PO02 – DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN

Resumen

Documento conteniendo la Declaración de Prácticas de Certificación de Firma Electrónica Avanzada

Este documento contiene información de uso interno, propiedad de IDOK. Antes de utilizar alguna copia de este documento, verifique que la Versión sea igual a la que muestra la Lista Maestra de Control de Documentos. Si este documento es una copia impresa, verifique la validez en el timbre de Copia Impresa Controlada. De no ser válido, destruya la copia para asegurar que no se haga de ésta un uso no previsto.

CONTENIDO

Información del Documento

HISTORIA DEL DOCUMENTO

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

Responsable del Documento:	Oficial de Seguridad	**Fecha de Creación:**	26 de Julio de 2017
Aprobado por:		**Fecha de Aprobación:**	

CONTROL DE VERSIONES

Versión	Fecha de Vigencia	Aprobación	Comentario
001	26 de Julio de 2017	Jorge Pizarro	Creación del documento
002	27 de agosto de 2017	Jorge Pizarro	Revisión del documento
003	4 de septiembre de 2018	Jorge Pizarro	Revisión del documento
004	15 de mayo de 2020	Jorge Pizarro	Nueva versión
005	5 de abril de 2021	Jorge Pizarro	Actualización del documento

1. Introducción

IDOK posee dos instrumentos para gestionar su Autoridad de Registro los cuales son la Declaración de Prácticas de Certificación y la Políticas de Certificación, los cuales se definen a continuación para ayudar en su interpretación.

Política de Certificación (CP) es el conjunto de reglas que definen la aplicabilidad de un certificado en una comunidad y/o en alguna aplicación, con requisitos de seguridad y utilización comunes, es decir, en general una Política de Certificación debe definir la aplicabilidad de tipos de certificado para determinadas aplicaciones que exigen los mismos requisitos de seguridad y formas de usos.

La Declaración de Prácticas de Certificación (CPS) es definida como un conjunto de prácticas adoptadas por una Autoridad de Certificación para la emisión de certificados. En general contiene información detallada sobre su sistema de seguridad, soporte, administración y emisión de los Certificados, además sobre la relación de confianza entre el Firmante/Suscriptor o Tercero que confía y la Autoridad de Certificación. Pueden ser documentos absolutamente comprensibles y robustos, que proporcionan una descripción exacta de los servicios ofertados, procedimientos detallados de la gestión del ciclo vital de los certificados, etc.

Estos conceptos de Políticas de Certificación y Declaración de Prácticas de Certificación son distintos, pero aun así es muy importante su interrelación.

Una Declaración de Prácticas de Certificación detallada no forma una base aceptable para la interoperabilidad de Autoridades de Certificación. Las Políticas de Certificación sirven mejor como medio en el cual basar estándares y criterios de seguridad comunes.
En definitiva, una Política define “qué” requerimientos de seguridad son necesarios para la emisión de los certificados. La Declaración de Prácticas de Certificación nos dice “cómo” se cumplen los requerimientos de seguridad impuestos por la Política.

2. Alcance

El Alcance de la Declaración de Prácticas de Certificación (CPS) detalla las condiciones de los servicios de certificación que presta IDOK para la emisión de sus certificados de Firma Electrónica Avanzada.

3. Referencias y glosario

La presente declaración de Políticas de Certificación se ha generado siguiendo las especificaciones del documento RFC 3647 “Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework”, y con las siguientes referencias:

- ETSI TS 102 042 V1.1.1 (2002-04). Technical Specification. Policy requirements for certification authorities issuing public key certificates.
- NCh2805.Of2003 Tecnología de la Información – Requisitos de las políticas de las autoridades certificadoras que emiten certificados de claves públicas.
- ETSI TS 102 042 V1.2.2 (2005-06) .RTS/ESI-000043.Keywords e-commerce, electronic signature, public key, security.
- ETSI TS 102 042 V2.1.1 (2009-05). Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates.
- ETSI TS 102 042 V2.1.2 (2010-04) Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates.
- NCh27002.Of2009 Tecnología de la información – Código de práctica para la gestión de seguridad de la información.
- ISO/IEC 15408-1:2009 Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model
- FIPS PUB 140-2: Security Requirements for Cryptographic Modules (mayo 2001).
- NCh.2820/1. Of2003 Tecnología de la información – Técnica de seguridad – Criterio de evaluación de la seguridad de TI – Parte 1: Introducción y modelo general.
- 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.

