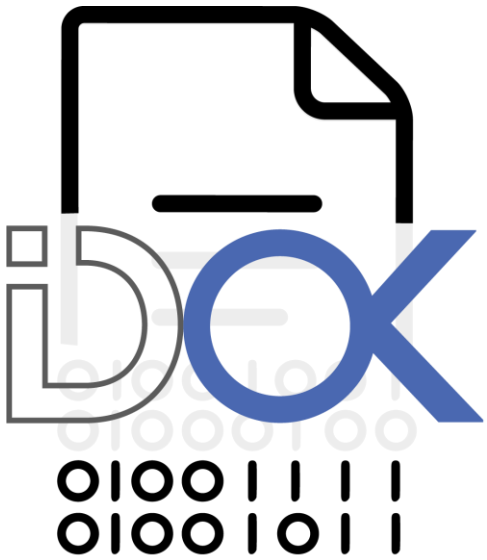

PO02 – DECLARACIÓN DE PRÁCTICAS DE SELLO DE TIEMPO

Resumen

Documento conteniendo la Declaración de Prácticas de Sello de Tiempo

1. Información del Documento

HISTORIA DEL DOCUMENTO

Nombre del Documento:	PO02 Declaración Prácticas de Sello de Tiempo.
Creado por:	Jorge Pizarro

Responsable del Documento:	Oficial de Seguridad	**Fecha de Creación:**	26 de Septiembre de 2018
Aprobado por:		**Fecha de Aprobación:**	

CONTROL DE VERSIONES

Versión	Fecha de Vigencia	Aprobación	Comentario
001	26 de Septiembre de 2018	Jorge Pizarro	Creación del documento
002	14 de Julio de 2020	Jorge Pizarro	Revisión del documento
003	26 de marzo de 2021	Jorge Pizarro	Revisión del documento

2. Objetivos

Comprobar que la Política y Prácticas de Certificación de Sello de Tiempo contiene los aspectos mínimos dispuestos por la Ley y su Reglamento.

3. Introducción

La Política de Sello de Tiempo (PST) es el conjunto de reglas que definen la forma en que opera el servicio de Sello de Tiempo de modo de entregar la confianza necesaria a sus usuarios.

Para cumplir con lo anteriormente expuesto, la PST expone en el presente documento las políticas que rigen al servicio en cada una de sus fases: al gestionar la información relacionada con el enrolamiento del Sello de Tiempo; durante la verificación del Sello de Tiempo; cuando se requiera verificar la vigencia de la llave privada a través de la CRL u OCSP; o si la llave privada llega a ser comprometida.

4. Alcance

El alcance de la Política de Sello de Tiempo (PST) detalla las condiciones de los servicios de certificación que presta IDOK para la emisión de sus certificados de la Autoridad de Sello de Tiempo (TSA: Time Stamping Authority).

5. Referencias y glosario

La presente declaración de Política de Sello de Tiempo se ha generado siguiendo las especificaciones de documentos y referencias que se indican a continuación:

- RFC 3628 “Policy Requirements for Time-Stamping Authorities”.
- RFC 3161 “Internet X.509 Public Key Infrastructure Time-Stamping Protocol (TSP)”.
- ETSI TS 102 023 “Electronic Signatures and Infrastructures (ESI) Policy Requirements for Time-Stamping Authorities”.
- Guía de Evaluación: Procedimiento de Acreditación Prestadores de Servicios de Certificación de Servicios de Certificación de Sello de Tiempo” en su versión 1.0 Ministerio de Economía, Fomento y Turismo del Gobierno de Chile.
- NCh27002.Of2009 Tecnología de la información – Código de práctica para la gestión de seguridad de la información.
- NCh2829.Of.2003 Tecnología de la Información – Requisitos de Seguridad para Módulos Criptográficos.

- NCh2832.Of2003 Tecnología de la información – Protocolos operacionales de infraestructura de clave pública LDAPv2 para Internet X.509.
- RFC 2559 BOEYEN, S. et al., “Internet X.509 Public Key Infrastructure. Operational Protocols LDAPv2”, abril 1999.
- RFC 3377 LDAPv3: Technical Specification, September 2002, Lightweight Directory Access Protocol (v3): Technical.

Glosario

- **Hashing**: Son una secuencia de caracteres que representan un documento. Esta secuencia es de tamaño fijo y reducido. La principal característica es que es una representación única del documento original y que si existe una alteración mínima el resultado es absolutamente distinto y deja de representar al documento original.
- **Tercera parte**: receptor de un token de sello de tiempo quien confía en este token de sello de tiempo.
- **Suscriptor**: entidad requiriendo el servicio provisto por una TSA y cual está explícitamente o implícitamente de acuerdo a sus términos y condiciones.
- **token de sello de tiempo**: objeto de datos
- **time-stamp token**: objeto asociado a la representación de un dato en un lapso de tiempo concreto, estableciendo así evidencia de que el dato existía antes de ese tiempo. Los token de sellado de tiempo deben emitirse de acuerdo al RFC 3161 “Internet X.509 Public Key Infrastructure Time Stamp Protocol (TSP)”.
- **autoridad de sellado de tiempo**: autoridad cual emite token de sellado de tiempo.
- **Declaración de divulgación de la TSA**: conjunto de declaraciones sobre las políticas y prácticas de la TSA que particularmente requieren énfasis o de la divulgación a los suscriptores y terceras partes de confianza,por ejemplo para cumplir con requisitos regulatorios.
- **Declaración de prácticas de la TSA**: declaración de prácticas que una TSA emplea para la emisión de tokens de sello de tiempo.
- **Sistema TSA**: composición de productos de tecnologías de la información y componentes organizados para soportar la provisión del servicio de sellado de tiempo.
- **Políticas de sellado de tiempo**: conjunto de reglas que indican la aplicabilidad de un token de sello de tiempo para una comunidad particular y/o clase de aplicación con requerimiento de seguridad comunes.
- **Unidad de sellado de tiempo**: conjunto de hardware y software que es administrado como una unidad y tiene una sola clave de firma para el token de sello de tiempo activo a la vez.

