Dichiarazione delle Pratiche di Certificazione

Servizi fiduciari

Evicertia
Novembre, 2024

Pubblico

Indice

1 Introduzione

1.1 Presentazione

Il presente documento enuncia le pratiche di certificazione dei servizi fiduciari di Uanataca, S.A.U., di seguito Evicertia.

1.2 Nome del documento e identificazione

Il presente documento rappresenta la "Dichiarazione delle Pratiche di Certificazione dei servizi fiduciari di Evicertia", di seguito "DPC".

1.3 Partecipanti ai servizi di certificazione

1.3.1 Fornitore di servizi di certificazione

Il Fornitore di Servizi di Certificazione Elettronica, di seguito "FSC", è la persona, fisica o giuridica, che presta uno o più servizi fiduciari.

Evicertia è un fornitore di servizi fiduciari elettronici che agisce in conformità alle disposizioni del 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, che abroga la direttiva 1999/93/CE, nonché in conformità alle norme tecniche dell'ETSI applicabili ai servizi fiduciari, al fine di facilitare l'adempimento dei requisiti legali e il riconoscimento internazionale dei propri servizi.

1.3.2 Autorità di Registro

L'Autorità di Registro, di seguito "RA" (dal termine inglese *Registry Authority*), è costituita dalle persone fisiche o giuridiche incaricate da Evicertia di identificare e verificare l'identità dei sottoscrittori dei servizi fiduciari.

Potranno agire come RA di Evicertia:

- la società madre stessa di Evicertia;
- qualsiasi ente autorizzato da Evicertia.

Per agire come RA, sarà necessario formalizzare contrattualmente il rapporto esistente tra Evicertia e l'ente autorizzato.

Le funzioni di queste RA, che agiscono per conto di Evicertia, comprendono:

- l'accertamento dell'identità del sottoscrittore attraverso la convalida, a titolo esemplificativo ma non esaustivo, delle condizioni personali del firmatario del contratto;
- la verifica delle informazioni fornite dal sottoscrittore nella formalizzazione del contratto di prestazione dei servizi;

- la custodia di tali informazioni relative all'identificazione e alla sottoscrizione dell'interessato con riferimento ai servizi fiduciari di Evicertia;
- la fornitura delle informazioni necessarie all'utilizzo dei servizi fiduciari, come ad esempio i certificati, le procedure di attivazione degli account per l'uso, etc.

1.3.3 Autorità di recapito qualificato

L'Autorità di recapito qualificato, di seguito "ARC", è il soggetto terzo fiduciario che presta il servizio di recapito qualificato "QERDS" (dal termine inglese *Qualified Electronic Registered Delivery Services*).

Evicertia è il fornitore di servizi di recapito qualificato che agisce come autorità di consegna per i messaggi con recapito qualificato.

1.3.4 Sottoscrittori del servizio di certificazione

I sottoscrittori sono gli utenti finali dei servizi fiduciari gestiti da Evicertia. I sottoscrittori del servizio possono essere:

- Le società, gli enti, le imprese o le organizzazioni che richiedono a Evicertia (direttamente o tramite terzi) l'utilizzo dei suoi servizi nel proprio contesto aziendale, societario od organizzativo.
- Persone fisiche che richiedono il servizio per se stesse.

Pertanto, i sottoscrittori dei servizi elettronici fiduciari sono i clienti dell'FSC.

1.3.5 Utenti

Gli utenti sono le persone e le organizzazioni che ricevono certificati, firme elettroniche, messaggi con recapito qualificato o qualsiasi altro servizio fiduciario dell'FSC.

Prima di fare affidamento su questi messaggi, gli utenti devono verificarli, come indicato nella presente Dichiarazione delle Pratiche di Certificazione e/o nelle istruzioni disponibili sul sito web dell'FSC.

1.3.6 Mittente e destinatario

I mittenti e i destinatari sono gli account di posta elettronica, appartenenti agli utenti, che inviano o ricevono messaggi elettronici con recapito qualificato.

1.4 Uso dei servizi fiduciari

Le informazioni sugli usi consentiti, i limiti e i divieti sono riportate nella dichiarazione delle pratiche e nella politica di ciascun profilo di certificati o di servizi fiduciari.

1.5 Gestione della politica

1.5.1 Organizzazione che gestisce il documento

I dati della società sono i seguenti:

- Uanataca, S.A.U. (Evicertia).
- P. IVA: ESA66721499.
- Indirizzo: Avenida Meridiana no. 350, terza planata, 08027 Barcellona.
- Registro delle Imprese di Barcellona Tomo 45264, Libro 0, Foglio 6, Sezione General, Pagina 482242, Iscrizione 1.

1.5.2 Dati di contatto dell'organizzazione

I dati di contatto di Evicertia sono i seguenti:

- Sito web: https://www.uanataca.com.
- E-mail: info@evicertia.com.
- Telefono: +34914237080.
- Fax: +34911410144.
- Domicilio postale: c/ Lagasca, 95. 28006, Madrid.

1.5.3 Procedure di gestione del documento

Il sistema documentale e organizzativo di Evicertia garantisce, attraverso l'esistenza e l'applicazione di apposite procedure, la corretta conservazione del presente documento e delle relative specifiche di servizio.

2 Control de versione

Versione.	Data	Osservazioni
1.4	18/06/2024	• La prima versione di questo documento è approvata. È numerato come 1.4 per avere la stessa numerazione degli altri documenti linguistici.
1.5	11/11/2024	• I riferimenti alle ragioni sociali sono aggiornati a causa della fusione di Evicertia, S.L.U. in Uanataca, S.A.U. • Le informazioni relative alla protezione dei dati personali sono migliorate.

3 Pubblicazione e conservazione

3.1 Archivio

Evicertia dispone di un Archivio in cui vengono pubblicate le informazioni relative al servizio fiduciario. L'archivio delle pubblicazioni è consultabile all'indirizzo https://www.uanataca.com/.

Tale servizio è disponibile 24 ore su 24, 7 giorni su 7. In caso di guasto del sistema al di fuori del controllo di Evicertia, questa farà del suo meglio per rendere nuovamente disponibile il servizio in base alle tempistiche e alle procedure di continuità operativa stabilite.

3.2 Pubblicazione delle informazioni del fornitore di servizi di certificazione

Nel suo archivio, Evicertia pubblicherà le seguenti informazioni:

- La Dichiarazione delle Pratiche di Certificazione (DPC).
- La dichiarazione delle pratiche e la politica di ciascun profilo di certificati o di servizi fiduciari.
- Gli elenchi dei certificati revocati.
- Le dichiarazioni di divulgazione corrispondenti, di seguito "DD" (in inglese *Policy Disclosure Statements*).
- Le chiavi pubbliche dei certificati utilizzati per il recapito qualificato.
- Con carattere previo, e qualora sia possibile, qualsiasi informazione relativa ai partecipanti ai servizi di certificazione.

3.3 Frequenza di pubblicazione

Le informazioni dell'FSC, compresa la DPC, vengono pubblicate non appena disponibili.

Le modifiche alla DPC qualificata sono disciplinate dalle disposizioni della procedura di gestione del presente documento e ai sensi della normativa vigente.

3.4 Control de acceso

Evicertia non limita l'accesso in lettura alle informazioni stabilite nella sezione "Pubblicazione delle informazioni del fornitore di servizi di certificazione", ma mette in atto dei controlli per impedire a persone non autorizzate di aggiungere, modificare o cancellare i record dell'Archivio al fine di proteggere l'integrità e l'autenticità delle informazioni.

Per l'archivio, Evicertia utilizza sistemi affidabili in modo che:

- Le annotazioni e le modifiche possono essere effettuate solo da persone autorizzate.
- È possibile verificare l'autenticità delle informazioni.
- È possibile rilevare qualsiasi modifica tecnica che influisca sui requisiti di sicurezza.

4 Identificazione e autenticazione

Le informazioni sull'identificazione e l'autenticazione di ciascun profilo di certificati o di servizi fiduciari di Evicertia sono riportate nella relativa dichiarazione delle pratiche e nella politica di ciascun profilo di certificati o di servizi fiduciari.