- **Certificado**: Es todo registro que evidencie el vínculo entre un firmante y los datos de creación de Firma Electrónica.
- **Firma electrónica**: Es un vínculo único e irrepetible representado en una secuencia de caracteres. Este vínculo es el resultado entre el algoritmo hash al contenido del documento y la llave privada del firmante. De esta forma se genera una asociación directa entre quien firmó el documento y el documento en sí y que se pueda detectar cualquier cambio posterior.
- **Suscriptor de un Certificado**: Corresponde a la persona o empresa a la cual se emitió el certificado. Este suscriptor posee una llave pública y otra privada que son utilizadas en cada firma que realice. Según la ley el suscriptor es la persona que tiene en su absoluto control el certificado de firma electrónica.
- **Certificador**: Es la persona o empresa que puede verificar la identidad de los solicitantes.
- **Autoridad de registro**: Es la empresa o institución que llevará el registro electrónico de los certificados emitidos por la Autoridad de registro. Este registro se realiza encargándose de la detección, comercialización y administración de las solicitudes de todos los tipos de certificados que comercializa IDOK.
- **Usuarios:** El usuario del certificado es la persona que decide usar los certificados emitidos por IDOK y hace uso de ellos.
- **CRL**: Listado de certificados revocados.
- **CPS**: Declaración de Prácticas de Certificación.
- **DAS**: Dispositivos de Almacenamiento Seguro.
- **PSC**: Prestador de Servicios de Certificación.
- **OCSP**: Online Certificate Status Protocol, Protocolo de consulta de estado de certificados en línea.
- **Clave Única del Estado (CUE).** Sistema de autenticación generado por el Servicio de Registro Civil e Identificación utilizado para los trámites de carácter público del Estado y emitido para cualquier ciudadano con cédula de identidad.

4. Antecedentes

El Modelo de confianza adoptado por IDOK se basa principalmente en implementar una infraestructura de confianza basada en PKI (Public Key Infrastructure), utilizando tecnología de llave pública y privada.

El modelo de confianza se basa principalmente en el tercero que confía (Trusted Third Party), este tercer elemento es la PSC.

5. Aplicabilidad y Comunidad de Usuarios

5.1. Comunidad de Usuarios

IDOK emitirá sus certificados digitales de firma electrónica avanzada en el estándar X.509 y serán emitidos a toda persona física. Para ello se requerirá asegurar la identidad del interesado o suscriptor frente a la autoridad de registro mediante:

a. Su presencia física en las oficinas de la PSC, o
b. De manera online mediante Clave Única del Estado (CUE) y un segundo factor de autenticación basado en responder de manera correcta un desafío de preguntas que la PSC genera en función de los servicios provistos por un proveedor calificado.

5.2. Aplicabilidad

Los certificados emitidos por IDOK no han sido diseñados ni se autoriza su uso para cualquier efecto que al ser usado éste se deriva en muerte, lesiones a personas o al medio ambiente o infrinja la ley de la república.

Los certificados emitidos por IDOK podrán ser uso en las siguientes necesidades de seguridad:

5.2.1. AUTENTIFICACIÓN

Proporciona suficientes garantías respecto a la identidad del suscriptor del certificado, al requerirse la presencia del suscriptor junto con su Cédula Nacional de Identidad o el control de su CUE y al exigir el almacenamiento de la llave privada en un dispositivo acreditado según norma FIPS-140 nivel 2.

5.2.2. NO REPUDIO

Las firmas electrónicas producidas con certificados emitidos por la de Entidad de Registro IDOK tiene la evidencia necesaria frente a que una persona deniegue la autoría de la firma digital o el contenido firmado digitalmente con el certificado emitido a dicha persona

5.2.3. INTEGRIDAD

La información firmada con un certificado digital emitido por la Entidad de Registro IDOK permite validar que el elemento firmado no cambia su contenido desde el momento de la firma.

5.2.4. PRIVACIDAD

La información firmada con un certificado digital emitido por la Entidad de Registro IDOK permite cifrar elementos que solo pueden ser visualizados por el titular de los datos de creación de firma electrónica.

6. Aplicabilidad Global

IDOK utiliza en la cúspide de su jerarquía un certificado raíz (IDOK ROOT) creado íntegramente en IDOK. Todos los certificados intermedios quedan firmados por este certificado raíz, en particular el de Firma Electrónica Avanzada, de esta forma se dispone un entorno de confianza global para todos los servicios basados en la PSC.
Este certificado raíz estará disponible tanto en la página web de acceso público psc.idok.cl como en la TSL.

