CertiNet
Identidad Digital

PRÁCTICAS DE SELLO DE TIEMPO

CERTINET

CONTROL DE CAMBIOS

Versión	Descripción	Fecha	Autor	Aprobador
1.0	Primera versión de las Prácticas de Sello de Tiempo	2018/10/30	F. Rojas / H. Mena / M. Robles	R. Riveros
1.1	Revisión Anual	2022/08/17	F. Donoso	I. Infante
1.2	Revisión Anual	2023/08/28	I.Infante	I.Infante

Índice

1 Introducción

En el siguiente documento se presenta la declaración de “Prácticas de sello de tiempo” para la emisión de sello de tiempo de Certinet. Estas consisten en una descripción detallada de los procedimientos o prácticas que Certinet declara convenir en la prestación de sus servicios de sello de tiempo, cuando emite y gestiona, en su rol de Autoridad de sello de tiempo (TSA).

Es así como en la presente Declaración de Prácticas de sello de tiempo, se detallan las normas y condiciones de los servicios de sello de tiempo, que están relacionados con requisitos para la sincronización del tiempo, el sistema de emisión de los sellos de tiempo y otros requerimientos específicos para el proceso. También se describen las medidas de seguridad técnica, los perfiles y los mecanismos de información que permiten verificar y administrar la vigencia de los certificados de sello de tiempo, así como el asegurar que el proceso de certificación es llevado a cabo en un ambiente seguro y de confianza a los usuarios sobre la calidad de los sellos de tiempo y servicios anexos proporcionados por Certinet.

Esta Declaración de Prácticas de sello de tiempo constituye el marco general de normas aplicables a toda la actividad certificadora de Certinet, actuando como Autoridad de sello de tiempo (TSA), siendo este documento un complemento a las Políticas de Sello de Tiempo de Certinet.

Las prácticas de Sello de Tiempo aquí descritas establecen el ciclo de vida de los servicios que provee Certinet, que incluyen desde la gestión de la solicitud de un sello de tiempo, la obtención de un tiempo confiable, hasta la emisión del sello de tiempo requerido. Es decir, son aquellas prácticas, tanto a nivel de sistemas como del personal que en base a prácticas estandarizadas a nivel internacional, otorgan seguridad y confianza a los sellos de tiempo y servicios provistos por Certinet.

2 Alcance

El alcance de la Declaración de Prácticas de Sello de Tiempo detalla las normas y condiciones de los servicios que presta Certinet para la emisión de estos.

3 Referencias

La presente Declaración de Prácticas se ha generado siguiendo las especificaciones del documento RFC 3628 “Policy Requirements for Time-Stamping Authorities” así como también de las especificaciones técnicas definidas en el documento ETSI TS 102 023 “Electronic Signatures and infraestructures (ESI) Policy Requirements for Time-Stamping Authorities” y el documento RFC 3161“Internet X.509 Public Key infraestructura Time-Stamping Protocol (TSP)”.

De manera complementaria a los documentos indicados, se ha utilizado el documento de nombre Guías de Evaluación Procedimiento de Acreditación Prestadores de Servicios de Certificación, Servicios de Certificación de Sello de Tiempo”, entregados por el Subsecretaria de Economía y Empresas de menor tamaño del Gobierno de Chile, como parte del proceso de acreditación.

4 Identificación

El presente documento se denomina “Prácticas de Sello de Tiempo de Certinet”, las que internamente se citan como Prácticas de Sello de Tiempo y están registradas con el número único internacional (OID).

Este número identifica únicamente a Certinet en un contexto global, el cual está registrado en Internet Assigned Number Authority (IANA) y el que se detalla a continuación:

- **Certinet S.A.:** 1.3.6.1.4.1.52428
- **Políticas de Certificación (General ADSS) {iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) 52428 certificate-policies-ca-adss-certinet(100)}**: 1.3.6.1.4.1.52428.100
- **Políticas de Certificación TSA: {iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) 52428 tsa-certification-policies-certinet(200)}:** 1.3.6.1.4.1.52428.200

4.1 Detalle de los contactos y administración de la TSA

Cualquier consulta respecto a las normas contenidas en este documento, puede ser realizada en la siguiente dirección:

Razón social: Certinet S.A

Dirección de e-mail: soporte@certinet.cl

Dirección: Paseo Huérfanos 1052, Piso 12, Santiago Centro, Chile

Número telefónico: (+56) 2 3221 9400

Página web: www.certinet.cl

5 Definiciones y Abreviaciones

5.1 Definiciones

Autoridad de Sellado de Tiempo: Entidad prestadora de servicios de certificación que proporciona la certeza de la preexistencia de determinados documentos electrónicos a un momento dado, por medio de una firma digital acreditada. En este caso Certinet desempeña este rol.

Autoridad Certificadora: Entidad de confianza, responsable de emitir y revocar los certificados, utilizando en ellos la firma electrónica, para lo cual se emplea la criptografía de clave pública. Su principal función es garantizar la seguridad del Sello de Tiempo emitido por la Autoridad de Sellado de Tiempo.

Entidad Acreditadora: Entidad independiente y de confianza que acredita las políticas y prácticas de las Autoridades de Sellado de Tiempo. En el caso chileno la entidad acreditadora de la Subsecretaria de Economía y Empresas de menor tamaño.

Titulares/Usuarios: individuos, empresas, sistemas u otros, que solicitan la emisión de sellos de tiempo a la Autoridad de Sellado de Tiempo y están de acuerdo con sus términos de uso y condiciones descritos en sus políticas y prácticas de Sello de Tiempo.

Sellado de Tiempo: Proceso que consiste enregistrar de manera segura el tiempo tanto de la creación como de la modificación de un documento electrónico. Este sellado de tiempo debe ser seguro, lo que significa que nadie, ni siquiera el dueño del documento, puede modificarlo una vez que ha sido guardado.

Sistema de Sellado de Tiempo: Por medio de un Token de sellado de tiempo se provee de manera confiable la fecha y hora de la emisión del sello, así como la identidad del dispositivo que lo creó. La fecha y la hora se registrará por convención en la hora de Greenwich (GMT), adoptando las normas del Tiempo Universal Coordinado (UTC).

Token de sellado de tiempo: Dispositivo de datos empleado en un proceso de creación de firma electrónica, que está asociado a una representación de un dato para un tiempo concreto. Los Tokens de sellado de tiempo son emitidos de acuerdo con el RFC 3161 “Internet X.509 Public Key Infrastructure Time Stamping Protocol (TSP)”.

Tiempo Universal Coordinado: Intervalo de tiempo, escalado al segundo, según lo definido por la Radio de la Unión Internacional de Telecomunicaciones UIT-R, el comité TF.460-5 y corresponde, de manera aproximada a Greenwich Time TMT.

Unidad de Sellado de Tiempo: Es el componente que provee el tiempo de la firma. Está conformado por un conjunto de hardware, software y un Token de sellado de tiempo firmado por una llave privada de la Autoridad de Sellado de Tiempo.

5.2 Abreviaciones

Utilizamos a continuación las siglas provenientes de los términos en inglés, para mantener la convención

SIGLA	SIGNIFICADO
TSA	Autoridad de Sellado de Tiempo
CA	Autoridad Certificadora
TSS	Servicio de Sellado de Tiempo
CSP	Certificate Service Provider
TST	Token de Sello de Tiempo
TSU	Unidad de Sello de Tiempo
UTC	Tiempo Universal Coordinado
HSM	Hardware Security Modules
PKI	Public Key Infrastructure
CRL	Lista de Revocación de Certificados

6 Conceptos Generales

6.1 Servicio de Sello de Tiempo (TSS)

El Servicio de Sello de Tiempo utilizado emplea un Token de Sello de Tiempo el que está protegido por una firma electrónica que usa el Modelo PKI, que genera Sellos de Tiempo, los que una vez emitidos, no pueden ser modificados.

El proceso de generación de Sellos de Tiempo, representado en la Fig. N.º 1, procede de la siguiente manera:

Primero, con la información de la solicitud de firma electrónica, realizada por el Titular/Usuario, se genera un primer hash, al que llamaremos hash 1.0.

