CertiNet
Identidad Digital

POLITICAS DE SELLO DE TIEMPO

2025

Versión 2.1

CONTROL DE CAMBIOS

Versión	Descripción	Fecha	Autor
1.0	Primera versión de las Políticas de Sello de Tiempo	2018/10/30	F. Rojas / H. Mena / M. Robles
1.1	Revisión anual	2022/08/17	F. Donoso
1.2	Revisión Anual	2023/08/28	I.Infante
1.3	Actualización certificado suspendido o revocado	2024/01/23	I.Infante
1.4	Revisión Anual, ajuste de formato	2024/08/30	I.Infante
1.5	Se agrega en párrafo 11.12 enlace a la política de privacidad	2024/08/11	A.Léniz
2.0	Se agrega párrafo 12.8 Auditorías	2025/01/15	A.Léniz
2.1	Revisión anual	2025/08/26	I.Infante

Contenido

1 Introducción.

En este documento se presenta la Política de Sello de Tiempo asociada a la emisión de sello de tiempo de Certinet. Esta política está constituida por un conjunto de reglas, las que se ajustan a los procedimientos y prácticas que Certinet declara en la prestación de sus servicios de sello de tiempo. Lo anterior tanto al momento de emitir o gestionar la información usada en la solicitud del sello, durante la verificación de los tokens de time-stamping, al momento de la confirmación de vigencia de la llave privada de la TSA - a través de la CRL - así como ante el evento de que la llave de la TSA haya sido comprometida; todo lo cual se encuentra definido en esta política. Se definen además los roles, responsabilidades y relaciones entre el usuario final y Certinet siendo la Declaración de Prácticas de Sello de Tiempo de nuestra empresa un complemento fundamental a este documento.

Las políticas de Sello de Tiempo aquí descritas establecen el ciclo de vida de los sellos de tiempo que provee Certinet, 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 políticas tanto a nivel sistémico, como de personal, que en base a sus buenas prácticas dan seguridad y confianza a los sellos de tiempo y servicios de certificación provistos por Certinet.

2 Alcance.

El alcance de la Política de Sello de Tiempo define las normas y condiciones de los servicios que presta Certinet para la emisión de estos en su actuar como TSA.

3 Referencias.

La presente Política de Sello de Tiempo se ha generado en base a 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, versión 1.1”, entregados por el Ministerio de Economía del Gobierno de Chile, como parte del proceso de acreditación.

4 Identificación.

El presente documento se denomina “Políticas de Sello de Tiempo de Certinet”, las que internamente se citan como Políticas 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). El cual 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. Una autoridad de certificadora despacha los certificados digitales, que ya contienen las identificaciones numéricas y las contraseñas que se necesitan, poniendo a disposición el procedimiento de verificación para validar el certificado proporcionado. 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 los Sellos de Tiempo es el Ministerio de Economía.

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 las políticas y prácticas de Sello de Tiempo declaradas.

Sellado de Tiempo: Proceso que consiste en contar 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 registrarán 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 sistema 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. Nº1, se describe en forma íntegra en la Declaración de Practicas de Sello de Tiempo.

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.

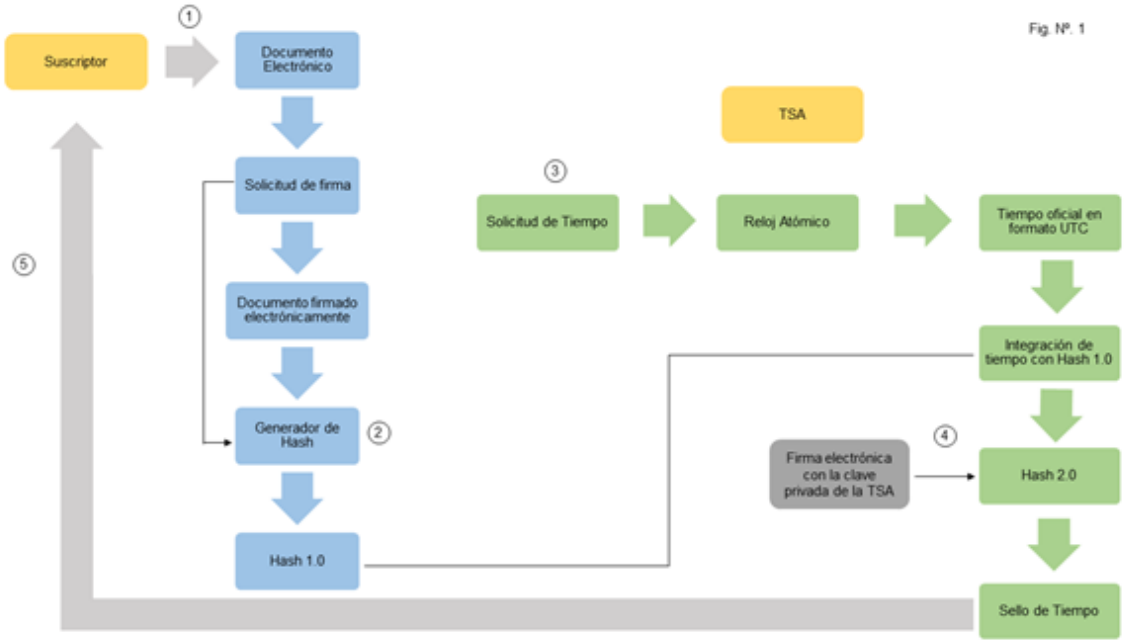
Adicionalmente el Servidor de Sellado de Tiempo de Certinet, proporciona un tiempo exacto de hasta ± 1 segundo, determinado con consultas a un servidor de tiempo basado en GPS que actúa como fuente de tiempo primaria en el nivel del Stratum 1. El servidor de tiempo se mantiene en una ubicación segura. 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 la componente de hardware confiable que proporciona los servicios HSM de Azure
- 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 el Ministerio de Economía.
- 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 dar el sí, 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 si tomarlo como válido o no.