5 Requisiti operativi

Le informazioni sui requisiti operativi sono riportate nella dichiarazione delle pratiche e nella politica di ciascun profilo di certificati o di servizi fiduciari.

6 Controlli di sicurezza fisica e gestione e controlli operativi

6.1 Controlli di sicurezza fisica

Evicertia ha stabilito dei controlli di sicurezza fisica e ambientale per proteggere le risorse degli impianti in cui si trovano i sistemi, i sistemi stessi e le apparecchiature utilizzate per le operazioni di fornitura dei servizi elettronici fiduciari.

In particolare, la politica di sicurezza di Evicertia applicabile ai servizi elettronici fiduciari stabilisce delle disposizioni su quanto segue:

- Controlli di accesso fisico.
- Protezione contro i disastri naturali.
- Misure di protezione antincendio.
- Guasto dei sistemi di supporto (alimentazione elettrica, telecomunicazioni, ecc.)
- Crollo della struttura.
- Alluvioni.
- Protezione antifurto.
- Rimozione non autorizzata di apparecchiature, informazioni, supporti e applicazioni relativi ai componenti utilizzati per i servizi del fornitore di servizi di certificazione.

Tali misure sono applicabili agli impianti da cui vengono erogati i servizi elettronici fiduciari, nei loro ambienti di produzione e di contingenza, che vengono controllati periodicamente ai sensi delle normative vigenti e delle apposite politiche di Evicertia.

Gli impianti sono dotati di sistemi di manutenzione preventiva e correttiva con assistenza h24/365 giorni all'anno, nonché nelle 24 ore successive alla notifica.

6.2 Ubicazione e costruzione degli impianti

La protezione fisica si ottiene creando, intorno ai servizi, dei perimetri di sicurezza delimitati in modo chiaro. La qualità e la resistenza dei materiali di costruzione degli impianti garantiscono livelli di protezione adeguati contro le intrusioni di forza bruta; inoltre, gli impianti sono situati in un'area a basso rischio di disastri che consente un accesso rapido.

La sala in cui vengono effettuate le operazioni crittografiche del Centro di Elaborazione Dati principale possiede un'infrastruttura ridondante e diverse fonti alternative di alimentazione e raffreddamento in caso di emergenza.

Evicertia è dotata di impianti che proteggono fisicamente l'erogazione dei servizi di approvazione delle richieste di certificati e di gestione delle revoche da compromissioni causate da accessi non autorizzati ai sistemi o ai dati, nonché dalla loro divulgazione.

6.2.1 Accesso fisico

Evicertia dispone di tre livelli di sicurezza fisica nel CED principale (ingresso all'Edificio in cui si trova, accesso alla sala del CED e accesso al Rack), con entrata dai livelli inferiori a quelli superiori.

L'accesso fisico ai locali di Evicertia dove si svolgono i processi di certificazione è limitato e protetto da una combinazione di misure fisiche e procedurali. Pertanto:

- l'accesso è limitato al personale espressamente autorizzato, con identificazione al momento dell'ingresso e relativa registrazione;
- l'accesso alle sale avviene tramite lettori di badge e/o serrature elettroniche gestiti da un sistema informatico che tiene un registro automatico degli ingressi e delle uscite;
- l'accesso alla sala dei processi crittografici richiede l'autorizzazione previa di Evicertia agli amministratori del servizio di *colocation*, che hanno la chiave per aprire la sala e la gabbia ma quella degli armadi.

6.2.2 Elettricità e aria condizionata

Gli impianti del CED principale di Evicertia dispongono di stabilizzatori di corrente e di un sistema di alimentazione elettrica per le apparecchiature duplicato con un gruppo elettrogeno.

Le sale che ospitano le apparecchiature informatiche sono dotate di sistemi di controllo della temperatura con impianti di aria condizionata.

6.2.3 Esposizione all'acqua

Gli impianti si trovano in un'area a basso rischio di inondazione. Le sale delle apparecchiature informatiche hanno un sistema di rilevamento dell'umidità.

6.2.4 Prevenzione e protezione antincendio

Gli impianti e gli asset del CED principale di Evicertia dispongono di sistemi automatici di rilevamento ed estinzione degli incendi.

6.2.5 Conservazione dei supporti

Solo il personale autorizzato ha accesso ai supporti di memorizzazione. Le informazioni con il più alto livello di classificazione sono conservate in una cassetta di sicurezza che si trova al di fuori degli impianti del Centro di Elaborazione Dati principale.

6.2.6 Trattamento dei residui

L'eliminazione dei supporti, sia cartacei che magnetici, avviene tramite meccanismi che garantiscono l'impossibilità di recuperare le informazioni.

Per quanto riguarda i supporti magnetici, possono essere eliminati, nel qual caso vengono distrutti fisicamente, oppure riutilizzati in seguito a cancellazione permanente o formattazione. Per quanto riguarda, invece, i documenti cartacei, possono essere eliminati mediante distruggidocumenti o gettati in appositi contenitori per la carta, per poi essere distrutti in maniera controllata.

6.2.7 Backup fuori sede

Per la custodia di documenti, dispositivi magnetici ed elettronici indipendenti dal Centro di Elaborazione Dati principale, Evicertia si avvale di un deposito sicuro fuori sede.

6.3 Controlli delle procedure

Evicertia assicura la gestione sicura dei propri sistemi; a tal fine, ha stabilito e applicato delle procedure per le funzioni riguardanti la fornitura dei suoi servizi.

Il personale di Evicertia svolge le procedure amministrative e gestionali in conformità alla politica di sicurezza.

6.3.1 Funzioni fiduciarie

Evicertia ha identificato, in base alla sua politica di sicurezza, le seguenti funzioni o ruoli considerati "di fiducia":

- **Amministratore di sistema:** è responsabile del corretto funzionamento dell'hardware e del software di supporto della piattaforma di certificazione
- **Revisore interno:** si occupa di garantire il rispetto delle procedure operative da parte degli appositi responsabili. Si tratta di una persona esterna al dipartimento dei Sistemi Informatici. I compiti del Revisore interno sono incompatibili nel tempo con le attività di certificazione e incompatibili con Sistemi. Tali funzioni saranno subordinate alla Direzione operativa, pertanto il Revisore interno riporterà sia a quest'ultima che alla Direzione tecnica.
- **Custode:** è responsabile della custodia delle carte crittografiche in cui viene memorizzata la chiave precondivisa secondo il modello di sicurezza n di m. Questa funzione è compatibile con il resto delle funzioni della presente DPC.
- **Addetto alla verifica dell'identità:** è responsabile di garantire i processi di verifica dell'identità dei sottoscrittori di alcuni servizi fiduciari di Evicertia, come ad esempio il recapito qualificato.
- **Operatore di sistema:** è il responsabile necessario, insieme all'Amministratore di sistema, del corretto funzionamento dell'hardware e del software di supporto della piattaforma di certificazione. L'Operatore di sistema è responsabile delle procedure di backup e di manutenzione delle operazioni quotidiane dei sistemi.
- **Proprietario del prodotto:** è responsabile del coordinamento, del controllo e della gestione dei team e dei deliverable degli sviluppi fiduciari di Evicertia. Si occupa delle attività di classificazione di errori e funzionalità ed è responsabile della relativa applicazione nei diversi ambienti.
- **Responsabile della sicurezza:** è responsabile del coordinamento, del controllo e dell'applicazione delle misure di sicurezza stabilite dalle politiche di sicurezza di Evicertia. Si occupa degli aspetti relativi alla sicurezza delle informazioni: logica, fisica, di rete, organizzativa, ecc.

Le persone che ricoprono le suddette posizioni sono soggette a specifiche procedure di indagine e verifica. Inoltre, nelle sue politiche Evicertia applica dei criteri di separazione delle funzioni come misura di prevenzione delle attività fraudolente.

6.3.2 Identificazione e autenticazione di ogni funzione

Le persone assegnate a ciascun ruolo sono individuate dal revisore interno, che si assicurerà che ognuna di queste svolga le operazioni per le quali è stata incaricata.

Ogni persona controlla soltanto i beni necessari al proprio ruolo: questo garantisce che nessuno abbia accesso a risorse non assegnate.