7. Rol frente a los suscriptores

El principal rol de IDOK es realizar todas las tareas, desarrollos y procedimientos orientados a mantener el modelo de confianza definido, correspondiente a las siguientes funciones:

- Administrar la CPS.
- Definición de requisitos y condiciones de aceptación de las Autoridades de Registro, manteniendo el modelo de confianza de IDOK.
- Operación de la Autoridad de Registro como PSC para Firma Electrónica Avanzada.

8. Requisitos de Integración

Los servicios de certificación de IDOK interactúan de manera nativa con las aplicaciones de uso de firma electrónica, tanto para la acción de firma como la consulta de CRL y OCSP, con los navegadores de uso común.
Los dispositivos de almacenamiento seguro entregados por IDOK disponen del software necesario para interactuar con software de terceros para el uso de parte del suscriptor de los certificados. Este software estará disponible en la página web psc.idok.cl.
Para la opción de integración de soluciones propietarias, se dispone de los protocolos PKCS11 para la implementación en conjunto con el suscriptor, previa evaluación de alcances.

Adicionalmente, para los certificados en Custodia Delegada, se disponen de mecanismos de integración con software de terceros mediante APIS para el envío y recepción de órdenes de firma de documentos.

9. Procedimiento de Emisión de Certificados

A continuación, se describe el ciclo de vida completo de la emisión de certificados de Firma Electrónica Avanzada IDOK.

9.1. Solicitudes

Todas las solicitudes de emisión deben comenzar con una primera instancia por parte del solicitante, mediante los cuatro canales dispuestos para ello: de forma presencial; mediante correo electrónico a soporte@idok.cl; mediante el formulario web dispuesto en la página psc.idok.cl; mediante servicios de integración en aplicaciones o servicios propios o de terceros autorizados por la PSC, en general, y en particular en las plataformas con nombre de Fantasía Signpass+ y FirmaYa, ambos provistos directamente por BPO Advisors, dentro de su marca IDOK.
Independiente del canal, la solicitud debe contener al menos tres datos:

- Rut del futuro suscriptor
- Email del futuro suscriptor
- Nombre Completo del futuro suscriptor

El PSC dará al solicitante las instrucciones para continuar con el procedimiento.

9.2. Firma Electrónica Avanzada

Se identificará a la persona física que solicite el certificado exigiendo su personación ante los encargados de verificarla y se acreditará mediante el documento nacional de identidad, pasaporte u otros medios admitidos en derecho; o de forma no presencial mediante la solicitud de autenticación mediantes dos factores: Clave Única del Estado y desafio de preguntas de seguridad. Adicionalmente se podrá hacer exigible otro mecanismo de autenticación entre los cuales pueden estar: evidencia visual de concurrencia, prueba de vida o biométrica, o en general cualquier medio, tecnología o evidencia que se necesite para su correcta identificación.
Una vez generado el Registro, se autorizará para la emisión del certificado.

9.3. Comprobación de Solicitud

De manera interna, IDOK verificará que la evidencia generada en la solicitud de certificado de Firma Electrónica Avanzada sea veraz y exacta, utilizando todos los mecanismos, tecnologías o servicios tanto públicos como privados que tengan a su alcance.

9.4. Solicitud Aceptada

Una vez confirmada la identidad del suscriptor se indicará al suscriptor mediante correo electrónico la documentación que debe presentar, si aplicase, además de los comprobantes del pago del importe correspondiente publicado en la página web psc.idok.cl o en línea en sus plataformas web IDOK, SignPass+ o FirmaYa.

Luego, dependendiendo del tipo de certificado solicitado:

- Con etoken: El solicitante deberá presentarse en las oficinas de atención de IDOK, Dr. Barros Borgoño 110, of. 0110, Piso -1, Providencia, Santiago, en horario de 09:00 a 18:00 horas, en días hábiles, o donde le indique la PSC en el correo de aceptación, para iniciar el proceso de emisión del certificado mediante un oficial de registro capacitado y autorizado por la PSC. O se enviará un oficial de registro a la dirección acordada con el titular.
- Custodia Delegada: El solicitante se autentica con su CUE y responderá el desafío de preguntas de seguridad presentado en las plataformas de la PSC de manera correcta.
- En el caso de no ser posible su autenticación de segundo factor con preguntas de seguridad, se utilizará como mecanismo suplementario al procedimiento indicado para la modalidad etoken, presencial, o con la verificación de control de cuenta bancaria a nombre del titular, mediante una transferencia de un monto que debe corroborar el titular.

