2024

Política y Declaración de Prácticas de Certificación

Índice

1 INFORMACIÓN DEL DOCUMENTO

1.1. NOMBRE Y RESPONSABLE

Nombre del documento	Política y Declaración de Prácticas de Certificación de BPO
Responsable documento	Responsable de la EC y la TSA
Tipo de documento	Público
Realizado por	INNOVATE DC

1.2 CONTROL DE VERSIONES

Versión	Fecha de vigencia	Aprobación	Comentario
1.0	Enero 2024	Responsable de la EC y la TSA	Creación del documento

1.3 OID

OID	1.3.6.1.4.1.50718.0.1.0.1.1

2 INTRODUCCIÓN

BPO ADVISORS SPA, SUCURSAL DEL PERÚ que en adelante llamaremos "BPO", es una empresa chilena fundada el 2016, la cual brinda servicios relacionados a la identificación digital, firma electrónica avanzada y cualificada que pueden ser integrados a sistemas documentales y plataformas web en diversos países de Latinoamérica y el mundo. La información relevante de BPO es aquella que sirve principalmente para la autenticación de la identidad de personas, empresas y sistemas automáticos, garantizar la manifestación de voluntad en procesos digitales, y reducir la posibilidad de suplantación de identidad en las transacciones con valor legal. De esta manera, se incursionará en la actividad de Entidad de Certificación, Autoridad de Sellado de Tiempo y Software de Firma Digital.

En calidad de Entidad de Certificación, BPO presta servicios de emisión, revocación y re-emisión de certificados digitales siguiendo la regulación establecida por el marco de la IOFE.

En calidad de Autoridad de Sellado de Tiempo, BPO brinda los servicios de valor añadido, emitiendo sellos de tiempo según la regulación establecida por el marco de la IOFE.

En calidad de Software de Firma Digital, BPO brinda una aplicación de firma digital que sigue la regulación establecida por el marco de la IOFE.

3 OBJETIVO

Este documento tiene como objeto la descripción de las operaciones y prácticas que utiliza BPO para la administración de sus servicios como Entidad de Certificación Digital – EC, en el marco del cumplimiento de los requerimientos de la "Guía de Acreditación de Entidades de Certificación Digital (EC)" establecida por el INDECOPI.

4 OBJETO DE LA ACREDITACIÓN

El alcance de la acreditación cubre la infraestructura y procesos de los servicios de certificación digital brindados por la Entidad de Certificación BPO.

5 DEFINICIONES Y ABREVIACIONES

5.1 ABREVIACIONES

AAC	Autoridad Administrativa Competente
DN	Distinctive Name: Nombre Distintivo
EC	Entidad de Certificación
CPS	Certification Practice Statement: Declaración de Prácticas Certificación
CRL	Lista de Certificados Revocados
IOFE	Infraestructura Oficial de Firma Electrónica
PC	Política de Certificación
RUC	Registro Único de Contribuyentes
SHA	Secure Hash Algorithm (Algoritmo de seguridad HASH)
CA	Certification Authority (Autoridad de Certificación)
DSCF	Dispositivo seguro de creación de firma
FIPS	Federal Information Processing Standards (Estándares Federales Procesamiento de la Información)
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
PKCS	Public-Key Cryptography Standards.
PKI	Infraestructura de llave pública

PSC	Prestador de Servicios de Certificación
RA	Autoridad de Registro
RFC	Request For Comments
RSA	Rivest, Shamir and Adleman.
SSL	Secure Sockets Layer
TSA	Time Stamping Authority
TSU	Time Stamping Unit

5.2 DEFINICIONES

Entidad de Certificación – EC	Entidad que presta servicios de emisión, revocación, re-emisión, modificación, suspensión de certificados digitales en el marco de la regulación establecida por la IOFE.
Entidad de Registro – ER	Entidad que realiza los procesos de verificación de identidad de los solicitantes de los servicios de certificación digital y que custodia de forma segura las evidencias de dichos procesos.
Autoridad de Sellado de Tiempo -TSA	Entidad que emite los sellos de tiempo. En este caso BPO.
Declaración de Prácticas de Certificación	Es el documento en el que consta de manera detallada los procedimientos que aplica la EC para la prestación de sus servicios. Una declaración de las prácticas que una EC emplea para emitir, gestionar, revocar y renovar certificados sin y con cambio de claves.
Política de Certificación	Conjunto de reglas que indican el marco de aplicabilidad de los servicios para una comunidad de usuarios definida.
Titular	Entidad que requiere los servicios provistos por la EC de BPO, y que está de acuerdo con los términos y condiciones de los servicios conforme a lo declarado en el presente documento.

Tercero que confía	Persona que recibe un documento, log, o notificación firmado digitalmente, y que confía en la validez de las transacciones realizadas.

5.3 PKI PARTICIPANTES

5.3.1 ENTIDAD DE CERTIFICACIÓN BPO (EC BPO)

BPO, en su papel de Entidad de Certificación, es la persona jurídica privada que presta indistintamente servicios de producción, emisión, gestión, revocación, cancelación u otros servicios inherentes a la certificación digital.

BPO, como Entidad de Certificación, le corresponderá la realización de todos los trámites y procedimientos ante la AAC a fin de poder ingresar a la IOFE.

5.3.2 ENTIDAD DE REGISTRO BPO

BPO a través de su Entidad de Registro afiliada será la encargada de validar la información suministrada por el solicitante de un certificado digital, mediante la verificación de su identidad y su registro.

5.3.3 AUTORIDAD DE SELLADO DE TIEMPO (TSA BPO)

BPO brinda también los servicios de Autoridad de Sellado de Tiempo, la cual se encarga de emitir sellos de tiempo. Un sello de tiempo es un conjunto de datos que representa el resumen de un documento sellado añadido a un registro del tiempo en el que el sello fue emitido. Este resumen es una característica única del documento, de modo que si el documento es modificado este sello pierde validez. Las particularidades sobre el uso, per les y especificaciones de la TSA, se describen en la respectiva Política de Sellado de Tiempo de BPO.

5.3.4 TITULAR

Titular es la persona natural o jurídica a cuyo nombre se expide un certificado digital y por tanto actúa como responsable del mismo confiando en él, con conocimiento y plena aceptación de los derechos y deberes establecidos y publicados en la CPS de BPO.

5.3.5 SUSCRIPTOR

Conforme a la IOFE, el Suscriptor es la persona natural responsable del uso de la clave privada, a quien se le vincula de manera exclusiva con un documento electrónico firmado digitalmente utilizando su clave privada.

En el caso que el titular del certificado digital sea una persona natural, sobre ella recaerá la responsabilidad de suscriptor.

En el caso que una persona jurídica sea el titular de un certificado digital, la responsabilidad del suscriptor recaerá sobre el representante legal designado por esta entidad. Si el certificado está designado para ser usado por un agente automatizado, la titularidad del certificado y de las firmas digitales generadas a partir de dicho certificado corresponderá a la persona jurídica. La atribución de responsabilidad del suscriptor, para tales efectos, corresponde a la misma persona jurídica.