- **Coordinated Universal Time (UTC)**: escala de tiempo basada sobre la segundo como se define en las recomendaciones ITU-R TF.460-5 [TF.460-5].

  NOTA: para propósitos más prácticos UTC es equivalente al tiempo solar en el primer meridiano. Más específicamente, UTC es el compromiso entre el altamente estable tiempo atómico (Temps Atomique International - TAI) y tiempo solar derivado de la rotación irregular de la tierra.

Para el propósito del presente documento, las siguientes abreviaciones aplican:

TSA Autoridad de Sellado de Tiempo
TSU Unidad de Sellado de Tiempo
TST Token de Sellado de Tiempo
UTC Hora Universal Coordinada

6. Antecedentes

Las prácticas de Sello de Tiempo aquí descritas establecen el ciclo de vida de los servicios que provee IDoK, que como antes se ha mencionado incluye 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 a nivel de sistemas como de personal, que en base a sus buenas prácticas dan seguridad y confianza a los sellos de tiempo y servicios provistos por IDoK.

7. Aplicabilidad y Comunidad de Usuarios

Los servicios de sello de tiempo emitidos por la Autoridad de Sellado de IDoK, están insertos en una infraestructura en que se relacionan distintas entidades, las cuales se indican a continuación:

a. Autoridad de Certificación: Para el servicio de sello de tiempo (TSS), los certificados de las unidades de sello de tiempo (TSU) son entregados por la Autoridad de Certificación (CA). Estos certificados permiten a las terceras partes confíen en la firma, al identificar a la autoridad de sello de tiempo (TSA).
b. Autoridad de sello de tiempo: Es la organización que opera y controla el funcionamiento de la sincronización del tiempo, emisión y otros procesos específicos de sellado de tiempo de un documento o dato, es decir la TSA tiene como obligación la provisión de los servicios de sellado de tiempo.

c. Suscriptores: Son entidades que pueden ser individuos, empresas, sistemas y otro tipo, que solicitan la emisión de sello de tiempo de la TSA y están de acuerdo con sus términos de uso descritos en las políticas y prácticas de sello de tiempo declaradas por la TSA.
d. Tercera parte que confía: Son entidades que pueden ser individuos, empresas, sistemas u otro tipo, que son receptores de un sello de tiempo, generado por una TSA bajo las políticas y prácticas que ella ha definido, y actúan de acuerdo al resultado de la verificación obtenida para el sello de tiempo recibido. Una tercera parte que confía no necesariamente es un suscriptor de la TSA. Para realizar la verificación de los sellos de tiempo emitidos por la TSA, la parte que confía debe contar con mecanismos que le permitan validar si se trata de un sello de tiempo auténtico.
e. Entidad Acreditadora: La comunidad de usuarios requiere de un organismo independiente y de confianza que acredite que las políticas y prácticas de la TSA, son coherentes con las necesidades del sello de tiempo y que la TSA cumple cabalmente con dichas políticas y prácticas. Por ejemplo, para los sellos de tiempo, la entidad acreditadora es el Ministerio de Economía; para los certificados válidos en el ámbito tributario la entidad acreditadora es el Servicio de Impuestos Internos.

7.1. APLICABILIDAD

Los sellos de tiempo emitidos por IDoK 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.

a. 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”.

b. Usos prohibidos

   Los sellos de tiempo emitidos por IDoK, 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 a la normativa vigente. Cualquier uso diferente a los indicados está expresamente prohibido.

7.2. ESTRUCTURAS DE LOS SELLOS DE TIEMPO

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

Cumplimiento

La TSA referencia el OID de las políticas de sello de tiempo, definidas por IDoK, 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 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, Fomento y Turismo.

Detalles 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:

Dirección e-mail: soporte@idok.cl
Dirección: Av. Manuel Barros Borgoño 110 of. 0110, Providencia. Santiago .
Número de teléfono: (562) 2582 7435

8. Obligaciones y Responsabilidades

8.1. OBLIGACIONES DE LA TSA

a) En general IDoK, en su calidad de Autoridad de Sello de Tiempo se obliga a:

Realizar sus operaciones y proveer todos los servicios de Time-Stamping de acuerdo a lo dispuesto en esta política, así como en la presente Declaración de Prácticas de sello de tiempo.

Para ello IDoK declara que ha desarrollado:

- Un análisis de riesgo de sus activos
- Un sistema de SGSI (Sistema de Gestión de Seguridad de la Información) a fin de mitigar los riesgos previamente detectados.
- Un seguimiento de la implantación de las medidas y controles propuestos por el SGSI

Definir en sus prácticas y política de sello de tiempo las obligaciones de los distintos actores del proceso.

Realizar una revisión periódica de las prácticas aquí descritas. Mantener actualizada estas prácticas y contar con la aprobación formal, ante cambios en las mismas, por parte del Comité de Seguridad.

Proveer a todos los suscriptores y terceros de confianza:

- La información de contacto.
- La política, la declaración de prácticas y los documentos relacionados a los servicios de sello de tiempo, garantizando el acceso a la versión mencionada.
- El algoritmo de hash utilizado como parte de las mismas políticas y prácticas publicadas.
- La vigencia de la raíz utilizada para la firma de sus sellos de tiempo.
- La precisión del tiempo utilizado como parte de las mismas políticas y prácticas publicadas.

- Las prohibiciones de uso de sus sellos de tiempo, como parte de las mismas políticas y prácticas publicadas.

- Las obligaciones tanto de los suscriptores como de los terceros de confianza, información contenida en las políticas y prácticas publicadas.
- Los mecanismos de verificación de los tokens emitidos por IDoK
- El periodo de permanencia de los log 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 de funcionamiento, emitida por la Entidad Acreditadora.