Un hash es como una huella digital electrónica, la que corresponde solamente a dicha información en dicho momento, lo que nos asegura que si la información original, cambia, también cambiará el hash.

Este hash 1.0 es enviado a la TSA, la que concatena dicha información con el tiempo oficial en formato UTC, generando un segundo hash, al que llamaremos hash 2.0.

Por último, la TSA firma electrónicamente con su clave privada este hash 2.0, generando el Sello de Tiempo.

La información del Sello de Tiempo es reenviada al solicitante del Sello de Tiempo, el que guarda dicha información, lo que lo hace inmodificable por cualquiera de las partes

Como los datos originales no pueden ser calculados a partir del hash (porque la función hash es una función de una sola dirección), la TSA nunca llega a ver los datos originales, lo que permite el uso de este método para datos confidenciales.

Con el objetivo de asegurar que el Sello de Tiempo sea producido de manera segura y que mantenga la hora correcta, Certinet utiliza los siguientes recursos:

1. La Unidad de Sello de Tiempo incluye una representación del dato (hash), el que tiene un Sello de Tiempo de acuerdo con la información entregada por el Titular/Usuario.
2. Cada Sello de Tiempo tiene un número de serie único, con el que es posible identificar no solo la fecha y la hora, sino que además la identidad del firmante.
3. Se utiliza un valor de tiempo, calibrado a ±1 un segundo con el UTC, para rastrear la fuente UTC(k).
4. La firma electrónica es creada por una clave usada solamente para el Sellado de Tiempo.

Adicionalmente el Servidor de Sellado de Tiempo de Certinet, proporciona un tiempo exacto de hasta ± 1 segundo, determinado con consultas a un servidor de tiempo basado en GPS que actúa como fuente de tiempo primaria en el nivel del Stratum 1. El servidor de tiempo se mantiene en una ubicación segura. Certinet posee medios técnicos adecuados que aseguran que el tiempo se sincronice con precisión con el UTC.

Si el reloj de la TSU se desvía del tiempo declarado y la calibración falla, la TSA no realizará el sellado de tiempo hasta que se restaure la hora correcta. La gestión manual del reloj del TSU solo puede ser realizada por personal autorizado.

La TSA también actúa también como una autoridad de certificación calificada y por ello se compromete a cumplir con los siguientes requisitos:

- El tamaño del dispositivo de firma (clave privada) de la TSA es de 2048 bits y está instalado en un componente de hardware confiable (HSM).
- El par de claves del servicio de sellado de tiempo es válido por 4 años a partir de la fecha de emisión.

- El par de claves debe ser reemplazado antes de la fecha de vencimiento, entre otras cosas por razones de cambios legales, así como por cambios en las pautas que definen el tamaño y / o tipo de algoritmo del dispositivo de firma de Certinet (clave privada), o por cualquier otra razón que requiera tal reemplazo. Cuando se produzca un reemplazo, Certinet publicará su nueva clave.

Los algoritmos utilizados para el Sello de Tiempo y sus parámetros cumplirán, en todo momento, con los requisitos de la Ley, las ordenanzas y las pautas del Ministerio. Si algún asunto no es tratado por lo anterior, se usarán estándares internacionales reconocidos por los organismos de estandarización.

6.2 PSC de Sello de Tiempo - Autoridad de Sellado de Tiempo (TSA)

La Autoridad de Sellado de Tiempo o TSA por sus siglas en inglés es la autoridad que provee los Servicios de Sellado de Tiempo, entregando Sellos de Tiempo en los que los usuarios del sistema (Titulares/Usuarios y terceros que confían), puedan confiar.

La Autoridad de Sellado de Tiempo:

- Opera, y es responsable del Sistema de Sellado de Tiempo.
- Puede operar a través de otras entidades que actúen en su nombre y bajo su responsabilidad.
- Está supervisada por la Entidad Acreditadora, en este caso la Subsecretaria de Economía y Empresas de menor tamaño.
- Puede operar más de un Sello de Tiempo a la vez, de ser el caso, cada servidor debe utilizar un dispositivo de firma por separado.
- Opera los Servicios de Sellado de Tiempo bajo una estructura PKI.
- Los Sellos de Tiempo emitidos por la TSA deben identificar a la empresa emisora, en este caso Certinet.

6.3 Subscriptores y Terceros que confían

Los Titulares/Usuarios de los Servicios de Sello de Tiempo, pueden ser tanto personas naturales como empresas. El Titular/Usuario debe aceptar de manera explícita, o no, los términos y condiciones del servicio. En el caso de que el Titular/Usuario sea una corporación o institución pública, el Titular/Usuario es el responsable de los actos y/u omisiones de sus órganos y/u organismos autorizados que actúen en su nombre.

Un Tercero que confía, es una persona natural, empresa o sistema, que recibe un Sello de Tiempo y decide sí tomarlo como válido o no.

7 Prácticas de Sellado de Tiempo

7.1 Identificación

El presente documento será individualizado como “Prácticas de Sello de Tiempo de Certinet”.

El presente documento está disponible de las siguientes formas: i) electrónica en el sitio de dominio electrónico ii) por correo electrónico si se solicita a la persona de contacto de Certinet.

7.2 Cumplimiento

La TSA referencia las políticas de sello de tiempo, definidas por Certinet, en cada uno de los sellos de tiempo emitidos. Certinet es periódicamente inspeccionada por la Entidad Acreditadora a fin de asegurar la correcta implantación de las prácticas de certificación definidas para la TSA, del cumplimiento de las obligaciones descritas en este documento para cada una de las partes, así como el haber cumplido con la implementación de los controles y procedimientos identificados en la política para garantizar la confianza en los sellos de tiempo que emite. Todo lo anterior se demuestra con el Plan de seguridad, que rige las acciones de Certinet, y en control de su cumplimiento a través de las reuniones periódicas de su Comité de Seguridad.

7.3 Aplicabilidad de los sellos de tiempo

Los sellos de tiempo emitidos por Certinet se utilizarán únicamente conforme a la función y finalidad que tengan establecidos en la presente Declaración de Prácticas de Certificación, en las correspondientes Políticas de Certificación de Sello de Tiempo, y en concordancia con la normativa legal vigente.

7.3.1 Uso

El uso de los sellos de tiempo aquí descrito está acotado a generar un certificado el cual contenga el resumen del documento, la hora obtenida desde de una fuente confiable - usada en la generación del sello de tiempo - así como la firma de la TSA que lo emite.

El conjunto de estos elementos permite demostrar que una serie de datos han existido y no han sido alterados desde un instante de tiempo específico y confiable.

Las normas que regulan la aplicabilidad de los sellos de tiempo, en determinados ambientes y comunidades se denominan “Políticas de certificación de Sello de Tiempo”.

7.3.2 Usos prohibidos

Los sellos de tiempo emitidos por Certinet, se utilizarán únicamente conforme a la función y finalidad que tengan establecida en este documento y en las correspondientes Políticas de sello de tiempo, y de acuerdo con la normativa vigente. Cualquier uso diferente a los indicados está expresamente prohibido.

7.3.3 Estructura de los sellos de tiempo

La estructura de los sellos de tiempo generados por Certinet se ajustan al documento RFC 3161“Internet X.509 Public Key infraestructura Time-Stamping Protocol (TSP)”.

8 Obligaciones

8.1 Obligaciones de la Autoridad de Sello de Tiempo

La TSA:

- Es responsable por aplicar lo expuesto en este documento.
- Debe velar porque las Políticas de Sellado de Tiempo se cumplan, sin perjuicio de que algunas actividades del proceso puedan ser realizadas por terceros debidamente autorizados.
- Es responsable de cumplir con los requisitos adicionales aplicados a su actividad, incluidas las directrices de la Entidad Acreditadora.
- Debe emplear -los medios necesarios para asegurar la compatibilidad total entre sus servicios como Autoridad de Sellado de Tiempo y este documento.
- Es responsable hacia el Titular/Usuario y el tercero que confía.

No obstante, lo anterior Certinet puede y podrá limitar su responsabilidad, incluidos los tipos de uso o las cantidades de las transacciones que emplean los servicios de sellado de tiempo.

Certinet no es ni será responsable de los daños que resulten de usos que excedan los límites establecidos en el Sello de Tiempo. Además, Certinet puede limitar su responsabilidad hacia los Titulares/Usuarios en el acuerdo de suscripción.

