2025

Política de Certificación de la CA

ÍNDICE

1. Información del documento 4
1.1. Creador del documento 4
1.2. Control de versiones 4
2. Introducción 5
3. Alcance 6
4. Referencias y glosario 7
4.1. Referencias 7
4.2. Glosario 8
5. Aplicabilidad y comunidad de usuarios 9
5.1. Comunidad de usuarios 9
5.2. Aplicabilidad 9
5.2.1. Autenticación 9
5.2.2. No Repudio 9
5.2.3. Integridad 10
6. Tipos y usos de certificados 10
7. Datos de contacto 10
8. Requerimientos generales y operacionales 11
8.1. Obligaciones 11
8.1.1. Obligaciones de CA Raíz 11
8.1.2. Obligaciones de CA 11
8.1.3. Obligaciones con los suscriptores 12
8.1.4. Obligaciones del suscriptor 12
8.1.5. Obligaciones Generales de BPO-Advisors|IDOK como PSC 12
8.1.6. Obligaciones del solicitante 13
8.1.7. Procedimiento de consultas o reclamos 13
8.2. Lista de revocación y estructura de información 14
8.2.1. Certificados de Firma Electrónica Avanzada 14
8.2.2. Confianza en la Firmas 14
8.2.3. Confianza en los Certificados 14
9. Protección de información 15

9.1. Información que se puede entregar 15
10. Declaración operacional 15
10.1. Registro inicial 15
10.2. Reemisión de certificados 16
10.3. Revocación 16
10.3.1. Posibles causas de Revocación 16
10.3.2. Formas de Revocación 16
10.3.3. Canales de atención para la Revocación 16
10.3.4. Publicación de la Revocación 17
10.4. Suspensión 17
10.5. Caducidad 17
10.6. Renovación 17
10.6.1. Solicitud de Renovación 18
10.6.2. Procedimiento de Renovación 18
10.7. Portabilidad 18
10.8. Término de actividades de la PSC 19
10.9. Auditorías 19
10.10. Administración y modificaciones 19
10.11. Publicación de modificaciones 20

1. Información del documento

1.1. Creador del documento

Responsable documento	Oficial de Seguridad

1.2. Control de versiones

Versión	Fecha de vigencia	Aprobación	Comentario
001	26 de julio de 2017	Oficial de Seguridad	Creación del documento
002	27 de agosto de 2017	Oficial de Seguridad	Revisión del documento
003	4 de septiembre de 2018	Oficial de Seguridad	Revisión del documento
004	15 de mayo de 2020	Oficial de Seguridad	Nueva versión
005	20 de marzo de 2021	Oficial de Seguridad	Revisión del documento
006	6 de diciembre de 2021	Oficial de Seguridad	Actualización del documento
007	15 de abril de 2022	Gerente General	Actualización del documento
008	16 de agosto de 2022	Comité de Seguridad	Actualización del documento
009	28 de octubre de 2022	Comité de Seguridad	Actualización del documento
010	5 de enero de 2023	Comité de Seguridad	Actualización del documento
011	Enero de 2024	Comité de Seguridad	Actualización del documento
012	Enero de 2025	Oficial de Seguridad	Observaciones IAO 2024
013	Junio de 2025	Oficial de Seguridad	Observaciones IAO 2024

2. Introducción

BPO-Advisors|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.

Definiciones:

- BPO-Advisors|IDOK es la empresa acreditada ante el Ministerio de Economía como Prestadora de Servicios de Certificación (PSC).
- IDOK es otro nombre legalizado de la empresa BPO-Advisors|IDOK.
- Los sitios web de ambas son www.bpo-advisors.net y www.idok.cl.
- Firmaya es el nombre del producto mediante el cual BPO-Advisors|IDOK entrega a sus clientes servicios de gestión documental y firmado con firma electrónica avanzada por uso o por actos de firma.
- El sitio web de Firmaya es www.firmaya.cl.
- El sitio web donde los clientes se registran para obtener los certificados de firma electrónica avanzada es signpass-plus.idok.cl. Dicho sitio web realiza el proceso de enrolamiento para nuevos clientes y el proceso de firma de los documentos con el certificado digital asociado al cliente.

En este contexto, Firmaya (www.firmaya.cl) como un gestor documental asociado de BPO-Advisors|IDOK, vende el servicio de firmado de documentos a clientes finales, pero todo el proceso de enrolamiento, gestión y custodia de los certificados digitales es responsabilidad de BPO-Advisors|IDOK.