L'accesso alle risorse avviene, a seconda dell'asset, tramite nome utente/password, certificato digitale, carta d'accesso fisica e/o chiavi.

6.3.3 Ruoli che richiedono la separazione dei compiti

Le funzioni fiduciarie vengono stabilite in base al principio del privilegio minimo: questo garantisce una separazione dei compiti, facendo in modo che la persona che ricopre un determinato ruolo non abbia un controllo completo o particolarmente ampio di tutte le funzioni di certificazione, assicurando un controllo e una supervisione adeguati e limitando, così, eventuali comportamenti fraudolenti a livello interno.

La concessione del privilegio minimo per le funzioni fiduciarie verrà effettuata tenendo conto del migliore sviluppo dell'attività e sarà il più limitata possibile, considerando in ogni momento la struttura organizzativa di Evicertia.

6.4 Controlli sul personale

6.4.1 Requisiti di curriculum, qualifiche, esperienza e autorizzazione

Tutto il personale è qualificato e/o è stato formato adeguatamente per eseguire le operazioni che gli sono state assegnate.

Il personale in posizioni di fiducia non ha interessi personali che entrino in conflitto con lo svolgimento della funzione assegnatagli.

In generale, Evicertia rimuoverà un dipendente da una posizione di fiducia qualora venga a conoscenza di un conflitto di interessi e/o della commissione di un reato che potrebbe influire sullo svolgimento delle sue funzioni.

Evicertia non assegnerà un incarico fiduciario o dirigenziale a una persona non adatta al ruolo, soprattutto nel caso in cui questa abbia commesso un'infrazione che ne pregiudichi l'idoneità alla posizione. Pertanto, viene effettuata un'indagine preventiva, ai sensi della legislazione applicabile, riguardo ai seguenti aspetti:

- Studi, compresi i titoli professionali presentati.
- Lavori realizzati in precedenza, fino a cinque anni prima, comprese le referenze professionali.

- Referenze professionali.

6.4.2 Procedure di indagine del curriculum

Prima di assumere una persona o prima che questa ricopra una posizione lavorativa, Evicertia effettua i seguenti controlli:

- Referenze dei lavori degli ultimi anni
- Referenze professionali
- Studi, compresi i titoli professionali presentati.

Per svolgere tale indagine preventiva, Evicertia deve ottenere il consenso inequivocabile dell'interessato, nonché trattare e proteggere tutti i suoi dati personali nel rispetto della normativa vigente in materia di protezione dei dati personali, ai sensi del Regolamento Generale sulla Protezione dei Dati 2016/679 del Parlamento europeo e del Consiglio e, in generale, di qualunque normativa nazionale eventualmente applicabile.

Tutti i controlli vengono effettuati nei limiti consentiti dalla legislazione vigente. I motivi che possono portare al rifiuto del candidato per una posizione fiduciaria sono i seguenti:

- False dichiarazioni effettuate dal candidato nella sua domanda di lavoro.
- Referenze professionali molto negative o inaffidabili nei confronti del candidato.

6.4.3 Requisiti di formazione

Evicertia forma il personale in posizioni fiduciarie e dirigenziali fino al raggiungimento delle qualifiche necessarie, conservando le registrazioni di tale formazione.

I programmi di formazione vengono controllati e aggiornati periodicamente.

La formazione comprende, almeno, i seguenti contenuti:

- Compiti che deve svolgere la persona.
- Politiche e procedure di sicurezza di Evicertia. Uso e funzionamento di apparecchiature e applicazioni installate.
- Gestione di incidenti e impegni in materia di sicurezza.
- Procedure di continuità operativa e di emergenza.
- Procedura di gestione e sicurezza in relazione al trattamento dei dati personali.

6.4.4 Requisiti e frequenza di aggiornamento della formazione

Evicertia aggiorna la formazione del personale in base alle esigenze e con una frequenza sufficiente a consentirgli di svolgere le proprie funzioni in modo competente e soddisfacente, soprattutto in caso di modifiche sostanziali ai compiti di certificazione.

6.4.5 Sequenza e frequenza della rotazione dei lavori

N.D.

6.4.6 Sanzioni per azioni non autorizzate

Evicertia dispone di un sistema sanzionatorio per appurare le responsabilità derivanti da azioni non autorizzate, ai sensi della legislazione del lavoro applicabile.

Le misure disciplinari includono la sospensione, l'allontanamento dalle funzioni e anche il licenziamento del responsabile dell'iniziativa dannosa, in base alla gravità dell'azione non autorizzata.

6.4.7 Sanzioni per azioni non autorizzate

I dipendenti assunti per svolgere mansioni di fiducia sottoscrivono preventivamente le clausole di riservatezza e i requisiti operativi utilizzati da Evicertia. Qualsiasi azione che comprometta la sicurezza dei processi accettati potrebbe, una volta valutata, comportare la risoluzione del contratto di lavoro.

Nel caso in cui tutti o parte dei servizi di certificazione siano gestiti da un soggetto terzo, i controlli e le disposizioni della presente sezione o di altre sezioni della Dichiarazione delle Pratiche di Certificazione dovranno essere applicati e rispettati dal soggetto terzo che svolge le funzioni di gestione dei servizi di certificazione. Ciò nonostante, il Fornitore dei Servizi Fiduciari sarà in ogni caso responsabile dell'effettiva esecuzione dei suddetti controlli e disposizioni. Questi aspetti vengono specificati nello strumento giuridico utilizzato per concordare la prestazione dei servizi di certificazione da parte di un soggetto terzo diverso da Evicertia.

6.4.8 Fornitura di documentazione al personale

Il fornitore di servizi di certificazione consegnerà sempre la documentazione strettamente necessaria al proprio personale, al fine di consentirgli di svolgere il proprio lavoro in modo competente e soddisfacente.

6.5 Procedure di audit di sicurezza

6.5.1 Tipi di eventi registrati

Evicertia produce e conserva i dati almeno dei seguenti eventi relativi alla sicurezza dell'ente:

- Accensione e spegnimento del sistema.
- Tentativi di creazione, cancellazione, impostazione di password o di modifica di privilegi.
- Tentativi di login e logout.
- Tentativi di accesso non autorizzato ai sistemi di supporto dei servizi fiduciari in rete.
- Tentativi di accesso non autorizzato al file system.
- Accesso fisico ai log.
- Modifiche alla configurazione e alla manutenzione del sistema.
- Registrazioni delle applicazioni.
- Attivazione e disattivazione delle applicazioni dei servizi fiduciari.
- Modifiche ai dettagli dei servizi fiduciari e/o alle loro chiavi.
- Registrazioni della distruzione dei supporti contenenti le chiavi e i dati di attivazione.

- Eventi relativi al ciclo di vita del modulo crittografico, come la ricezione, l'utilizzo e la disinstallazione dello stesso.
- Sessione di generazione delle chiavi e database di gestione delle chiavi.
- Registrazioni di accesso fisico.
- Manutenzioni e modifiche alla configurazione del sistema.
- Cambiamenti nel personale.
- Rapporti sugli impegni e sulle discrepanze.
- Registrazioni della distruzione di materiale contenente informazioni di chiavi, dati di attivazione o informazioni personali del sottoscrittore, in caso di certificati individuali, o della persona fisica identificata nel certificato, in caso di certificati dell'organizzazione.
- Rapporti completi sui tentativi di intrusione fisica nelle infrastrutture di supporto del servizio.
- Eventi relativi alla sincronizzazione e alla ricalibrazione dell'orologio.

Le voci di registro includono i seguenti elementi:

- Data e ora della voce.
- Numero di serie o sequenza della voce, nei log automatici.
- Identità dell'ente che inserisce il log.
- Tipo di voce.

6.5.2 Frequenza di elaborazione dei registri di audit

Evicertia esamina i suoi log quando si verifica un allarme di sistema provocato dall'esistenza di un imprevisto.

L'elaborazione dei registri di audit consiste in una revisione degli stessi che include la verifica dell'assenza di manomissioni, una breve ispezione di tutte le voci di registro e un'indagine più profonda di eventuali avvisi o irregolarità nei registri. Le azioni intraprese a partire dalla revisione di audit sono documentate.

