizio di Conservazione**.
- **Responsabile della Funzione Archivistica**.
- **Responsabile del Trattamento dei Dati Personali**.
- **Responsabile della Sicurezza**.
- **Responsabile dei Sistemi Informativi**.
- *Responsabile dello Sviluppo e della Manutenzione.

Tutti i dati relativi alle persone e ai ruoli specifici ricoperti dai vari responsabili del Servizio di Conservazione eCON sono disponibili nel manuale di conservazione eCON, pubblicato sia sul sito dell'Agenzia per l'Italia Digitale che sul sito di Entaksi.

I compiti e le aree di responsabilità in conflitto sono segregati per ridurre le opportunità di modifiche non autorizzate o non intenzionali, o l'uso improprio degli asset di Entaksi.

Entaksi Solution SpA è responsabile della fornitura del servizio, e il Responsabile del Servizio di Conservazione è il ruolo incaricato per i compiti di fornitura del servizio.

In conformità con l'art. 38 del Decreto del Presidente del Consiglio dei Ministri del 22 febbraio 2013, all'interno dell'organizzazione sono nominate le seguenti persone in aggiunta ai ruoli sopra elencati:

- Responsabile della sicurezza.
- Responsabile del servizio qualificato.
- Responsabile della conduzione tecnica dei sistemi.
- Responsabile dei servizi tecnici e logistici.
- Responsabile delle verifiche e delle ispezioni (auditing).

4.1. Clienti

Un cliente è la persona fisica o giuridica vincolata da un accordo con un fornitore di servizi.

I clienti possono firmare l'accordo di servizio ("Condizioni generali del servizio") con il fornitore di servizi di conservazione Entaksi, al fine di accedere al Servizio di Conservazione eCON.

4.2. Parti coinvolte

Entaksi non coinvolge nessuna parte esterna per eseguire compiti critici sul servizio di conservazione eCON.
Tuttavia altre terze parti possono essere coinvolte nel processo, come gli organi di controllo legale, le autorità e i revisori.
Entaksi richiede sempre accordi di non divulgazione per qualsiasi accesso non contrattuale al sistema, come per gli audit, e

applica l'anonimizzazione e la minimizzazione dei dati personali ove possibile.

4.3. Fornitori

Entaksi Solutions ha deciso di:

- Utilizzare un'infrastruttura di server in housing / hosting. I server che ospitano e forniscono i vari componenti del servizio di conservazione eCON e le altre attività dell'azienda si trovano in data center gestiti da fornitori specializzati. I contratti tra Entaksi e tali fornitori vengono periodicamente riesaminati, al fine di ottenere le migliori prestazioni secondo il valore di mercato. La stessa considerazione avviene per l'utilizzo dei servizi generali di rete (come i nomi a dominio e i relativi DNS), anch'essi affidati a servizi esterni.
- Utilizzare per tutti i dipendenti e collaboratori un contratto basato sul lavoro a distanza.

Il risultato di queste affermazioni è che l'azienda opera interamente in rete, non utilizzando sedi fisiche. Quindi Entaksi non regola direttamente il controllo degli accessi fisici alle infrastrutture, ma verifica i fornitori in fase di qualifica, monitora gli SLA definiti da contratto e se necessario conduce appositi audit.

Dunque Entaksi garantisce il rispetto dei requisiti sulla gestione della sicurezza fisica dell'infrastruttura centrale attraverso un accurato processo di qualificazione e monitorando i fornitori, che vengono selezionati in base alla convenienza del mercato e allo standard qualitativo garantito in termini di sicurezza, come ad esempio la certificazione ISO/IEC 27001:2013. Entaksi richiede inoltre, secondo i limiti del contratto, la possibilità per il fornitore di essere sottoposto a verifiche e ispezioni, al fine di individuare eventuali elementi non sufficientemente coperti dalle condizioni contrattuali o dalle certificazioni stesse.

Per quanto riguarda gli altri fornitori non legati all'infrastruttura fisica, Entaksi utilizza marche temporali esterne, fornite solo da Time-Stamping Authority (TSA) qualificate. Il processo di qualificazione richiede gli stessi livelli di sicurezza e la facoltà di condurre audit così come definito per la fornitura dei server.

5. Politiche

5.1. Affidabilità dell'organizzazione

La direzione di Entaksi è costantemente impegnata a garantire l'affidabilità dell'intera organizzazione e in particolare del servizio di conservazione eCON fornito ai clienti.