Mantener su llave privada bajo adecuadas medidas de seguridad, para evitar cualquier mal uso de esta, controlando el ciclo de vida de ella, así como también del hardware criptográfico. Tal como se indica en el punto “Administración del ciclo de vida de la llave”, incluida en este mismo documento.

Mantener un identificador único, para cada token de sello de tiempo emitido, así como el incluir una referencia a la política bajo la cual fue emitido; tal como se indica en el punto “Sello de tiempo” de este documento.

Mantener sincronizado el reloj de la TSU con la precisión de la fecha y la hora declarada con respecto al tiempo UTC.

Contar con la infraestructura requerida para prestar el servicio de sello de tiempo conforme al nivel de calidad comprometido.

Mantener los controles de seguridad física, de procedimiento y personales definidos para estos servicios, de acuerdo a lo comprometido en este documento.

Proporcionar antecedentes e información fidedigna al momento de emitir sellos de tiempo de IDoK de acuerdo con la información conocida en el momento de su emisión, y libres de errores de entrada de datos.

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.

Garantizar mediante revisiones y auditorías que todos los requerimientos de la TSA cumplen con los controles requeridos por la legislación aplicable, las políticas, prácticas y procedimientos internos.

Las obligaciones específicas, pertinentes al certificado de sello de tiempo emitido se detallan en las

b) Obligaciones de la TSA hacia sus suscriptores

La TSA de IDoK garantiza el acceso permanente a los servicios de sellado de tiempo, donde la precisión del tiempo UTC, que está incluido en los desviación máxima 1 segundo. La TSA de IDoK garantiza un nivel de servicio superior al 95%, sin considerar los procesos de mantenimiento de sistemas y equipos. Los procesos de mantenimiento técnicos son planificados anticipadamente, teniendo una duración determinada y se debe dar aviso a los suscriptores del servicio, utilizando los medios de difusión disponibles. La TSA de IDoK garantiza que no hay ningún procesamiento de datos personales asociado a la operación de la Autoridad de Sellado de Tiempo (TSA), a través de su política de privacidad de datos personales disponible en su sitio web.

c) Obligaciones del suscriptor

El suscriptor debe verificar que el token de time-stamping se ha firmado de manera correcta, confirmando que la llave privada de la TSA que firma dicho token se encuentra vigente – a través de la CRL o servicio OCSP - y que no ha sido comprometida. Conocer las normas estipuladas en las políticas y prácticas de certificación de sello de tiempo de IDoK, y asentir lo que allí se estipule en forma previa a la emisión de un sello de tiempo. Conocer el propósito y alcance de un sello de tiempo obtenido en IDoK o en algún Prestador de Servicios de Sellos de Tiempo acreditado, acorde a lo estipulado en las Políticas de sellos de tiempo definidas por IDoK.

d) Obligaciones de partes que confían

Las partes que confían deben verificar la firma del sello de tiempo, comprobando el estado del certificado de la TSA y su periodo de validez. Deberá verificar que la llave de la TSA no ha sido comprometida hasta el momento de la verificación, utilizando para ello la CRL publicada por IDoK. En el caso de la verificación de un sello de tiempo, después de la expiración del certificado de la TSA, se debe verificar que el número de serie del certificado de la TSA no se encuentra en la CRL, o determinar la validez del certificado de

la TSA en el momento que se generó el sello. Conocer el propósito y alcance de un sello de tiempo emitidos por IDoK o algún Prestador de Servicios de Sellos de Tiempo acreditado, acorde a lo estipulado en las Políticas de sellos de tiempo definidas por IDoK. Notificar o dar aviso sobre cualquier situación considerada anómala con respecto al servicio de sellado y/o a los sellos de tiempo emitidos, lo cual puede ser considerado como causa de revocación del mismo.

8.2. RESPONSABILIDADES

a. Responsabilidades Legales

IDoK 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 suscriptores o terceras partes que confían.

Los servicios de sellado de tiempo de IDoK 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. IDoK 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.

IDoK 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 llegare a existir. En particular la TSA de IDoK cuenta con un seguro en conformidad al artículo 14 de Ley 19799. La cobertura señalada no podrá ser invocada directamente por el suscriptor 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.

b. Responsabilidades Generales

IDoK 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 relativas a la protección de datos personales o en la Ley 19.496, sobre 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 suscriptores o terceras partes interesadas, o no acorde con las políticas y prácticas establecidas por la TSA de IDoK.

IDoK, 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.

c. Fuerza Mayor
IDoK queda exenta de responsabilidad en caso de pérdida o perjuicio, en los servicios que presta, producto de:

d. Guerra, desastres naturales o cualquier otro caso de fuerza mayor.
Los cuales le hagan imposible proveer los servicios de time-stamping de acuerdo a lo definido y publicado en sus políticas y prácticas de certificación.

9. Ciclo de vida del Certificado de Sello de Tiempo

El certificado de Sello de Tiempo dejará de firmar documentos un año antes de su fecha de vencimiento. En ese momento se emitirá un nuevo certificado para ser utilizado en reemplazo del que está por vencer.
El procedimiento para emitir un nuevo Certificado de Sello de Tiempo se describe en el punto “Administración del ciclo de vida de las claves”, “Generación”, “Protección”, “Distribución” en el documento “PO01 - Política de Sello de Tiempo”.

10. Ciclo de vida de la Autoridad de Sello de Tiempo

El ciclo de vida de la Autoridad de Sello de Tiempo dejará de emitir certificados un año antes de su fecha de vencimiento. En ese momento se emitirá un nuevo certificado para ser utilizado en reemplazo del que está por vencer.
El procedimiento para emitir un nuevo Certificado de Sello de Tiempo se describe en el punto “Administración del ciclo de vida de las claves”, “Generación”, “Protección”, “Distribución” en el documento “PO01 - Política de Sello de Tiempo”.