Evicertia mantiene un sistema che garantisce:

- Spazio sufficiente per la memorizzazione dei log.
- Impossibilità di riscrittura dei file di log.
- Le informazioni salvate comprendono almeno: tipo di evento, data e ora, utente che esegue l'evento e risultato dell'operazione.
- I file di log devono essere memorizzati in file strutturati che possono essere inseriti in un database per la successiva analisi.

6.5.3 Periodo di conservazione dei registri di audit

Evicertia conserva le informazioni dei log per un periodo compreso tra 1 e 15 anni, a seconda del tipo di informazioni registrate.

6.5.4 Protezione dei registri di audit

I file di registro di audit sono protetti da controlli fisici e logici contro l'accesso, la lettura, la modifica e l'eliminazione non autorizzati.

L'accesso ai file di log è riservato solo alle persone autorizzate. Esiste una procedura interna che illustra i processi per la gestione dei dispositivi contenenti dati di log di audit.

6.5.5 Procedure di backup

Evicertia dispone di un'adeguata procedura di backup che, in caso di perdita o distruzione di file rilevanti, rende disponibili le copie di backup dei log corrispondenti entro un breve periodo di tempo.

6.5.6 Posizione del sistema di accumulo dei registri di audit

Le informazioni relative agli audit degli eventi vengono raccolte internamente e in modo automatizzato dal sistema operativo, dalle comunicazioni di rete e dal software dei servizi fiduciari, oltre che dai dati generati manualmente, che verranno archiviati da personale debitamente autorizzato. Tutto questo costituisce il sistema di accumulo dei registri di audit.

6.5.7 Notifica dell'evento di audit al responsabile dell'evento

Quando il sistema di accumulo dei log di audit registra un evento, non è necessario inviare una notifica alla persona, all'organizzazione, al dispositivo o all'applicazione che ha causato l'evento.

6.5.8 Analisi delle vulnerabilità

L'analisi delle vulnerabilità è coperta dai processi di audit di Evicertia.

Le analisi di vulnerabilità devono essere eseguite, ripassate e controllate attraverso l'esame di questi eventi monitorati. Queste analisi devono essere effettuate periodicamente secondo l'apposita procedura interna.

I dati di audit dei sistemi vengono archiviati per essere utilizzati nelle indagini di eventuali criticità e per individuare le vulnerabilità.

6.6 Archivi informativi

6.6.1 Periodo di conservazione dei registri

Evicertia archivia i registri specificati precedentemente per almeno 15 anni, o per il periodo stabilito dalla legislazione vigente.

Ai sensi della normativa applicabile, il file informativo sarà disponibile per l'eventuale consultazione di un revisore qualificato.

6.6.2 Protezione del file

Evicertia protegge il file in modo da consentirne l'accesso esclusivo a persone debitamente autorizzate. Il file è protetto contro la visualizzazione, la modifica, l'eliminazione o qualsiasi altra manomissione mediante salvataggio su un sistema affidabile.

Evicertia assicura la corretta protezione dei file assegnandone l'elaborazione e la conservazione a personale qualificato in strutture sicure fuori sede.

6.6.3 Procedure di backup

Evicertia dispone di un centro di archiviazione esterno al CED principale per garantire la disponibilità di copie dell'archivio dei file. I documenti fisici sono conservati in luoghi sicuri con accesso limitato al solo personale autorizzato.

Evicertia effettua, almeno quotidianamente, delle copie di backup di tutti i suoi documenti elettronici ai fini del recupero dati.

6.6.4 Requisiti per la marcatura di data e ora

I registri sono datati con una fonte affidabile tramite NTP. Per queste informazioni, non è necessaria la firma digitale.

6.6.5 Posizione del sistema di archiviazione

Evicertia dispone di un sistema centralizzato per la raccolta di informazioni sull'attività dei team coinvolti nel servizio di gestione dei certificati.

6.6.6 Procedure di conseguimento e verifica delle informazioni d'archivio

Evicertia dispone di una procedura che descrive il processo di verifica della correttezza e dell'accessibilità delle informazioni archiviate. Evicertia fornisce le informazioni e i mezzi di verifica al revisore.

6.7 Rinnovo delle chiavi

Le chiavi e i certificati dei servizi fiduciari sono associati in modo univoco al sistema che fornisce tale servizio. Prima dell'utilizzo delle chiavi private dei servizi fiduciari, verrà effettuata la modifica delle chiavi o la revoca di quelle attuali.

6.8 Compromissione delle chiavi e ripristino di emergenza

6.8.1 Procedure di gestione di criticità e compromissioni

Evicertia ha sviluppato delle politiche di sicurezza e di continuità operativa che le consentono di gestire e recuperare i sistemi in caso di incidenti e di compromissione delle proprie attività.

6.8.2 Corruzione di risorse, dati o applicazioni

Quando si verifica un evento di corruzione di risorse, dati o applicazioni, verranno seguite le procedure di gestione opportune in conformità alle politiche di sicurezza e di gestione degli imprevisti di Evicertia, che comprendono miglioramento, indagine e risposta all'incidente. Se necessario, verranno avviate le procedure di compromissione delle chiavi o di ripristino di emergenza di Evicertia.

6.8.3 Compromissione delle chiavi private dell'ente

In caso di sospetto o conoscenza di compromissione da parte di Evicertia, verranno attivate, in base alle politiche di sicurezza, gestione degli imprevisti e continuità operativa, le procedure di compromissione delle chiavi che consentano il ripristino dei sistemi critici, se necessario in un centro dati alternativo.

6.8.4 Continuità operativa dopo un'emergenza

Evicertia ristabilirà i servizi critici in conformità con il piano di imprevisti e continuità operativa esistente, ripristinando il normale funzionamento dei servizi precedenti entro 24 ore dal verificarsi dell'emergenza.

6.9 Termine del servizio

Evicertia garantisce che le eventuali interruzioni per i sottoscrittori dei servizi e i soggetti terzi sono minime, come conseguenza della cessazione dei servizi del fornitore di servizi di certificazione. In questo senso, Evicertia garantisce il mantenimento continuo dei registri definiti e per il tempo stabilito in conformità alla presente Dichiarazione delle Pratiche di Certificazione.

Fermo restando quanto sopra, Evicertia intraprenderà, se del caso, tutte le azioni necessarie per trasferire a terzi o a un deposito notarile gli obblighi di conservazione dei registri specificati per il periodo di tempo indicato nella presente Dichiarazione delle Pratiche di Certificazione o ai sensi della disposizione di legge applicabile.

Prima di terminare i propri servizi, Evicertia elabora un piano di conclusione, con le seguenti disposizioni:

- Fornirà i fondi necessari, compresa un'assicurazione di responsabilità civile, per portare avanti la fine delle attività di revoca.
- Informerà della cessazione tutti i Sottoscrittori del servizio, il Soggetto Terzo fiduciario e, in generale, qualunque soggetto terzo con cui abbia accordi o altri tipi di rapporti con almeno 2 mesi di anticipo.
- Trasferirà ai sottoscrittori e agli utenti i propri obblighi relativi al mantenimento delle informazioni del registro e dei log per il periodo di tempo indicato.
- Distruggerà le chiavi private responsabili dei servizi fiduciari o ne disabiliterà l'utilizzo.
- Eseguirà i compiti necessari per trasferire gli obblighi di mantenimento delle informazioni di registro e dei file di log degli eventi per i rispettivi periodi di tempo.

- Comunicherà la cessazione dell'attività all'Organismo di Vigilanza spagnolo competente con almeno 2 mesi di anticipo.
- Inoltre, notificherà allo stesso l'avvio di eventuali procedure fallimentari nei confronti di Evicertia, nonché ogni altra circostanza rilevante che possa impedire la prosecuzione dell'attività.

7 Controlli di sicurezza tecnica

Evicertia utilizza sistemi e prodotti affidabili, protetti da qualunque tipo di alterazione e che garantiscono la sicurezza tecnica e crittografica dei processi di certificazione supportati.

7.1 Generazione e installazione della coppia di chiavi

Le informazioni sulla generazione e installazione della coppia di chiavi di ciascun profilo di certificati o dei servizi fiduciari di Evicertia sono riportate nella relativa dichiarazione delle pratiche e nella politica di ciascun profilo di certificati o di servizi fiduciari.