Entaksi si impegna ad essere non discriminatoria e a garantire l'accesso al Servizio di Conservazione eCON a tutti i richiedenti le cui attività rientrano nel campo operativo dichiarato e che accettano di rispettare i loro obblighi come specificato nei termini e nelle condizioni del servizio.

5.2. Risorse umane

Entaksi si impegna a impiegare personale qualificato che possieda le competenze, l'affidabilità, l'esperienza e le qualifiche necessarie per lavorare nell'ambito del Servizio di Conservazione eCON. Fornisce anche una formazione costante per quanto riguarda le norme di sicurezza e di protezione dei dati personali, come richiesto per i servizi offerti e la funzione lavorativa.

Il personale ha accesso alle funzioni del servizio solo dopo che la Direzione ha effettuato i controlli necessari.

I ruoli fiduciari definiti per il servizio di conservazione eCON sono elencati nel capitolo Ruoli e responsabilità.

Il processo di revisione degli ambiti di formazione e dell'esperienza acquisita dal personale avviene periodicamente, almeno su base annuale. Le competenze maturate sono registrate nei database Entaksi.

Il personale di Entaksi (sia temporaneo che permanente) ha descrizioni delle mansioni definite dal punto di vista dei ruoli svolti e vengono applicate la segregazione dei compiti e la regola del minimo privilegio. Le posizioni sono basate sulle mansioni e sui livelli di accesso, sullo screening dei precedenti incarichi e sulla formazione e consapevolezza dei dipendenti.

Entaksi prevede nella sua documentazione, formalmente accettata dal dipendente, che possano essere messe in atto adeguate sanzioni disciplinari al personale che viola le politiche o le procedure di sicurezza.
Il personale esercita mansioni e processi amministrativi e gestionali che sono in linea con le procedure di gestione di Entaksi. La procedura di accettazione comporta una revisione da parte della direzione e la firma del dipendente sul documento di incarico.

I ruoli e le responsabilità di sicurezza sono chiaramente identificati nelle descrizioni delle mansioni e nei documenti interni, costantemente disponibili per tutto il personale interessato. I ruoli sono differenziati tra funzioni generali e funzioni specifiche

del Servizio di Conservazione eCON.
Entaksi definisce i requisiti minimi per ricoprire i ruoli: tutto il personale deve possedere esperienza o formazione rispetto al servizio fornito, familiarità con le procedure di sicurezza, con la sicurezza delle informazioni e la valutazione dei rischi sufficiente per svolgere le funzioni di gestione.

Tutto il personale impiegato nei ruoli definiti per il Servizio di Conservazione eCON deve essere libero da conflitti di interesse che potrebbero pregiudicare l'imparzialità delle operazioni di Entaksi.

5.3. Risorse finanziarie

Entaksi organizza le sue risorse finanziarie in modo da commisurarle alla fornitura del Servizio di Conservazione eCON, e mira a garantire la stabilità finanziaria e le risorse necessarie per operare in conformità con questa politica.

Il mantenimento di un livello costante e adeguato di risorse per garantire il corretto funzionamento delle operazioni tecniche e strutturali del Servizio di Conservazione eCON si ottiene grazie a una revisione costante dei valori derivanti dai dati di monitoraggio.

Oltre a queste misure di monitoraggio e adeguamento, le attività di sviluppo e l'erogazione dei servizi sono coperte da una polizza assicurativa, in linea con i requisiti della legge italiana.

Entaksi dispone di politiche e procedure per la risoluzione dei reclami e delle controversie ricevute dai clienti o da altri soggetti affidatari in merito all'erogazione del Servizio di Conservazione eCON o a qualsiasi altra questione correlata.

5.4. Asset

Entaksi assicura un livello appropriato di protezione dei suoi asset, compresi gli asset informatici, ed è responsabile dell'impegno di tutto il personale a gestire tutti i supporti in modo sicuro, in conformità alle sue politiche e procedure.

Entaksi utilizza un proprio software per gestire le risorse, un Configuration Management Data Base (CMDB) che costituisce un inventario di tutto il patrimonio informativo, e dichiara per ogni oggetto censito una classificazione coerente con la valutazione dei rischi.