Otras empresas, servicios o plataformas asociadas comercialmente a BPO-Advisors|IDOK para la gestión documental, o con las cuales existen integraciones, alianzas o convenios pueden ser consultadas en la página web https://alianzas.idok.cl. Dentro de dicha web se dispone de toda la información relacionada a dichos convenios y alianzas y se establecen canales de consulta para usuarios o clientes finales.

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.

3. Alcance

El Alcance de la Declaración de Políticas de Certificación (CP) detalla las condiciones de los servicios de certificación que presta BPO-Advisors|IDOK para la emisión de sus certificados de Firma Electrónica Avanzada.

4. 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:

4.1. 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.

4.2. 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 BPO-Advisors|IDOK.
Usuarios: El usuario del certificado es la persona que decide usar los certificados emitidos por BPO-Advisors|IDOK y hace uso de ellos.
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.

5. Aplicabilidad y comunidad de usuarios

5.1. Comunidad de usuarios

BPO-Advisors|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.
b. En su defecto, 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 BPO-Advisors|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.

Los certificados emitidos por BPO-Advisors|IDOK podrán ser uso en las siguientes necesidades de seguridad:

5.2.1. Autenticación

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 BPO-Advisors|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 BPO-Advisors|IDOK permite validar que el elemento firmado no cambia su contenido desde el momento de la firma.

6. Tipos y usos de certificados

BPO-Advisors|IDOK posee la infraestructura para la emisión de certificados de Firma Electrónica Avanzada. La estructura de estos certificados cumple y es compatible con el estándar ISO/IEC 9594-8 y el contenido de cada certificado cumple con el Reglamento de la Ley 19.799. Dicha estructura debe contener al menos los siguientes datos:

- RUT
- Correo electrónico del suscriptor
- Nombre completo del suscriptor
- Tipo de certificado
- Datos de BPO-Advisors|IDOK y de su acreditación.

7. Datos de contacto

Cualquier consulta respecto a lo contenido en este documento puede ser realizada en la siguiente dirección:

- Nombre: BPO-Advisors|IDOK PSC
- Dirección de contacto: Dr. Barros Borgoño 110, of. 0110, Piso -1, Providencia, Santiago
- Correo electrónico: contacto@idok.cl

8. Requerimientos generales y operacionales

8.1. Obligaciones

BPO-Advisors|IDOK, en su calidad de PSC se obliga a ejecutar sus actividades de certificación acorde con las Prácticas de certificación asociadas a cada tipo de certificador. Para mayores detalles, remitirse a lo especificado en la Declaración de Prácticas de Certificación (CPS).

8.1.1. Obligaciones de CA Raíz

El certificado raíz de BPO-Advisors|IDOK (IDOK ROOT) permite firmar aquellos certificados de sus CA subordinadas. De esta manera, el modelo de confianza de toda la jerarquía se basa en este certificado raíz que BPO-Advisors|IDOK ha generado para sí mismo, con el que en particular firmará el certificado Intermedio de Firma Electrónica Avanzada.

8.1.2. Obligaciones de CA

BPO-Advisors|IDOK, como CA, cumple con las obligaciones necesarias y legales para prestar servicios de certificación electrónica, como, por ejemplo:

- Identificar y autenticar correctamente al suscriptor o usuario de firma electrónica usando correctamente los procedimientos de CA para estos efectos.
- Controles de Seguridad Física.
- Emitir certificados a quienes lo soliciten.
- Administrar un sistema de llaves (PKI) para hacer operativa la certificación y firma electrónica.
- Emitir y mantener la lista de certificados emitidos y revocados.
- Cumplimiento a todas las obligaciones legales necesarias para el ejercicio de esta actividad.
- Emisión de Certificados:
  - BPO-Advisors|IDOK emitirá certificados que sean solicitados previa aprobación de los antecedentes necesarios de la persona.
- Administración de llaves:
  - BPO-Advisors|IDOK puede emitir de forma automática la llave pública y privada que se le entrega al titular, o manual dentro de un dispositivo seguro de almacenamiento, garantizando en ambos casos la confidencialidad de la llave privada.
  - BPO-Advisors|IDOK puede almacenar de manera delegada la llave privada de un titular, bajo su expreso consentimiento dentro de un dispositivo de

almacenamiento seguro cumpliendo los mismos estándares de seguridad y asegurando mediante los mecanismos pertinentes que solamente el titular tendrá acceso a su llave personal.