7 Política de Sellado de Tiempo

7.1 Identificación.

El presente documento será individualizado como “Políticas de Certificación TSA 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 del Sello de Tiempo.

La política de Certinet es garantizar un proceso confiable para emitir una Unidad de Sellado de Tiempo de acuerdo con la Ley y las pautas del Ministerio de Economía.

El dispositivo de firma y esta CSP se ajustan a requisitos técnicos de ETSI TS 101.861 y RFC 3161.

El dispositivo de firma de Sellado de Tiempo de Certinet está reservado para los servicios de Sellado de tiempo.

La unidad de sellado se emite con una precisión de tiempo de ± 1 segundo con respecto a la Hora Universal Coordinada.

La TSA referencia el OID de las políticas de sello de tiempo, definidas por Certinet, en cada uno de los sellos de tiempo emitidos como en su página web. Declarando así la correcta implantación de éstas, a fin de asegurar el cumplimiento de las obligaciones descritas en este documento para cada una de las partes. Es por ello por lo que realiza la implementación de los controles y procedimientos identificados en esta política y en las prácticas para garantizar la confianza en los sellos de tiempo que emite, ya que es periódicamente inspeccionada por la Entidad Acreditadora del Ministerio de Economía.

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 establecida en estas Políticas de Certificación de Sello de Tiempo y la Declaración de Prácticas de Sello de Tiempo, en concordancia con la normativa vigente para garantizar el no repudio.

7.3.1 Uso.

El uso de los sellos de tiempo aquí descrito está acotado a demostrar que una serie de datos, han existido y no han sido alterados desde un instante de tiempo específico y confiable. El

conjunto de normas que regulan la aplicabilidad de los sellos de tiempo, en determinados ambientes y comunidades se denomina “Política 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 se tenga establecida en la presente Política de Sello de tiempo y las prácticas de sellos 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)”.

7.3.4 Estructura de los Certificados.

7.3.4.1 Certificado Raíz.

General		Observaciones
Este certificado está destinado a los siguientes propósitos:	Todas las directivas de la aplicación	
	Todas las directivas de emisión	
	Otros... OID	
Emitido para:	Certinet S.A. Raíz Autoridad Certificadora	
Emitido Por:	Certinet S.A. Raíz Autoridad Certificadora	
Válido desde	30 años	Configurar en el template
Hasta		
Hasta	La utilizacion de este certificado esta sujeta a las politicas de certificado (CP) y practicas de certificacion (CPS) establecidas por Certinet S.A., y disponibles publicamente en www.certinet.cl.	