Per evitare che i dati sensibili memorizzati negli asset possano essere esposti a minacce che ne compromettano confidenzialità, integrità e disponibilità, Entaksi stabilisce specifiche procedure interne che descrivono:

- come impostare gli asset per assicurare il massimo livello di protezione;
- come gestire i backup e le copie;
- come agire quando è necessario spostare il dispositivo o disporne per un altro uso;
- requisiti specifici per assicurare la cancellazione sicura di tutte le informazioni contenute, se necessario.

5.5. Valutazione del rischio

Entaksi applica tutti i controlli di sicurezza e le procedure operative che sono necessarie per implementare le misure di trattamento del rischio scelte, come documentato nella Politica di Sicurezza delle Informazioni e nel Preservation Service Practice Statement.

Entaksi esegue regolarmente una valutazione dei rischi per identificare, analizzare e valutare i rischi relativi al servizio di conservazione eCON.

5.6. Gestione degli incidenti

Si definisce "incidente di sicurezza" qualsiasi evento che comprometta o minacci di compromettere il corretto funzionamento dei sistemi e/o delle reti dell'organizzazione o l'integrità e/o la riservatezza delle informazioni in esse memorizzate o in transito, o che violi le politiche di sicurezza definite o le leggi in vigore, con particolare riferimento al Regolamento dell'Unione Europea n° 2016/679 sulla protezione dei dati.

Il Team di risposta agli incidenti (Incident Response Team, IRT) è un gruppo di membri dell'organizzazione adeguatamente qualificati e di fiducia che gestisce gli incidenti durante il loro ciclo di vita.

Le procedure di gestione degli incidenti sono conformi alla norma ISO/IEC 27035:2016. Il processo di gestione degli incidenti è articolato nelle seguenti fasi:

- **Pianificare e preparare** - si stabilisce una politica di gestione degli incidenti di sicurezza delle informazioni, viene formato un Incident Response Team (IRT), l'organizzazione si prepara a rispondere a qualsiasi evento dannoso.

- **Rilevazione e segnalazione**: vengono riconosciuti uno o più eventi di sicurezza come incidente e a ogni incidente ne viene assegnato un livello di gravità.
- **Valutazione e decisione**: l'Incident Response Team (IRT) verifica l'attendibilità e nel caso l'incidente venga confermato lo qualifica.
- **Risposta**: vengono attuate le contromisure, allo scopo di minimizzare i danni causati dall'incidente, se necessario vengono adeguate le risorse, e si procede al ripristino.
- **Attività successive**: viene aggiornata l'analisi dei rischi e verificata l'adeguatezza delle procedure di gestione degli incidenti
- **Lezioni apprese**: la Direzione revisiona l'incidente e vengono identificati i possibili punti di miglioramento.

Per quanto riguarda la fase "Pianificare e preparare":

- la direzione nomina personale di ruolo di fiducia per seguire le segnalazioni di eventi di sicurezza potenzialmente critici e garantire che gli incidenti rilevanti siano segnalati in linea con le procedure di Entaksi;
- le attività di sistema riguardanti l'accesso ai sistemi IT, l'uso dei sistemi IT e le richieste di servizio sono costantemente monitorate;
- le attività di monitoraggio tengono conto della sensibilità delle informazioni raccolte o analizzate;
- il responsabile IRT valuta quali parametri monitorare, come le funzioni di log, la disponibilità del servizio, la rete, la memoria, ecc;
- Entaksi definisce e mantiene un piano di continuità da attuare in caso di disastro.

Per quanto riguarda la fase di "Rilevamento e segnalazione":

- le attività anomale del sistema che indicano una potenziale violazione della sicurezza, compresa l'intrusione nella rete di Entaksi, sono rilevate e segnalate come allarmi;
- Entaksi deve affrontare qualsiasi vulnerabilità critica o evento rilevato rapidamente, non più tardi di 48 ore dopo la sua scoperta.

Per quanto riguarda la fase di "Valutazione e decisione":

- sono disponibili per l'IRT procedure per la valutazione dell'incidente, e il personale è adeguatamente formato e ha sempre a disposizione strumenti appropriati per valutare gli eventi.

Per quanto riguarda la fase di "Risposta":

- il personale di Entaksi è addestrato ad agire in modo tempestivo e coordinato per rispondere rapidamente agli incidenti e per limitare l'impatto delle violazioni della sicurezza;
- le procedure di segnalazione e risposta agli incidenti sono impiegate in modo tale che i danni derivanti da incidenti di sicurezza e malfunzionamenti siano ridotti al minimo.