8.1.3. Obligaciones con los suscriptores

- Garantizar que la información suscrita en el certificado es exacta y fiel reflejo de la información entregada por el suscriptor en el acto de emisión del certificado, utilizando si es necesario todas las herramientas de verificación a su alcance.
- Hacer uso de la tecnología adecuada, tanto en Hardware como Software, para la emisión de los certificados.
- Informar preventivamente la proximidad de la caducidad de los certificados.
- Revocar los certificados que no cumplan con las prácticas adecuadas de firma electrónica, o a petición del suscriptor.
- Proveer lista de certificados revocados actualizada al menos una vez al día.
- Poseer procedimientos y políticas adecuadas para el resguardo de la llave privada del suscriptor.

8.1.4. Obligaciones del suscriptor

- Conservar y dar uso adecuado al certificado.
- Dar correcta custodia al certificado, resguardar su clave privada y no dar mal uso a ambos.
- Proteger el uso de su certificado mediante PIN dentro de un dispositivo token, o delegar su custodia a la PSC en un Dispositivo de Almacenamiento Seguro (HSM).
- Informar a la PSC inmediatamente por cualquier situación que afecte directamente la validez del certificado, o si su clave privada se ve comprometida.
- Realizar un uso adecuado del certificado según lo descrito en contrato de suscripción.

8.1.5. Obligaciones Generales de BPO-Advisors|IDOK como PSC

- BPO-Advisors|IDOK tiene políticas claras respecto al uso de infraestructura de llaves pública (PKI) para Firma Electrónica Avanzada y se encuentra publicada en su página web psc.idok.cl, disponible de manera pública.
- Si BPO-Advisors|IDOK decide dar término a sus funciones de firma electrónica avanzada, dará a conocer su decisión a todos sus suscriptores activos y transferirá todos sus certificados a otro prestador de firma electrónica avanzada. Los suscriptores pueden negarse a dicha transferencia, en cuyo caso el certificado quedará en estado revocado.
- BPO-Advisors|IDOK cumplirá todas las leyes que rigen este tipo de actividades, como la Ley Nº19.496, Sobre Protección a los Derechos del Consumidor y de protección de la vida privada Nº19.628.

- BPO-Advisors|IDOK mantiene los registros de todos sus certificados emitidos y revocados durante el período que exige y que rige la actividad de firma electrónica avanzada, ley Nº 19.799. Este registro estará disponible para el acceso público en el sitio web psc.idok.cl.
- BPO-Advisors|IDOK debe publicar todas las resoluciones de la entidad acreditadora, con acceso al público general en la página web psc.idok.cl.
- BPO-Advisors|IDOK informará preventivamente a la entidad acreditadora de cualquier evento que afecte directamente la continuidad operacional como entidad acreditada para PSC.
- Cada certificado de firma electrónica avanzada emitido por BPO-Advisors|IDOK representa la identidad del suscriptor, y es por esa razón que cada solicitud de certificado requiere la comparecencia de la persona o su correcta identificación de manera remota mediante Clave Única del Estado y segundo factor de autenticación.
- BPO-Advisors|IDOK se compromete a pagar anualmente el arancel de supervisión que realiza la entidad acreditadora.
- BPO-Advisors|IDOK se compromete a mantener vigente el seguro de responsabilidad civil que exige la Ley de Firma Electrónica y Documentos Electrónicos Nº19.799.
- BPO-Advisors|IDOK se compromete a mantener constantemente el registro electrónico de los antecedentes de los suscriptores.
- BPO-Advisors|IDOK se compromete a almacenar de forma segura la documentación que evidencie la emisión de sus certificados a algún suscriptor por el período de tiempo que exija la ley.

8.1.6. Obligaciones del solicitante

- Entregar toda la información de identificación personal que se le solicite, lo que puede incluir, datos personales, datos de contacto, documento de identificación, evidencia visual de concurrencia, prueba de vida o biométrica, o en general cualquier medio, tecnología o evidencia que se necesite para su correcta identificación.
- El solicitante deberá cancelar la tarifa establecida y publicada en la página web https://psc.idok.cl

8.1.7. Procedimiento de consultas o reclamos

BPO-Advisors|IDOK dado cumplimiento a la Ley Nº19.496, Sobre Protección de los Derechos de los Consumidores, ha desarrollado un procedimiento para la atención de consultas y reclamos:
El cliente, que tenga alguna consulta o reclamo, podrá realizarlas mediante alguna de las siguientes opciones:

- Por correo electrónico a soporte@idok.cl.
- En la página web https://psc.idok.cl/contacto, donde deberá ingresar su correo, nombre e indicar su consulta o reclamo.