5.3.6 SOLICITANTE

Se entenderá por Solicitante, la persona natural o jurídica que solicita un Certificado emitido bajo la CPS de BPO.

En el caso de los certificados de persona natural puede coincidir con la figura del Titular.

5.3.7 TERCERO QUE CONFÍA

Tercero que confía son todas aquellas personas naturales o jurídicas que deciden aceptar y confiar en los certificados digitales emitidos por la Entidad de Certificación de BPO a un titular. El Tercero que confía, a su vez puede ser o no titular.

5.3.8 ENTIDAD A LA CUAL SE ENCUENTRA VINCULADO EL TITULAR

En su caso, la persona jurídica u organización a la que el Titular se encuentra estrechamente relacionado mediante la vinculación acreditada en el Certificado.

6 SERVICIOS DE CERTIFICACIÓN DIGITAL

BPO brinda los servicios de emisión, re-emisión, revocación y distribución de los certificados digitales.

Los certificados y las prácticas relacionadas a la gestión de su ciclo de vida son descritas en la Declaración de Prácticas y la Política de Certificación de BPO publicadas en:

https://bpoperu.idok.cl/

7 RESPONSABILIDADES

Las responsabilidades contractuales, garantías financieras y coberturas de seguros son brindadas por la Entidad de Certificación de BPO y representan todos los aspectos de ejecución de obligaciones contractuales, responsabilidad y mediación entre las personas jurídicas y naturales del Estado Peruano y la Entidad de Certificación.

Asimismo, su Entidad de Registro afiliada brinda los servicios de registro o verificación conforme a las Guías de Acreditación del INDECOPI, para realizar la verificación de identidad de las personas jurídicas y naturales solicitantes de los certificados digitales.

8 USO DEL CERTIFICADO

Los certificados emitidos por BPO 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.

8.1 TIPOS DE CERTIFICADOS

BPO emite los siguientes tipos de certificados:

- **Certificado de Persona Natural:** Es el tipo de certificado que permite a una persona natural acreditarse y firmar digitalmente como tal, asumiendo la responsabilidad de suscriptor y titular de dicho certificado. Dentro de este tipo de certificados, se encuentran los certificados de profesional como persona natural.
- **Certificado de Persona Jurídica:** Es el tipo de certificado que identifica al firmante como Representante legal o Apoderado de una Organización o Entidad. Dentro de este tipo de certificados, se encuentran los certificados de profesional vinculado a una empresa y de atributos (identifica al firmante como colaborador, funcionario, entre otros).
- **Certificado de Agente Automatizado:** Es el tipo de certificado que identifica a un dispositivo informático perteneciente a una persona jurídica que realiza las operaciones de firma y descifrado de forma automática, y cuyas acciones se encuentran bajo la responsabilidad del suscriptor del certificado. Dentro de este tipo de certificados, se encuentran los de Operador de Servicios Electrónicos (OSE) y de facturación electrónica.
- **Certificados para Sellado de Tiempo:** La TSA emite certificados a una Unidad de Sellado de Tiempo - TSU. Dichas TSU son las que proveen sellos de tiempo desde una fuente de tiempo confiable al recibir una solicitud estandarizada que siga las especificaciones del RFC 3161. BPO cuenta con una Política de Sellado de Tiempo que detalla este servicio.

8.2 USOS ADECUADOS DEL CERTIFICADO

Los Certificados emitidos bajo esta Política y CPS pueden ser utilizados con los siguientes propósitos:

- **Identificación del Titular**: El Titular del Certificado puede autenticar, frente a otra parte, su identidad, demostrando la asociación de su clave privada con la respectiva clave pública, contenida en el Certificado.

- **Integridad del documento** firmado: La utilización del Certificado garantiza que el documento firmado es íntegro, es decir, garantiza que el documento no fue alterado o modificado despúés de firmado por el Titular. Se certifica que el mensaje recibido por el Receptor o Destino que confía es el mismo que fue emitido por el Titular.

- **No repudio de origen**: Con el uso de este Certificado también se garantiza que la persona que firma el documento no puede repudiarlo, es decir, el Titular que ha firmado no puede negar la autoría o la integridad del mismo.

8.3 USOS PROHIBIDOS DEL CERTIFICADO

Los Certificados emitidos bajo esta CPS no pueden ser utilizados para las siguientes circunstancias: Cuando contravengan la Ley de Firmas y Certificados Digitales – Ley 27269, las Guías de Acreditación del INDECOPI o sus anexos.

9 PERSONA DE CONTACTO

Datos de la Entidad de Certificación:

Nombre	Teresa Prado Alarcón
Teléfono	+56 951104076
Correo electrónico:	teresa.prado@bpo-advisors.net
Página Web:	https://bpoperu.idok.cl/

10 RESPONSABILIDADES DE LOS TITULARES Y SUSCRIPTORES

Los usuarios y solicitantes de los certificados digitales provistos por BPO son responsables de revisar la presente Política y CPS de BPO, a fin de que se puedan enterar de las características de la plataforma de servicios, infraestructura y procedimientos empleados en la gestión del ciclo de vida de los certificados digitales, Raíz, Intermedios y de usuario final, así como las obligaciones de cada parte.

Asimismo es responsabilidad 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 BPO 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.

11 ORGANIZACIÓN QUE ADMINISTRA LOS DOCUMENTOS DE POLÍTICA Y DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN

BPO administra los documentos Política y Declaración de Prácticas de Certificación de BPO, Política y Plan de Seguridad, Política y Plan de Privacidad, y todos los documentos normativos de la EC de BPO.

Para cualquier consulta contactar:

Nombre	Teresa Prado Alarcón
Teléfono	+56 951104076

Correo electrónico:	teresa.prado@bpo-advisors.net
Página Web:	https://bpoperu.idok.cl/

12 PUBLICACIÓN DE LA DECLARACIÓN DE PRÁCTICAS

La Política y Declaración de Prácticas de Certificación de BPO, así como la Política y Plan de Seguridad, Política y Plan de Privacidad, y otra documentación relevante son publicadas en la siguiente dirección:

https://bpoperu.idok.cl/

Todas las modificaciones relevantes en la documentación de BPO, serán comunicadas al INDECOPI y las nuevas versiones del documento serán publicadas en el mismo sitio web que son revisadas de manera anual. La auditoría anual validará estos cambios y emitirá el informe de cumplimiento.

El presente documento es firmado por el Responsable de la EC de BPO antes de ser publicado, y se controlan las versiones del mismo, a fin de evitar modificaciones y suplantaciones no autorizadas.

Las modificaciones relativas a la Política y Declaración de Prácticas de Certificación de BPO u otra documentación relativa, serán publicadas luego de ser aprobadas por el INDECOPI.

13 RESPONSABILIDADES SOBRE REPOSITORIOS Y PUBLICACIÓN DE INFORMACIÓN

Certificado Raíz	https://bpoperu.idok.cl/
Certificados Subordinadas	https://bpoperu.idok.cl/
Lista de Certificados Revocados (CRL)	https://bpoperu.idok.cl/
Declaración de Prácticas de Certificación (CPS)	https://bpoperu.idok.cl/

13.1 PUBLICACIÓN DE LA INFORMACIÓN DE CERTIFICACIÓN

El Responsable de la EC de BPO es el encargado de la autorización de la publicación de la Política y CPS y es responsable de asegurar la integridad y disponibilidad de la información publicada en la página Web:

https://bpoperu.idok.cl/

La Lista de Certificados Revocados es publicada en la página web de BPO y está firmada digitalmente por la Entidad de Certificación BPO.