9.5. Solicitud Rechazada

Si la información de suscripción, la documentación solicitada o los requisitos de admisibilidad no son correctos, no concuerden o sean inconsistentes entre sí, se rechazará la solicitud.

9.6. Emisión de Certificados

Una vez aceptada y aprobada la solicitud se generará el certificado de acuerdo con el procedimiento técnico para la emisión de los mismos, cumpliendo con la generación de la clave privada dentro de un dispositivo de almacenamiento seguro, los cuales estarán previamente configurados para proteger su contenido con un PIN de exclusivo conocimiento del suscriptor.

El suscriptor puede delegar la custodia de la clave privada de su certificado en la PSC, la que dispondrá de un DAS tipo HSM que cumpla con los mismos estándares FIPS 140-2 nivel 3 al menos, aplicando mecanismos y procedimientos seguros para la emisión y posterior uso de las claves, los que tendrán las siguientes características:

- Se aplicarán los procedimientos técnicos pertinentes al DAS utilizado para asegurar que la clave privada nunca estará expuesta, generando en el DAS en modo no exportable y protegiéndola con un PIN de exclusivo dominio del suscriptor.
- Se aplicará un mecanismo de transporte encriptado del PIN del suscriptor mediante claves RSA emitidas dentro del DAS, para la comunicación entre el DAS y la aplicación o servicio de captura del PIN, tanto para su establecimiento como uso posterior.
- El DAS tipo HSM no deberá estar expuesto a la red pública.
- Las aplicaciones o servicios que con posterioridad requieran el uso de la clave privada deberán contar con una autorización del suscriptor mediante su PIN y proveerán a la PSC toda la documentación y evidencia necesaria para la certificación del cumplimiento del procedimiento de su captura y transporte.
- Si la PSC lo requiere, utilizará un segundo factor de autenticación para el uso de los certificados delegados mediante una contraseña de un solo uso (OTP) enviada por los canales habilitados en el enrolamiento, por ejemplo SMS a número celular ingresado por el usuario; email al correo indicado en su CUE; cualquier otro mecanismo que se haya validado en pleno control del titular en el enrolamiento.

El suscriptor con el acto de aceptación del certificado, recepción del token o delegación de custodia y firma del contrato de suscripción se obliga a:

- No revelar la clave privada del certificado, así como el PIN que la protege en el DAS.
- Custodiar el certificado, previniendo su pérdida y uso inadecuado o delegar dicha custodia en la PSC.
- Notificar a IDOK cualquier compromiso de la clave privada, robo, falsificación o pérdida.
- Devolver el certificado en caso de que IDOK lo solicite.
- Destruir el certificado si no se utiliza.
- Notificar pérdida de control de mecanismos de autenticación remota como primer factor, en particular su Clave Única del Estado (CUE).
- Notificar pérdida de control de mecanismos de autenticación de segundo factor, indicados en el proceso de solicitud de su certificado (Email, Número de teléfono).

La duración de los certificados de Firma Electrónica Avanzada será de uno, dos o tres años, de acuerdo con lo contratado por el titular.

10. Condiciones de Uso de Certificados de Firma Electrónica Avanzada

Los certificados de Firma Electrónica Avanzada emitidos por IDOK dentro de un etoken pueden ser utilizados por toda su comunidad de clientes en los lugares y operaciones que el suscriptor estime conveniente y cumpliendo con sus obligaciones como suscriptor.
Los certificados de Firma Electrónica Avanzada con Custodia Delegada emitidos por IDOK pueden ser utilizados en las plataformas que la PSC dispone para ello, o en los software o sistemas de terceros que la PSC autorice.

11. Verificación de Certificados

Mediante el protocolo OCSP toda la comunidad de clientes de IDOK y terceros que confían pueden verificar el estado de los certificados de Firma Electrónica Avanzada emitidos. Las instrucciones de uso estarán publicadas en la página web psc.idok.cl. Los usuarios que no tengan acceso al servicio pueden consultar en un formulario provisto en la misma página web.
La lista de certificados revocados (CRL) se puede utilizar para consultar los certificados que haya revocado el PSC. El repositorio de esta lista está en la página web psc.idok.cl y se puede consultar dentro de los atributos de los certificados emitidos por IDOK.
La autoridad de Registro directamente indicará costos asociados al servicio de consulta en línea de certificados OCSP, si aplicase.