Detalles		
Versión:	V3	
Número de Serie	Asignado por la máquina. Debe cumplir que sean series únicas.	
Algoritmo de firma	SHA256 RSA	
Algoritmo Hash de firma	SHA256	
Emisor	CN = Certinet S.A. Raíz Autoridad Certificadora	
	E = ca_certinet@certinet.cl	Revisar alcances de éste dato
	O = Certinet S.A.	
	C = CL	
	~~OU = N/A~~	
Válido desde	20 Años	
Válido Hasta		
Sujeto:	CN = Certinet S.A. Raíz Autoridad Certificadora	
	E = ca_certinet@certinet.cl	
	O = Certinet S.A.	
	C = CL	
	~~OU = N/A~~	
Cláve Pública RSA (2048 Bits)	Es generada por el sistema	
Identificador de clave de entidad emisora	Generado por sistema	Id. de clave=15 24 fc 87 7f 07 c4 bc 29 b3 12 74 b9 ae 7f e7 fa 6a 1d 95
Identificador de clave del titular	Generado por sistema	
Uso de la clave	Firma de certificados (04)	
Directiva de Certificados	[1]Directiva de certificados:	
	Identificador de directiva=1.3.6.1.4.1.52428.100	OID
	[1,1]Información de certificador de directiva:	
	Id. de certificador de directiva=CPS	
	Certificador:	
	https://www.certinet.cl/CP	
	[1,2]Información de certificador de directiva:	
	Id. de certificador de directiva=Aviso de usuario	
	Certificador:	
	Referencia de aviso:	
	Organización=Certinet S.A.	
	Número de aviso=1	
	Texto de aviso=La utilizacion de este certificado esta sujeta a las politicas de certificado (CP) y practicas de certificacion (CPS) establecidas por Acepta.com, y disponibles publicamente en www.certinet.cl.	
Nombre Alternativo del Emisor	Otro nombre:	http://www.guiadigital.gob.cl/sites/default/files/reglamento_ley19799__documento_electronico.pdf
	1.3.6.1.4.1.8321.1=16 0a 39 39 35 33 32 38 33 30 2d 35	Página 18
Nombre Alternativo del Titular	Otro nombre:	http://www.guiadigital.gob.cl/sites/default/files/reglamento_ley19799__documento_electronico.pdf
	1.3.6.1.4.1.8321.1=16 0a 39 39 35 33 32 38 33 30 2d 35	Página 18
Restricciones básicas	Tipo de asunto=Entidad de certificación (CA)	
	Restricción de longitud de ruta=Ninguno	
algoritmo de identificación	SHA1	
Huella digital	Es generada por el sistema	

Ruta de Certificación		
	Certinet S.A. Raíz Autoridad Certificadora	

7.3.4.2 Certificado Intermedio.

General		**Observaciones**
Este certificado está destinado a los siguientes propósitos:	OID	
	Todas las directivas de la aplicación	
	Otros..	
Emitido para:	Certinet S.A. Autoridad de Sellado de Tiempo	
Emitido Por:	Certinet S.A. Raíz Autoridad Certificadora	
Válido desde	20 años	
Hasta		
Declaración del emisor	La utilizacion de este certificado esta sujeta a las politicas de certificado (CP) y practicas de certificacion (CPS) establecidas por Certinet S.A., y disponibles publicamente en www.certinet.cl.	

Detalles		
Versión:	V3	
Número de Serie	Es generado por sistema	
Algoritmo de firma	sha256RSA	
Algoritmo Hash de firma	sha256	
Emisor	CN = Certinet S.A. Raiz Autoridad Certificadora	
	E = ca_certinet@certinet.cl	
	O = Certinet S.A.	
	C = CL	
	~~OU = N/A~~	
Válido desde	20 años	
Válido Hasta		
Sujeto:	CN = Certinet S.A. Autoridad de Sellado de Tiempo	
	E = ca_certinet@certinet.cl	
	O = Certinet S.A.	
	C = CL	
	~~OU = N/A~~	
Clave Pública RSA (2048 Bits)	Es generada por el sistema	
Identificador de clave entidad emisora	Es generada por el sistema	
Identificador de clave del Titular	Es generada por el sistema	
Uso de la clave	Firma de certificados, Firma CRL sin conexión, Firma de lista de revocación de certificados (CRL) (06)	
Directivas del certificado	[1]Directiva de certificados:	
	Identificador de directiva=1.3.6.1.4.1.52428.100	Copiar OID
	[1,1]Información de certificador de directiva:	
	Id. de certificador de directiva=CPS	
	Certificador:	
	https://www.certinet.cl/CP	Es el mismo que en certificado raiz
	[1,2]Información de certificador de directiva:	
	Id. de certificador de directiva=Aviso de usuario	
	Certificador:	
	Referencia de aviso:	
	Organización=Certinet S.A.	
	Número de aviso=1	
	Texto de aviso=La utilizacion de este certificado esta sujeta a las politicas de certificado (CP) y practicas de certificacion (CPS) establecidas por Certinet S.A., y disponibles publicamente en www.Certinet.cl.	
Nombre Alternativo del Emisor	Otro nombre:	http://www.guiadigital.gob.cl/sites/default/files/reglamento_ley19799_documento_electronico.pdf
	1.3.6.1.4.1.8321.1=16 0a 39 39 35 33 32 38 33 30 2d 35	Página 18
Nombre Alternativo del Titular	Otro nombre:	http://www.guiadigital.gob.cl/sites/default/files/reglamento_ley19799_documento_electronico.pdf
	1.3.6.1.4.1.8321.1=16 0a 39 39 35 33 32 38 33 30 2d 35	Página 18
Restricciones básicas	Tipo de asunto=Entidad de certificación (CA)	
	Restricción de longitud de ruta=Ninguno	
Algoritmo de identificación	SHA1	
Huella Digital	Es generada por el sistema	