Riguardo alla fase "Attività successive":

- Entaksi ha stabilito delle procedure per notificare ai clienti e alle parti interessate qualsiasi violazione della sicurezza o perdita di integrità che abbia un impatto significativo sul servizio fiduciario fornito e sui dati personali ivi conservati entro 24 ore dall'individuazione della violazione, in linea con le norme regolamentari applicabili;
- se la violazione della sicurezza o la perdita di integrità può avere ripercussioni negative su una persona fisica o giuridica a cui è stato fornito il servizio fiduciario, Entaksi è tenuta anche a notificare alla persona fisica o giuridica la violazione della sicurezza o la perdita di integrità senza indebito ritardo, come descritto in Protezione dei dati personali.

Per quanto riguarda la fase "Lezioni apprese":

- la direzione e il personale di Entaksi riesaminano i dati ed eseguono l'analisi dei rischi per ogni incidente avvenuto, al fine di migliorare il sistema. Una vulnerabilità può essere scoperta anche senza che venga rilevato un evento. Tuttavia il processo di trattamento delle vulnerabilità è il medesimo degli incidenti, quindi, dato il potenziale impatto, Entaksi:
- creerà e implementerà un piano per mitigare la vulnerabilità, come per l'incidente; o
- documenterà i motivi per i quali la vulnerabilità non richiede un rimedio.

In caso di disastro, compresa la compromissione di una chiave di firma privata o la compromissione di qualche altra credenziale del servizio di conservazione eCON, le operazioni devono essere ripristinate entro il termine stabilito nel piano di continuità, dopo aver affrontato qualsiasi causa del disastro che potrebbe ripetersi (ad esempio una vulnerabilità di sicurezza) con misure di riparazione appropriate.

5.7. Monitoraggio e logging

I sistemi di Entaksi sono costantemente monitorati: questa attività include il monitoraggio o la revisione regolare dei log di audit per identificare prove di attività malevole, implementando meccanismi automatici per elaborare i log di audit e allertare il personale riguardo a possibili eventi critici per la sicurezza.

Entaksi registra e conserva nel suo Servizio di Conservazione eCON i log degli eventi prodotti dai suoi sistemi per almeno 6 mesi. Questi log sono archiviati integralmente come confidenziali, e possono fornire prove in procedimenti legali e al fine di garantire la continuità del servizio.
La politica di conservazione dei log è la stessa dei documenti, delle firme digitali e dei sigilli, al fine di mantenere la riservatezza e l'integrità delle registrazioni relative al funzionamento del servizio.

Ogni log contiene l'ora esatta dell'evento, un riferimento all'utente e la descrizione dell'operazione. I log sono registrati in ordine cronologico, e l'ora utilizzata per registrare gli eventi come richiesto nell'audit log è sincronizzata con l'ora UTC almeno una volta al giorno.

5.8. Controlli

Entaksi implementa diversi tipi di controlli per evitare perdite, danni o compromissione di beni e interruzione delle attività aziendali.

5.8.1. Controlli operativi

Entaksi utilizza sistemi e prodotti affidabili che sono protetti da modifiche, e garantisce la sicurezza tecnica e l'affidabilità dei processi supportati da essi.
Tutte queste procedure organizzative sono stabilite e implementate per tutti i ruoli fiduciari e amministrativi che hanno un impatto sulla fornitura del Servizio di Conservazione eCON.

Un'analisi dei requisiti di sicurezza è effettuata nella fase di progettazione e di specifica dei requisiti per ogni progetto di sviluppo di sistemi intrapreso dalla direzione tecnica per assicurare che la sicurezza sia implementata all'interno dei sistemi.

Le procedure di controllo dei cambiamenti sono applicate per rilasci, modifiche e correzioni di emergenza del software, per qualsiasi software operativo o modifica della configurazione che sia interessata dalla politica di sicurezza di Entaksi. Le procedure includono la documentazione e la registrazione delle modifiche. Qualsiasi cambiamento che potrebbe avere un impatto sul livello di sicurezza stabilito deve essere approvato dalla direzione di Entaksi.

L'integrità del Servizio di Conservazione eCON e delle informazioni dell'organizzazione è fortemente protetta da virus, software malevoli o non autorizzati, come specificato nei paragrafi Sicurezza fisica, Sicurezza della rete e Sicurezza degli accessi.