11. Requerimientos en prácticas de la TSA

11.1. PRÁCTICAS Y DECLARACIONES DE DIVULGACIÓN

a. Declaraciones de prácticas de TSA

La TSA de IDoK, a partir del análisis de riesgo aplicado al servicio de la TSA, ha generado una planificación orientada a mitigar los riesgos detectados, a través de un Sistema de Gestión de Seguridad de la Información (SGSI); el cual es controlado y aprobado formalmente por el comité de seguridad de IDoK Esta planificación se encuentra alineada con las políticas y prácticas que detallan el servicio prestado desde el punto de vista de los actores participantes del proceso, sus obligaciones, del personal a cargo de la prestación del servicio, de los aspectos técnico asociados a dicha prestación, de los aspectos documentales y organizativos, así como de los cumplimientos legales que rige la actividad de IDoK como TSA.

b. Declaración de divulgación de TSA

LA TSA de IDoK entrega como parte de estas políticas su información de contacto a los suscriptores 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, Fomento y Futuro.

11.2. GESTIÓN DE CICLO DE VIDA DE LAS LLAVES

a. Generación de llave de la TSU

El módulo criptográfico adoptado por IDoK, es capaz de generar llaves en base al algoritmo de encriptación de llave pública SHA256RSA con al menos 2048 bits de encriptación; 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. Para controlar el acceso a la llave privada de IDoK y de sus Autoridades Intermedias, la PSC implementó un sistema criptográfico, basado en el equipo HSM especializado de la marca Utimaco, y una aplicación nativa de la marca para realizar operaciones de criptografía contra el equipo, el cual implementa seguridad de acceso a información criptográfica a través de diferentes niveles.

- Tarjetas o token de Administración (ACS): Es un grupo de token físicos que guardan la llave para encriptar el material criptográfico. Ellas habilitan y protegen el ambiente completo del sistema.
- Tarjetas de operación y protección (OCS): Es un grupo de token físicos autorizados explícitamente para almacenar el material criptográfico, y además restringen el acceso a este material estando este presente físicamente en los token definidos.

Para acceder a funcionalidades del equipo HSM Utimaco sobre el que se ejecutan las operaciones, se utilizan estos medios físicos de protección lógica (ACS y OCS), los que controlan el acceso al material criptográfico y además poseen características de protección contra intentos de intrusión física en concordancia con el estándar FIPS 140-2 nivel 3, logrando él mismo deshabilitar su contenido en caso de detectar riesgos evidentes.

La encriptación aplicada a la llave privada de la Autoridad Certificadora, bajo las ACS y OCS, permiten minimizar un posible compromiso de esta llave en ausencia de los controles de acceso definidos en el sistema criptográfico, el cual establece un quórum de tarjetas físicas de operación para poder funcionar. Con respecto a este quórum se establece una cantidad de token físicos para poder realizar tareas sobre el material criptográfico en el equipo HSM Utimaco, y de igual manera existe un quórum para administración del ambiente completo, que es una protección adicional en caso que el o los equipos sean comprometidos por un tercero. El quórum establecido para la administración es 3 de 5 token.

La llave usada por la TSU de IDoK son generadas de acuerdo a las Políticas y Prácticas definidas para el proceso de Firma Electrónica Avanzada; utilizando tanto los algoritmos de encriptación como el largo de llave en estos documentos definidos.

Del mismo modo, la TSA de IDoK utiliza para la generación de la llave antes mencionada, un módulo criptográfico HSM que cumple con el estándar FIPS 140-2 nivel 3, el cual sólo puede ser accesado por personal autorizado, altamente confiable y que son parte del quórum de administración definido durante la Ceremonia de llaves del equipo HSM.

IDoK declara que satisface los requerimientos identificados en CEN Workshop Agreement 14167-2 [CWA 14167-2] o ISO 15408 al cumplir con la ETSI TS 102 042 que fue la que dio origen al ciclo de vida de la llave aquí descrito.

b. Protección de la llave privada de la TSU

IDoK 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, permanezca de manera confidencial y mantenga su integridad. Esto incluye el uso de un HSM; certificado FIPS 140-2 nivel 3. Cuando la llave privada es respaldada, son copiadas, almacenadas y recuperadas sólo por el personal con roles de confianza y bajo un ambiente seguro.

Así, IDoK realiza la protección de las llaves a través de:

- Módulos criptográficos: El HSM "Hardware Security Module" (Módulo de Seguridad Hardware), es un dispositivo hardware de seguridad criptográfica que genera y protege claves privadas. Los nuevos HSM de IDoK cumplen el criterio FIPS 140-2 Nivel 3 o equivalente.
- Control multipersona de la llave privada: Las claves privadas utilizadas por las autoridades de certificación de IDoK y sus jerarquías se encuentran bajo control multipersona, es decir, es necesario un mínimo de 3 personas de un total de 5 para modificar el ambiente criptográfico.
- Depósito de la llave privada: La clave privada está cifrada y queda contenida en el repositorio asociado a dispositivo HSM.
- Copia de respaldo de la llave privada: Existe un procedimiento de recuperación de claves de los módulos criptográficos HSM de la AC (raíz o intermedias) que se puede aplicar en caso de contingencia para la TSA. El procedimiento de recuperación de claves de módulos criptográficos corresponde al contexto de procesos certificados que posee el dispositivo HSM.
- Introducción de la clave privada en el módulo criptográfico: Las claves privadas se crean en el módulo criptográfico HSM en el momento de la creación de cada una de las entidades de IDoK que hacen uso de dichos módulos.
- Método de activación de la clave privada: Las claves privadas de las autoridades de certificación de IDoK y que componen sus jerarquías, se activan mediante la inicialización del software de AC y la activación del hardware criptográfico que contiene las claves.
- Método de desactivación de la clave privada: Un Administrador puede proceder a la desactivación de la clave privada de las AC de IDoK o de sus claves intermedias (Clave de la TSA), mediante la detención del software de la AC.

- Método de destrucción de la clave privada: Existe un procedimiento de destrucción de claves de la AC, así como de las claves intermedias de la jerarquía.