Ruta de Certificación		
	Certinet S.A. Raíz Entidad Certificadora	
	Certinet S.A. Autoridad de Sellado de Tiempo	

7.3.4.3 Certificado Certinet TSA.

General		Observaciones
Este certificado está destinado a los siguientes propósitos:	Permite que los datos sean firmados con la hora actual	
Emitido para:	Certinet S.A. Emisor Sello de Tiempo	
Emitido Por:	Certinet S.A. Autoridad de Sellado de Tiempo	
Válido desde	18 años	
Hasta		
Declaración del emisor	Certificado emisor de sello de tiempo. Resolucion exenta xxxxx, dia/mes/año, Subsecretaria de Economia, Fomento y Reconstruccion.	Agregar fecha de resolución

Detalles		
Versión:	V3	
Número de Serie	Es generado por sistema	
Algoritmo de firma	sha256RSA	
Algoritmo Hash de firma	sha256	
EMISOR	CN = Certinet S.A. Autoridad de Sellado de Tiempo	
	E = Certinet@certinet.cl	
	O = Certinet S.A.	
	C = CL	
Válido desde	20 años	
Válido Hasta		
SUJETO	CN = Certinet S.A. Emisor Sello de Tiempo	
	E = Certinet@certinet.cl	
	O = Certinet S.A.	
	C = CL	
Cláve Pública RSA (2048 Bits)	Es generado por sistema	
Identificador de clave entidad emisora	Es generado por sistema	
Identificador de clave del Titular	Es generado por sistema	
Directivas del certificado	[1]Directiva de certificados:	
	Identificador de directiva=1.3.6.1.4.1.6891.200	OID
	[1,1]Información de certificador de directiva:	
	Id. de certificador de directiva=CPS	
	Certificador:	
	https://ENLACE CP TSA CERTINET	Enlace Prácticas TSA
	[1,2]Información de certificador de directiva:	
	Id. de certificador de directiva=Aviso de usuario	
	Certificador:	
	Referencia de aviso:	
	Organización=Certinet S.A.	
	Número de aviso=3	
	Texto de aviso=Certificado emisor de sello de tiempo. Resolucion exenta xxxxx, dia/mes/año, Subsecretaria de Economia, Fomento y Reconstruccion.	Agregar Resolución exenta del ministerio
Nombre Alternativo del Emisor	Otro nombre:	http://www.guiadigital.gob.cl/sites/default/files/reglamento_ley19799__documento_electronico.pdf
	1.3.6.1.4.1.8321.1=16 0a 39 39 35 33 32 38 33 30 2d 35	Página 18
Nombre Alternativo del Titular	Otro nombre:	http://www.guiadigital.gob.cl/sites/default/files/reglamento_ley19799__documento_electronico.pdf
	1.3.6.1.4.1.8321.1=16 0a 39 39 35 33 32 38 33 30 2d 35	Página 18
Acceso a la información de entidad emisora	[1]Acceso a información de autoridad	
	Método de acceso=Protocolo de estado de certificado en línea (1.3.6.1.5.5.7.48.1)	OID Firma Avanzada
	Nombre alternativo:	
	Dirección URL=https://OSCP_SELLO_TIEMPO_Certinet	
Puntos de distribución CRL	[1]Punto de distribución CRL	
	Nombre del punto de distribución:	
	Nombre completo:	
	Dirección URL=https://CRL_SELLO_TIEMPO_CERTINET	
Uso Mejorado de Claves	Impresión de fecha (1.3.6.1.5.5.7.3.8)	OID TSA
Algoritmo de identificación	SHA1	
Huella Digital	Es generado por sistema	

Ruta de Certificación		
	Certinet S.A. Raíz Autoridad Certificadora	
	Certinet S.A. Autoridad de Sellado de Tiempo	
	Certinet S.A. Emisor Sello de Tiempo	

8 Obligaciones.

8.1 Obligaciones de la Autoridad de Sello de Tiempo.

La TSA:

- Es responsable por aplicar lo expuesto en este documento y en el documento complementario de Prácticas de Sello de Tiempo de Certinet.
- Debe velar porque las Políticas de Sellado de Tiempo se cumplan, a pesar de que muchas de las actividades del proceso puedan ser realizadas por otros.
- Es responsable de cumplir con los requisitos adicionales aplicados a su actividad, incluidas las directrices de la Entidad Acreditadora.
- Debe emplear todos los medios necesarios para asegurar la compatibilidad total entre sus servicios como Autoridad de Sellado de Tiempo y este documento.
- Es responsable hacia ambos, el Titular/Usuario y el tercero que confía.
- En caso de subcontratar en el futuro alguno de los servicios, asegurará que los contratistas mantengan un fiel cumplimiento de estas políticas, así como de las prácticas de Time Stamping.
- Se compromete a utilizar sistemas y productos fiables que estén protegidos contra toda alteración y que garanticen la seguridad técnica y criptográfica de los procesos de sello de tiempo a los que sirven de soporte.
- Garantiza el acceso permanente a los servicios de sellado de tiempo, donde la precisión del tiempo UTC, que está incluido en los sellos, se asegura con una desviación máxima 1 segundo.
- Garantiza que no exista ningún procesamiento de datos personales asociado a la operación de la Autoridad de Sellado de Tiempo y se garantiza un nivel de servicio superior al 95% que permite dar el cumplimiento a las normas técnicas.

Para un mayor detalle, remítase a lo especificado en la Declaración de Prácticas de sello de tiempo de Certinet.

8.2 Identificación y Autentificación de Titular/Usuario:

Con el fin de dar fiel cumplimiento a la Ley 19.799, Certinet, será responsable de autentificar fidedignamente a los Titulares/Usuarios, en a lo menos los siguientes aspectos:

- Identificar y verificar en forma inequívoca a los solicitantes de un Certificado, de conformidad al procedimiento establecido en ley 19.799.
- Registrar y custodiar los antecedentes requeridos a los solicitantes que permitan una identificación plena de los mismos.
- Aprobar o denegar las Solicitudes de Emisión de Certificados.
- Entregar al Titular/Usuario su Certificado o dar las instrucciones para su retiro.
- Recibir y Cursar las Solicitudes de revocación o suspensión de Certificados.

- Conservar en forma segura, la información recibida en el proceso de emisión, suspensión y revocación de un certificado por el período que la Ley de Firma Electrónica y su Reglamento indiquen.

8.3 Obligaciones de los subscriptores.

El Titular/Usuario debe verificar que el token de time-stamping se ha firmado de manera correcta y comprobar en la CRL el estado del certificado de la TSA.

Además, debe conocer las normas estipuladas en las políticas y prácticas de certificación de sello de tiempo de Certinet, así como el propósito y alcance de un sello de tiempo obtenido en Certinet o en algún Prestador de Servicios de Sellos de Tiempo acreditado.

Para un mayor detalle, remítase a lo especificado en la Declaración de Prácticas de sello de tiempo de Certinet.

8.4 Obligaciones de las partes que confían.

Las partes que confían deben tener conocimiento del alcance y uso del sello de tiempo recibido, como de las normas legales que sigue el Proveedor de Servicios de Certificación, además será responsable de verificar la firma del sello de tiempo, comprobando el estado del certificado de la TSA y su periodo de validez. Adicionalmente deberán dar aviso a la TSA de cualquier situación anómala ya sea en el servicio o en los sellos de tiempo emitidos por la TSA.

Para un mayor detalle sobre la verificación de sello de tiempo, remítase a lo especificado en la Declaración de Prácticas de sello de tiempo de Certinet.

9 Responsabilidades.

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, Ley 19.628 y Ley 19.496 de Chile, así como la Ley N° 27269, Ley 29733. Certinet, como proveedor de servicios de Sello de Tiempo, adhiere además a los estándares internacionales que rigen esta actividad, siendo ellos los documentos RFC 3628, RFC 3161 y su equivalente ETSI 102 023.

Para un mayor detalle del cumplimiento de las responsabilidades generales, remítase a lo especificado en la Declaración de Prácticas de sello de tiempo de Certinet.

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. Las responsabilidades asumidas por Certinet como TSA, se encuentran declaradas en sus prácticas de sello de tiempo y en los contratos o

acuerdos de suscripción. Para asumir éstas, Certinet cuenta con un seguro de responsabilidad civil en conformidad al artículo 14 de Ley 19.799 para Chile.

Para un mayor detalle de las responsabilidades legales, remítase a lo especificado en la Declaración de Prácticas de sello de tiempo de Certinet.

9.3 Fuerza Mayor.

Certinet queda exenta de responsabilidad en caso de pérdida o perjuicio, siendo esto el resultado de un evento de fuerza mayor que le impida proveer los servicios de Time-Stamp. Para un mayor detalle, remítase a lo especificado en la Declaración de Prácticas de sello de tiempo de Certinet.

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 información establecida en este documento se completa con el documento de prácticas de sello de tiempo que detalla la implementación de los controles que son necesarios para cumplir con esta política de sellado de tiempo, así como políticas, normativas, procedimientos, ya sean estos operacionales y/o técnicos para uso interno de Certinet, que garantizan la fiabilidad y la confianza del servicio de sellos de tiempo.