La información del estado de los certificados digitales vigentes está disponible para consulta mediante protocolo OCSP y CRL.

13.2 PLAZO O FRECUENCIA DE LA PUBLICACIÓN

•Certificado Raíz
El certificado raíz se publicará y permanecerá en la página Web de la Entidad de Certificación BPO, durante todo el tiempo en que se estén prestando servicios de certificación digital.

•Certificado Subordinada
El certificado de la EC Subordinada se publicará y permanecerá en la página Web de la Entidad de Certificación BPO, durante todo el tiempo en que se estén prestando servicios de certificación digital.

•Lista de Certificados Revocados (CRL)
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://bpoperu.idok.cl/

•Declaración de Prácticas de Certificación (CPS)
Con autorización del Responsable de la Entidad de Certificación de BPO y el INDECOPI, se publicará la versión finalmente aprobada. Los cambios generados en cada nueva versión serán previamente informados al INDECOPI y publicados en la página Web de La Entidad de Certificación BPO junto con la nueva versión. La Auditoría anual validará estos cambios y emitirá el informe de cumplimiento.

13.3 CONTROLES DE ACCESO A LOS REPOSITORIOS

La consulta a los repositorios disponibles en la página Web de La Entidad de Certificación BPO, antes mencionada, es de libre acceso al público en general. La integridad y disponibilidad de la información publicada es responsabilidad de la EC BPO, que cuenta con los recursos y procedimientos necesarios para restringir el acceso a los repositorios con otros fines diferentes a la consulta y a la página Web por parte de personas ajenas.

14 IDENTIFICACIÓN Y AUTENTICACIÓN

14.1 NOMBRES

14.1.1 TIPOS DE NOMBRES

El Suscriptor/Titular del certificado se describe en este mediante un nombre distintivo (DN, distinguished name, Subject) conforme al estándar X.501.

Las descripciones del campo DN están reflejadas en cada una de las fichas de perfil de los certificados. Asimismo, incluye un componente "Common Name"(CN =).

La estructura y el contenido de los campos de cada certificado emitido por BPO, así como su significado semántico se encuentran descritos en cada una de las fichas de perfil de los certificados.

- **Personas naturales**: En certificados correspondientes a personas naturales la identificación del signatario estará formada por su nombre y apellidos, más su identificador fiscal.
- **Personas Jurídicas**: En certificados correspondientes a personas jurídicas, esta identificación se realizará por medio de su denominación o razón social, y su identificación fiscal.
- **Componentes o dispositivos**: Los certificados de entidad final que describen componentes o dispositivos incorporan un nombre identificativo de la máquina o servicio, adicionalmente la entidad jurídica propietaria de dicho servicio en el campo organización "O" del "CN".

La estructura para los certificados de EC subordinada, TSU, TSA, OCSP, incluye como mínimo:

- Un nombre descriptivo que identifica a la Entidad de Certificación (CN).
- La persona jurídica responsable de las claves (O).
- El identificador fiscal de la organización responsable de las claves.
- El certificado de Servidor Seguro incluye dependiendo del tipo de certificado el dominio FQDN (Fully Qualified Domain Name) sobre el cual la organización "O" descrita en el certificado tiene propiedad y control.
- Los certificados de ROOT tienen un nombre descriptivo que identifica a la Entidad de Certificación y en el campo (O) el nombre la organización responsable de la Entidad de Certificación

14.1.2 NECESIDAD DE QUE LOS NOMBRES TENGAN SIGNIFICADO

En los casos en que un producto de BPO permite el uso de un rol o nombre de departamento y donde se incluye el campo de OU en el DN, se pueden agregar elementos únicos adicionales al DN dentro del campo de OU para permitir que los terceros que confían diferencien entre los certificados con los Elementos comunes DN. Cabe destacar que, en caso se emitan certificados de prueba se colocará como CN "Prueba"

14.1.3 ANONIMATO Y PSEUDO ANONIMATO DE LOS TITULARES

BPO, puede emitir Certificados anónimos o seudónimos de entidad final, siempre que dichos códigos no estén prohibidos por la política aplicable y, si es posible, se conserva la singularidad del espacio de nombres.

En el certificado del representante legal quedarán registrados sus atributos, los cuales le permitirán utilizar el certificado para realizar transacciones en nombre de la persona jurídica. Tratándose de certificados digitales solicitados por personas jurídicas para su utilización a través de agentes automatizados, la titularidad de certificados y de las firmas digitales generadas a partir de dicho certificado corresponderá a la persona jurídica. La atribución de responsabilidad, para tales efectos, corresponde al representante legal, que en nombre de la persona jurídica solicita el certificado digital

14.1.4 REGLAS PARA LA INTERPRETACIÓN DE VARIAS FORMAS DE NOMBRE

BPO atiende en todo caso a lo marcado por el estándar X.500.

14.1.5 SINGULARIDAD DE LOS NOMBRES

BPO no reasigna un nombre a un suscriptor que ya hubiera sido asignado a otro diferente. Para lo cual, la identificación del titular debe estar formada por su nombre y apellidos, más su DNI.

Asimismo, cuando aparezcan datos de personas jurídicas, esta identificación se debe realizar por medio de su denominación o razón social y su RUC. Además del nombre y apellidos del suscriptor, más su DNI.

14.1.6 RECONOCIMIENTO, AUTENTICACIÓN Y PAPEL DE LAS MARCAS RECONOCIDAS.

BPO no podrá volver a asignar un nombre de titular que ya haya sido asignado a un titular diferente. No obstante, BPO no se compromete a buscar evidencias acerca de los derechos de uso sobre marcas registradas u otros signos distintivos con anterioridad a la emisión de los certificados.

15 VALIDACIÓN INICIAL DE LA IDENTIDAD

15.1 MÉTODO PARA DEMOSTRAR LA POSESIÓN DE LA CLAVE PRIVADA

BPO emplea diversos circuitos para la emisión de certificados donde la clave privada se gestiona de diferente forma. La clave privada puede ser generada tanto por el usuario como por la EC.

El modelo de generación de claves utilizado viene indicado en el propio certificado, tanto en su identificador de Política como en el atributo Descripción del campo DN del certificado. Estos códigos están descritos en las fichas de perfiles de los certificados.

a) Generación de claves por parte de la EC.

En Software, se entregan al Suscriptor mediante correo a través de ficheros protegidos utilizando el Standard PKCS#12. La seguridad del proceso queda garantizada debido a que el código de acceso PKCS#12 que posibilita la instalación de este en las aplicaciones, es entregada por un medio distinto al utilizado en la recepción inicial.

En Hardware, la generación de claves se realiza en un dispositivo que cumple el estándar FIPS 140-2 nivel 2 ó + con un rol de confianza del correspondiente o personal de la empresa autorizada para realizar dicha actividad.

b) Generación de las claves por el Suscriptor.