7.2 Protezione delle chiavi private

7.2.1 Standard dei moduli crittografici

I moduli di gestione delle chiavi di Evicertia sono conformi alla certificazione *Common Criteria EAL4+* o equivalente.

7.2.2 Controllo delle chiavi private

La gestione dell'accesso alle chiavi private dei certificati dei servizi fiduciari avviene in base ai controlli stabiliti dall'HSM (modulo di sicurezza hardware) in cui sono conservate. Inoltre, i dispositivi crittografici sono protetti fisicamente come stabilito nel presente documento.

7.2.3 Backup delle chiavi private

Evicertia effettua delle copie di sicurezza delle chiavi private dei certificati, in modo da poterle recuperare in caso di disastro, perdita o deterioramento. Sia la generazione della copia che il suo recupero richiedono la partecipazione di almeno due persone.

Questi file di recupero vengono conservati in armadi ignifughi e in un deposito alternativo.

7.2.4 Inserimento delle chiavi private nel modulo crittografico

Le chiavi private sono generate direttamente nei moduli crittografici di produzione di Evicertia, dove vengono memorizzate in forma criptata.

7.2.5 Metodo di attivazione delle chiavi private

Le chiavi private di Evicertia vengono attivate mediante l'esecuzione della corrispondente procedura di avvio sicuro del modulo crittografico.

7.2.6 Metodo della disattivazione delle chiavi private

Per la disattivazione delle chiavi private di Evicertia, bisognerà seguire i passaggi descritti nel manuale dell'amministratore dell'apparecchiatura crittografica corrispondente.

7.2.7 Metodo di distruzione delle chiavi private

Per la distruzione delle chiavi private, verranno seguiti i passaggi descritti nel manuale dell'amministratore dell'apparecchiatura crittografica in questione.

Prima della distruzione delle chiavi, verrà emessa una revoca del certificato delle chiavi pubbliche ad esse associate.

- I dispositivi contenenti una qualsiasi parte delle chiavi private di Evicertia saranno distrutti fisicamente o resettati a basso livello. Per il reset, verranno seguiti i passaggi descritti nel manuale dell'amministratore dell'apparecchiatura crittografica.
- Infine, i backup saranno distrutti in modo sicuro.

7.3 Controlli di sicurezza informatica

Evicertia utilizza dei sistemi affidabili per offrire i suoi servizi di certificazione. Per questo, ha effettuato controlli e audit informatici al fine di stabilire una gestione adeguata del proprio patrimonio informatico con il livello di sicurezza richiesto nella gestione dei sistemi di certificazione elettronica.

Per quanto riguarda la sicurezza delle informazioni, Evicertia applica i controlli dello schema di certificazione sui sistemi di gestione delle informazioni ISO 27001.

Inizialmente, le apparecchiature utilizzate vengono configurate con i profili di sicurezza adeguati dal personale sistemistico di Evicertia, nei seguenti aspetti:

- Configurazione di sicurezza del sistema operativo.
- Configurazione di sicurezza delle applicazioni.
- Dimensionamento corretto del sistema.
- Configurazione di Utenti e autorizzazioni.
- Configurazione degli eventi di Log.
- Piano di backup e ripristino.
- Requisiti del traffico di rete.

Le funzionalità esposte sono realizzate attraverso una combinazione di sistema operativo, software di PKI, protezione fisica e procedure.

7.4 Controlli tecnici del ciclo di vita

7.4.1 Controlli di sviluppo dei sistemi

Le applicazioni sono sviluppate e implementate da Evicertia in conformità agli standard di sviluppo e controllo delle modifiche.

Le applicazioni dispongono di metodi per la verifica dell'integrità e dell'autenticità, nonché della correttezza della versione da utilizzare.

7.4.2 Controlli di gestione della sicurezza

Evicertia svolge delle attività specifiche di formazione e sensibilizzazione dei dipendenti in materia di sicurezza. I materiali di formazione e i documenti di descrizione dei processi vengono aggiornati dopo la relativa approvazione da parte di un gruppo di gestione della sicurezza. Per questa funzione, è disponibile un piano di formazione annuale.

Evicertia richiede delle misure di sicurezza equivalenti da parte di qualsiasi fornitore esterno coinvolto in attività di servizi elettronici fiduciari.

7.4.2.1 Classificazione e gestione delle informazioni e degli asset

Evicertia mantiene un inventario degli asset e della documentazione e una procedura per la gestione di questo materiale per garantirne l'utilizzo.

La politica di sicurezza di Evicertia descrive in dettaglio le procedure di gestione delle informazioni, che vengono classificate in base al livello di riservatezza.

I documenti sono catalogati in tre livelli: PUBBLICO, USO INTERNO e RISERVATO.

7.4.2.2 Operazioni di gestione

Evicertia dispone di un'adeguata procedura di gestione delle criticità e di risposta mediante l'implementazione di un sistema di allerta e la generazione di rapporti periodici.

Il documento sulla sicurezza di Evicertia illustra in dettaglio il processo di gestione delle criticità.

Evicertia ha documentato tutte le procedure relative alle funzioni e alle responsabilità del personale coinvolto nel controllo e nella gestione degli elementi contenuti nel processo di certificazione.

7.4.2.3 Trattamento dei supporti e sicurezza

Tutti i supporti vengono trattati in modo sicuro nel rispetto dei requisiti di classificazione delle informazioni. Se non sono più necessari, i supporti contenenti dati sensibili vengono distrutti in modo sicuro.

7.4.2.4 Pianificazione del sistema

Il servizio clienti di Evicertia mantiene un registro delle capacità delle apparecchiature. Insieme all'applicazione di controllo delle risorse di ciascun sistema, è possibile prevedere un ridimensionamento.

7.4.2.5 Rapporti delle criticità e risposta

Evicertia dispone di una procedura di monitoraggio delle criticità e della loro risoluzione in cui vengono registrate le risposte e di una valutazione del processo di risoluzione della criticità.

7.4.2.6 Procedure operative e responsabilità

Evicertia definisce le attività assegnate a persone con un ruolo di fiducia in modo diverso rispetto alle attività assegnate a persone che non hanno quel ruolo, che non sono quindi riservate.

7.4.2.7 Gestione del sistema di accesso

Evicertia compie ogni ragionevole sforzo per confermare che l'accesso al sistema sia limitato esclusivamente alle persone autorizzate.

In particolare:

- Sono disponibili dei controlli basati su firewall ad alta disponibilità.
- I dati sensibili sono protetti da tecniche crittografiche o da controlli di accesso con autenticazione forte.
- Evicertia ha una procedura documentata di gestione di registrazioni e cancellazioni degli utenti e di politica di accesso che è dettagliata nella sua politica di sicurezza.
- Evicertia dispone di procedure per garantire che le operazioni siano effettuate nel rispetto della politica dei ruoli.
- Ogni persona ha un ruolo associato per eseguire le operazioni di certificazione.
- Il personale di Evicertia è responsabile delle proprie azioni mediante l'impegno di riservatezza sottoscritto con l'azienda.

7.4.2.8 Gestione del ciclo di vita dell'hardware crittografico

Evicertia garantisce che l'hardware crittografico utilizzato per la firma di certificati o servizi fiduciari non venga manomesso durante il trasporto, ispezionando il materiale consegnato.

In particolare:

- L'hardware crittografico viene trasportato su supporti predisposti per evitare qualsiasi manomissione.
- Evicertia registra tutte le informazioni rilevanti del dispositivo da aggiungere al catalogo degli asset.
- L'uso dell'hardware crittografico richiede almeno due dipendenti di fiducia.
- Evicertia esegue dei test periodici per garantire il corretto funzionamento del dispositivo.
- Il dispositivo hardware crittografico viene maneggiato solo da personale fidato.
- Le chiavi private dei certificati di Evicertia memorizzate nell'hardware crittografico saranno cancellate una volta rimosso il dispositivo.
- La configurazione, le modifiche e gli aggiornamenti del sistema di Evicertia sono documentati e controllati.
- Le modifiche o gli aggiornamenti sono autorizzati dal responsabile della sicurezza e vengono riportati nei verbali di lavoro corrispondenti. Queste configurazioni verranno effettuate da almeno due persone di fiducia.