A esta comunicación, se le asignará un ejecutivo y generará un número de ticket, que será enviado a su correo electrónico.
Posteriormente, se contactará para resolver la consulta o reclamo.
Las posibles soluciones incluyen las opciones indicadas por la Ley del Consumidor, además de resolver consultas de operación u otras, relacionadas con su adquisición.

8.2. Lista de revocación y estructura de información

En la página web de BPO-Advisors|IDOK https://psc.idok.cl están los repositorios donde se informan los certificados emitidos y revocados para Firma Electrónica Avanzada.

8.2.1. Certificados de Firma Electrónica Avanzada

URL del repositorio de la lista de certificados revocados: http://pki.idok.cl:8080/ejbca/publicweb/webdist/certdist?cmd=crl&issuer=E=soporte@idok.cl,CN=CA FIRMA ELECTRONICA AVANZADA IDOK,OU=RUT-76610718-4,OU=Autoridad Certificadora,O=BPO Advisors SpA,L=Santiago,C=CL

8.2.2. Confianza en la Firmas

Las personas o entidades que reciben alguna firma electrónica avanzada realizada con un certificado emitido por BPO-Advisors|IDOK tienen derecho a confiar en ello:

- Que la operación que se utilizó para firmar tiene todos los resguardos de seguridad y uso de llaves privadas y públicas del suscriptor.
- Que el certificado que se utilizó en el acto de firma del elemento no tenga estado caducado al momento de la firma.

8.2.3. Confianza en los Certificados

Las personas que utilicen o reciban un elemento firmado por un certificado de firma electrónica avanzada emitido por BPO-Advisors|IDOK tendrán derecho a confiar en dicho certificado.

9. Protección de información

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. Sin perjuicio de lo anterior, se utilizará la siguiente información dentro de los certificados emitidos:

9.1. Información que se puede entregar

Según la ley Nº 19.799 y todos sus procedimientos técnicos exigidos, la información contenida en los certificados será:

- RUT
- Correo electrónico del suscriptor
- Nombre completo del suscriptor
- Tipo de certificado
- Datos de BPO-Advisors|IDOK y de su acreditación.

Para el caso de la información de certificados emitidos y revocados por BPO-Advisors|IDOK, los procedimientos y/o listas se encuentran disponibles en el sitio web https://psc.idok.cl

10. Declaración operacional

10.1. Registro inicial

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 mediante dos factores: Clave Única del Estado y desafío de preguntas de seguridad.

Toda la información generada durante el proceso de solicitud de certificado será digitalizada para su almacenamiento y búsqueda en caso de ser requerido, en un sistema definido especialmente para este propósito.

Una vez generado el Registro, se autorizará para la emisión del certificado.

10.2. Reemisión de certificados

Los certificados de firma electrónica avanzada emitido por BPO-Advisors|IDOK, con el fin de asegurar su no repudio, no consideran la reemisión de estos ya que sólo consideran dos estados: Vigente o Revocado.

10.3. Revocación

Las solicitudes de revocación de los certificados de firma electrónica avanzada emitidos por BPO-Advisors|IDOK se realizarán por vía electrónica en la página web https://psc.idok.cl, o por correo electrónico directo a soporte@idok.cl.

El procedimiento de revocación es presencial, donde el solicitante debe llenar un "Formulario de Solicitud de Revocación" y el oficial de registro validará su identidad por medio del documento nacional de identidad, pasaporte u otros medios admitidos en derecho.

Toda la información generada durante el proceso de revocación será digitalizada para su almacenamiento y búsqueda en caso de ser requerido, en un sistema definido especialmente para este propósito.

10.3.1. Posibles causas de Revocación

- Solicitud del titular del certificado.
- Fallecimiento del titular o disolución de la persona jurídica que represente, en su caso.
- Resolución judicial ejecutoriada.
- Que el titular del certificado al momento de solicitarlo no proporcionó los datos de la identidad personal u otras circunstancias objeto de certificación, en forma exacta y completa.
- Que el titular del certificado no ha custodiado adecuadamente los mecanismos de seguridad del funcionamiento del sistema de certificación que le proporcione el certificador.
- Que el titular del certificado no ha actualizado sus datos al cambiar éstos.