Una vez aceptada y aprobada la solicitud se generará el certificado de acuerdo con el procedimiento técnico para la emisión de estos, 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.

15.2 AUTENTICACIÓN DE UNA IDENTIDAD INDIVIDUAL (PERSONA NATURAL)

La RPS de la entidad de registro afiliada de BPO describe específicamente los procedimientos de autenticación, documentación requerida y validación de la identidad de personas naturales.

15.3 AUTENTICACIÓN DE LA IDENTIDAD DE UNA ORGANIZACIÓN (PERSONA JURÍDICA)

La RPS de la entidad de registro afiliada de BPO describe específicamente los procedimientos de autenticación, documentación requerida y validación de la identidad de Personas jurídicas.

15.4 AUTENTICACIÓN DE LA IDENTIDAD DE UNA ORGANIZACIÓN (PERSONA JURÍDICA CON ATRIBUTO)

La RPS de la entidad de registro afiliada de BPO describe específicamente los procedimientos de autenticación, documentación requerida y validación de la identidad de los suscriptores.

15.5 AUTENTICACIÓN DE LA IDENTIDAD DE UNA ORGANIZACIÓN (PERSONA JURÍDICA AGENTE AUTOMATIZADO)

La RPS de la entidad de registro afiliada de BPO describe específicamente los procedimientos de autenticación, documentación requerida y validación para certificados de agente automatizado.

15.6 INFORMACIÓN DE TITULAR NO VERIFICADA

Bajo ninguna circunstancia BPO omitirá las labores de verificación que conduzcan a la identificación del Suscriptor y que se traduce en la solicitud de exhibición de los documentos mencionados para organizaciones y personas naturales.

15.7 VALIDACIÓN DE LA AUTORIDAD

La validación de la Entidad de Certificación de BPO respecto a la propiedad de un dominio se realiza a través de la comprobación de la existencia de un correo que contiene la dirección del dominio en cuestión y/o verificación de datos de registro de dominio respectivo.

Los procedimientos de autenticación y de validación son descritos en el documento de Declaración de Prácticas de Registro o Verificación de la entidad de registro afiliada.

15.8 CRITERIOS PARA LA INTEROPERABILIDAD

La Entidad de Certificación BPO únicamente emitirá certificados a ER afiliadas, que estén directamente vinculadas o terceros con vínculo contractual los cuales se someten al cumplimiento de las CP y CPS de la EC de BPO.

16 IDENTIFICACIÓN Y AUTENTICACIÓN PARA PETICIONES DE RE-EMISIÓN DE CLAVES

16.1 IDENTIFICACIÓN Y AUTENTICACIÓN PARA RE-EMISIÓN DE RUTINA

Los procedimientos de autenticación son descritos en el documento de Declaración de Prácticas de Registro o Verificación de la entidad de registro afiliada de BPO.

16.2 IDENTIFICACIÓN Y AUTENTICACIÓN TRAS UNA REVOCACIÓN

Debido a que una revocación implica la expedición de un nuevo certificado, La Entidad de Certificación BPO, solicita un nuevo proceso de autenticación del solicitante.

Los procedimientos de autenticación son descritos en el documento de Declaración de Prácticas de Registro o Verificación de la entidad de registro afiliada de BPO.

17 IDENTIFICACIÓN Y AUTENTICACIÓN PARA PETICIONES DE REVOCACIÓN

BPO, atiende las peticiones de revocación de conformidad con las causales de revocación especificadas en el documento de Declaración de Prácticas de Registro o Verificación de la entidad de registro afiliada de BPO, y autentica la identidad de quien solicita la revocación de certificado.

Los procedimientos de autenticación de la identidad de los titulares y suscriptores son descritos en la RPS de la entidad de registro afiliada de BPO.

18 REQUISITOS OPERACIONALES PARA EL TIEMPO DE VIDA DE LOS CERTIFICADOS

18.1 SOLICITUD DEL CERTIFICADO

Dicho procedimiento le compete a la Entidad de Registro y por lo tanto se describe en el documento Declaración de Prácticas de Registro o Verificación de la entidad de registro afiliada de BPO.

18.2 QUIÉN PUEDE SOLICITAR UN CERTIFICADO

Los procedimientos relativos a la Entidad de Registro son descritos en el documento de Declaración de Prácticas de Registro o Verificación de la entidad de registro afiliada de BPO.

18.3 PROCESO DE REGISTRO Y RESPONSABILIDADES

Los procedimientos relativos a la Entidad de Registro son descritos en el documento de Declaración de Prácticas de Registro o Verificación de la entidad de registro afiliada de BPO.

19 TRAMITACIÓN DE SOLICITUD DE CERTIFICADOS

19.1 REALIZACIÓN DE LAS FUNCIONES DE IDENTIFICACIÓN Y AUTENTICACIÓN

Los procedimientos relativos a la Entidad de Registro son descritos en el documento de Declaración de Prácticas de Registro o Verificación de la entidad de registro afiliada de BPO.

19.2 APROBACIÓN O RECHAZO DE LAS SOLICITUDES DE CERTIFICADO

Los procedimientos relativos a la Entidad de Registro son descritos en el documento de Declaración de Prácticas de Registro o Verificación de la entidad de registro afiliada de BPO.

19.3 PLAZO PARA PROCESAR LAS SOLICITUDES DE CERTIFICADO

Los procedimientos relativos a la Entidad de Registro son descritos en el documento de Declaración de Prácticas de Registro o Verificación de la entidad de registro afiliada de BPO.

20 EMISIÓN DE CERTIFICADOS

20.1 ACTUACIONES DE LA EC DURANTE LA EMISIÓN DE CERTIFICADOS

Una vez aprobada la solicitud se procederá a la emisión del certificado, que deberá ser entregado de forma segura al Suscriptor.

20.1.1 EMISIÓN DE CERTIFICADOS MEDIANTE SOFTWARE (.PFX O .P12)

- La Entidad de Certificación recibe la solicitud de la Entidad de Registro asociada una vez que la validación de identidad fue completada correctamente.
- El Operador de Registro aprueba la solicitud usando su firma digital.
- El solicitante recibe el enlace de descarga del certificado en el correo electrónico indicado en el pedido.

20.1.2 EMISIÓN DE CERTIFICADOS MEDIANTE HARDWARE

- La Entidad de Certificación recibe la solicitud de la Entidad de Registro asociada una vez que la validación de identidad fue completada correctamente.
- El Operador de Registro aprueba la solicitud usando su firma digital.
- El certificado se instala directamente en el dispositivo criptográfico del solicitante usando Internet Explorer mediante el formato PKCS#11.

20.2 NOTIFICACIÓN AL SUSCRIPTOR POR LA EC DE LA EMISIÓN DEL CERTIFICADO

La EC de BPO notificará al Suscriptor la emisión del certificado y el método de descarga si es necesario.

21 ACEPTACIÓN DEL CERTIFICADO

21.1 FORMA EN LA QUE SE ACEPTA EL CERTIFICADO

El certificado se considera aceptado una vez que es descargado. La EC de BPO cuenta con un mecanismo para saber cuándo es que el certificado digital es descargado a fin de dar la conformidad correspondiente.