En particular Certinet, como TSA establece que ha realizado:

- Una determinación de activos y riesgo asociado a c/u de los activos relevantes que participan en los servicios de la TSA.
- Una planificación para mitigar los riesgos detectados en el análisis de riesgo, el cual es controlado por un comité de seguridad, el que define los cursos de acción y aprueba las mejoras a los controles implantados.
- Una política y práctica que permita proveer los servicios de su TSA, así como las modificaciones a estos documentos que han sido formalmente aprobadas.
- La publicación hacia la comunidad de la información relevante asociada a este servicio tales como las condiciones bajo las que se provee los servicios de la TSA.

Además, se detallan los mecanismos y procedimientos establecidos para cumplir con las obligaciones y responsabilidades, control de seguridad, así como modificaciones y planes de mejora, elementos de información de contacto, características técnicas del servicio de sello, leyes y estándares, entre otros que constituyen el funcionamiento de la TSA, las que deben ser contempladas por todas las organizaciones externas incluyendo las políticas y prácticas de sello de tiempo aplicables. Para un mayor detalle, remítase a lo especificado en la Declaración de Prácticas de sello de tiempo de Certinet.

10.1.2 Declaración de divulgación de TSA.

LA TSA de Certinet entrega como parte de estas políticas su información de contacto a los Titulares/Usuarios y terceros, da a conocer la política que rige su operación incluyendo en esta última: el algoritmo de hash utilizado, vigencia de la firma, la precisión del tiempo registrado en cada uno de los TST emitidos, responsabilidades y obligaciones de las partes que participen del proceso asociado al servicio de la TSA, información que permita verificar la validez del TST, el periodo de retención de los logs de eventos, normativa legal aplicada, limitación de responsabilidades, solución de conflicto entre las partes, resolución que aprueba la operación como Autoridad de sello de Tiempo emitida por el Ministerio de Economía.

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 pública 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 que se evidencia en el documento asociado al proceso.

10.2.2 Protección de la llave privada de la TSU.

Certinet cuenta con niveles de seguridad del HSM donde se almacena la clave bajo control, a fin de asegurar la confidencialidad e integridad.

10.2.3 Distribución de la llave pública.

El certificado de la TSA incluye su clave pública, la cual se distribuye a través de la página web de Certinet. Este certificado digital utilizado por la TSA es generado por la PSC de Certinet, de acuerdo con las políticas y prácticas de certificación inspeccionadas por el Ministerio de Economía para esta PKI.

10.2.4 Reemisión de llaves de la TSU.

Por motivo de seguridad y 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.

10.2.5 Termino del ciclo de vida de la llave del TSU.

La llave privada de la TSU debe ser reemplazada al momento de su expiración o ante un evento de seguridad que vulnere dicha llave. La TSU de Certinet rechazará cualquier intento de emitir un sello de tiempo cuando esta llave privada haya expirado.

El detalle del proceso de término del ciclo de vida de la llave de la TSU se encuentra especificado en la Declaración de Prácticas de sello de tiempo de Certinet.

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 de dicho ciclo

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.

La TSA de Certinet declara utilizar una fuente fiable de tiempo que considera el SHOA con una desviación máxima de 1 segundo.

11 Gestión de la TSA y operaciones.

11.1 Gestión de la seguridad.

La TSA de Certinet desarrollará una administración activa de la seguridad que permitirá administrar los riesgos identificados en el análisis de riesgo.

En particular:

a) Certinet declara que su TSA es responsable por todos los aspectos asociados a la provisión de servicios de sello de tiempo y no subcontrata los servicios de sello de tiempo.

b) Todo su personal tiene acceso a sus prácticas y políticas de sello de tiempo.

d) 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 plan de administración de riesgos.

e) Certinet declara que los procedimientos y controles operacionales de la TSA se encuentran documentados, se mantienen y se implementan.

f) Certinet no subcontrata los servicios de sello de tiempo.

Para mayor detalle remitirse a lo especificado en la Declaración de Prácticas de sello de tiempo de Certinet.

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 siguiendo una metodología y herramientas basadas en la norma ISO 27001, para el cual se hace un levantamiento de los activos. Todo lo anterior se encuentra documentado y clasificado, siendo esta documentación revisada de forma periódica en auditorias.

Para mayor detalle remitirse a lo especificado en la Declaración de Prácticas de sello de tiempo de Certinet.

11.3 Seguridad del personal.

11.3.1 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, El detalle de esto lo puede encontrar en la Declaración de Prácticas de Sello de Tiempo de Certinet.

11.3.2 Requerimientos de contratación.

- ✓ Firmar un acuerdo de confidencialidad, tal como es especificado en la Declaración de Prácticas de Sello de Tiempo de Certinet.
- ✓ Entrega de documentación Organizacional al personal
- ✓ Control de cumplimiento
- ✓ Finalización de contratos

11.4 Seguridad física y ambiental.

La seguridad física y ambiental se detalla en la Declaración de Prácticas de Sello de Tiempo de Certinet.