Sin embargo, el límite de responsabilidad de Certinet no puede contradecir la Ley, los términos de este documento y las normas que regulan la actividad de la empresa como Autoridad de Certificación calificada.

En el caso que un Titular/Usuario pida un uso limitado de un Sello de Tiempo, se requiere que el Titular/Usuario realice una solicitud explícita.

Certinet y sus representantes:

- No garantizan que un Titular/Usuario no renuncie a un Sello de Tiempo o a un mensaje electrónico firmado con un Sello de Tiempo.
- No garantizan la compatibilidad con los estándares o reglas de ningún software que no sea la tecnología y el software que sirve para el Sistema de Sellado de Tiempo de Certinet y la Unidad de Sellado de Tiempo que la empresa lo proporciona.
- No son responsables de los daños causados como resultado de confiar en un Sello de Tiempo no válido, siempre que Certinet haya demostrado que emplea todas las medidas razonables necesarias para cumplir con sus obligaciones de acuerdo con la Ley y este documento.
- Se liberan de cualquier responsabilidad por daños indirectos y solo son responsables de daños directos, que no excedan las limitaciones de uso del Sello de Tiempo, que resultan de la confianza en un Sello de Tiempo aparentemente en estado correcto del que después se compruebe que es defectuoso.
- Los servicios de Sellado de Tiempo no están destinados para ser utilizados con equipos de control y/o usos que requieran rendimientos a prueba de fallas tales como instalaciones nucleares, navegación aérea, sistemas de comunicación, sistemas de control de aire, sistemas de control de armas. Por lo tanto, cualquier falla que pueda resultar directamente en la muerte, lesión corporal o daño ambiental, por el uso indebido de los Servicios de Sellado de Tiempo, no será responsabilidad de Certinet.
- Certinet y sus representantes no serán responsables por ningún incumplimiento del deber, demora o abstención de realizar los servicios de Sello de Tiempo, como resultado de eventos de

fuerza mayor fuera de su control, como guerras, períodos de emergencia económica, plagas, interrupciones de electricidad, terremotos y otros desastres, siempre y cuando, Certinet y sus representantes no hayan podido prepararse razonablemente para estos eventos.

- En cualquier caso, que un Sello de Tiempo, emitido por Certinet, sea parte de un mensaje electrónico firmado por una firma electrónica calificada y certificada con un certificado electrónico emitido por Certinet en su calidad de autoridad de certificación calificada, la responsabilidad de Certinet por los servicios de Sellado de Tiempo no excederá su total responsabilidad combinada como una autoridad de certificación calificada.

8.2 Obligaciones de los subscriptores

El hardware que contiene la unidad de sellado de tiempo puede ser suministrado por la empresa o por el Titular/Usuario. En el caso en que el componente de hardware sea suministrado por el Titular/Usuario, Certinet se reserva el derecho de negarse a emitir una Unidad de sellado de tiempo en un componente de hardware que, a discreción profesional de Certinet, no cumpla con los estándares legales que aplican a los servicios de Sellado de Tiempo.

El subscriptor:

- Debe proteger el componente integrado con la unidad de sellado de tiempo de los riesgos de daños, pérdida, divulgación, cambio o uso no autorizado.
- Se compromete a utilizar la Unidad de Sellado de Tiempo de una manera que cumpla con las reglas de la ley y este documento.
- Se compromete a inspeccionar la Unidad de Sellado de Tiempo inmediatamente después de la instalación, verificar que esté en el orden correcto y avisar a Certinet sobre cualquier falla y / o mal funcionamiento en la Unidad de Sellado de Tiempo inmediatamente después de tomar conocimiento de ello.
- En el caso que desee limitar el uso de su sello de tiempo emitido, debe Informara la empresa por escrito y abstenerse de cualquier uso de los servicios de sellado de tiempo antes de verificar que Certinet incluyó la limitación en la unidad de sellado de tiempo y / o el certificado electrónico de manera accesible.

8.3 Obligaciones de las partes que confían

Al confiar en un sello de tiempo, un tercero debe:

- Verificar que el Sello de tiempo se haya firmado con una firma válida y que el dispositivo de firma utilizado sea válido en el momento de la verificación.
- Considerar las limitaciones sobre el uso del Sello de tiempo como se especifica en el Sello de tiempo y en este documento.
- Emplear todas las medidas de seguridad y control, ya sea explícitamente en cualquier acuerdo u otro documento a través de mensajes firmados electrónicamente.

Una parte confiante que elija confiar en un Sello de tiempo no válido y/o en un Sello de tiempo cuya validez no se puede verificar, será responsable de todos los riesgos resultantes.

9 Responsabilidades

Certinet es responsable de proveer los servicios de sellado de tiempo cumpliendo todas las exigencias materiales requeridas en las presentes Prácticas de Sello de Tiempo, y en conformidad con los datos entregados por el Titular/Usuario.

Certinet no será responsable por ningún daño o perjuicio actual o futuro, directo o indirecto, previsto o imprevisto, emergente o lucro cesante, pérdida de datos u otros, debidos, ocasionados o conectados con el uso indebido, no uso, uso tardío de los servicios de TSA y/o cualquier otro servicio ofrecido o contemplado por estas Prácticas de Certificación, aun cuando el Prestador de Servicios de Certificación hubiera sido advertido de la posibilidad de producción de tales daños.

Certinet no será responsable del uso indebido o incorrecto de los certificados o sus claves.

Certinet quedará exento de toda responsabilidad y liberada del cumplimiento de sus obligaciones, si por razones de caso fortuito o fuerza mayor tales como sismos, cortes de energía eléctrica y/o del servicio telefónico y/o de líneas de transmisión de datos, intervenciones de redes por partes de terceros, no funcionamiento de redes públicas y/o privadas, actos terroristas, huelgas u otros similares, no se pudiere mantener en funcionamiento u operativo el servicio contratado.

9.1 Responsabilidades Generales

Certinet garantiza el cumplimento de sus obligaciones legales como prestador de servicios de certificación, de conformidad con la Ley N° 19.799, y en virtud de esto, responderá por los daños y perjuicios que cause en el ejercicio de la actividad que le es propia, así como por el incumplimiento de las prescripciones contenidas en la Ley N° 19.628 relativa a la protección de datos personales o en la Ley 19.496sobre protección de los derechos de los consumidores.

En ningún caso será responsable de cualquier perjuicio que derive de una utilización negligente, por parte de los Titulares/Usuarios o terceras partes interesadas, o no acorde con las políticas y prácticas establecidas por la TSA de Certinet.

Certinet, como proveedor de servicios de Sello de Tiempo, adhiere a los estándares internacionales que rigen esta actividad, siendo ellos los documentos RFC 3628, RFC 3161 y su equivalente ETSI 102 023.

9.2 Responsabilidades Legales

Certinet no será responsable de cualquier perjuicio que derive de una utilización negligente o no acorde a las políticas y/o declaración de prácticas de sello de tiempo, por parte de los Titulares/Usuarios o terceras partes que confían.

Los servicios de sellado de tiempo de Certinet no han sido diseñados, autorizados o destinados para su aplicación en transacciones relacionadas con actividades que requieran funcionamiento a prueba de errores, como es el caso de instalaciones nucleares, sistemas de navegación o tráfico aéreo, sistemas de comunicación o de control de armamento, sistemas de equipos médicos o de todo otro sistema digital en que un error pueda conducir a la muerte, a las lesiones de personas, o a daños ambientales. Certinet no será responsable en caso de producirse daños por el uso de sus servicios de sello de tiempo en ámbitos como los indicados en esta cláusula.

Certinet declara que las responsabilidades por ella asumidas en esta declaración de prácticas y en los contratos o acuerdos de suscripción que a ellas se remitan serán aseguradas y reaseguradas conforme a las prácticas que habitualmente se aplican para los seguros de responsabilidad civil, y en concordancia con lo estipulado por la legislación que exista o llegase a existir. En particular la TSA de Certinet cuenta con un seguro en conformidad al artículo 14 de Ley 19799. La cobertura señalada no podrá ser invocada directamente por el Titular/Usuario o signatario titular de los sellos de tiempo, a menos que este sea la parte perjudicada. Los límites de responsabilidad a aplicar en cada sello se señalan en las políticas y prácticas de sello de tiempo correspondientes.