En lo que respecta a la generación de la llave de la TSU, el módulo criptográfico utilizado por IDoK mantiene la confidencialidad de la llave en su ciclo de tiempo completo, restringiendo el acceso a éste al personal autorizado solamente. De detectarse un acceso no autorizado, este se registra ya sea de manera física (tampering físico) o a través de log a ser usado durante la auditoría. Este equipo contempla además mecanismos de backup y respaldo de la llave, manteniendo la seguridad de estos respaldos a través de métodos criptográficos.

c. Distribución de la llave pública

El certificado digital utilizado por la TSA de IDoK es generado por la PSC de IDoK, de acuerdo a las políticas y prácticas de certificación inspeccionadas por el Ministerio de Economía, Fomento y Turismo para esta PKI.

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 que IDoK, 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 TSA certificadas ante el Ministerio de Economía.

Estos certificados, se encuentran disponibles en el sitio web de IDoK, 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 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 a esta

instalación, es verificar si el almacén de raíces de confianza incluye a este certificado recién instalado.

Al estar este certificado instalado en el repositorio de confianza del cliente, cualquier sello que haya sido emitido y firmado por esta TSA podrá ser validado por el cliente, ya que el certificado raíz de la TSA contiene la llave pública que permitirá verificar el certificado emitido. Una forma de complementar esta cadena de confianza, es instalar además del certificado raíz de la TSU (raíz intermedia de la PSC), el certificado raíz de la PSC utilizado para firmar el certificado de la TSU.

d. Remisión de llaves de la TSU
   Por motivo de seguridad y evitar el repudio a un certificado, IDoK como PSC no procede a realizar la reemisión de llaves una vez generado el certificado de la TSU, esto de acuerdo a 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.

e. Revocación y suspensión de certificados
   La CA se asegurará de que los certificados se revoquen de manera oportuna en función de las solicitudes de revocación de certificados validadas y autorizadas.

   En particular:

   Gestión de revocación

   - La CA deberá documentar como parte de su declaración de prácticas de certificación los procedimientos para revocación de certificados que incluyen:
     - quién puede presentar informes y solicitudes de revocación;
     - cómo pueden presentarse;
     - cualquier requisito para la confirmación posterior de informes y solicitudes de revocación, por ejemplo, es posible que se requiera una confirmación del suscriptor si un tercero informa un compromiso;
     - si los certificados pueden suspenderse y por qué motivos;
     - el mecanismo utilizado para distribuir información sobre el estado de revocación;
     - la demora máxima entre la recepción de una solicitud o informe de revocación y el cambio al estado de revocación, información disponible para todas las partes que confían.

- Solicitudes e informes relacionados con la revocación, por ejemplo, debido al compromiso de la clave privada del sujeto, muerte del sujeto, terminación inesperada del acuerdo o funciones comerciales de un suscriptor o sujeto, violación de obligaciones contractuales, se tramitarán a su recepción.
- Las solicitudes e informes relacionados con la revocación se autentican, comprobando que proceden de una fuente autorizada. Dichos informes y solicitudes se confirman según lo requieran las prácticas de la CA.
- El estado de revocación de un certificado puede establecerse en "suspendido" mientras se confirma la revocación. La CA se asegurará de que un certificado no se mantenga suspendido durante más tiempo del necesario para confirmar su estado (el soporte para la suspensión de certificados es opcional).
- El sujeto, y en su caso el suscriptor, de un certificado revocado o suspendido, será informado del cambio de estado del certificado.
- Cuando se utilicen listas de revocación de certificados (CRL) que incluyan cualquier variante, por ejemplo, Delta CRL, estas se deberán publicar.
- Cuando las listas de revocación de certificados (CRL), incluidas las variantes, Delta CRL, se utilizan como únicos medios para proporcionar información sobre el estado de la revocación:
    - cada CRL indicará una hora para la próxima emisión de CRL programada; y
    - se puede publicar una nueva CRL antes de la hora indicada para la próxima emisión de CRL;
    - la CRL deberá estar firmada por la autoridad de certificación o una autoridad designada por la CA. Para maximizar la interoperabilidad, se recomienda que la CA emite Listas de revocación de certificados como se define en la Recomendación UIT-T X.509 [9].

Estado de revocación

La información sobre el estado de la revocación estará disponible según se especifica en la Práctica de certificación de la CA.

La información sobre el estado de la revocación estará disponible las 24 horas del día, los 7 días de la semana. Ante una indisponibilidad del sistema, servicio u otros factores que no están bajo el control de la CA, la CA hará todo lo posible para garantizar que este servicio de información no esté disponible por más tiempo que el período de tiempo máximo indicado en la declaración de prácticas de certificación. La información sobre el

estado de revocación puede proporcionarse, por ejemplo, mediante el servicio de estado de certificados en línea o mediante la distribución de CRL a través de un repositorio.

- Se protegerá la integridad y autenticidad de la información del estado.
- Si la CA está emitiendo un certificado al público, la información sobre el estado de la revocación estará disponible pública e internacionalmente.
- La información sobre el estado de la revocación incluirá información sobre el estado de los certificados al menos hasta que expire.

e. Término 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 IDoK 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 IDoK 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: suscriptores, terceros de confianza y autoridades de sello de tiempo acreditadas.

IDoK comunicará a cada uno de sus suscriptores el 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 suscriptores, 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 a 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.

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

Los equipos HSM con que cuenta IDoK y que son usados para firmar el certificado utilizado por la TSU para la firma de sus sellos de tiempo; así como para la firma de los mismos sellos de tiempo, cuenta con la detección de intrusión a los equipos, ya sea por sellos holográficos y/o detectores de intrusión. Así mismo, para evitar la intrusión de dispositivos en el hardware del módulo de seguridad, este dispositivo se coloca en la parte posterior a los ventiladores del HSM. El equipo HSM posee varios niveles de detección de intrusión física a la funcionalidad criptográfica, informando estos eventos al administrador y en último caso obligando a reiniciar el equipo a sus condiciones de salida de fábrica. Los eventos antes mencionados son desplegados en la pantalla del equipo.