12. Revocación, Suspensión de Certificados

Los certificados revocados se encuentran en la lista de revocación (CRL), publicadas en la página web psc.idok.cl.
Las causales de revocación de los certificados de Firma Electrónica Avanzada son:

- Solicitud del suscriptor.
- Pérdida del certificado o alteración física del dispositivo token que almacena el certificado.
- Fallecimiento del suscriptor.
- Por alguna eventualidad que comprometa la llave privada del suscriptor.
- Por incumplimiento de suscripción, por parte de la PSC o el suscriptor.
- Por resolución judicial o administrativa.
- Por cualquier otro motivo que exponga claramente o ponga en riesgo la llave privada del suscriptor, o no se cumpla el contrato de suscripción.

13. Expiración de Certificados

Una vez que se cumple la fecha de expiración de los certificados de Firma Electrónica Avanzada emitidos por IDOK, quedan automáticamente deshabilitados para su uso. Sin perjuicio de lo anterior, IDOK notificará a los suscriptores cuyos certificados vayan a expirar para ofrecerles la alternativa de renovación del certificado.
Los certificados de Firma Electrónica Avanzada emitidos por IDOK tienen una duración de 1 año.

14. Contenido y Estructura de Certificados

A continuación, se detallan las características del contenido de los certificados de Firma Electrónica Avanzada de IDOK:

- Versión. Deberá ser versión 3.
- Número de Serie. Identificador Único de los certificados emitidos por IDOK.
- Algoritmo de Firma. Será SHA256 con RSA.
- Datos del Emisor de la Firma. DN en formato x.500, incluyendo al menos: Tipo de certificado, email de contacto, Nombre del emisor, Rut del emisor.
- Período de validez. Fecha de inicio y término de vigencia del certificado.
- Datos del Suscriptor. Nombre completo, email, Rut como número de serie, localidad y país.
- Rut del Emisor y de Titular en OID de acuerdo a Reglamento.
- Clave Pública.

Respecto a la clave privada, ésta no podrá ser de una longitud menor a 2048 bits.

15. Almacenamiento de Certificados

Dispositivo de Almacenamiento Seguro (e-token)

Los suscriptores que operen con certificados de Firma Electrónica Avanzada emitidos por IDOK, deberán hacerlo utilizando Dispositivos de Almacenamiento Seguro, para emitir la clave privada de forma segura, con procedimientos validados por la PSC. Los DAS deben cumplir con el estándar de seguridad FIPS 140 nivel 2, de tal modo que nunca exponga la clave privada del suscriptor, la que quedará protegida por un PIN; así como su inhabilitación en caso de reiterados intentos fallidos de uso.

DAS-HSM

En el caso que el suscriptor ceda la custodia de su clave privada a la PSC en DAS de tipo HSM, el procedimiento debe asegurar que el PIN de acceso a la clave privada sea de exclusivo dominio del titular, mediante mecanismos de transporte de claves encriptadas al momento de la emisión de la misma y en el uso posterior. En cuanto a la no exposición de la clave privada y la inhabilitación en caso de reiterados intentos fallidos de uso (pin incorrecto) aplican los mismos mecanismos y procedimientos.
Se incorpora a criterio de la PSC un segundo factor de autenticación para el uso de estos certificados mediante contraseña de un solo uso (OTP) enviado por canales verificados en la etapa de enrolamiento, o cualquier otro mecanismo que la PSC determine y que informe debidamente al titular, dentro de las plataformas que opera la PSC para tales efectos (IDOK, Signpass+, FirmaYa).

16. Obligaciones del suscriptor

- El suscriptor se obliga a almacenar su certificado en los dispositivos autorizados por la PSC.
- Utilizar el certificado emitido para los fines solicitados, informando de manera oportuna a IDOK en caso de presentarse un compromiso de seguridad del mismo.
- Solicitar la revocación del certificado en caso de cumplirse las condiciones establecidas.
- No revelar la clave privada ni el PIN para acceder a ella.
- Verificar y asegurar que la información contenida en el certificado es fidedigna e informar a IDOK de cualquier información incorrecta o inexacta.

17. Confidencialidad de la información de los solicitantes

- La alta gerencia de IDOK reconoce la importancia de velar por la privacidad de la información de nuestros clientes.
- Cumplimos con las disposiciones que indica la Ley 19.496, sobre Protección al Consumidor.
- Cumplimos con las disposiciones que indica la Ley 19.628, sobre Protección a la Vida Privada.
- La información entregada por nuestros clientes es sólo para uso interno, y no es divulgada a terceras partes, salvo que un organismo competente como un Juzgado lo solicite en cumplimiento con la Legislación Chilena.