Sono definite da Entaksi apposite procedure per garantire che i supporti utilizzati all'interno dei sistemi dell'organizzazione siano gestiti in modo sicuro per proteggere i supporti da danni, furto, accesso non autorizzato e obsolescenza, come specificato nel paragrafo Asset.
In particolare le procedure di gestione degli asset descrivono come proteggere dall'obsolescenza e dal deterioramento i supporti per il periodo di tempo in cui i dati devono essere conservati nel Servizio di Conservazione eCON.

Per quanto riguarda i controlli operativi di gestione del servizio, procedure specifiche assicurano che:

- le patch di sicurezza siano applicate entro un tempo ragionevole dopo la loro disponibilità;
- le patch di sicurezza non siano applicate se introducono ulteriori vulnerabilità o instabilità che superano i benefici della loro applicazione; e che
- le ragioni per non applicare le patch di sicurezza siano documentate.

5.9. Sicurezza fisica

Come dichiarato nel capitolo Fornitori, Entaksi non regolamenta direttamente il controllo dell'accesso fisico alle infrastrutture, ma applica controlli sulla fase di qualificazione dei fornitori.

Come per i server, una considerazione analoga vale per le postazioni di lavoro, per lo più dispositivi portatili assegnati a dipendenti e collaboratori. In questo caso, Entaksi richiede al personale l'adozione di comportamenti corretti nella gestione del dispositivo e impone contromisure volte a preservare ad ogni costo la protezione logica dei dispositivi, come la protezione degli accessi, la crittografia dello storage, ed altre.

Tutte queste politiche permettono di garantire un'adeguata protezione su tutte le infrastrutture fisiche e, laddove queste dovessero comunque essere violate, la società si assume il rischio di perdere il dispositivo purché la perdita non comporti alcuna violazione dei dati, poiché questi saranno stati resi inaccessibili a terzi.

5.10. Sicurezza della rete

Entaksi applica adeguati controlli di sicurezza per proteggere la sua rete e i suoi sistemi da qualsiasi attacco.

La Direzione Tecnica ha identificato le reti critiche finalizzate alla fornitura del servizio, basandosi sulla valutazione del rischio e considerando la relazione funzionale, logica e fisica (inclusa l'ubicazione) tra sistemi e servizi affidabili.
I controlli di sicurezza sono eseguiti su tutte le reti.

Entaksi afferma che:

- l'ambiente di produzione deve essere separato dagli ambienti di sviluppo e di test;
- sebbene sia applicata la separazione degli ambienti, vengono applicati i più alti livelli di controlli di sicurezza sulle connessioni in qualsiasi configurazione;
- la comunicazione tra i clienti e il Servizio di Conservazione eCON deve avvenire solo attraverso canali fidati;
- qualsiasi connessione o servizio non necessario deve essere esplicitamente vietato o disattivato;
- i sistemi utilizzati per l'amministrazione dell'implementazione della politica di sicurezza non devono essere utilizzati per altri scopi;
- la comunicazione tra sistemi distinti è stabilita solo attraverso canali affidabili che sono logicamente distinti da altri canali di comunicazione e forniscono un'identificazione garantita dei suoi punti finali e garantiscono la protezione dei dati del canale da modifiche o divulgazione;
- la connessione di rete esterna è ridondante per garantire la disponibilità dei servizi in caso di un singolo guasto.

La politica e le caratteristiche tecniche della rete sono revisionate almeno annualmente, o dopo ogni cambiamento significativo.

5.11. Test di vulnerabilità e intrusione

Entaksi si sottopone regolarmente a un Vulnerability Assessment e Penetration Test. La scansione delle vulnerabilità è fatta su indirizzi IP pubblici e privati identificati dal Responsabile della Sicurezza, ed è eseguita da un ente esterno con le competenze, gli strumenti, la professionalità, il codice etico e l'indipendenza necessari per fornire un rapporto affidabile.

I test di vulnerabilità e intrusione sui sistemi di Entaksi sono impostati almeno annualmente o dopo aggiornamenti o modifiche significative dell'infrastruttura o dell'applicazione.

Entaksi archivia nei suoi sistemi le registrazioni, le valutazioni e i verbali di tutti i test eseguiti.