Por otro lado, el titular/suscriptor puede dar a conocer su inconformidad con algún dato del perfil del certificado digital a través de un medio no repudiable como un correo electrónico o documentos firmados digitalmente, por ejemplo.

21.2 PUBLICACIÓN DEL CERTIFICADO POR LA EC

Los procedimientos relativos a la Entidad de Registro son descritos en el documento de Declaración de Prácticas de Registro o Verificación de la entidad de registro afiliada de BPO.

21.3 NOTIFICACIÓN DE LA EMISIÓN DEL CERTIFICADO POR LA EC A OTRAS ENTIDADES

La EC de BPO notifica sobre la emisión de un certificado digital a través de la plataforma de la ER afiliada.

22 USO DE LA CLAVE PRIVADA Y DEL CERTIFICADO

22.1 USO DE LA CLAVE PRIVADA Y DEL CERTIFICADO POR EL TITULAR

Los suscriptores deben proteger su clave privada teniendo cuidado de evitar la divulgación a terceros. El contrato de Suscriptor identifica las obligaciones del Suscriptor con respecto a la Protección de Clave Privada. Las claves privadas sólo se deben utilizar como se especifica en los campos de uso de clave y de uso extendido de clave como se indica en el Certificado correspondiente. Donde es posible hacer una copia de seguridad de una clave privada, los suscriptores deben utilizar el mismo nivel de cuidado y protección atribuido a la clave privada en vivo. Al final de la vida útil de una clave privada, los suscriptores deben eliminar de forma segura la clave privada y los fragmentos que se han dividido para fines de copia de seguridad.

22.2 USO DE LA CLAVE PRIVADA Y DEL CERTIFICADO POR TERCEROS QUE CONFÍAN

De acuerdo con la CPS de BPO las condiciones bajo las cuales los terceros que confían pueden confiar en los certificados incluyendo los servicios de certificado apropiados disponibles para verificar la validez del certificado como CRL y/u OCSP. Los terceros que confían deben utilizar la información para realizar una evaluación del riesgo y, como tales, son las únicas responsables de realizar la evaluación del riesgo antes de confiar en el Certificado o de cualquier garantía realizada.

El software utilizado por los terceros que confían debe ser totalmente compatible con las normas X.509, incluyendo las mejores prácticas para encadenar decisiones en torno a políticas y uso de claves.

23 RE-EMISIÓN DEL CERTIFICADO SIN CAMBIO DE CLAVES

La EC de BPO no permite la re-emisión de certificados sin renovación de claves.

24 RE-EMISIÓN DEL CERTIFICADO CON CAMBIO DE CLAVES

Para la Entidad de Certificación de BPO, un requerimiento de re-emisión de un certificado con cambio de claves es un requerimiento normal de solicitud de un certificado digital como si fuera uno nuevo y por consiguiente implica el cambio de claves y así lo reconoce y acepta el solicitante.

La EC de BPO comunicará al suscriptor, con una anticipación de al menos 30 días antes de la expiración del certificado, para que pueda renovar a tiempo dicho certificado. Si el suscriptor no solicita la re-emisión de certificado, el certificado expirará. Luego de ello, el suscriptor deberá realizar el proceso de validación de identidad desde la etapa inicial.

24.1 CIRCUNSTANCIAS PARA LA RE-EMISIÓN DE CERTIFICADOS CON CAMBIO DE CLAVES

Las circunstancias son definidas en la Declaración de Prácticas de Registro de la entidad de registro afiliada de BPO.

24.2 QUIÉN PUEDE SOLICITAR UNA RE-EMISIÓN CON CAMBIO DE CLAVES.

Las precisiones sobre quién puede solicitar una re-emisión son definidas en la Declaración de Prácticas de Registro de la entidad de registro afiliada de BPO.

24.3 TRÁMITES PARA LA SOLICITUD DE RE-EMISIÓN DE CERTIFICADOS CON CAMBIO DE CLAVES.

El procedimiento para re-emisión de certificados digitales es definido en la Declaración de Prácticas de Registro de la entidad de registro afiliada de BPO.

24.4 NOTIFICACIÓN AL TITULAR DE LA EMISIÓN DE UN NUEVO CERTIFICADO CON CAMBIO DE CLAVES

El procedimiento para re-emisión de certificados digitales es definido en la Declaración de Prácticas de Registro de la entidad de registro afiliada de BPO

24.5 FORMA EN LA QUE SE ACEPTA LA RE-EMISIÓN DE UN CERTIFICADO

El procedimiento para re-emisión de certificados digitales es definido en la Declaración de Prácticas de Registro de la entidad de registro afiliada de BPO

24.6 PUBLICACIÓN DEL CERTIFICADO RE-EMITIDO POR LA EC

El procedimiento para re-emisión de certificados digitales es definido en la Declaración de Prácticas de Registro de la entidad de registro afiliada de BPO

24.7 NOTIFICACIÓN DE LA EMISIÓN DE UN CERTIFICADO RE-EMITIDO POR LA EC A OTRAS ENTIDADES

El procedimiento para re-emisión de certificados digitales es definido en la Declaración de Prácticas de Registro de la entidad de registro afiliada de BPO.

25 MODIFICACIÓN DE CERTIFICADOS

La modificación del certificado se define como la producción de un nuevo certificado que tiene detalles que difieren de un certificado previamente emitido. BPO trata la modificación de la misma manera que la emisión de un nuevo certificado.

26 REVOCACIÓN Y SUSPENSIÓN DE CERTIFICADOS

26.1 CIRCUNSTANCIAS PARA LA REVOCACIÓN DE UN CERTIFICADO

Como norma general se procederá a la revocación de un certificado por:

- Modificación de alguno de los datos contenidos en el certificado.
- Descubrimiento que alguno de los datos aportados en la solicitud de certificado es incorrecto o incompleto, así como la alteración o modificación de las circunstancias verificadas para la expedición del certificado.
- Falta de pago del certificado.
- Por circunstancias que afectan la seguridad de la clave o del certificado
- Compromiso de la clave privada o de la infraestructura o sistemas de la Entidad de Certificación que emitió el certificado, siempre que afecte a la fiabilidad de los certificados emitidos a partir de este incidente.
- Infracción, por la Entidad de Certificación, de los requisitos previstos en los procedimientos de gestión de certificados, establecidos en esta CPS.
- Compromiso o sospecha de compromiso de la seguridad de la clave o del certificado del Firmante o del responsable del certificado.
- Acceso o utilización no autorizada, por un tercero, de la clave privada del Firmante o del responsable de certificado.
- El uso irregular del certificado por el Firmante o del responsable de certificado, o falta de diligencia en la custodia de la clave privada.
- Por circunstancias que afectan la seguridad del dispositivo criptográfico
- Compromiso o sospecha de compromiso de la seguridad del dispositivo criptográfico.
- Pérdida o inutilización por daños del dispositivo criptográfico.
- Acceso no autorizado, por un tercero, a los datos de activación del Firmante o del responsable del certificado.
- Por circunstancias que afectan al Firmante o responsable del certificado.
- Finalización de la relación entre Entidad de Certificación y Firmante o responsable del certificado.