- El detalle de las políticas de privacidad se encuentra publicado en el sitio psc.idok.cl, en la sección **Políticas**.

La administración de la PSC de FEA a través de su ciclo de vida se garantiza por medio de los siguientes controles:

- Se resguarda la confidencialidad y la integridad de la información almacenada en el repositorio de uso privado.
- La base de datos de FEA se respalda en forma regular, para recuperarla en caso de falla.
- En caso de finalización del giro del PSC de FEA, los datos almacenados serán destruidos.

18. Ciclo de vida del PSC de FEA

La administración de la PSC de FEA a través de su ciclo de vida se garantiza por medio de los siguientes controles:

- Se resguarda la confidencialidad y la integridad de la información personal de los usuarios almacenada en el repositorio de uso privado.
- La base de datos de usuarios (información pública de los certificados) se respalda en forma regular, para recuperarla en caso de falla.
- En caso de finalización del giro del PSC de FEA, y si existen certificados vigentes, se contempla el traspaso de la infraestructura existente a otra PSC o quien el organismo regulador considere pertinente, para dar continuidad al servicio, sin contemplar la emisión de nuevos certificados, de modo de una vez cumplida la fecha de caducidad, se procederá a la eliminación de toda la información relacionada con la PSC de FEA.

19. Controles de Seguridad Técnica

19.1. Manejo de llaves

19.1.1. GENERACIÓN DE LLAVES DE LA AUTORIDAD CERTIFICADORA

Para el resguardo de las llaves de la CA raíz y la CA de Firma Electrónica Avanzada se utiliza un dispositivo HSM que cumple con el estándar FIPS 140-2 nivel 3 de marca Utimaco, modelo CryptoServer Se-Series Gen2. Para resguardar la integridad y confidencialidad de la parte privada de los certificados, la ceremonia de inicialización del HSM Utimaco y la generación de la llave de

la CA raíz internamente en el HSM (sin salir de él) se llevó a cabo en un sitio privado que cuenta con medidas de control de acceso con la presencia de 5 custodios de confianza en esquema 3 de 5. El acta de inicialización y creación de la clave raíz asegura que las claves se crearon en forma fiable, asegurando en todo momento la seguridad de las claves privadas, cumpliento con el estándar FIPS 140-2 nivel 3 y con ETSI TS 102 042. Las llaves creadas hacen uso del algoritmo de firma SHA-256, y del algoritmo de cifrado RSA con clave de largo 2048 bits, ambos reconocidos por la industria.

19.1.2. ALMACENAMIENTO, RESPALDO Y RECUPERACIÓN DE LA LLAVE PRIVADA

Las claves privadas de los certificados CA raíz y de la CA de Firma Electrónica Avanzada se almacenan durante todo su ciclo de vida en un dispositivo criptográfico (HSM) marca Utimaco modelo CryptoServer Se-Series Gen2 que cumple con el estándar FIPS 140-2 nivel 3. Las llaves privadas son respaldadas en caso de contingencia (por ejemplo: falla irrecuperable del HSM Utimaco productivo). El respaldo está cifrado con una clave AES de largo 256 bits que se encuentra dividida en un esquema 3 de 5, es decir, para descifrar y recuperar el respaldo es necesario la presencia de al menos 3 de las 5 personas. Para efectos de recuperación de las llaves privadas en caso de desastre se cuenta con otro dispositivo HSM marca Utimaco idéntico al que se encuentra en producción.

19.1.3. DISTRIBUCIÓN DE LA LLAVE PÚBLICA

Los componentes públicos de las llaves CA raíz y CA de Firma Electrónica Avanzada se encuentran disponibles para el acceso público en el sitio web de IDOK, y además son entregadas a la Entidad Acreditadora de manera de cumplir con el modelo de confianza que requiere la regulación existente.

19.1.4. USO DE LAS LLAVES PRIVADA

IDOK ha definido controles para el uso de la llave de la CA raíz donde se define que sólo puede ser usada para firmar CA's intermedias y no puede ser utilizada para emitir otro tipo de certificados. El repositorio de la CA raíz está resguardada de modo que no es posible acceder a ella desde redes no autorizadas.

De acuerdo a la norma vigente el uso de la llave de la CA de Firma Electrónica Avanzada puede ser utilizada sólo para firmar certificados de usuario de final del tipo firma electrónica y para emitir información relacionada con la revocación de certificados. La emisión de certificados de Firma Electrónica Avanzada requiere de al menos dos roles, uno de solicitante y otro de validador-emisor.