11.4.1 Emisión y administración de sellos de tiempo.

La Emisión de sellos de tiempo, es realizada por el personal autorizado, así como su administración será de acuerdo con lo especificado en la Declaración de Prácticas de Sello de Tiempo de Certinet, ello a fin de evitar daños, pérdidas, interrupción o compromiso de los activos críticos de la TSA.

11.4.2 Suspensión y Revocación

Certinet se ajusta a las CP y CPS FEA Certinet, específicamente los párrafos 4.6 de la Política y 4.6 de las Prácticas de Certificación.

11.4.3 Control de los módulos criptográficos.

El control de los módulos criptográficos se llevará a cabo para evitar la pérdida de información y están de acuerdo con lo especificado en la Declaración de Prácticas de Sello de Tiempo de Certinet y el documento de "Gestión del ciclo de vida de las llaves".

11.5 Controles físicos y ambientales.

11.5.1 Data Center y Oficinas Centrales.

Los sistemas e infraestructura del Servicio de Emisión de sellos se encuentran alojados en AZURE que cumple con las exigencias solicitadas por el Ministerio.

Respecto a Certinet ella cuenta con accesos vigilados, área de recepción, así como control de visitas y acceso biométrico del personal. Para más información remítase a lo especificado en la Declaración de Prácticas de Sello de Tiempo de Certinet.

11.5.2 Seguridad Física Data Center.

Certinet opera con Data Centers seguros y confiables que cuentan con niveles de protección y solidez que exige el Ministerio, suministrados por MICROSOFT AZURE.

11.6 Gestión de las operaciones.

La TSA de Certinet establece que su sistema y componentes son fiables, ya que se encuentran operados de manera correcta con un riesgo mínimo de falla en la emisión, el control de sellos de tiempo, el manejo correcto de los medios, el control y planificación de los sistemas, control y reporte de incidentes. Los componentes del sistema de la TSA son protegidos de virus, código malicioso e incorporación de código no autorizado.

Respecto al manejo de medios y seguridad, Certinet declara un apropiado tratamiento de sus activos a través de la realización de un análisis anual de riesgo riesgos basados en la norma ISO 27001, el cual genera como parte de su preparación la lista de activos de la TSA, su nivel de protección, así como los procedimientos adicionales a seguir para minimizar su riesgo.

Para el 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 para que realicen correcciones oportunas.

Además, considera los siguientes roles de confianza que manejan las operaciones:

- Administrador de Sistemas.
- Administrador de Seguridad.
- Responsable de formación, soporte y comunicación.
- Responsable de Seguridad.
- Responsable de Documentación.

En cuanto a la Planificación de la capacidad, se debe mantener un manejo de la capacidad para la demanda, monitoreando y proyectando de acuerdo con los futuros requerimientos, de manera que la capacidad de proceso como la de almacenamiento siempre sean las adecuadas.

Para efectuar esto, Certinet cuenta con un procedimiento formal de gestión de capacidad de sus instalaciones. Respecto a los procedimientos operacionales y responsabilidades, Certinet cuenta con la operación del servicio de Sello de Tiempo de la TSA, el que opera de manera independiente de otros servicios provistos por la PSC; siendo éstas desarrolladas por el personal confiable como se encuentra definido en la estructura de la PSC de Certinet y en su Declaración de Prácticas de Sello de Tiempo de Certinet.

11.7 Gestión de acceso a los sistemas.

La TSA de Certinet, asegura que el acceso a su sistema (hardware, software y datos) se encuentra protegido compartiendo las medidas de seguridad físicas que dan protección al sistema en un entorno de confianza y está limitado al personal autorizado. Los administradores de Certinet realizan un monitoreo continuo para detectar intentos o accesos no autorizados a los activos de la TSA.

Es por ello por lo que se cuenta con Firewalls, Administración de usuarios, Restricciones de acceso a la información y sistemas, un control apropiado del personal autorizado, Logs de las operaciones.

Para mayor detalle remítase a lo especificado en la Declaración de Prácticas de Sello de Tiempo de Certinet.

11.8 Mantenimiento e Implementación de sistemas de confianza.

En la TSA de Certinet se asegura que el sistema y productos están protegidos contra modificaciones no autorizadas, es por ello por lo que se establece monitorear y registrar cada cambio en los sistemas.

Para cualquier cambio en los sistemas se lleva a cabo un análisis de requerimientos de seguridad, procedimientos de control de cambio para nuevas versiones y la generación de las llaves siempre se lleva a cabo dentro del entorno de confianza, por personal critico autorizado.