- Modificación o extinción de la relación jurídica subyacente o causa que provocó la emisión del certificado al Firmante o responsable del certificado.
- Infracción por el solicitante del certificado de los requisitos preestablecidos para la solicitud de éste.
- Infracción por el Firmante o responsable del certificado, de sus obligaciones, responsabilidad y garantías, establecidas en el instrumento jurídico correspondiente o en esta Declaración de Prácticas de Certificación.
- La incapacidad sobrevenida o la muerte del Firmante o responsable del certificado.
- La extinción de la persona jurídica Firmante del certificado, así como la finalidad de la autorización del Firmante al responsable del certificado o la finalización de la relación entre Firmante y responsable del certificado.
- Solicitud del Firmante de revocación del certificado, de acuerdo con lo establecido en esta CPS.
- Resolución firme de la autoridad administrativa o judicial competente.
- La finalización del servicio de la Entidad de Certificación, de acuerdo con lo establecido en la sección correspondiente en esta CPS.

Para justificar la necesidad de revocación que se alega se deberán presentar ante la ER o la EC los documentos correspondientes, en función de la causa que motiva la solicitud.

Si solicita la revocación el titular del certificado o la persona física solicitante de un certificado de persona jurídica, deberá presentar una declaración firmada por él donde indique el certificado a revocar y la causa de esta solicitud e identificarse ante la ER.

Si la revocación la solicita un tercero deberá presentar una autorización bien del titular persona física bien del representante legal de la persona jurídica titular donde se indiquen además las causas por las que se solicita la revocación del certificado e identificarse ante la ER.

Si solicita la revocación la Entidad vinculada al titular por causa de la terminación de la relación con éste, deberá acreditar dicha circunstancia (revocación de poderes, terminación contrato) e identificarse ante la ER como facultado para representar a la Entidad.

26.2 QUIÉN PUEDE SOLICITAR UNA REVOCACIÓN

La revocación de un certificado podrá solicitarse por:

- El Suscriptor/Firmante.
- El Solicitante responsable.
- La Entidad (a través de un representante de la misma).
- La ER o la EC. Adicionalmente las que marquen las políticas de certificación concretas.

26.3 PROCEDIMIENTO DE SOLICITUD DE REVOCACIÓN

El procedimiento para revocación de certificados digitales es definido en la Declaración de Prácticas de Registro de la entidad de registro afiliada de BPO.

26.4 PERIODO DE GRACIA DE SOLICITUD DE REVOCACIÓN

Para los certificados de entidad final. El periodo de revocación desde que BPO tiene conocimiento autenticado de la revocación de un certificado esta se produce de manera inmediata, incorporándose en la próxima CRL a emitir y en la base de datos de la plataforma de gestión donde se alimenta el respondedor OCSP.

26.5 PLAZO EN EL QUE LA EC DEBE RESOLVER LA SOLICITUD DE REVOCACIÓN

Los procedimientos relativos a la Entidad de Registro son descritos en el documento de Declaración de Prácticas de Registro o Verificación de la entidad de registro afiliada de BPO.

26.6 REQUISITOS DE VERIFICACIÓN DE LAS REVOCACIONES POR LOS TERCEROS QUE CONFÍAN

Los procedimientos relativos a la Entidad de Registro son descritos en el documento de Declaración de Prácticas de Registro o Verificación de la entidad de registro afiliada de BPO.

26.7 FRECUENCIA DE EMISIÓN DE LAS CRLS

Un certificado de Entidad Final contiene un CDP (CRL Distribution Point), luego que la CRL se actualiza cada 24 horas y es válida por 7 días.

26.8 TIEMPO MÁXIMO DE LATENCIA DE LAS CRLS

El tiempo entre la generación y publicación de la CRL es menor a una (1) hora, tal como lo establece el INDECOPI.

26.9 DISPONIBILIDAD DE VERIFICACIÓN DEL ESTADO

BPO publicará la información relativa a la CRL, estará disponible en línea con un mínimo de 99% anual y un tiempo programado de inactividad máximo de 0.5% anual.

26.10 REQUISITOS DE COMPROBACIÓN DE LA REVOCACIÓN ON-LINE

Para el uso de servicio de la CRL de BPO, se debe tener en cuenta que esta Lista se encuentre firmada por la Autoridad de Certificación de BPO y que sea la última Lista emitida

26.11 OTRAS FORMAS DISPONIBLES DE DIVULGACIÓN DE INFORMACIÓN DE REVOCACIÓN

No Aplica

26.12 REQUISITOS ESPECIALES DE RENOVACIÓN DE CLAVES COMPROMETIDAS

BPO, utilizará métodos comercialmente razonables para informar a los Suscriptores de que su Clave Privada puede haber sido comprometida. Esto incluye los casos en los que se han descubierto nuevas vulnerabilidades o cuando BPO, a su propia discreción, decide que la evidencia sugiere que se ha producido un posible compromiso de claves. Cuando el Compromiso de claves no sea disputado, BPO revocará los certificados de las ECs emisoras o los certificados de entidades finales de suscriptores dentro de las 24 horas y publicará CRL en línea dentro de los treinta (30) minutos de creación y ARL dentro de las doce (12) horas.

26.13 COMPROMISO DE LA CLAVE PRIVADA DE LA EC

El compromiso de la clave privada de una EC, ya sea Raíz o Subordinada, se considera un evento especialmente crítico, ya que invalida los certificados emitidos y la información sobre el estado de revocación firmados con esa clave. Por lo tanto, se presta especial atención a la protección de la clave privada de la EC y a todas las actividades de desarrollo y mantenimiento del sistema que puedan tener un impacto sobre ella.

Una vez comprobado el compromiso de la clave privada de una EC bajo esta DPC, BPO procederá con la mayor brevedad posible a:

- Si la EC es una EC Subordinada, revocar su/s certificado/s asociado/s a la clave privada comprometida.
- Informar al INDECOPI en las siguientes 24 horas.
- Informar a las ER afectadas, a los clientes afectados (Suscriptores y Titulares de certificados de entidad final activos emitidos por la EC, y/o Entidades propietarias de EC Subordinadas externas con certificados activos emitidos por la EC), a las Partes que Confían y a otras entidades afectadas con las que tenga acuerdos u otro tipo de relaciones, a través de comunicación directa cuando sea posible, y a través de comunicación en el sitio web de BPO.
- Indicar en las informaciones anteriores:
    - Fecha y hora en que se tuvo conocimiento del compromiso de la clave privada de la EC.
    - En caso de su conocimiento, fecha y hora en que se produjo o se sospecha que se produjo el compromiso de la clave privada de la EC.
    - Que los certificados y la información sobre el estado de revocación firmados con la clave privada comprometida de la EC pueden ya no ser válidos.
    - Medidas tomadas y/o planeadas para invalidar la clave privada comprometida de la EC (revocación de su/s certificado/s asociados) y para proporcionar de forma fiable la información sobre el estado de revocación de los certificados emitidos por la EC.