19.1.5. TÉRMINO DE CICLO DE VIDA DE LA CA DE FIRMA AVANZADA

En conformidad con el estándar ETSI TS 102 042 nos comprometemos a que las llaves de la CA de Firma Electrónica Avanzada no serán utilizadas más allá del final de su ciclo de vida. El uso de la llave privada de la CA de Firma Electrónica Avanzada se limita a los algoritmos y largo de la claves con un mínimo 2048 bits, algoritmo de firma SHA-256, y del algoritmo de cifrado RSA con clave de largo 2048 bits. En conformidad con el estándar ETSI TS 102 042 nos comprometemos a destruir todas las copias de las llaves privadas de la CA de Firma Electrónica Avanzada al finalizar su ciclo de vida.

19.1.6. ADMINISTRACIÓN DE CICLO DE VIDA DEL HSM

La administración de la seguridad del HSM a través de su ciclo de vida se garantiza por medio de los siguientes controles:

- La información del estado del certificado y de la revocación que firma el hardware criptográfico no se altera durante el envío al repositorio público.
- La información del estado del certificado y la revocación que firma el hardware criptográfico no se manipula durante su almacenamiento.
- La instalación, activación, copia de seguridad y recuperación de las claves privadas de la CA de Firma Electrónica Avanzada en hardware criptográfico requerirá el control simultáneo de al menos tres de cinco empleados de confianza.
- La información del estado del certificado y de la revocación que firma el hardware criptográfico está funcionando correctamente.
- Las claves privadas de la CA de Firma Electrónica Avanzada almacenadas en el hardware criptográfico de CA se destruyen al retirarse el dispositivo. Esta destrucción no afecta a todas las copias de la clave privada. Sólo se destruirá la instancia física de la clave almacenada en el hardware criptográfico considerado.

19.1.7. ADMINISTRACIÓN DE LAS LLAVES DE LOS TITULARES

Las llaves generadas para los clientes de Firma Electrónica Avanzada de IDOK utilizan el algoritmo de cifrado RSA con un largo de 2048 bits y algoritmo de firma SHA-256.
La generación del componente privado de la llave del cliente se hace en forma segura en un token que queda en poder del cliente. IDOK solo almacena las llaves privadas de los usuarios que delegan su custodia, dentro de un DAS HSM.

19.1.8. PREPARACIÓN DE LOS DISPOSITIVOS

Los dispositivos seguros entregados a los usuarios para almacenar su certificado de Firma Electrónica avanzada cumplen con los estándares de seguridad FIPS 140-2 nivel 3. Para emitir un certificado de Firma Electrónica Avanzada, el solicitante debe cumplir los requisitos de validación.

En el caso de custodia delegada, el compartimiento que aloja el certificado del titular se inicializa con el PIN generado por el usuario.

19.2. Acceso físico

19.2.1. SALA DE SERVIDORES

- Está ubicada en una zona con baja probabilidad de sufrir desastres.
- Está alejada de canalizaciones de agua (cocinas, baños, etc.).
- Cuenta con salidas de emergencia.
- Cuenta con controles para evitar daños por fuego (incendio) o agua (inundaciones).

19.2.2. DISEÑO Y CONSTRUCCIÓN

- Considera recomendaciones de Bomberos.
- Cuenta con espacios separados para servidores, sala de impresoras y consolas de operadores.
- Las puertas cuentan con sistemas de video vigilancia y sensores para evitar que permanezcan abiertas.
- No se permite la existencia de ventanas.

19.2.3. EQUIPO DE EMERGENCIA

- Se considera equipo de emergencia en cada piso del edificio.
- El equipo de emergencia incluye:
    - Alarma de incendio
    - Extintor de fuego clase ABC
    - Manguera
    - Hacha
    - Botiquín de Primeros Auxilios

- Se ha designado un encargado en caso de emergencia por cada piso del edificio.
- Los empleados son entrenados en el correcto uso de los extintores y el equipo de emergencia.

19.2.4.SUMINISTRO ELÉCTRICO

- Se considera el suministro ininterrumpido de la energía eléctrica (UPS) para el equipamiento crítico.
- Se identifican enchufes conectados a la UPS para evitar conectar equipo que no corresponda a este suministro.
- Los tableros de energía eléctrica se mantienen seguros, con llave.
- Se cuenta con al menos dos botones de pánico para el corte de energía eléctrica en caso de emergencia, en el ingreso principal y en la salida de emergencia.
- Se protegen los botones de pánico para evitar una activación casual.
- Se verifica la conexión a tierra.