9.3 Fuerza Mayor

Certinet queda exenta de responsabilidad en caso de pérdida o perjuicio, en los servicios que presta, producto de guerra, desastres naturales o cualquier otro caso de fuerza mayor, los cuales le hagan imposible proveer los servicios de time-stamping de acuerdo con lo definido y publicado en sus políticas y prácticas de certificación.

10 Requerimientos de la Autoridad de Sellado de Tiempo

10.1 Prácticas y Declaraciones de divulgación

10.1.1 Declaración de prácticas de TSA

La TSA de Certinet, a partir del análisis de riesgo aplicado al servicio de la TSA, ha generado una planificación orientada a mitigar los riesgos detectados; el cual es conocido, controlado y aprobado formalmente por el comité de seguridad de Certinet.

10.1.2 Declaración de divulgación de TSA

En la presente declaración de prácticas de sello de tiempo detallan la implementación de los controles necesarios para cumplir con la política de sellado de tiempo, garantizando fiabilidad y confianza del servicio de sellos.

Entre los elementos más relevantes que considera este documento se encuentran:

- La información de contacto.
- Características del servicio de sello de tiempo
- El algoritmo de hash
- La precisión del tiempo
- Las prohibiciones de uso de sus sellos de tiempo
- Las obligaciones tanto de los Titulares/Usuarios como de los terceros de confianza
- Los mecanismos de verificación de los tokens emitidos por Certinet.
- El periodo de permanencia de los logs que maneja la TSA.
- Las leyes, reglamentos y estándares bajo los cuales se regula la actividad de la TSA.
- Un punto de contacto para presentar sus reclamos o no conformidades al servicio.
- La resolución que autoriza su funcionamiento emitida por la Entidad Acreditadora.

Certinet declara que tendrá a disposición pública, a través de su sitio web, la información relativa a los servicios prestados y formalizados en la Política y declaración de práctica de la TSA. De igual forma como parte de su proceso de Certificación ante la Entidad Acreditadora, Certinet deja a disposición de sus Titulares/Usuarios como también de los terceros, de la Resolución que aprueba la operación como Autoridad Certificadora de Tiempo emitida por el Subsecretaria de Economía y Empresas de menor tamaño de Chile.

10.2 Gestión del Ciclo de Vida de las claves

10.2.1 Generación de la llave de la TSU

El módulo criptográfico adoptado por Certinet, es capaz de generar llaves en base al algoritmo de encriptación de llave publica SHA2RSA con al menos 2048 bits de encriptación tal como se solicita en el criterio común de operación criptográfica CC P2 FCS_COP.1 y así mismo cuenta con

capacidad de firmar, cifrar y distribuir las llaves tal como se solicita en el criterio común de distribución de llaves criptográficas CC P2 FCS_CKM.2.

La TSA de Certinet utiliza para la generación de la llave en un módulo criptográfico HSM de Azure, el cual sólo puede ser accedido por personal autorizado y que se encuentra desactivado y protegido por procedimientos definidos por personal asignado en Certinet.

10.2.2 Protección de la llave privada de la TSU

Certinet lleva a cabo un conjunto de acciones de manera tal de asegurar que la llave privada de la TSU, usada para firmar los sellos de tiempo, permanece de manera confidencial y mantenga su integridad en un HSM dedicado e individualizado en Azure.

10.2.3 Distribución de la llave pública

El certificado digital utilizado por la TSA de Certinet es generado por la PSC de Certinet, de acuerdo con las políticas y prácticas de certificación inspeccionadas por el Subsecretaria de Economía y Empresas de menor tamaño de Chile

La forma en que se establece la confianza con una TSA - descrita para que un tercero que desee confiar - se basa en la instalación del certificado raíz de la TSU respecto a la cual se desea confiar. Es así como Certinet, como parte de los servicios que provee a sus clientes y terceros, publica en su sitio web los certificados raíces tanto de su propia TSA como de las TSAs certificadas ante el Subsecretaria de Economía y Empresas de menor tamaño de Chile. Estos certificados, se encuentran disponibles en el sitio web de Certinet, a través de una conexión segura (https).

Al estar este certificado instalado en el repositorio de confianza del cliente, cualquier sello que haya sido firmado por la TSA podrá ser validado por el cliente, ya que el certificado raíz de la TSA contiene la llave pública que permitirá verificar el sello emitido.

A continuación, se presenta la secuencia general del modelo de confianza:

- Se descarga certificado raíz de la TSA que ha emitido el sello a validar. Este certificado debe ser descargado a través de un canal seguro, que debe poseer el sitio de descarga de dicha raíz.
- Descargado el certificado raíz, este se procede a instalar en el repositorio de entidades emisoras raíz de confianza del equipo cliente.
- El sistema indicará si la importación e instalación del certificado ha sido correcta. De ser así, cualquier mensaje que sea firmado con un certificado de sello de tiempo, que ha sido emitido y firmado con esta raíz, podrá ser validado automáticamente en el equipo cliente. Una forma de validación adicional de esta instalación es verificar si el almacén de raíces de confianza incluye a este certificado recién instalado.

10.2.4 Reemisión de llaves de la TSU

Por motivos de seguridad y para evitar el repudio a un certificado, Certinet como PSC no procede a realizar la reemisión de llaves una vez generado el certificado de la TSU, esto de acuerdo con las políticas y prácticas que rigen la operación de su CA. Sin embargo, la llave privada de la TSU será reemplazada antes del fin de su periodo de validez, en caso de que el algoritmo o largo de la llave se determine como potencialmente vulnerable.

Las claves privadas caducadas se almacenan por un periodo no inferior a 10 años, siendo Certinet la ejecutora del procedimiento y la responsable de esta decisión. Las claves públicas se almacenan por un periodo adicional no inferior a 15 años, para permitir la verificación de sellos de tiempo emitidos con dichas claves.

10.2.5 Termino del ciclo de vida de la llave del TSU

La llave privada de la TSU será reemplazada al momento de su expiración. La TSU rechazará cualquier intento de emitir un sello de tiempo cuando esta llave privada haya expirado. Después de expirada, la llave privada es destruida.

La TSA de Certinet tiene la capacidad de revocar el certificado raíz activo de la TSU, en el momento que estime conveniente, ya sea por un evento de seguridad o bien por un cese de actividades.

En el evento que Certinet vaya a descontinuar sus operaciones como Autoridad de sello de tiempo, procederá a notificar por escrito y con la debida antelación a todas las partes involucradas con sus servicios de sello de tiempo: Titulares/Usuarios, terceros de confianza y autoridades de sello de tiempo acreditadas.

Certinet comunicará a cada uno de sus Titulares/Usuarios del cese de sus funciones. La citada comunicación se llevará a cabo con una antelación mínima de dos meses al cese efectivo de la actividad.

La TSA procederá a transferir los datos de sus sellos de tiempo a otro prestador de servicios, en la fecha en que el cese se produzca. Esta información incluirá como mínimo la información de los Titulares/Usuarios, los certificados de la TSU revocados, así como la transferencia de las obligaciones para mantener logs, archivos de auditoría, así como acceso a las llaves públicas o certificado usado por los terceros que confían por un periodo de tiempo razonable. La llave privada de la TSU, así como sus respaldos son destruidos inmediatamente al momento de la terminación de la TSA.

El procedimiento por seguir para el término de actividades, así como las medidas a tomar para el archivo de los registros y documentación necesaria, estará en conformidad con la ley aplicable de la República de Chile.

10.2.6 Gestión del ciclo de vida de los módulos criptográficos usados para las firmas de sello de tiempo.

Respecto al ciclo de vida del hardware criptográfico el personal de Certinet y terceros involucrados deben cumplir la normativa del dicho ciclo que a continuación se detalla:

10.3 Sellado de Tiempo (token, sincronización)

10.3.1 Token de sello de tiempo

La TSA de Certinet garantiza que los tokens de sellado de tiempo son emitidos en forma segura e incluyen un identificador único de política (OID), valores de fecha y hora proveniente de una fuente confiable de tiempo UTC sincronizado en la precisión definida en esta política.