26.14 CIRCUNSTANCIAS PARA LA SUSPENSIÓN

BPO no brinda el servicio de suspensión de certificados digitales, únicamente revocación.

26.15 QUIÉN PUEDE SOLICITAR LA SUSPENSIÓN

BPO no brinda el servicio de suspensión de certificados digitales, únicamente revocación.

26.16 PROCEDIMIENTO DE SOLICITUD DE SUSPENSIÓN

BPO no brinda el servicio de suspensión de certificados digitales, únicamente revocación.

26.17 LÍMITES DEL PERIODO DE SUSPENSIÓN

BPO no brinda el servicio de suspensión de certificados digitales, únicamente revocación.

26.18 NOTIFICACIÓN DE LA REVOCACIÓN DE UN CERTIFICADO

BPO no brinda el servicio de suspensión de certificados digitales, únicamente revocación.

27 SERVICIOS DE INFORMACIÓN DEL ESTADO DE CERTIFICADOS

27.1 CARACTERÍSTICAS OPERACIONALES

BPO cuenta con una CRL que es publicada en su página web, sin restricciones de acceso.

27.2 DISPONIBILIDAD DEL SERVICIO

BPO mantendrá la disponibilidad del 99.9% 24x7 de los servicios de estado del certificado y podrán optar por utilizar mecanismos de red de distribución de contenido adicionales basados en la nube para ayudar a la disponibilidad del servicio.

28 CONTROLES FÍSICOS DE LA INSTALACIÓN, GESTIÓN Y OPERACIONALES

Los controles de seguridad son garantizados por nuestro centro de datos que abarcan el ambiente físico, las redes, los sistemas, entre otros; los cuales se especifican a continuación.

28.1 CONTROLES FÍSICOS

El acceso físico a BPO dispone de un esquema de control de acceso. Asimismo, el acceso físico a los sistemas de Entidad de Certificación será bajo estrictas normas de seguridad y monitoreo incluyendo esquemas electrónicos de identificación y control. Adicionalmente, este lugar dispone de elementos adecuados para la operación tales como aire acondicionado, sistema de detección y prevención de incendios, esquema seguro de respaldos externos para eventuales catástrofes.

28.1.1 SERVICIOS EN LA SALA DEL DATA CENTER

Las instalaciones de BPO tienen a disposición diferentes servicios en las salas como:

- Carro multi - periféricos.
- Enchufes de servicios.
- Wifi corporativa
- Télefono en sala.
- Sala de armado.
- Operadores NOC.
- Manos remotas.
- Sala Pretest.

28.1.2 INGRESO PROGRAMADO AL DATA CENTER

1. Al ingresar al Data Center se hará entrega de una credencial de acceso, la cual debe permanecer visible todo el tiempo que dure su visita.
2. Todo acceso al edificio o sala Data Center realizado por clientes, contratistas u otros deben ser programado y autorizado previamente.
3. El acceso al Data Center estará limitado a las áreas específicas donde el cliente tiene instalados sus equipos, mediante una tarjeta de acceso que será entregada al momento de su registro y en recepción. Esta tarjeta es de uso individual y debe ser devuelta al momento de abandonar el Data Center
4. Se debe informar el retiro del Data Center por medio de los teléfonos que se encuentran en cada una de las salas. Un operador revisará el estado de la instalación y cerrará con llave el rack respectivo.

28.1.3 INGRESO AL DATA CENTER EN CASO DE EMERGENCIA

Al dirigirse al Data Center, será atendido por un operador, quien lo asistirá revisando contactos válidos. pudiendo orientarlo en su solicitud.

28.1.4 INGRESO AL DATA CENTER CON EQUIPOS

Al dirigirse al Data Center, será atendido por un operador, quién lo asistirá revisando contactos válidos, pudiendo orientarlo en su solicitud.

1. Todo ingreso, retiro o cambio de equipo debe ser informado en la solicitud de ingreso al Data Center, existe una opción habilitada para ello.
2. Todo ingreso de equipos se debe realizar con guía de despacho, la que debe ser entregada a un operador.
3. Todo retiro de equipo debe ser con guía de despacho. Cada retiro debe ser informado a un operador para que genere la guía de despacho correspondiente.
4. Todo equipo a instalar debe contar con su respectivo kit de montaje.
5. Todo equipo a instalar debe contar con su(s) respectivo(s) cable(s) de poder. Además se recuerda que todo cable de poder debe ser previamente revisado y aprobado por el personal del Data Center con el fin de evitar fallas por cortocircuito u otros inconvenientes.
6. No se permite la instalación y cadena de PDU (Daisy Chain), que no sea previamente autorizada por personal del Data Center.

7. Para nuevas instalaciones, retiros o cambio de equipos, se recomienda gestionar el acceso al Data Center con 24 horas de anticipación, así podrá asignar a un operador para que los asista.
8. Los equipos deben ser instalados con fuente de poder y flujo de aire caliente hacia pasillo caliente.
9. Todo equipo de rack compartido debe pasar por pre-test.
10. Equipos deben estar rotulados e identificados por cliente.
11. Para nuevas instalaciones donde los equipos lleven pallet, el cliente los debe retirar del DC.

28.1.5 OTRAS NORMAS

1. Se prohíbe fumar, ingresar con alimentos y/o líquidos.
2. Pos seguridad se prohíbe entorpecer el libre tránsito en los pasillos. Embalaje de equipos y accesorios no pueden estar en los pasillos
3. Se prohíbe dañar o alterar la infraestructura de las salas (pinturas, tubos, escalerillas, cables, sensores, dispositivos, etc.)
4. Se prohíbe dejar basura en lugares no habilitados para ello.
5. Por seguridad, se prohíbe dejar elementos inflamables dentro del Rack, tales como cajas, cartón, papel, bolsas, etc. En caso de existir, el área Data Center gestionará con el ejecutivo comercial y con el personal a cargo del rack el retiro de estos.
6. No se recomienda dejar instalados dispositivos periféricos (adaptadores USB, HDD externos, mouse, teclados, etc.) de forma permanente en los equipos que se encuentren alojados en los rack. Una mala manipulación u error, puede provocar una fácil desconexión de estos dispositivos.
7. Se prohíbe tomar fotos o grabar videos en el Data Center.
8. Se prohíbe el ingreso de tabaco o productos derivados del tabaco, explosivos, armas, químicos, drogas ilegales.
9. Se recomienda no permanecer más de 3 horas dentro de la sala Data Center. Si se excede dicho plazo, se recomienda salir por 5 minutos.
10. Es responsabilidad del cliente gestionar la autorización de ingreso a personas de empresas externas u otros.
11. Es responsabilidad exclusiva del cliente la manipulación o trabajos que se realicen en los rack o servicios contratados.
12. Es responsabilidad del cliente mantener actualizados los datos personales, datos comerciales, correos electrónicos, números telefónicos, etc,
13. Se prohíbe la habilitación de puntos de accesos inalámbricos sin previa autorización del personal del Centro de Datos.

28.2 CONTROLES DE PROCEDIMIENTO

28.2.1 ROLES DE CONFIANZA

Los roles de confianza garantizan una segregación de funciones que disemina el control y limita el fraude interno, no permitiendo que una sola persona controle de principio a fin todas las funciones de certificación.