19.2.5.CONTROL DE AMBIENTE

- Las condiciones ambientales de la sala cumplen con los requerimientos de los equipos que alberga.
- Los ductos utilizados para el aire acondicionado (HVAC) son incombustibles.
- Los sistemas de HVAC están conectados al sistema de alarma de modo de cortar el suministro en caso de emergencia.
- Los equipos de HVAC están protegidos para evitar una manipulación por personal no autorizado.
- Se considera un sistema de alarma para la temperatura y humedad ambiental.

19.2.6.VIGILANCIA

- La cantidad de vigilantes es adecuada para el tamaño de las instalaciones a supervisar.
- Los vigilantes reciben una instrucción básica para:
    - Reconocer la ubicación y propósitos generales de las instalaciones
    - Todo personal que accede a las instalaciones debe contar con las autorizaciones pertinentes.
    - Debe conocer las políticas de seguridad que debe cumplir.
    - Debe controlar que el personal no coma o beba dentro de las instalaciones.

- Se encuentra prohibido fumar dentro de las instalaciones.

20. Controles de Seguridad no Técnica

RRHH

- Los candidatos a ocupar puestos de trabajo en IDOK son investigados, usando los contactos de referencia de IDOK anteriores. Este proceso deberá buscar antecedentes de veracidad del Currículo, confirmación de credenciales académicas y profesionales, así como de los documentos de identidad presentados.
- Todos los colaboradores de IDOK firman un acuerdo de confidencialidad
- Los roles y responsabilidades en la seguridad están debidamente documentados.
- Los colaboradores de IDOK son entrenados en los aspectos de las políticas y procedimientos de seguridad, así como en lo que respecta a requerimientos de seguridad, responsabilidades legales y controles en uso, herramientas de trabajo, aplicaciones, etc., antes de autorizar su acceso a información. El entrenamiento se hace extensivo a colaboradores de terceros que deban realizar actividades que involucren acceso a información de carácter sensible para IDOK.
- Los colaboradores que deliberadamente no respeten las políticas, procedimientos e instructivos de seguridad de la información serán sancionados de acuerdo al modelo definido en el reglamento interno de trabajo.

21. Personal para prestación de servicios

El proceso de administración llaves considera personal entrenado y confiable encargado de las siguientes actividades:

- Administrador de la AC
    - Instala y configura el sistema operativo y software básico.
    - Instala y configura el software EJBCA y sus componentes relacionados.
    - Se preocupa de mantener actualizados los productos indicados en los puntos anteriores.
    - Verifica la publicación y actualización periódica de las listas de revocación (CRL y OCSP).
    - Activar los registros de auditoría.
    - Realizar el respaldo de la información según la frecuencia definida.

    - Responsable de recuperación ante la falla de un componente o ante un desastre.
- Oficial de Seguridad
    - Vela por el cumplimiento de las políticas de seguridad definidas y aprobadas por la dirección de IDOK.
    - Vela por la seguridad de todos los componentes que forman el servicio de Firma Electrónica Avanzada de IDOK.
- Custodios
    - Tienen a su cargo proteger el material criptográfico maestro del HSM (Master Key).
- Operador de Registro
    - Encargado del ingreso de la solicitud del cliente de Firma Electrónica Avanzada.
    - Se preocupa de validar la identidad de quien solicita comprobando los datos en base a un documento emitido por la autoridad competente.
- Operador de Validación
    - Valida la información entregada por el solicitante.
    - Autoriza la emisión del certificado.
    - Encargado de gestionar la revocación de certificados.

22. Formato del Certificado y registro de acceso público

El formato y la estructura de los certificados se describe en el documento “TB01 Estructura Certificados”.
El registro de acceso público para solicitar certificados se encuentra en https://psc.idok.cl/solicitud-de-certificado/.

23. Administración de la Política de Certificación

La Política de Certificación de la PSC de FEA es revisada en forma anual, teniendo en consideración los cambios en la regulación, en el personal, las tecnologías y los requerimientos del servicio.

El procedimiento para cambiar, publicar y notificar los cambios a la política son los siguientes:

- Elaboración del documento con los cambios que se estimen necesarios
- Aprobación del documento por el Comité de Seguridad
- Notificación al Ministerio de Economía por medio de la Oficina de Partes
- Publicación en el sitio web https://psc.idok.cl