- Las demás causas que convengan el prestador de servicios de certificación con el titular del certificado, por ejemplo: la CA puede revocar o suspender unilateralmente en caso de sospecha de compromiso de claves o suplantación de identidad.

10.3.2. Formas de Revocación

La revocación se genera mediante solicitud previa, por cualquiera de los canales que posee la CPS para estos efectos o por la concurrencia del suscriptor del certificado.

10.3.3. Canales de atención para la Revocación

- Por correo electrónico a soporte@idok.cl.
- En la página web https://psc.idok.cl

10.3.4. Publicación de la Revocación

El acto de revocación será comunicado al suscriptor, así como el origen de la decisión, de la misma, vía correo electrónico.

Cualquier forma de acción o solicitud de revocación será publicada en la lista de certificados revocados (CRL), disponible en https://psc.idok.cl

10.4. Suspensión

La suspensión de certificados, se trata como un caso particular de revocación, con la diferencia de que es a criterio de la PSC y considera un código especial de estado de revocación el cual es “Certificado retenido (6)” (“Certificate Hold”). Este estado de revocación tiene la particularidad de poder revertirse, es decir, regresar el certificado a estado “válido”, eliminándolo de la CRL.

El procedimiento para suspender un certificado, es el siguiente:

- Se solicita internamente mediante un ticket la suspensión de un certificado indicando la causa.
- El administrador de la Autoridad Certificadora procede a identificar y suspender el certificado.
- Se emite una nueva versión de la CRL y se verifica que el certificado está en suspensión.
- Se deja constancia de la suspensión del certificado en el mismo ticket

Posibles causales de suspensión de un certificado:

a. Solicitud del titular del certificado.
b. Decisión del prestador de servicios de certificación en virtud de razones técnica:.

- Falta de cumplimiento temporal de requisitos contractuales.

  Cuando el suscriptor incumpla, de manera temporal y subsanable, alguna obligación relacionada con el contrato de suscripción del certificado digital.

- Investigación en curso sobre el uso del certificado.

  Si el certificado está involucrado en una investigación por posible mal uso o uso no autorizado, se podrá suspender mientras se esclarecen los hechos.

- Mantenimiento o actualización del sistema de certificación.

  En casos donde se realicen actualizaciones, mantenimientos o migraciones que puedan requerir la suspensión temporal del certificado por razones técnicas.

El efecto de la suspensión del certificado es el cese temporal de los efectos jurídicos del mismo conforme a los usos que le son propios e impide el uso legítimo del mismo por parte del titular.

La suspensión del certificado terminará por cualquiera de las siguientes causas:

a. Por la decisión del prestador de servicios de certificación de revocar el certificado, en los casos previstos en la Ley.
b. Por la decisión del prestador de servicios de certificación de levantar la suspensión del certificado, una vez que cesen las causas técnicas que la originaron.
c. Por la decisión del titular del certificado, cuando la suspensión haya sido solicitada por éste.

Una vez que se han subsanado las causales de suspensión el certificado se revierte al estado válido quitándolo de la siguiente CRL que se emite, de acuerdo al siguiente procedimiento:

- Se solicita internamente mediante un ticket, indicando que las causales de suspensión están subsanadas.
- El administrador de la Autoridad Certificadora procede a identificar y revertir la suspensión del certificado en la PKI.
- Se emite una nueva versión de la CRL y se verifica que ya no está revocado el certificado.
- Se deja constancia de que la suspensión del certificado se ha revertido en el mismo ticket.

10.5. Caducidad

Luego de finalizado el período de vigencia del certificado, caduca de forma automática. Se informará al suscriptor del certificado de forma anticipada a la fecha de caducidad para que pueda decidir preventivamente su total caducidad o renovación.

La caducidad del certificado produce su invalidez de forma automática, caducando también los servicios de certificación.

10.6. Renovación

El procedimiento de renovación se ejecutará cuando el certificado está próximo a caducar y el suscriptor decida su renovación con el mismo PSC.

Se emitirá un nuevo certificado y se generarán nuevas llaves, requiriendo una nueva verificación de identidad del suscriptor.