Para cada sello de tiempo se incluye:

- La representación (Hash) del dato que provee el Titular/Usuario para que sea sellado con el sello de tiempo.
- Un identificador para la política de marca de tiempo.
- Un número serial único que será usado para ordenar los TSTs, así como para identificar un sello de tiempo específico.
- El tiempo calibrado a 1 segundo de la UTC, indicando la fuente de tiempo confiable.
- La firma electrónica que ha sido generada usando una llave que es sólo usada para la firma de los sellos de tiempo.
- La identificación de la TSA y de la TSU.

La TSA de Certinet establece todo el procedimiento asociado a la generación de los tokens de sello de tiempo, utilizando el protocolo descrito en RFC3161.

10.4 Sincronización de los relojes con UTC

En Certinet la TSA utiliza una fuente fiable de tiempo, mediante el servidor NTP que ofrece el SHOA

11 Gestión de la TSA y operaciones

11.1 Gestión de la seguridad

La TSA de Certinet desarrolla una administración activa de la seguridad basado en el análisis de riesgo desarrollado por la TSA de Certinet, a fin de detectar sus brechas de seguridad y planificar las mitigaciones de estas a través de un plan de trabajo

En particular:

- Certinet declara que su TSA es responsable por todos los aspectos asociados a la provisión de servicios de sello de tiempo
- Todo su personal tiene acceso a sus prácticas y políticas de sello de tiempo.
- Certinet cuenta con un Comité de seguridad de la información, un oficial de seguridad, y una oficina técnica, los que en su conjunto velan por el cumplimiento del control de os riesgos detectados.
- Certinet declara que los procedimientos y controles operacionales de la TSA se encuentran documentados, se mantienen y se implementan. Estos procedimientos son inspeccionados mensualmente a través de auditorías internas y anualmente por la Entidad Acreditadora del Subsecretaria de Economía y Empresas de menor tamaño de Chile.
- La TSA de Certinet no subcontrata los servicios de sello de tiempo.

11.2 Gestión y clasificación de activos

Los activos de la TSA de Certinet reciben un apropiado nivel de protección. Para ello la TSA de Certinet realiza anualmente un análisis de riesgos, basados en la norma ISO 27001.

En este análisis se ha levantado el inventario de los activos existentes en el proceso de sello de tiempo, junto con su clasificación de riesgo. Producto de lo anterior la TSA de Certinet generó un plan de gestión de seguridad que incluye las mitigaciones a los riesgos detectados. Para el cumplimiento de este plan, así como su seguimiento, Certinet cuenta con un Comité de seguridad de la información, un oficial de seguridad y una oficina técnica, los que en su conjunto velan por el su cumplimiento; desarrollando las acciones para controlar y mitigar cualquier desviación de los controles de los riesgos detectados. Tal como se indica anteriormente, todos estos procedimientos y controles operacionales de la TSA se encuentran documentados, se mantienen y se implementan.

Estos procedimientos son inspeccionados mensualmente a través de auditorías internas y anualmente por la Entidad Acreditadora del Subsecretaria de Economía y Empresas de menor tamaño.

11.2.1 Requerimientos de antecedentes y experiencia

Certinet requiere que todo el personal asociado a la TSA cuente con una calificación y experiencia acorde a la prestación de servicios de certificación, lo cual incluye:

- Conocimientos y formación sobre entornos de certificación digital y sellos de tiempo.
- Formación adecuada sobre seguridad en sistemas de información.
- Formación específica para su función y/o rol.
- Título académico o experiencia equivalente en la industria.
- El personal que realiza un rol de confianza no debe tener conflictos de interés que afecten la imparcialidad de las operaciones de la TSA.

11.2.2 Comprobación de antecedentes

Mediante CV y entrevistas realizadas al momento de la vinculación.

11.2.3 Roles de confianza

Certinet declara que sus roles de confianza al cumplir su función de TSA corresponden a:

- Oficial de seguridad.
- Administrador de Sistemas.
- Administrador de Seguridad.
- Auditor.

11.2.4 Requerimientos de formación y reentrenamiento

Como parte de las recomendaciones en que Certinet ha trabajado, se considera para el personal asociado a la TSA, cursos de capacitación, los cuales en contenido, duración y fechas estimadas se encuentran descritos en el plan de capacitación anual de Certinet para la PSC de Certinet. Este plan incluirá labores de reentrenamiento de existir cambios tecnológicos, en las políticas o prácticas de certificación o cualquier documento que se considere relevante de ser informado.

11.2.5 Frecuencia de rotación de tareas

No es aplicable para Certinet, ya que las personas mantienen su cargo.

11.2.6 Sanciones

Certinet informa y entrega al momento del contrato, a cada empleado el Reglamento Interno, el cual en uno de sus capítulos explicita los deberes, las obligaciones y las sanciones en caso de incumplimiento de las obligaciones.

11.2.7 Requerimientos de contratación

Como parte del contrato, todo trabajador de la PSC firma un acuerdo de confidencialidad, el cual se detalla a continuación:

“El TRABAJADOR se obliga en este acto y por el presente instrumento a mantener la más absoluta y total confidencialidad y reserva de toda información que pueda llegar a su conocimiento, de forma directa o indirecta, relativa a los negocios, clientes y/o actividades particulares o generales de CERTINET S.A., en específico respecto de aquellos datos personales que sean objeto de procesamiento o tratamiento por CERTINET S.A. como asimismo sobre cualesquiera otros datos y antecedentes relacionados con dichas bases de datos, estándole en consecuencia prohibido reproducir, transmitir, comentar y en general hacer cualquier uso de esa información para beneficio propio o de terceros. La infracción de esta obligación será considerada siempre un incumplimiento grave por parte del trabajador a las obligaciones que le impone el contrato, sin perjuicio de las acciones civiles y/o penales a que dicho incumplimiento pueda dar lugar.”

11.2.8 Documentación entregada al personal

El personal de la TSA tendrá a su disposición el siguiente material:

- Declaración de Prácticas de Certificación.
- Políticas de certificación.
- Política de privacidad.
- Política de Seguridad de la Información.
- Organigrama y funciones del personal.

11.2.9 Control de cumplimiento

De acuerdo con el Plan de seguridad se mide el control de cumplimiento de las actividades programadas de manera anual.

11.2.10 Finalización de contratos

La finalización de contratos cuenta con un procedimiento en el cual se suprimen los privilegios de acceso del individuo a las instalaciones e información de la organización, a excepción de la considerada PÚBLICA, una vez informado el individuo de su marcha y de su pérdida de privilegios, se verifica la devolución del material entregado y se le informa al resto de la organización, a los

proveedores y entidades externas a Certinet de que el individuo ya no representa a la TSA de Certinet.

11.3 Seguridad física y ambiental

Certinet en su calidad de PSC y TSA, opera en Data Center seguros y confiables provistos por AZURE, bajo certificación ISO 27001, ISO 22301, ISO 27018, FIPS 140-2, estando sus servicios en acuerdo a estas prácticas de certificación lo que queda ratificado en el reporte de auditoria SOC3 efectuado por DELOITTE el 30 de abril de 2018, que en resumen dictamina:

> "En nuestra opinión, la Organización de Servicio mantuvo, en todos los aspectos importantes, controles efectivos para cumplir con los criterios aplicables de los servicios fiduciarios durante el período comprendido entre el 1 de abril de 2017 y el 31 de marzo de 2018, para brindar una seguridad razonable de que:
>
> - El sistema estaba protegido contra acceso, uso o modificación no autorizados,
> - El sistema estaba disponible para su funcionamiento y uso como comprometido o acordado,
> - La información dentro del sistema, designada como "confidencial", estaba protegida comprometida o acordada, y
> - El procesamiento del sistema fue completo, válido, preciso, oportuno y autorizado
>
> Basado en los principios del servicio de confianza de AICPA y los criterios de seguridad, disponibilidad, integridad de procesamiento y confidencialidad.
>
> Deloitte & Touch LLP
>
> 30 de abril de 2018"

11.3.1 Emisión y administración de sellos de tiempo

- Los accesos físicos solo son limitados al personal autorizado y relacionados al servicio de sello de tiempo.
- Plan de continuidad operacional tanto para su PSC con TSA, los cuales son probados periódicamente a fin de verificar su operación, así como para realizar mejoras que podrían resultar de estos simulacros.