Ante la detección de los eventos que se indican previamente, no se debe poner en producción dicho equipo, ya sea que los eventos se han producido durante el almacenamiento o transporte del equipo. El administrador de dicho equipo debe proceder a reiniciar el equipo a sus condiciones de salida de fábrica. Posterior a esto, se debe reconectar el equipo así como recuperar la información clave del equipo, haciendo uso del quórum que otorgan el set de tarjetas de administración definidas.

En particular si se ha detectado apertura de la tapa del equipo, este genera un evento indicando dicha intrusión, lo que implica que la seguridad del equipo se ha comprometido. Bajo este escenario no se debe pasar a producción dicho equipamiento bajo motivo alguno. Si el evento indicado, se produce durante el tránsito del equipo desde el fabricante de dicho equipo, el administrador debe contactarse inmediatamente con el fabricante. En cambio de ocurrir este evento posterior a la instalación, adicionalmente se deben revisar las políticas y procedimientos de seguridad que permitieron dicho incidente.

Entre las revisiones que deben realizarse al equipo, tanto posterior a su transporte o durante su almacenamiento es:

- Controlar que los sellos de seguridad no hayan sido alterados.
- Que las tapas permanecen completamente ajustadas al chasis del equipo.

- Que no se presentan daños aparentes a la estructura general del equipo.
- Que no se detecten daños evidentes en ventilaciones del equipo o que se haya intentado
- introducir algún componente a través de estos espacios.

El equipo HSM utilizado por IDoK tanto para su PSC como TSA, implementa seguridad de acceso a información criptográfica a través de diferentes niveles.

- Token de administración (ACS): Es un grupo de token físicos que guardan la llave para encriptar el material criptográfico. Ellas habilitan y protegen el ambiente completo del sistema.
- Token de operación y protección (OCS): Es un grupo de token físicos autorizadas explícitamente para almacenar el material criptográfico, y además restringen el acceso a este material estando este presente físicamente en las tarjetas definidas. Estas tarjetas permitirán a las aplicaciones externas utilizar el sistema para realizar el trabajo de almacenamiento seguro de llaves.

Para acceder a funcionalidades del equipo HSM, sobre el que se ejecutan las operaciones de instalación, respaldo y recuperación, se utilizan estos medios físicos de protección lógica (ACS y OCS), los que controlan el acceso al material criptográfico y además poseen características de protección contra intentos de intrusión física en concordancia con el estándar FIPS 140-2 nivel 3, logrando él mismo deshabilitar su contenido en caso de detectar riesgos evidentes. La encriptación aplicada a la llave privada de la Autoridad Certificadora, utilizada para la generación del certificado de la TSU, bajo las ACS y OCS, permiten minimizar un posible compromiso de esta llave en ausencia de los controles de acceso definidos en el sistema criptográfico, el cual establece un quórum de tarjetas físicas de operación para poder funcionar. Con respecto a este quórum se establece una cantidad de tarjetas físicas para poder realizar tareas en el equipo HSM sobre el material criptográfico, y de igual manera existe un quórum para administración del ambiente completo, que es una protección adicional en caso que el o los equipos sean comprometidos por un tercero. El quórum establecido para la administración es 3 de 5 token.

Una vez instalado de manera exitosa el hardware y software asociado al HSM, IDoK ha definido como criterio de verificación del correcto funcionamiento de los equipos, la emisión de un certificado de prueba, partiendo desde su solicitud hasta su emisión y a

continuación la revocación del mismo. Con este ciclo se probará la correcta generación de claves, servicios OCSP y listas de revocación de certificados. Una vez desarrollada esta actividad, se podrá proceder a generar las llaves intermedias utilizadas por los distintos servicios de la PSC, en particular para este caso, la llave de la TSU utilizada para la firma de los sellos de tiempo a emitir.

Finalmente, en caso de requerir mover el equipo a otra instalación o el envío del mismo a la fábrica por motivos de garantía, IDoK ha definido que se debe dejar el equipo a sus condiciones originales que tenía a la salida de fábrica, borrando con ello todo su contenido de configuraciones interna del equipo HSM. En particular, para el caso de equipos, esto se puede realizar a través del menú de opciones de administración, opción "factory reset". Esto llevará a que el equipo borre todo su contenido.

12. Sello de tiempo

12.1. Token de Sello de Tiempo

La TSA de IDoK garantiza que los token 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 suscriptor 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 TST's así como para identificar un sello de tiempo específico.
- El Token de Sello de 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 IDoK establece todo el procedimiento asociado a la generación de los tokens de sello de tiempo, utilizando el protocolo descrito en RFC3161.

12.2. Sincronización de los relojes con UTC

La TSA de IDoK declara utilizar una fuente fiable de tiempo, mediante un servidor basado en el protocolo NTP que sincronice con el tiempo UTC a través de una red de satélites GPS o en

caso excepcional contra múltiples fuentes que incluyen el “National Measurement Institute”, el cual provee tiempo UTC; lo anterior con una desviación máxima de 1 segundo. Esta fuente de tiempo está basada en el protocolo NTP (Network Time Protocol) haciendo que la exactitud no disminuya por debajo de los requerimientos.

De manera más específica:

- La calibración de la TSU es desarrollada de tal manera de que el reloj no escape más allá de la precisión declarada.
- El reloj de la TSU se encuentra protegido contra amenazas ambientales que puedan afectar su precisión fuera del rango declarado.
- En caso de producirse una desviación más allá de la precisión declarada, esto será informado a la comunidad a través del sitio web de la TSA.
- En caso de detectarse una desviación más allá de la precisión declarada, la TSU no generará nuevos TST hasta que el tiempo correcto sea restaurado.
- IDoK declara que la precisión declarada es mantenida con una desviación de 1 segundo tal como se incluye en el TST.