Los certificados emitidos por BPO-Advisors|IDOK tienen una vigencia de 1, 2 y 3 años y para su renovación se debe cumplir:

- Que exista un certificado previo emitido por la PSC para el suscriptor
- Que el suscriptor solicite la renovación antes de la fecha de caducidad del certificado original.
- Que el PSC verifique que no exista una revocación previa del certificado original.

10.6.1. Solicitud de Renovación

Se utilizará el mismo formulario de solicitud de certificado indicando que es una renovación, en la página web psc.idok.cl. Si se cumplen los requisitos para la renovación se le enviará un correo al suscriptor indicando e incluyendo los pasos siguientes del procedimiento.

En el caso que el certificado emitido sea en modalidad custodia delegada la renovación será inmediata una vez el suscriptor previa autenticación complete el formulario provisto para ello y haya cancelado el arancel correspondiente a la renovación.

10.6.2. Procedimiento de Renovación

Una vez recibida la solicitud y verificado que cumple con los requisitos. Se procesa la solicitud de la misma forma como se procesa una solicitud de certificado de firma electrónica avanzada, con las siguientes diferencias:

- Se verificará la vigencia de la evidencia almacenada que confirma la identidad del suscriptor, requiriendo un nuevo procedimiento de enrolamiento si se considera vencido.
- Se utilizará el mismo dispositivo de almacenamiento de las llaves e-token, si está operativo; se le solicitará al suscriptor la adquisición de uno nuevo; o en dispondrá en el dispositivo de almacenamiento seguro indicado si existe una cesión de custodia a la PSC.

10.7. Portabilidad

Si un suscriptor de la modalidad de certificación con custodia delegada lo desea, puede solicitar el traspaso de su certificado custodiado a un ETOKEN adquirido previamente en BPO-Advisors|IDOK. Para esto se establece el siguiente procedimiento:

- Suscriptor solicita la portabilidad con correo electrónico a contacto@idok.cl, indicando su voluntad y si posee el dispositivo ETOKEN. Si no lo posee se le ofrecerá adquirir uno. Además, se le indicará si aplican cargos para el procedimiento y las alternativas de pago.
- Se coordinará con el suscriptor visita a las oficinas de la PSC para realizar procedimiento.
- El suscriptor, al acudir a la oficina debe portar su cédula de identidad vigente, con la cual el oficial de registro realizará todas las validaciones que aplican.
- Se solicitará al suscriptor el ETOKEN para su preparación.
- El suscriptor ingresará directamente en el ETOKEN su pin de acceso.
- El suscriptor deberá autenticarse en las interfaces de la autoridad de registro de custodia delegada
- El suscriptor debe ingresar el pin de acceso de su certificado con custodia delegada
- Se completa el procedimiento y se entrega ETOKEN al suscriptor.

10.8. Término de actividades de la PSC

En el caso del cese de actividades de la PSC se declaran las siguientes medidas:

- Comunicación preventiva del cese de actividades:
  - Notificación por correo certificado o correo ordinario.
  - Publicación de un anuncio en al menos dos diarios de divulgación nacional.

- Toda información se realizará al menos 60 días antes de la fecha indicada de cese definitivo.

- Se transferirán todas las obligaciones y derechos de los certificados a otra PSC existente, bajo el pleno conocimiento del suscriptor.
- Si no es posible transferir los certificados, se revocarán.
- Se indemnizará a los suscriptores que lo soliciten por sus certificados revocados con fecha anterior a la fecha de vigencia, del mismo, con tope el costo del servicio descontando los días de vigencia hasta la fecha de revocación.

10.9. Auditorías

Los procedimientos y frecuencia de las Auditorías de la Entidad Acreditadora dependiente del Ministerio de Economía están regidos por las guías de acreditación y a lo informado en la página web http://www.entidadacreditadora.gob.cl.

10.10. Administración y modificaciones

BPO-Advisors|IDOK podrá hacer cambios en sus procedimientos manteniendo siempre los estándares exigidos y justificables desde un punto de vista Técnico, Comercial y/o Jurídico, las veces que estime conveniente y debidamente publicado.

10.11. Publicación de modificaciones

Todo cambio en la CP o CPS o cualquier política que involucre directamente la operación de los certificados será informada por los canales adecuados a todos sus suscriptores y solicitantes en un período no superior a 10 días hábiles desde la aplicación de los cambios.

Luego del comunicado. Y si no se recibe ninguna declaración por escrito de suscriptores o solicitantes en contra de lo comunicado, las modificaciones se declararán como aceptadas por la comunidad de usuarios.