11.3.2 Control de los módulos criptográficos

Certinet mantiene los controles de sus módulos criptográficos tanto para la generación de la llave, así como la protección de estas tal como se indican en la "Gestión del ciclo de vida de las llaves" de este mismo documento.

11.3.2.1 Telecomunicaciones

Tomando en cuenta la importancia que tiene la infraestructura de comunicaciones para el negocio de Certinet, es que se ha diseñado en ambos sitios sobre una plataforma de reconocimiento mundial, Azure.

11.4 Gestión de las operaciones

La TSA de Certinet asegura que su sistema y componentes son seguros y se encuentran operados de manera correcta, con un riesgo mínimo de falla.

Los componentes del sistema de la TSA son protegidos de virus, código malicioso e incorporación de código no autorizado. Lo anterior a través de la aplicación de normativas de desarrollo de aplicaciones, protección de malware, adquisición de nuevos componentes y procedimiento de paso a producción.

- **Manejo de medios y seguridad:** Los activos de la TSA de Certinet reciben un apropiado nivel de protección. Para ello la TSA de Certinet realiza anualmente un análisis de riesgos, basados en la norma ISO 27001. En este análisis se ha levantado el inventario de los activos existentes en el proceso de sello de tiempo, junto con su clasificación de riesgo. Producto de lo anterior la

TSA de Certinet generó plan de gestión de seguridad que incluye las mitigaciones a los riesgos detectados previamente. Para el cumplimiento de este plan, así como su seguimiento, Certinet cuenta con un Comité de seguridad de la información, un oficial de seguridad, y una oficina técnica, los que en su conjunto velan por el su cumplimiento; desarrollando las acciones para controlar y mitigar cualquier desviación a dicho plan, o incorporar medidas adicionales con consideradas durante su generación. Tal como se indica anteriormente, todos estos procedimientos y controles operacionales de la TSA se encuentran documentados, se mantienen y se implementan. Estos procedimientos son inspeccionados mensualmente a través de auditorías internas y anualmente por la Entidad Acreditadora del Subsecretaria de Economía y Empresas de menor tamaño de Chile.

- **Manejo de incidentes y su respuesta:** Certinet cuenta con un sistema de gestión de incidentes que asegura que los eventos y debilidades de la seguridad de la información, asociados con los sistemas de información de los procesos de la PSC y su TSA, son comunicados a los roles encargados de la gestión de los incidentes, de una manera que permite el que se realicen las acciones correctivas oportunas, documentadas y estructuradas para resolver estos incidentes en el menor tiempo posible.

  La gestión de incidentes en Certinet, es a través de diferentes canales; esto es; telefónico, web y se registra en un sistema de control de gestión de incidentes que permite revisar los incidentes y resolverlos en los sla´s que se acuerden.

  El documento, que describe la gestión de incidentes de seguridad en Certinet, se ha estructurado siguiendo los lineamientos planteados tanto en el Anexo Guías de Evaluación Procedimientos de Acreditación v2.1 la cual tiene como referencia la ISO 27002 como, a la vez, la norma ISO 27035 Técnicas de seguridad y Gestión de incidentes de seguridad de la información (antigua ISO 18044).

- **Procedimientos operacionales y responsabilidades:** La operación del servicio de Sello de Tiempo de la TSA de Certinet opera de manera independiente de otros servicios provistos por la PSC: estas operaciones son desarrolladas por personal confiable definida en la estructura de la PSC de Certinet y sus Prácticas de Certificación. Dentro de los roles de confianza se tiene:

  - ***Administrador de Sistemas***
    - La instalación y configuración de sistemas operativos, de productos de software y del mantenimiento y actualización de los productos y programas instalados. Cuentan con capacidad para configurar y mantener los sistemas, pero sin acceso a los datos.
    - Activar los servicios de la TSA
    - Establecer y documentar los procedimientos de monitorización de los sistemas y de los servicios que prestan.
    - Responsable de mantener la información suficiente que permita restaurar eficientemente cualquiera de los sistemas.
    - Debe mantener el inventario de servidores y equipamiento que compone el núcleo de la plataforma de certificación.

  - ***Administrador de Seguridad***
    - Debe cumplir y hacer cumplir las políticas de seguridad de Certinet, y debe encargarse de cualquier aspecto relativo a la seguridad de la TSA Certinet, desde seguridad física hasta la seguridad de las aplicaciones, pasando por seguridad de la red. Esta función estará soportada a través de una oficina de seguridad técnica, además del oficial de seguridad.

  - ***Responsable de formación, soporte y comunicación***
    - Se encarga del mantenimiento de contenidos de la web de Certinet.
    - Se encarga de definir el plan de formación para usuarios finales, para agentes de soporte al cliente y para personal implicado directamente en la operación y administración de la plataforma de la TSA de Certinet.
    - Debe revisar mensualmente los reportes de incidencias y nivel de cumplimiento de los SLA´s definidos

- El Responsable de formación, soporte y comunicación contará con la colaboración de las áreas de RRHH, Marketing o Post venta de estimarse necesario.

- ***Responsable de Seguridad***
  - Se asigna esta tarea al Comité de Seguridad de la Información de Certinet, asumiendo la responsabilidad general en cuanto a la actualización e implantación de las políticas y procedimientos de seguridad que han sido aprobadas.
  - Gestionará que los sitios donde se encuentran los sistemas de Certinet, cumplan con gestionar los sistemas de protección perimetral y la correcta gestión de los sistemas de detección de intrusiones (IDS) y de las herramientas asociadas a éstos.
  - Es el responsable de resolver o hacer que se resuelvan las incidencias de seguridad producidas, de eliminar vulnerabilidades detectadas, y otras tareas relacionadas.
  - Es responsable de autorizar movimientos de material fuera de las instalaciones del PSC.
  - Debe encargarse de efectuar la selección y determinar la contratación de terceros especialistas que puedan colaborar en la mejora de la seguridad del PSC de Certinet.

- ***Auditor***
  - Encargado de realizar auditorías internas. En definitiva, debe comprobar todos los aspectos recogidos en la política de seguridad, política de copias, prácticas de certificación, políticas de certificación, etc. tanto en el núcleo de sistemas dela TSA de Certinet y su personal. Para esta labor se hará uso de Auditores internos como también la contratación de una auditoría externa anual.

- ***Responsable de Documentación***
  - Se encargará de mantener el repositorio de documentación y los archivos de documentación en papel.
  - Controlará que cada área lleve a cabo la actualización de documentos cuando se requiera.
  - Se encargará de mantener actualizado el fichero de índice de documentos y será el único habilitado para almacenar, borrar o modificar documentos en el repositorio de documentación.

11.5 Gestión de acceso a los sistemas

La TSA de Certinet, declara y asegura que el acceso a su sistema (hardware, software y datos) sólo está limitado al personal autorizado. En particular, la PSC de Certinet cuenta con:

- Firewalls apropiados para proteger la red interna de accesos no autorizados incluyendo a Titulares/Usuarios y terceros que confían.
- Administración de usuarios, para mantener la seguridad de los sistemas, incluyendo administración de cuentas, logs y modificación o eliminación de accesos
- Restricciones de acceso a la información y sistemas de aplicación de acuerdo con la política de control de acceso, así como desagregación de funciones en los roles de confianza definidos.
- Un control apropiado del personal autorizado tanto en su identificación como autenticación, previo a tener acceso a las aplicaciones relacionadas con los sellos de tiempo. En particular Certinet cuenta con un inventario de activos, incluyendo los roles y personas que cubren cada rol.
- Logs de las operaciones que realiza el personal para auditorías posteriores

Los administradores de Certinet realizan un monitoreo continuo para detectar intentos o accesos no autorizados a los activos de la TSA.

11.6 Mantenimiento e Implementación de sistemas de confianza

La TSA asegura que sus sistemas y productos están protegidos contra modificaciones no autorizadas.