13. Gestión de la TSA y operaciones

13.1. Gestión de la Seguridad

La TSA de IDoK desarrollará una administración activa de la seguridad a través de un Sistema de Gestión de Seguridad de la Información (SGSI), el que considera las mejores prácticas y estándares de la industria. El estándar que aplica la TSA de IDoK como parte de su SGSI es el estándar ISO 27001. En particular:

- IDoK 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.
- Todo su personal tienen acceso a sus prácticas y políticas de sello de tiempo.
- Todo el personal es auditado mensualmente a fin de verificar el cumplimiento de la planificación del SGSI.
- IDoK cuenta con un Comité de seguridad de la información, un oficial de seguridad, un oficial adjunto y una oficina técnica, los que en su conjunto velan por el cumplimiento del plan anual definido por el SGSI.
- IDoK declara que los procedimientos y controles operacionales de la TSA se encuentran documentados, se mantienen y se implementan.
- IDoK no subcontrata los servicios de sello de tiempo.

13.2. GESTIÓN Y CLASIFICACIÓN DE ACTIVOS

Los activos de la TSA de IDoK reciben un apropiado nivel de protección. Para ello la TSA de IDoK realiza anualmente un análisis de riesgos. 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 IDoK generó un plan de gestión de seguridad que incluye las mitigaciones a los riesgos detectados previamente.

Para el cumplimiento de este plan, así como su seguimiento, IDoK cuenta con un Comité de seguridad de la información, un oficial de seguridad, un oficial adjunto y una oficina técnica, los que en su conjunto velan por 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 Ministerio de Economía.

14. Seguridad del personal

14.1. REQUERIMIENTOS DE ANTECEDENTES Y EXPERIENCIA

IDoK 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 básica sobre seguridad en sistemas de información.
- Formación específica para su puesto.
- Título académico o experiencia en la industria equivalente.
- El personal que realiza un rol de confianza no debe tener conflictos de interés que afecten la imparcialidad de las operaciones de la TSA.

14.2. COMPROBACIÓN DE ANTECEDENTES

En IDoK se realiza una comprobación de los antecedentes, de acuerdo a lo especificado en la Declaración de Prácticas de Sello de Tiempo de IDoK antes de asignar un rol de confianza.

14.3. Roles de Confianza

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

- Oficial de seguridad: es responsable de la administración e implementación de las prácticas de seguridad.
- Administrador de Sistemas: está autorizado a instalar, configurar y mantener los sistemas de confianza de la TSA, para la administración de sello de tiempo, Además es responsable por la operación de los sistemas y autorizado para realizar el respaldo y recuperación.
- Administrador de Seguridad: Es el encargado de verificar la mantención de los sistemas de confianza de la TSA.
- Auditor: Es el encargo de revisar archivos y log de auditoría de la TSA.

14.4. Requerimientos de formación y reentrenamiento

Como parte de las recomendaciones en que IDoK 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 IDoK para la PSC de IDoK. 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.

14.5. Frecuencia de rotación de tareas

La frecuencia de rotación de tareas las establecen los Gerentes de Operaciones y Gerente de Tecnología de acuerdo a las necesidades del negocio y en concordancia con los lineamientos de la Gerencia General.

14.6. Sanciones

IDoK informa y entrega al momento del contrato, a cada empleado el Reglamento Interno, el cual en uno de sus capítulos indica obligaciones.

14.7. Requerimientos de contratación

Como parte de los requerimientos de contratación, todo trabajador de la PSC y de su servicio de TSA debe firmar un acuerdo de confidencialidad.

14.8. Documentación entregada al personal

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

- Declaración de Prácticas de Certificación
- Políticas de Certificación
- Políticas de Privacidad
- Políticas de Seguridad de la Información
- Organigrama y funciones del personal

14.9. Control de Cumplimiento

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

14.10. 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 les informa al resto de la organización, a los proveedores y entidades externas a IDoK de que el individuo ya no representa a la TSA de IDoK.

15. Seguridad Física y ambiental

La seguridad física y ambiental se detalla en la política de seguridad, dando cumplimiento a la norma ISO 27001 en la cual se basa. Los servicios de IDoK además de acuerdo a las prácticas de certificación de Sello de tiempo.

15.1. Emisión de sellos de tiempo, así como su administración

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

15.2. Control de módulos criptográficos

El control de los módulos criptográficos se llevarán a cabo para evitar la pérdida de información y están de acuerdo a lo especificado en esta Declaración de Prácticas de Sello de Tiempo de IDoK y el documento de “Gestión del ciclo de vida de las llaves”.

15.3. CONTROLES FÍSICOS Y AMBIENTALES

a) Data Center y Oficinas Centrales

Los sistemas e infraestructura del Servicio de Emisión de sellos, se encuentran alojados en un sitio principal y uno secundario. Las características generales comprenden una Zonificación en Alta Criticidad y una Zona de Media Criticidad.

Ambos cuentan con medidas que mantienen un perímetro de seguridad el cual restringe el acceso sólo a personal autorizado. Respecto a la casa matriz de IDoK ella cuenta con accesos vigilados, área de recepción, así como control de visitas y acceso biométrico del personal.

b) Seguridad física Data Center

IDoK opera en un par de Data Center seguros y confiables que cuentan con niveles de protección y solidez de la construcción y con vigilancia durante las 24 horas al día, los 7 días a la semana. Ambos Data Center cuentan con controles definidos, para proteger los elementos que forman parte de la solución de IDoK, se basan en procedimientos y estándares de seguridad física para las instalaciones informáticas. Estos a su vez se encuentran elaborados según la norma ISO 27001, para la cual ambos sitios se encuentran certificados.

c) Sistema Energía Eléctrica

IDoK cuenta en los sitios con todos los resguardos necesarios para mantener una continuidad de energía suficiente y su operación, por largos periodos de tiempo. Para redundante a través de UPS y grupos electrógenos Para un mayor detalle sobre el Sistema de Energía Eléctrica se encuentra especificado en esta Declaración de Prácticas de Sello de Tiempo de IDoK.

d) Sistema de Control Ambiental

Ambos sitios cuentan con un suministro continuo de climatización (aire acondicionado, humedad, polvo en suspensión) en modalidad 24x7x365, garantizando el buen funcionamiento de los equipos. Las especificaciones son:

- Temperatura: 21°C+/-3°C.
- Humedad relativa: 45%+/-10%.
- Polvo en suspensión: 75 Microgramos por m3, como máximo.

