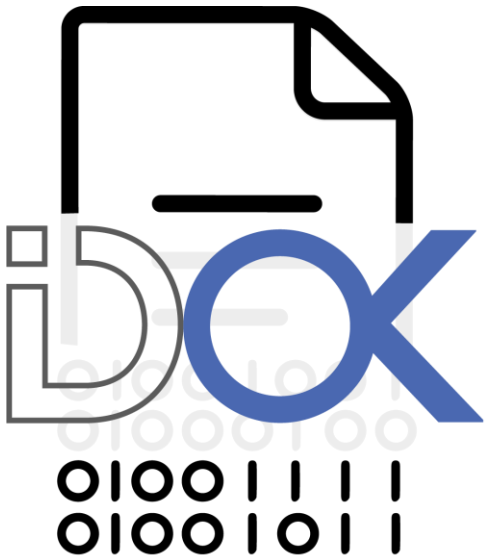

# PO01 – POLÍTICA DE CERTIFICACIÓN


## Resumen

Documento conteniendo la Política de Certificación de Firma Electrónica Avanzada

# 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 Políticas de Certificación (CP) 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 Infraestrure Certificate Policy and Certification Practices Framewrok”, 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.
- **Subscriptor de un Certificado**: Corresponde a la persona o empresa a la cual se emitió el certificado. Este subscriptor posee una llave pública y otra privada que son utilizadas en cada firma que realice. Según la ley el subscriptor 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 llevara 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.

# 4. Aplicabilidad y Comunidad de Usuarios

### 4.1. 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 su presencia física.

### 4.2. 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.
Los certificados emitidos por IDOK podrán ser uso en las siguientes necesidades de seguridad:

#### 4.2.1. 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 y al exigir el almacenamiento de la llave privada en un dispositivo acreditado según norma FIPS-140 nivel 2.

#### 4.2.2. 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

#### 4.2.3. Integridad

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

#### 4.2.4. PRIVACIDAD

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

## 5. Tipos y usos de Certificados

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 subscriptor
- Nombre completo del subscriptor
- Tipo de certificado
- Datos de IDOK y de su acreditación.

## 6. Datos de Contacto

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

- Nombre: IDOK PSC
- Dirección de contacto: AV. Dardignac 08 piso 4, Providencia, Santiago
- Correo electrónico: contacto@idok.cl

## 7. Requerimientos Generales y Operacionales

### 7.1. OBLIGACIONES

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, remitir a lo especificado en la Declaración de Prácticas de Certificación (CPS).

#### 7.1.1. OBLIGACIONES DE CA RAÍZ

El certificado raíz de 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 IDOK ha generado para sí mismo, con el que en particular firmará el certificado Intermedio de Firma Electrónica Avanzada.

#### 7.1.2. OBLIGACIONES DE CA

IDOK, como CA, cumple con las obligaciones necesarias y legales para restar 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:
    - IDOK emitirá certificados que sean solicitados previa aprobación de los antecedentes necesarios de la persona.
- Administración de llaves:
    - 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.
    - 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.

#### 7.1.3. 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 cono 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.

#### 7.1.4. 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.

#### 7.1.5. OBLIGACIONES GENERALES DE IDOK COMO PSC

- 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 IDOK decide dar término a sus funciones de firma electrónica avanzada, dará a conocer su decisión a todos sus suscriptores activos y transferir 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.
- IDOK cumplirá todas las leyes que rigen este tipo de actividades, como la ley del consumidor Nº 19.496 y de protección de la vida privada Nº 19.628.
- IDOK mantiene los registros de todos sus certificados emitido 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.
- IDOK debe publicar todas las resoluciones de la entidad acreditadora, con acceso al público general en la página web psc.idok.cl.
- 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 IDOK representa la identidad del suscriptor, y es por esa razón que cada solicitud de certificado requiere la comparecencia de la persona.
- IDOK se compromete a pagar anualmente el arancel de supervisión que realiza la entidad acreditadora.
- IDOK se compromete a mantener vigente el seguro de responsabilidad civil que exige la ley de firma electrónica y documentos electrónicos Nº 19.799.
- IDOK se compromete a mantener constantemente el registro electrónico de los antecedentes de los suscriptores.
- 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.

#### 7.1.6. 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 psc.idok.cl.

### 7.2. Lista de Revocación y Estructura de Información

En la página web de IDOK psc.idok.cl están los repositorios donde se informan los certificados emitidos y revocados para Firma Electrónica Avanzada.

#### 7.2.1. 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=C

#### 7.2.2. Confianza en la Firmas

Las personas o entidades que reciben alguna firma electrónica avanzada realizada con un certificado emitido por 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.

#### 7.2.3. Confianza en los Certificados

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

## 8. 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:

### 8.1. 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 subscriptor
- Nombre completo del subscriptor
- Tipo de certificado
- Datos de IDOK y de su acreditación.

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

# 9. Declaración Operacional

### 9.1. 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. 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.

### 9.2. Reemisión de Certificados

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

### 9.3. Revocación

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

#### 9.3.1. Posibles causas de Revocación

- 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.

#### 9.3.2. 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.

#### 9.3.3. Canales de atención para la Revocación

- Comunicación telefónica para inicio del procedimiento, al número: +56 23 231 72 78
- Por correo electrónico a soporte@idok.cl
- En la página web psc.idok.cl.

#### 9.3.4. 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 psc.idok.cl.

### 9.4. 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.

### 9.5. Renovación

El procedimiento de renovación se ejecuta cuando el certificado está próximo a caducar y el suscriptor decide su renovación con la misma PSC.
Se emitirá un nuevo certificado y se generarán nuevas llaves, requiriendo una nueva verificación de identidad del suscriptor.
Los certificados emitidos por IDOK tienen una vigencia de 1 año 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 la PSC verifique que no exista una revocación previa del certificado original.

#### 9.5.1. 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 indicándolo e incluyendo los pasos siguientes del procedimiento.

#### 9.5.2. PROCEDIMIENTO DE RENOVACIÓN

Una vez recibida la solicitud y verificado que cumple con los requisitos. Se procesará 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 vencida.
- 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.

### 9.6. 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 el cese.
  - 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 consentimiento 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.

### 9.7. AUDITORÍAS

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

### 9.8. ADMINISTRACIÓN Y MODIFICACIONES

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.

### 9.9. 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 escritor de suscriptores o solicitantes en contra de lo comunicado, las modificaciones de declararán como aceptadas por la comunidad de usuarios.