7.5 Controlli di sicurezza della rete

Evicertia protegge l'accesso fisico ai dispositivi di gestione della rete ed è dotata di un'architettura che ordina il traffico generato in base alle sue caratteristiche di sicurezza, creando delle sezioni di rete chiaramente definite. Tale suddivisione avviene mediante l'utilizzo di firewall.

Le informazioni sensibili trasferite su reti non protette vengono crittografate mediante l'uso di protocolli TLS o di VPN con autenticazione a due fattori.

7.6 Controlli ingegneristici dei moduli crittografici

I moduli crittografici sono soggetti ai controlli ingegneristici previsti dalle norme indicate in questa sezione.

Gli algoritmi di generazione delle chiavi impiegati sono comunemente accettati per l'utilizzo della chiave a cui sono destinati.

Tutte le operazioni crittografiche di Evicertia vengono eseguite su moduli certificati *Common Criteria 4 EAL+* o equivalenti.

7.7 Fonti di Tempo

Tutti i dispositivi utilizzati da Evicertia sono sincronizzati tramite NTP (*Network Time Protocol*) su Internet (*RFC 1305 Network Time Protocol*), utilizzando uno dei seguenti server *NTP stratum 1*, come il Real Osservatorio della Marina spagnola (ROE), RedIris o i pool di server temporali del progetto NTP (http://www.ntp.org/).

8 Profili e revoca dei certificati

Le informazioni sui profili dei certificati emessi o utilizzati da Evicertia sono riportate nella corrispondente dichiarazione delle pratiche e nella politica di ciascun profilo di certificati o di servizi fiduciari.

9 Audit di conformità

Evicertia ha comunicato l'inizio della sua attività di fornitore di servizi di certificazione mediante l'Organismo di Vigilanza spagnolo, ed è soggetta alle verifiche di controllo ritenute necessarie da tale organismo.

9.1 Frequenza dell'audit di conformità

Evicertia conduce un audit di conformità con cadenza annuale, oltre agli audit interni che effettua a propria discrezione o in qualsiasi momento in caso di sospetta violazione di una misura di sicurezza.

9.2 Identificazione e qualifica del revisore

Gli audit vengono eseguiti da una società di revisione esterna indipendente che dimostri competenza tecnica ed esperienza in materia di sicurezza informatica, sicurezza dei sistemi informativi, audit di conformità dei servizi di certificazione a chiave pubblica ed elementi correlati.

9.2.1 Rapporto del revisore con l'ente sottoposto a audit

Le società di revisione sono di riconosciuto prestigio e dispongono di dipartimenti specializzati nell'esecuzione di audit informatici, pertanto non esiste alcun conflitto di interessi che possa alterarne le prestazioni nei confronti di Evicertia.

9.3 Elenco degli elementi da sottoporre ad audit

Per quanto riguarda Evicertia, l'audit verifica:

- Che l'ente disponga di un sistema di gestione a garanzia della qualità del servizio fornito.
- Che l'ente sia conforme ai requisiti della Dichiarazione delle Pratiche di Certificazione e a quelli di ulteriori documenti relativi all'emissione dei diversi certificati digitali.
- Che la Dichiarazione delle Pratiche di Certificazione e l'ulteriore documentazione legale correlata siano conformi a quanto concordato da Evicertia e a quanto stabilito dalla normativa vigente.
- Che l'ente gestisca adeguatamente i propri sistemi informativi

9.4 Azioni da intraprendere a seguito di un difetto di conformità

Una volta ricevuto il rapporto dell'audit di conformità, la direzione analizza, insieme alla società di revisione, le carenze riscontrate, sviluppando e mettendo in atto delle misure correttive per la risoluzione di tali carenze.

Qualora Evicertia non sia in grado di sviluppare e/o eseguire delle misure correttive o le carenze riscontrate rappresentino una minaccia immediata alla sicurezza o all'integrità del sistema, ne darà immediata comunicazione al proprio Comitato Direttivo, che potrà intraprendere le seguenti azioni:

- Cessare temporaneamente le operazioni.
- Chiedere la revoca delle chiavi dei certificati dei servizi fiduciari e ripristinare l'infrastruttura.
- Terminare il servizio fiduciario interessato.
- Altre azioni complementari eventualmente necessarie.

9.5 Trattamento dei rapporti di audit

I rapporti sui risultati dell'audit vengono consegnati al Comitato Direttivo di Evicertia entro il termine massimo di 15 giorni dall'esecuzione dell'audit.

10 Requisiti commerciali e legali

10.1 Tariffe

10.1.1 Tariffa dei servizi fiduciari

Evicertia può stabilire una tariffa per l'utilizzo dei propri servizi fiduciari che, se del caso, comunicherà tempestivamente ai sottoscrittori.

10.1.2 Politica di rimborso

Nessuna clausola.

10.2 Capacità finanziaria

Evicertia dispone di risorse economiche sufficienti per mantenere le proprie attività e adempiere ai propri obblighi, nonché per far fronte al rischio di responsabilità per danni, come previsto dalla norma ETSI EN 319 401-1 7.12 c), in relazione alla gestione della conclusione dei servizi e del piano di cessazione.

10.2.1 Copertura assicurativa

Evicertia dispone di una sufficiente garanzia di copertura per la propria responsabilità civile attraverso un'assicurazione di responsabilità civile professionale, che mantiene ai sensi della normativa vigente.

10.2.2 Altri asset

Nessuna clausola.

10.2.3 Copertura assicurativa per sottoscrittori e soggetti terzi che si affidano ai servizi fiduciari

Evicertia dispone di una sufficiente garanzia di copertura per la propria responsabilità civile attraverso un'assicurazione di responsabilità civile professionale, per i servizi elettronici fiduciari, con un importo minimo assicurato di 3.000.000 €.

10.3 Riservatezza

10.3.1 Informazioni riservate

Evicertia mantiene riservate le seguenti informazioni:

- Le richieste di servizio, così come qualsiasi altra informazione personale ottenuta per la fornitura del servizio stesso, a eccezione delle informazioni indicate nella sezione seguente.
- Registri delle transazioni, compresi i registri completi e quelli degli audit delle transazioni.
- Registri di audit interni ed esterni

- Piani di continuità operativa e di emergenza.
- Piani di sicurezza.
- Documentazione delle operazioni, archiviazione, monitoraggio e simili.
- Tutte le altre informazioni identificate come “Riservate”.

10.3.2 Divulgazione legale delle informazioni

Evicertia non divulgherà le informazioni riservate se non nei casi previsti dalla legge.

10.4 Protezione dei dati personali

Evicertia garantisce il rispetto della normativa vigente in materia di protezione dei dati personali, ai sensi del Regolamento Generale sulla Protezione dei Dati 2016/679 del Parlamento europeo e del Consiglio e, in generale, di qualunque normativa nazionale eventualmente applicabile.

In conformità a ciò, Evicertia ha documentato nella presente Dichiarazione delle Pratiche di Certificazione gli aspetti e le procedure di sicurezza e organizzative, al fine di garantire che tutti i dati personali a cui ha accesso siano protetti contro la perdita, la distruzione, il danneggiamento, la falsificazione e il trattamento illecito o non autorizzato.

Di seguito, sono riportate tutte le informazioni necessarie sul trattamento dei dati personali effettuato da Evicertia:

10.4.1 Responsabile del trattamento

Il responsabile del trattamento dei dati personali sarà:

- Uanataca, S.A.U. (Evicertia).
- P. IVA: ESA66721499.
- Indirizzo: Avenida Meridiana no. 350, terza planata, 08027 Barcellona.
- Registro delle Imprese di Barcellona Tomo 45264, Libro 0, Foglio 6, Sezione General, Pagina 482242, Iscrizione 1ª.

10.4.2 Dati di contatto dell’organizzazione

I dati di contatto del responsabile della protezione dei dati sono:

- https://support.evicertia.com (principale).
- E-mail: support+gdpr@evicertia.com.
- Domicilio postale: c/ Lagasca, 95. 28006, Madrid. SPAGNA.
- Telefono: 914237080.
- Fax: 911410144.