Para cumplir esta función los sitios cuentan con equipos de climatización precisa que detectan y controlan la humedad relativa del ambiente, lo que permite mantener ambientes óptimos de temperatura y humedad, en las distintas salas. Ambos cuentan además con un sistema redundante de climatización dimensionado para asegurar una temperatura estable y continua a las salas de equipamiento y a las áreas de operación. En caso de fallas del sistema de aire acondicionado, éste cuenta con un sistema de respaldo que garantiza la continuidad del servicio.

e) Sistema de Extinción y control de incendio

El Sistema de Extinción y Control de Incendios cuenta con el suministro e instalación de un sistema de protección contra incendios sobre la base de detección temprana, que se realiza bajo vía un sistema de aspiración de partículas del ambiente y de extinción automática con FM-200, aprobación UL, e instalado bajo norma NFPA.

f) Telecomunicaciones

Las especificaciones respecto a las Telecomunicaciones se basan en una plataforma robusta, segura y escalable, utilizando para ello los servicios WAN, estos servicios provistos por los principales carriers del país que nos aseguran redes confiables y con tecnología de última generación.

g) Seguridad Lógica Data Center Los Data Center cuentan con aspectos de seguridad lógica.

13. Gestión de las operaciones

La TSA de IDoK 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 están protegidos de virus, código malicioso e incorporación de código no autorizado. Respecto al manejo de medios y seguridad, IDoK 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, IDoK 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
- Auditor
- 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 a los futuros requerimientos, de manera que la capacidad de proceso como de almacenamiento siempre sean las adecuadas. Para efectuar esto, IDoK cuenta con un procedimiento formal de gestión de capacidad de sus instalaciones.

Respecto a los procedimientos operacionales y responsabilidades, IDoK 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 IDoK y en su Declaración de Prácticas de Sello de Tiempo de IDoK.

14. Gestión de acceso a los sistemas

La TSA de IDoK, 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 IDoK realizan un monitoreo continuo para detectar intentos o accesos no autorizados a los activos de la TSA. Es por ello que se cuenta con Cortafuegos, Administración de usuarios, Restricciones de acceso a la información y sistemas, un control apropiado del personal autorizado, Logs de las operaciones. Adicionalmente, los

componentes de la red local se mantienen en Data Center bajo ambiente seguro y con una auditoría periódica.

15. Mantenimiento e implementación de sistemas de confianza

En la TSA de IDoK se asegura que el sistema y productos están protegidos contra modificaciones no autorizadas, es por ello 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 crítico autorizado.

16. Compromiso de los servicios de TSA

La TSA de IDoK declara que, ante cualquier compromiso de los servicios de sello de tiempo, se harán efectivos los procedimientos correspondientes al plan de continuidad de IDoK. 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 a través de su sitio web a sus suscriptores y terceros que en ella confían, dicha información del evento. Ante los eventos antes mencionados, la TSA de IDoK no emitirá nuevos TST hasta superar el compromiso declarado

17. Cese de la TSA

En el momento en que IDoK vaya a descontinuar sus operaciones como Autoridad de sello de tiempo, procederá a comunicar el cese de sus funciones con la debida antelación a todas las partes involucradas con sus servicios de sello de tiempo ya sean suscriptores, terceros de confianza y autoridades de sello de tiempo acreditadas. Además, la TSA procederá a 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 IDoK, estas deben ser borradas y destruidas, de manera que estas no puedan ser recuperadas, de acuerdo a lo especificado en la Declaración de Prácticas de Sello de Tiempo de IDoK.

En el procedimiento para el término de actividades, se dispondrá de los costos necesarios para los requerimientos indicados.

18. Cumplimiento de requerimientos legales

IDoK 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. IDoK cuenta con procedimientos de control y de seguridad de la información, a objeto de proteger la información personal de sus suscriptores 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 a lo especificado en la Declaración de Prácticas de Sello de Tiempo de IDoK.

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

La TSA de IDoK debe mantener registros de la información relevante, concerniente a su operación. Estos registros corresponden a la información personal de los suscriptores que se ha recolectado y se encuentra protegida de acuerdo con la Política de Privacidad de datos personales publicados por IDoK en su sitio web, tal como se detalla en la Declaración de Prácticas de Sello de Tiempo de IDoK.
Todos los registros concernientes a la operación del servicio de sello de tiempo se encuentran disponibles sólo al suscriptor o en caso que lo solicite una corte a través de un requerimiento legal.
La integridad de esta información es mantenida por la PSC de IDoK 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 IDoK 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 IDoK.

20. Organización

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

La TSA de IDoK cumple con: Sus políticas y procedimientos bajo los que opera no incluyen cláusulas discriminatorias. IDoK provee su servicio de sello de tiempo a cualquier suscriptor que cumpla y esté de acuerdo con las obligaciones declaradas en las prácticas y políticas de sello de tiempo. IDoK 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, artículo 14, ante daños o perjuicios producto de su operación. IDoK es anualmente auditada respecto sus estados financieros y el cumplimiento de la normativa vigente. IDoK 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.

IDoK 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. IDoK mantiene un su repositorio documental todo contrato, acuerdos de confidencialidad y servicios prestados por cada uno de los proveedores de la TSA.

21. 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 IDoK que invalida la llave de firma y por ende al TST emitido. La TSA de IDoK asegura que hash incluido en su TST corresponde al enviado por el suscriptor en su request.

22. Controles de Seguridad no Técnica

Para mantener los niveles de seguridad del servicio de Sello de Tiempo desde el punto de vista no técnico, se consideran los siguientes controles:

- Evaluación anual del personal a cargo del servicio
- Evaluación anual de las políticas de seguridad