5.12. Sicurezza degli accessi

Tutti gli utenti che accedono al servizio di conservazione eCON sono assegnati a un gruppo specifico, al fine di proteggere la segregazione dei ruoli e delle informazioni.
L'accesso è limitato agli individui autorizzati.

Tutti i controlli di accesso sono definiti per proteggere la rete interna di Entaksi da intromissioni non autorizzate.
I controlli di sicurezza dell'accesso includono la separazione dei ruoli fiduciari, i log, la separazione delle funzioni di amministrazione e funzionamento della sicurezza, l'uso controllato dei programmi di utilità del sistema.
I firewall sono configurati per impedire tutti i protocolli e gli accessi non necessari al funzionamento del servizio di conservazione eCON.

Il personale di Entaksi deve essere identificato e autenticato prima di utilizzare applicazioni critiche relative al servizio. Gli utenti di Entaksi sono responsabili delle loro attività, e i log degli eventi sono archiviati quotidianamente nel servizio di conservazione eCON.

Il Responsabile del Servizio di Conservazione amministra l'accesso di tutti gli operatori del servizio di conservazione eCON, che include clienti e terze parti, amministratori e auditor del sistema. Tutti i clienti sono collegati a un sistema di gestione degli account utente, che include informazioni sui log, i privilegi degli utenti, la convalida degli accessi. La procedura di rimozione è collegata ai termini e alle condizioni del contratto.

Entaksi fornisce una descrizione della politica di gestione degli accessi e delle pratiche di controllo controllo della sicurezza degli accessi nei manuali d'uso e nella documentazione pubblica, disponibile per la consultazione sul sito web di Entaksi.

5.13. Protezione della chiave privata e controlli del modulo crittografico

Entaksi assicura che sono stati implementati appropriati controlli di sicurezza per la gestione dei dispositivi crittografici e delle chiavi private.

La direzione ICT si impegna a controllare costantemente che l'algoritmo utilizzato per la crittografia dei dati non perda efficacia.

5.14. Accessibilità

Entaksi lavora costantemente per rendere il suo software accessibile e per rimuovere ogni possibile discriminazione relativa all'accesso e all'usabilità.

Il servizio di conservazione eCON è progettato e revisionato costantemente per implementare i "Requisiti di accessibilità per prodotti e servizi ICT" come richiesto dalla norma ETSI "EN 301 549".

Entaksi è attenta ad ascoltare tutte le richieste dei clienti con disabilità al fine di migliorare il servizio e la sua accessibilità.

6. Altre disposizioni

6.1. Conformità e audit

Il sistema giuridico applicabile è dichiarato nel capitolo Riferimenti.

La configurazione del Servizio di Conservazione eCON è regolarmente controllata dalla direzione per evitare qualsiasi modifica che violi le politiche di sicurezza di Entaksi.

Il Servizio di Conservazione eCON di Entaksi è supervisionato dall'Agenzia dell'Italia Digitale (AgID), che ha la responsabilità di verificare e revisionare periodicamente la conformità del sistema ai requisiti definiti in base alla normativa italiana sulla conservazione digitale.

Inoltre, il sistema è verificato almeno annualmente da un organismo di certificazione accreditato, riconosciuto da Accredia, l'Ente Italiano di Accreditamento.

I verbali di audit e i documenti di controllo sono classificati come confidenziali.
I certificati di conformità e i loro aggiornamenti sono pubblicati sul sito web Entaksi in conformità ai risultati della valutazione.

6.2. Protezione dei dati personali

Nell'ambito del trattamento dei dati personali relativi allo svolgimento delle attività previste per il Servizio di Conservazione eCON, Entaksi agisce in qualità di Responsabile del trattamento, in virtù di specifica delega conferita dal Cliente.

Entaksi opera nell'Unione Europea, ed opera in conformità al Regolamento dell'Unione Europea n° 2016/679 sulla protezione dei dati che abroga la Direttiva 95/46/CE.

L'insieme completo delle disposizioni relative al trattamento dei dati personali è riportato nel documento "Condizioni Generali del Servizio", capitolo "Trattamento dei dati personali" e anche sul sito web di Entaksi.

La Direzione di Entaksi opera per garantire che adeguate misure tecniche ed organizzative saranno costantemente adottate contro il trattamento non autorizzato o illegale dei dati personali e contro perdita o distruzione accidentale o danneggiamento dei dati personali.