10.4.3 Finalità del trattamento

Evicertia ha il dovere di informare gli utenti che tutti i dati personali forniti vengono trattati per le seguenti finalità:

- **Fornitura dei Servizi Elettronici Fiduciari.** I dati vengono raccolti mediante apposito contratto ed elaborati allo scopo di eseguire i servizi elettronici richiesti e sottoscritti dagli utenti, il tutto sulla base di quanto previsto dalla presente Dichiarazione delle Pratiche di Certificazione.
    - Certificazione dei processi di comunicazione, tra cui (i) la certificazione del contenuto comunicato (che può includere dati personali) mediante meccanismi di controllo dell'integrità crittografica, (ii) la certificazione degli indirizzi o dei numeri di telefono del mittente e del destinatario e (iii) la certificazione del processo di consegna e/o apertura.
    - Certificazione dei processi di consenso: servizi per la visualizzazione sicura dei contenuti (che possono includere dati personali) e/o la firma dei contenuti mediante un meccanismo di identificazione e autenticazione.
    - Custodia delle prove: (i) conservazione a lungo termine dei contenuti e delle prove relative ai processi di certificazione (dichiarazioni giurate e cronologia degli eventi) e (ii) fornitura di servizi di ricerca e interrogazione, compresa la possibilità di effettuare ricerche in base all'indirizzo del destinatario o del firmatario (ove applicabile).
    - In questo caso, Evicertia agisce in qualità di responsabile del trattamento, mentre il Titolare del trattamento è il soggetto che invia la comunicazione. Lo scopo è la gestione delle comunicazioni inviate ad esso.
- **Supporto alla prestazione dei servizi.** Mantenimento dei dati di contatto per facilitare la gestione delle richieste e delle criticità inerenti alla fornitura dei Servizi. Ad esempio, il CLIENTE, o l'Utente direttamente, può fornire i propri dati di contatto per cercare di risolvere una criticità relativa ai problemi con i servizi offerti da Evicertia.
- **Rapporto commerciale.** Mantenimento dei dati di contatto dei dipendenti del CLIENTE per facilitare la gestione commerciale, la fatturazione, il monitoraggio e la gestione dei Servizi.

Evicertia informa che i dati personali forniti saranno trattati solo ed esclusivamente in modalità compatibile con le finalità sopra descritte.

10.4.4 Legittimazione del trattamento

In conformità alle finalità di trattamento indicate, la base giuridica per il trattamento dei dati personali degli utenti è:

- La legittimità del trattamento per la Fornitura dei Servizi Elettronici Fiduciari è l'esecuzione del contratto per i servizi richiesti, in cui l'utente, che ne è parte integrante, presta espressamente e inequivocabilmente il consenso mediante azione positiva e previa all'uso del servizio, con l'accettazione delle condizioni.
- La legittimità del trattamento per occuparsi delle domande e richieste si basa sul legittimo interesse, ad esempio per rispondere al destinatario di una comunicazione o convalidare un documento firmato derivante dalla fornitura di servizi.

Il consenso al trattamento può essere revocato in qualsiasi momento inviando una richiesta a https://support.evicertia.com o un'e-mail all'indirizzo di posta elettronica specificato nella sezione Dati di contatto dell'organizzazione.

L'utente garantisce che i dati forniti sono veri, esatti, completi e aggiornati ed è responsabile di qualsiasi danno diretto o indiretto eventualmente derivante dall'inosservanza di tale obbligo.

10.4.5 Dati trattati e conservazione

Le categorie di dati personali trattati da Evicertia comprendono, a titolo esemplificativo ma non esaustivo, i dati identificativi (nome, cognome e dati d'identità), i dati di contatto (indirizzo postale, e-mail e numero di telefono) e alcuni dati aggiuntivi come l'indirizzo IP, dati del browser e dati di tracciabilità.

I dati personali saranno conservati per tutto il tempo necessario alla risposta di domande e richieste, fino al termine del rapporto contrattuale e, successivamente, per i periodi di tempo legalmente richiesti a seconda dei casi, come definito nella presente Dichiarazione delle Pratiche di Certificazione. In caso di imperativo legale, i dati personali rimarranno bloccati e a esclusiva disposizione di giudici e tribunali per i periodi di tempo stabiliti dalla legge.

10.4.6 Cessione e trasferimento internazionale dei dati

I dati personali non vengono divulgati o ceduti a terzi, salvo:

- Obbligo legale
- Interesse legittimo nei confronti dei dati, come nel caso del destinatario delle comunicazioni o dei firmatari dei documenti, oggetto dei Servizi Elettronici Fiduciari, contenenti tali dati
- Per ottemperare alla richiesta di un'autorità giudiziaria o di qualsiasi autorità amministrativa competente che lo richieda
- Termine dei servizi

Non verranno effettuati trasferimenti internazionali al di fuori dell'Unione europea o dello Spazio Economico Europeo (SEE).

10.4.7 Diritti degli utenti

- **Conferma.** Tutti gli utenti hanno diritto a ottenere la conferma che Evicertia stia trattando dati personali che li riguardano.
- **Accesso e rettifica.** Gli utenti hanno il diritto di accedere a tutti i loro dati personali, nonché di richiedere la rettifica di eventuali dati errati o inesatti.
- Cancellazione o annullamento. Gli utenti potranno richiedere la cancellazione o l'annullamento dei dati personali qualora, tra gli altri motivi, questi non siano più necessari alle finalità per cui sono stati raccolti.
- **Limitazione e opposizione.** L'utente potrà richiedere la limitazione del trattamento per evitare l'applicazione dei suoi dati personali alle operazioni corrispondenti. In determinate circostanze e per motivi legati alla sua situazione particolare, l'utente potrà opporsi al

trattamento dei dati; pertanto, Evicertia sarà obbligata, salvo in caso di motivi legittimi impellenti o di esercizio o difesa di eventuali reclami, a interromperne il trattamento.

- **Portabilità.** Gli interessati potranno chiedere la ricezione dei propri dati personali o l'invio degli stessi a un altro responsabile del trattamento in un formato elettronico strutturato e di uso comune.

Per esercitare i propri diritti, gli utenti possono presentare una richiesta all'indirizzo https://support.evicertia.com o inviare un'e-mail o una lettera all'indirizzo di contatto specificato nella sezione **Dati di contatti dell'organizzazione**. In tale richiesta, dovranno allegare una copia del proprio documento d'identità e indicare chiaramente quale diritto vogliono esercitare.

10.5 Diritti di proprietà intellettuale

Evicertia detiene i diritti di proprietà intellettuale della presente Dichiarazione delle Pratiche di Certificazione.

10.6 Obblighi e responsabilità civile

10.6.1 Obblighi di Evicertia

Evicertia garantisce, sotto la sua piena responsabilità, di rispettare tutti i requisiti stabiliti nella Dichiarazione delle Pratiche di Certificazione, essendo responsabile dell'adempimento delle procedure descritte secondo le indicazioni contenute nel presente documento.

Evicertia fornisce i servizi elettronici fiduciari in conformità alla presente Dichiarazione delle Pratiche di Certificazione.

Evicertia informa il sottoscrittore dei termini e delle condizioni relativi alla fornitura del servizio fiduciario, del suo prezzo e delle limitazioni d'uso, mediante un contratto di abbonamento che include per riferimento le dichiarazioni di divulgazione (DD) del servizio.

Il documento della dichiarazione di divulgazione, noto anche come DD, è conforme agli standard ETSI pertinenti e può essere trasmesso per via elettronica, utilizzando un mezzo di comunicazione durevole nel tempo e un linguaggio comprensibile.

Evicertia vincola i sottoscrittori e i soggetti terzi che fanno affidamento sui certificati mediante la suddetta dichiarazione di divulgazione o DD, in una lingua scritta e comprensibile e con i seguenti contenuti minimi:

- Requisiti di adempimento alle disposizioni del presente documento.
- Limiti all'utilizzo dei servizi fiduciari.
- Modo in cui viene garantita la responsabilità patrimoniale del Fornitore di Servizi di Certificazione.
- Limitazioni di responsabilità applicabili, compresi gli usi per i quali il Fornitore di Servizi di Certificazione accetta o esclude la propria responsabilità.
- Periodo di archiviazione dei registri di audit.