Para ello, la TSA de Certinet y su PSC previo a cualquier cambio en sus sistemas o productos lleva a cabo:

- Un análisis de requerimientos de seguridad es llevado a cabo durante el diseño y especificación de requerimientos. Es así como, cuando se pongan en marcha los proyectos para el desarrollo e implantación de nuevos sistemas, o ampliación/mejora de los ya existentes, además de las actividades tradicionales de cada una de las fases de éstos, se llevarán a cabo igualmente las actividades para determinar e implementar los requerimientos de seguridad necesarios. Esto ocurrirá tanto cuando se vaya a adquirir un producto o cuando este se desarrolle internamente; estableciendo igualmente los requerimientos de seguridad que debe cumplir y revisando dicho cumplimiento antes de su compra o desarrollo. Lo anterior se encuentra documentado en la “Política de adquisición de componentes nuevos”.
- Un procedimiento de control de cambio para nuevas versiones, modificaciones y/o correcciones de emergencia al software. El propósito de este Procedimiento es establecerlas actividades necesarias para llevar a cabo los cambios y actualizaciones en los sistemas de una manera eficiente, incluido las nuevas versiones y los pasos a producción, minimizando el impacto y las incidencias que se puedan producir debido a ellos. Certinet documenta estos pasos a través de su Procedimiento de Gestión de Cambio.
- Respecto a la generación de la llave de la TSA, utilizada por la TSU en la entrega de sus sellos de tiempo TST, siempre es creada en un ambiente seguro tal como se describe en Generación de la llave de la TSU de este mismo documento.

11.7 Compromiso de los servicios de TSA

La TSA de Certinet declara que ante cualquier evento de seguridad que afecte sus servicios, incluyendo compromiso de la llave de firma de la TSU o perdida de precisión declarada de su reloj, esto es informado directamente o a través de su sitio web a sus Titulares/Usuarios y terceros que en ella confía.

El PSC de Certinet y en particular su TSA ha:

- Desarrollado un Plan de continuidad operacional, el cual incluye los escenarios de compromiso de llave, pérdida de la precisión declarada del reloj de la TSA o falla de componentes que afecten directamente la operación del sitio principal de la TSA. Para estos escenarios Certinet ha definido un plan que permite la recuperación de servicios frente a estos eventos. Dichos escenarios son probados periódicamente a fin de probar la eficacia y eficiencia del plan e incorporar mejoras producto de la misma ejecución de estos escenarios.
- Ante los eventos antes mencionados, la TSA de Certinet no emitirá nuevos TST hasta superar el compromiso declarado.
- Ante perdida de la precisión, compromiso de este o sospecha de compromiso en el tiempo de la TSA; Certinet dejará esta información a los Titulares/Usuarios y terceros que confían indicando la descripción del evento. Esta comunicación será directa o a través de su sitio web
- En caso de comprometerse ya sea la llave o la precisión declarada, se informará a los Titulares/Usuarios y terceros que confían de aquella información que permite detectar los sellos de tiempo afectados, a menos que esta información vulnere su política de privacidad de datos personales - disponible en su sitio web - de sus usuarios o la seguridad de los servicios de la TSA de Certinet.

11.8 Cese de una TSA

La TSA de Certinet tiene la capacidad de revocar el certificado raíz activo de la TSU, en el momento que estime conveniente, ya sea por un evento de seguridad o bien por un cese de actividades.

En el evento que Certinet vaya a descontinuar sus operaciones como Autoridad de sello de tiempo, procederá a notificar por escrito y con la debida antelación a todas las partes involucradas con sus

servicios de sello de tiempo: Titulares/Usuarios, terceros de confianza y autoridades de sello de tiempo acreditadas.

Certinet comunicará a cada uno de sus Titulares/Usuarios del cese de sus funciones. La citada comunicación se llevará a cabo con una antelación mínima de dos meses al cese efectivo de la actividad.

La TSA procederá a transferir los datos de sus sellos de tiempo a otro prestador de servicios, en la fecha en que el cese se produzca. Esta información incluirá como mínimo la información de los Titulares/Usuarios, los certificados de la TSU revocados, así como la transferencia de las obligaciones para mantener logs, archivos de auditoría, así como acceso a las llaves públicas o certificado usado por los terceros que confían por un periodo de tiempo razonable. La llave privada de la TSU, así como sus respaldos son destruidos inmediatamente al momento de la terminación de la TSA.

El procedimiento por seguir para el término de actividades, así como las medidas a tomar para el archivo de los registros y documentación necesaria, estará en conformidad con la ley aplicable de la República de Chile.

11.9 Cumplimiento de requerimientos legales

Certinet como Autoridad de sello de tiempo, actúa en conformidad con la Ley N° 19.799, su reglamento, así como la Ley N° 19.628 relativas a la protección de datos personales, la ley N° 19.496 sobre los derechos de los consumidores y las directrices técnicas establecidas por los organismos calificadores (ETSI, ISO, RFC, etc.). Además, su operación se encuentra regulada por la Entidad Acreditadora de la Subsecretaria de Economía y Empresas de menor tamaño de Chile y sus Guías de Acreditación

Certinet cuenta con procedimientos de control y de seguridad de la información, al objeto de proteger la información personal de sus Titulares/Usuarios, manteniendo la confidencialidad y la integridad de los datos; todo ello ante un procesamiento no autorizado o ilegal, así como ante la destrucción o daño de dicha información ya sea de manera accidental o intencional. Certinet usa esta información sólo para los fines que fueron entregados por parte del Titular/Usuario.

La información con data del Titular/Usuario es protegida de divulgación, a menos que sea solicitada por él mismo o por orden judicial u otro requisito legal.

11.10 Registro de información relativa a las operaciones del servicio de sello de tiempo

La TSA de Certinet mantiene registros de la información relevante, concerniente a su operación. La información personal de los Titulares/Usuarios, que ha recolectado la PSC de Certinet como parte de su operación, está protegida de acuerdo con la Política de Privacidad de datos personales publicados por Certinet en su sitio web.

Todos los registros concernientes a la operación del servicio de sello de tiempo se encuentran disponibles sólo al Titular/Usuario o en caso de que lo solicite una corte a través de un requerimiento legal. Lo anterior a fin de proteger la confidencialidad de dichos datos. La integridad de esta información es mantenida por la PSC de Certinet por un periodo de 5 años posterior a la expiración de la validez de la llave usada para la firma por parte de la TSU.

Estos registros incluyen:

- Requerimiento de sello de tiempo
- Sello de tiempo creado
- Eventos relacionados con la administración de la TSA, incluyendo:
  - Registros de eventos correspondientes al ciclo de vida de las llaves de la TSU
  - Registros de eventos correspondientes a los certificados de la TSU
  - Registros relacionados con la sincronización del reloj de usado por la TSU en sus TST
  - Registros asociados a eventos de detección de pérdida de sincronización

Los registros antes mencionados, son almacenados por Certinet y no son de fácil eliminación o destrucción dentro del periodo de tiempo previamente declarado. A estos registros, sólo tiene acceso el personal autorizado por la PSC de Certinet.

11.11 Organización

La Autoridad de Sellado de Tiempo se encuentra soportada por la PSC de Certinet, la cual se encuentra acreditada en su operación por la Entidad Acreditadora del Subsecretaria de Economía y Empresas de menor tamaño de Chile.

En particular la TSA de Certinet cumple con:

- Sus políticas y procedimientos bajo los que opera no incluyen cláusulas discriminatorias que contravengan la Ley N° 19.496 sobre los derechos de los consumidores.
- Certinet provee su servicio de sello de tiempo a cualquier Titular/Usuario que cumpla y este de acuerdo con las obligaciones declaradas en las prácticas y políticas de sello de tiempo.
- Certinet para la provisión de sus servicios cumple con la normativa legal vigente, respecto a la formación y operación de empresas y personas jurídicas.
- Certinet como parte de su cumplimiento de la Ley 19799, cuenta con un seguro de responsabilidad civil, ante daños o perjuicios producto de su operación.
- Certinet es anualmente auditada respecto sus estados financieros y el cumplimiento de la normativa vigente.
- Certinet como PSC certificada por el Subsecretaria de Economía y Empresas de menor tamaño en Chile, cuenta con un personal calificado para la prestación de sus servicios, así como realiza una capacitación continua de este personal a través de sus planes anuales de capacitación.
- Certinet ante un conflicto con un cliente, el cual no pueda ser resuelto favorablemente por las partes, utilizará los Tribunales de Justicia a modo que ellos actúen como árbitro arbitrador del conflicto.
- Certinet mantiene un su repositorio documental todo contrato, acuerdos de confidencialidad servicios prestados por cada uno de los proveedores de la TSA.