11.9 Compromiso de los servicios de TSA.

La TSA de Certinet declara que, ante cualquier compromiso de los servicios de sello de tiempo, se harán efectivos los procedimientos correspondientes al plan de continuidad de Certinet. Si este compromiso afecta a la llave de firma de la TSU o pérdida de precisión de su reloj, se declarará un evento de seguridad y se informará directamente o a través de su sitio web a sus Titulares/Usuarios y terceros que en ella confía, dicha información del evento. Ante los eventos antes mencionados, la TSA de Certinet no emitirá nuevos TST hasta superar el compromiso declarado Para mayor detalle remítase a lo especificado en la Declaración de Prácticas de Sello de Tiempo de Certinet.

11.10 Cese de una TSA.

En el momento en que Certinet vaya a descontinuar sus operaciones como Autoridad de sello de tiempo, procederá a comunicar del cese de sus funciones con la debida antelación a todas las partes involucradas con sus servicios de sello de tiempo ya sean Titulares/Usuarios, terceros de confianza y autoridades de sello de tiempo acreditadas. Además, la TSA procederá revocar los certificados de la TSU y transferir los datos de sus sellos de tiempo a otro prestador de servicios, en la fecha en que el cese se produzca. En el caso de las claves y copias de respaldo de la TSA de Certinet, estas deben ser borradas y destruidas, de manera que estas no puedan ser recuperadas, de acuerdo con lo especificado en la Declaración de Prácticas de Sello de Tiempo de Certinet. En el procedimiento para el término de actividades, se dispondrá de los costos necesarios para los requerimientos indicados.

11.11 Cumplimiento de requerimientos legales.

Certinet como Autoridad de sello de tiempo, actúa en conformidad con la Ley N° 19.799 y 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 gestión y operación de servicios se encuentra regulada por la Entidad Acreditadora del Ministerio de Economía 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 de divulgación, 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. A menos que sea solicitada por él mismo o por orden judicial u otro requisito legal, de acuerdo con lo especificado en la Declaración de Prácticas de Sello de Tiempo de Certinet.

11.12 Registro de información relativa a las operaciones del servicio de sello de tiempo.

La TSA de Certinet debe mantener registros de la información relevante, concerniente a su operación. Estos registros corresponden a la información personal de los Titulares/Usuarios que se ha recolectado y se encuentra protegida de acuerdo con la Política de Privacidad de datos personales publicados por Certinet en su sitio web (https://www.certinet.cl/politicadeprivacidad), tal como se detalla en la Declaración de Prácticas de Sello de Tiempo de Certinet.

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. 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.

11.13 Organización.

La Autoridad de Sellado de Tiempo es un servicio adicional que se encuentra soportada por la PSC de Certinet, la cual se encuentra acreditada en su operación por la Entidad Acreditadora del Ministerio de Economía. La TSA de Certinet cumple con:

- Sus políticas y procedimientos bajo los que opera no incluyen cláusulas discriminatorias.
- 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 en Chile.
- Cuenta con un seguro de responsabilidad civil, de la Ley 19799, articulo 14, 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 Ministerio de Economía, cuenta con un personal calificado para la prestación de sus servicios, así como realiza una capacitación continua de este personal.
- 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 y 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 y 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) y se almacena en un servidor ubicado en la zona segura de Certinet. 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 nivel 3 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.

Se debe tener presente que, al momento del chequeo de validez de los TST, por parte de un tercero que confía, el certificado de firma de la TSU debe ser válido y no se encuentra revocado, ya que la validez del TST es cierta sólo para el momento en que se efectúa dicho chequeo, pues en un tiempo posterior puede existir un compromiso de la llave privada de la TSU de Certinet que invalida la llave de firma y por ende al TST emitido. La TSA de Certinet asegura que hash incluido en su TST corresponde al enviado por el Titular/Usuario en su request. Para mayor detalle de las consideraciones de seguridad, remítase a lo especificado en la Declaración de Prácticas de Sello de Tiempo de Certinet

12.8 Auditorías

CertiNet, realiza a lo menos una auditoría al año a sus procedimientos y procesos, además se somete a un proceso de inspección anual independiente que realiza la Subsecretaría de Economía y Empresas de Menor Tamaño para mantener nuestra acreditación como Prestador de Servicios de Certificación calificado.

Debe incluirse en el plan de auditoría la revisión de las garantías, seguros y la concordancia de las políticas de certificado, prácticas de certificación con los procedimientos operacionales.

El detalle del plan de auditoría se encuentra definido en el documento "01_modelo operacional_ca_tsa_2024", párrafo 3.3.8.

Está cláusula se encuentra también en nuestra CPS-FEA CertiNet en la sección 2.6.

El resultado de las auditorías debe ser presentado al Comité de Riesgo Operacional y Seguridad de la Información.

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.

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.

13.2 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.