- Procedure di risoluzione delle controversie applicabili.
- Legge vigente e giurisdizione competente.

10.6.2 Obblighi di terzi a sostegno dei servizi dell'FSC

Gli obblighi di terzi a sostegno dei servizi offerti dall'FSC devono fornire, in generale, le seguenti garanzie:

- Osservare e facilitare il rispetto di tutte le clausole della presente DPC e delle politiche di certificazione dell'FSC.
- I servizi la cui infrastruttura è impiegata presso terzi devono offrire gli stessi livelli di sicurezza e affidabilità che avrebbero se fossero impiegati sulle infrastrutture dell'FSC.
- Il soggetto terzo dovrà conoscere e seguire le disposizioni della presente DPC e delle politiche di certificazione, che andranno rispettate come se questi fosse l'FSC stesso.
- Inoltre, nel caso in cui il soggetto terzo sia tenuto ad archiviare le informazioni e i dati, dovrà farlo nelle stesse condizioni e tempi previsti dalla DPC e dalle politiche di certificazione.
- Il soggetto terzo dovrà informare l'FSC di qualsiasi modifica da apportare all'infrastruttura o alle procedure al fine di sottoporli alla sua valutazione. In ogni caso, tali modifiche dovranno garantire il rispetto dei requisiti della presente DPC e delle politiche di certificazione.

10.6.3 Obblighi dei sottoscrittori

Gli obblighi dei sottoscrittori riguardo ai servizi fiduciari di Evicertia sono:

- Rispettare le disposizioni della presente DPC, nonché le pratiche e le politiche di Evicertia.
- Formalizzare un contratto di prestazione di servizi fiduciari con Evicertia.
- Utilizzare i servizi fiduciari di Evicertia secondo le procedure e, se necessario, le componenti tecniche fornite da Evicertia, in conformità alle disposizioni della Dichiarazione delle Pratiche di Certificazione (di seguito DPC) e della documentazione di Evicertia.
- Verificare le firme elettroniche e le marche temporali elettroniche, compresa la validità del certificato utilizzato nei diversi servizi fiduciari di Evicertia.
- Notificare qualsiasi criticità o evento riguardante i servizi fiduciari di Evicertia.

10.6.4 Garanzie offerte ai sottoscrittori e ai soggetti terzi che si affidano ai suoi servizi

Nella documentazione che la lega ai sottoscrittori e ai soggetti terzi che si affidano ai suoi servizi, Evicertia stabilisce e rifiuta le garanzie e le limitazioni di responsabilità applicabili.

Evicertia assicura al sottoscrittore che i servizi fiduciari sono conformi a tutti i requisiti materiali stabiliti nella presente Dichiarazione delle Pratiche di Certificazione e alle norme di riferimento.

Evicertia garantisce ai soggetti terzi che si affidano ai suoi servizi fiduciari che le informazioni contenute o integrate nei suoi servizi sono corrette, salvo ove diversamente indicato.

10.6.5 Rifiuto di ulteriori garanzie

Evicertia rifiuta ogni altra garanzia non legalmente applicabile, ad eccezione di quelle previste nel presente documento.

10.6.6 Limitazioni di responsabilità

Evicertia limita la propria responsabilità alla fornitura dei servizi fiduciari, che saranno regolati dal relativo contratto.

Evicertia non sarà responsabile di alcun danno diretto e/o di terzi derivante dall'uso improprio dei servizi fiduciari.

10.6.7 Caso fortuito e forza maggiore

Evicertia include nella dichiarazione di divulgazione o DD delle clausole che limitano la sua responsabilità per caso fortuito e forza maggiore.

10.6.8 Giurisdizione applicabile

Evicertia dichiara, nel contratto con il sottoscrittore e/o nella dichiarazione di divulgazione o DD, che la legge applicabile alla fornitura dei servizi, comprese la politica e le pratiche di certificazione, è quella spagnola.

10.6.9 Clausole di separabilità, sopravvivenza, accordo integrale e notifica

Evicertia prevede, nel contratto di sottoscrizione e/o nella dichiarazione di divulgazione o DD, delle clausole di separabilità, sopravvivenza, accordo integrale e notifica:

- In virtù della clausola di separabilità, l'invalidità di una clausola non influirà sul resto del contratto.
- In virtù della clausola di sopravvivenza, alcune norme resteranno in vigore anche dopo la cessazione del rapporto giuridico che regola il servizio tra le parti. A tal fine, l'Ente di Certificazione garantisce che almeno i requisiti contenuti nelle sezioni **Obblighi e responsabilità**, **Audit di conformità** e **Riservatezza** continuino a essere in vigore anche oltre il termine del servizio e delle condizioni generali di emissione/utilizzo.
- In virtù della clausola di accordo integrale, si intenderà che il documento legale che regola il servizio contiene la volontà completa e tutti gli accordi tra le parti.
- In virtù della clausola di notifica, si stabilirà la procedura con cui le parti si notificano reciprocamente gli eventi.

10.6.10 Clausola di giurisdizione competente

Evicertia stabilisce, nel contratto di sottoscrizione e nella dichiarazione di divulgazione o DD, una clausola di giurisdizione competente, indicando che la competenza giurisdizionale internazionale spetta ai giudici spagnoli.

La competenza territoriale e funzionale verrà stabilità in base alle norme di diritto internazionale privato e alle norme di diritto processuale applicabili.

10.6.11 Risoluzione dei conflitti

Nel contratto di sottoscrizione e/o nella dichiarazione di divulgazione o DD, Evicertia prevede le procedure di mediazione e risoluzione dei conflitti applicabili.

11 Allegato I - Acronimi

Di seguito, sono riportati gli acronimi utilizzati nella presente Dichiarazione delle Pratiche di Certificazione.

- CA: *Certification Authority*.
- RA: *Registration Authority*.
- CN: *Common Name*.
- CP: *Certificate Policy*.
- CED: Centro Elaborazione Dati.
- CPS: *Certification Practice Statement*.
- CRL: *Certificate Revocation List*. Elenco dei certificati revocati.
- CSR: *Certificate Signing Request*. Richiesta di firma del certificato.
- DES: *Data Encryption Standard*. Standard di crittografia dei dati.
- DN: *Distinguished Name*. Nome distintivo all'interno del certificato digitale.
- DPC: Dichiarazione sulle Pratiche di Certificazione.
- DSA: *Digital Signature Algorithm*. Standard dell'algoritmo di firma.
- DCCF: Standard dell'algoritmo di firma.
- ETSI: *European Telecommunications Standards Institute* o Istituto europeo per le norme di telecomunicazione o Istituto europeo per le norme di telecomunicazione.
- QSCD: *Qualified Signature Creation Device*. Dispositivo qualificato per la creazione di firme.
- FIPS: *Federal Information Processing Standard Publication*.
- ISO: *International Organization for Standardization*. Organizzazione internazionale per la standardizzazione.
- LRC: Elenchi di revoche di certificati.
- LDAP: *Lightweight Directory Access Protocol*. Protocollo di accesso alla directory.
- NTP: *Network Time Protocol*.
- OCSP: *On-line Certificate Status Protocol*. Protocollo di accesso allo stato del certificato.
- OID: *Object Identifier*. Identificatore dell'oggetto.

- OTP: *One-Time Password*.
- PA: *Policy Authority*.
- PC: Politica di certificazione.
- PDS: Disclosure Statement. Testo informativo.
- PIN: Personal Identification Number. Numero di identificazione personale.
- PKCS: Public-Key Cryptography Standards.
- PKI: *Public Key Infrastructure*. Infrastruttura a chiave pubblica.
- PSC: Fornitore di servizi fiduciari/certificazione elettronica.
- RSA: *Rivest-Shimar-Adleman*. Tipo di algoritmo di crittografia.
- SHA: *Secure Hash Algorithm*. Algoritmo hash sicuro.
- SSL: *Secure Sockets Layer*.
- TCP/IP: *Transmission Control. Protocol/Internet Protocol.*
- URL: *Uniform Resource Locator* o localizzatore uniforme di risorse.