12 Seguridad

Certinet y sus representantes utilizan solamente sistemas confiables que cumplen con los requisitos técnicos establecidos por los estándares universales de TSA.

Certinet usa sistemas de seguridad de datos confiables. Estos sistemas no están abiertos al público, pero son auditados por organismos externos, como parte de una auditoría anual, la que asegura, la confiabilidad de los sistemas y la adherencia a las prácticas y las pautas del Ministerio.

Certinet lleva a cabo una revisión de riesgos anual del sistema por un experto externo independiente de seguridad de datos aprobado por el Ministerio. La empresa cumple con los estándares de seguridad de datos ISO 27001 y es auditada para este efecto por organismos independientes.

12.1 Seguridad y manejo de personal

Certinet emplea personal experimentado con conocimiento, experiencia y calificaciones apropiadas y requeridas para los requisitos del trabajo y los servicios suministrados por Certinet.

Certinet opera bajo procedimientos de administración de personal destinados a garantizar que los empleados sean confiables, profesionales y de confianza capaces de cumplir con sus tareas con énfasis especial en la gestión y contratación de empleados para puestos de confianza.

Estos procedimientos se refieren al nombramiento de funcionarios en la empresa, incluidos los documentos necesarios, la verificación de antecedentes, la experiencia y las calificaciones de los candidatos, la ejecución de la confidencialidad, la ausencia de compromisos de conflicto de intereses y la realización de controles de fiabilidad adicionales.

Certinet mantiene un programa de instrucción para empleados como parte de un programa anual de instrucciones. Las instrucciones incluyen el conocimiento de la Ley y los procedimientos. Las definiciones de trabajo se actualizan y se extraen conclusiones de seguridad y otros eventos.

En cada compromiso de Certinet con subcontratistas para la ejecución de actividades que conlleven el permiso del subcontratista para participar en cualquier actividad de Sellado de Tiempo que tenga un acceso limitado, el subcontratista debe asumir un compromiso contractual para mantener los más estrictos requisitos de seguridad. a lo cual Certinet está comprometida por esta CPS, la Ley y ordenanzas, y además están obligados a compensar a Certinet por cualquier daño que resulte del incumplimiento de la seguridad de datos.

12.2 Seguridad física

Certinet opera bajo un sistema de seguridad basado en estrictos estándares de seguridad de hardware, software y procedimientos de trabajo que son auditados y aprobados por el Ministerio. Estos proporcionan un alto nivel de disponibilidad, actividad ininterrumpida la aplicación de procedimientos de seguridad, así como una respuesta satisfactoria a la seguridad ante amenaza

Certinet realiza una evaluación de riesgos para determinar los requisitos de seguridad y los procedimientos operativos requeridos. La evaluación del riesgo, junto con la política y los procedimientos de seguridad existentes, son examinados por los auditores de riesgos, así como por el Ministerio, a fin de cerciorarse de que efectivamente se trataron todos los riesgos identificados.

La revisión de riesgos se realiza al menos una vez al año por un experto externo independiente en seguridad de datos que fue aprobado por el Ministerio. Certinet se compromete a solucionar todos los fallos de funcionamiento inmediatamente después de recibir la revisión de riesgos. Se registra un informe sobre la ejecución de las actividades de reparación con el Ministerio.

12.3 Seguridad lógica del dispositivo de firma de servicios de sellado de tiempo

El dispositivo de firma de Servicio de Sellado de Tiempo (clave privada) está encriptado, en su totalidad, en un módulo de seguridad de hardware HSM Azure. Las claves de acceso al módulo de seguridad se almacenan en una caja de seguridad externa con acceso limitado solo al gerente de seguridad y sujeto a los procedimientos de separación de funciones (SOD) de Certinet.

En su calidad de autoridad de certificación calificada, el dispositivo utilizado para certificados electrónicos de sellado de tiempo es utilizado solo por Certinet y está bajo su control exclusivo.

El dispositivo de firma de Certinet y/o de cualquiera de sus representantes está protegido por un hardware confiable de acuerdo con los requisitos de las Ordenanzas de Firma Electrónica (software y hardware), es decir, el dispositivo de firma de Certinet cumple con los siguientes requisitos:

- Se basa en una clave RSA o DSA de al menos 2048 bits.
- Está protegido con un dispositivo que cumple, al menos, el requisito de FIPS 140-2.
- Se respalda con medios protegidos y seguros y la copia de seguridad se guarda por separado.
- Cumple con los requisitos adicionales del Ministerio diseñados para mantener un nivel razonable de seguridad contra incumplimiento, interrupción o mal uso.

12.4 Compromiso de los servicios TSA

El compromiso del dispositivo de firma de Certinet se define como un desastre Para manejar dicho desastre, Certinet prepara y mantiene un programa de continuidad de negocios para un evento de desastre. El plan de recuperación ante desastres presenta una solución en caso de compromiso o sospecha de compromiso del dispositivo de firma de Certinet y/o el dispositivo firmante de la TSA.

12.5 Controles Operacionales

Certinet mantiene controles operacionales que incluyen control organizacional, control de recursos humanos, y otros. Estos controles contienen requisitos que se refieren al entrenamiento y a la instrucción de los empleados y/o representantes de Certinet, estableciendo una política que regule la asignación de funciones dentro de la empresa, requisitos de documentación y pre-ajuste procedimientos y auditorías.

El encargado de seguridad emplea controles operacionales que verifican la operación de acuerdo con los procedimientos.

12.6 Terminación de los servicios TSA de Certinet

Seguridad de copia de seguridad y registros Certinet y / o sus representantes mantendrán, de manera confiable, registros relativos a la unidad de sellado de tiempo expedida a los certificados electrónicos de la Compañía en su calidad de autoridad de certificación calificada por el término indicado en la autoridad de certificación calificada CPS. Registros relacionados con un sellado de tiempo**.**

Los registros se mantendrán de forma segura servidor y estará sujeto a los procedimientos de Certinet que se aplican a la protección de datos confidenciales y evitar el compromiso de su privacidad.

12.7 Consideraciones de seguridad

Cuando una parte que confié en los TST emitidos por Certinet requiera chequear su validez, debe asegurar que el certificado de firma de la TSU de Certinet es verdadero (modelo de confianza) y no se encuentra revocado, ya sea a través de la CRL de Certinet o del servicio OCSP que ella provee a sus usuarios externos.

La validez de un TST es cierta sólo para el momento en que se efectúa el chequeo antes mencionado y debe ser verificado si se hace necesario en un tiempo posterior, ya que puede existir un compromiso dela llave privada de la TSU de Certinet.

Certinet asegura que el hash incluido en su TST corresponde al enviado por el Titular/Usuario en su request.

13 Revisión y aprobación del documento

13.1 Revisión

Este documento es revisado anualmente a fin de verificar su validez y eficacia, o en un plazo menor en caso de producirse cambios significativos que ameriten su revisión de acuerdo con el marco regulatorio, comercial, legal o técnico.

13.2 Control de cambios

Cada vez que se requiera efectuar una modificación, esta debe ser incorporada al documento y reflejada bajo un control de cambio. Para ello se debe ingresar una nueva entrada en el control de cambios de la portada del documento que a continuación se detalla:

CONTROL DE CAMBIOS

Versión	Descripción	Fecha	Autor	Aprobador

Con esto se logrará el mantener una traza respecto a las actualizaciones que ha sufrido este documento.

Esta nueva versión del documento será almacenada en el sistema documental de Certinet, con su respectivo control de versión, posterior a su aprobación.

13.3 Aprobación

Este documento, así como las modificaciones que él sufra deben ser aprobados por el dueño del documento y en comité de seguridad, a fin de que sea incorporado como la nueva versión vigente al sistema de gestión documental y para posteriormente proceder a su difusión con los empleados y partes externas pertinentes.