Para determinar la sensibilidad de la función, se tienen en cuenta los siguientes elementos:

- Deberes asociados a la función.

- Nivel de acceso.
- Monitorización de la función.
- Formación y concienciación.
- Habilidades requeridas.

Rol	Responsabilidades	Mecanismo de Autenticación
Administrador del Sistema Operativo	- Instalar y configurar el sistema operativo para la aplicación de AC (EJBCA). - Establecer las cuentas de usuario y credenciales en los sistemas anteriores. - Controlar el acceso de administración a los sistemas anteriores.	Multifactor (tarjeta y contraseña)
Titular de las partes de las llaves	- Tomar custodia de los materiales de activación del HSM, esto es, de sus propias tarjetas inteligentes, donde cada nombre deberá estar debidamente rotulado. - Proteger las tarjetas inteligentes asignadas y sus PINes correspondientes y mantenerlos bajo estricta reserva personal.	Multifactor (tarjeta y contraseña)
Administrador de la aplicación de la AC	- Instalar y configurar la aplicación de AC (EJBCA) de acuerdo al procedimiento establecido. - Establecer cuentas de usuarios en la aplicación de AC (EJBCA).	Multifactor (tarjeta y contraseña)
Custodio de Materiales criptográficos	- Mantener el inventario de los materiales de la ceremonia de generación de claves de CA. - Garantizar que los materiales de la ceremonia están sellados con precintos de seguridad a prueba de manipulación. - Asegurar que los materiales de la ceremonia estén almacenados de forma segura después de la ceremonia.	LLave de las cajas fuertes donde se encuentran las tarjetas de los titulares de las llaves
Oficial de Seguridad y Privacidad	Responsable general para aprobar, administrar y velar por el cumplimiento de las políticas de seguridad y la privacidad de datos personales de los clientes.	N/A
Responsable de Desarrollo	Responsable de asegurar los objetivos de la empresa a través de la planificación estratégica y dirección del desarrollo de software, cumpliendo plazos, costos, calidad y seguridad de la información.	N/A

Responsable de Diseño del Producto	Responsable de asegurar los objetivos técnicos de los productos y servicios activos y de los nuevos, sobre la base de los requerimientos del mercado y usuarios, buscando satisfacer las necesidades de estos y asegurando los resultados de la empresa.	N/A
Responsable de Recursos Humanos	Responsable de gestionar la contratación, desarrollo y bienestar de los empleados. Se encarga del reclutamiento, capacitación, evaluación del desempeño y manejo de asuntos laborales.	N/A
Responsable de Atención al cliente	Responsable de brindar información, atender consultas y dar soporte a suscriptores, terceros de confianza y a los usuarios en general.	N/A
Responsable de Operaciones e Infraestructura	Responsable de asegurar los objetivos a través de la planificación estratégica y dirección de la operación, la infraestructura tecnológica y soporte a clientes de productos o servicios contratados.	N/A
Responsable legal	Responsable de supervisar y asesorar en cuestiones legales de la empresa. Se encarga de contratos, cumplimiento normativo, litigios y garantiza la conformidad legal en todas las operaciones.	N/A

28.2.2 NÚMERO DE PERSONAS REQUERIDAS POR TAREA

BPO garantiza al menos dos personas para realizar las tareas clasificadas como sensibles. Principalmente en la manipulación del dispositivo de custodia de las claves de EC Root y EC intermedias.

28.2.3 SEGREGACIÓN DE FUNCIONES

Los roles que presentan incompatibilidad son los siguientes: el de administrador de la aplicación de la AC y el de titular de las partes de las llaves.

28.2.4 IDENTIFICACIÓN Y AUTENTICACIÓN PARA CADA ROL

Cada persona sólo controla los activos necesarios para su rol, asegurando así que ninguna persona accede a recursos no asignados. El acceso a recursos se realiza dependiendo del activo mediante login/password, certificados digitales, tarjetas de acceso físico y llaves.

28.3 CONTROLES DE PERSONAL

28.3.1 REQUISITOS SOBRE LA CALIFICACIÓN, EXPERIENCIA Y CONOCIMIENTO PROFESIONALES

Todo el personal que realiza tareas calificadas como confiables, lleva al menos un año trabajando en BPO y tiene contratos laborales fijos.

Todo el personal está calificado y ha sido instruido convenientemente para realizar las operaciones que le han sido asignadas. El personal en puestos de confianza se encuentra libre de intereses personales que entran en conflicto con el desarrollo de la función que tenga encomendada.

BPO, retirará de sus funciones de confianza a un empleado cuando se tenga conocimiento de la existencia de la comisión de algún hecho delictivo que pudiera afectar al desempeño de sus funciones.

BPO no asignará a un sitio confiable o de gestión a una persona que no sea idónea para el puesto, especialmente por haber sido condenada por delito o falta que afecte su idoneidad para el puesto. Por este motivo, previamente se realiza una investigación, hasta donde permita la legislación aplicable, relativa a los siguientes aspectos:

- Estudios, incluyendo titulación alegada.
- Trabajos anteriores, hasta cinco años, incluyendo referencias profesionales y comprobación que realmente se realizó el trabajo alegado.
- Morosidad

28.3.2 PROCEDIMIENTO DE COMPROBACIÓN DE ANTECEDENTES

BPO, realiza las investigaciones pertinentes antes de la contratación de cualquier persona para realizar funciones de confianza.

28.3.3 REQUISITOS DE FORMACIÓN

El personal encargado de tareas de confianza ha sido formado en los términos que establece la Política y Declaración de Prácticas de Certificación.

28.3.4 REQUISITOS Y FRECUENCIA DE ACTUALIZACIÓN DE FORMACIÓN

BPO realiza los cursos de actualización necesarios para asegurarse de la correcta realización de las tareas de certificación, especialmente cuando se realicen modificaciones sustanciales en las mismas.

28.3.5 FRECUENCIA Y SECUENCIA DE ROTACIÓN DE TAREAS

No estipulado.

28.3.6 SANCIONES POR ACTUACIONES NO AUTORIZADAS

BPO, dispone de un régimen sancionador interno, para su aplicación cuando un empleado realice acciones no autorizadas pudiéndose llegar a su cese.

28.3.7 REQUISITOS DE CONTRATACIÓN DE TERCEROS

Los empleados contratados para realizar tareas confiables deberán firmar con anterioridad las cláusulas de confidencialidad y los requerimientos operacionales empleados por BPO. Cualquier acción que comprometa la seguridad de los procesos aceptados podrían una vez evaluados dar lugar al cese del contrato laboral. En el caso de que todos o parte de los servicios de certificación sean operados por un tercero, los controles y previsiones realizadas en esta sección, o en otras partes de la CPS, serán aplicados y cumplidos por el tercero que realice las funciones de operación de los servicios de certificación, la entidad de certificación será responsable en todo caso de la efectiva ejecución. Estos aspectos quedan concretados en el instrumento jurídico utilizado para acordar la prestación de los servicios de certificación por tercero distinto de BPO debiendo obligarse los terceros a cumplir con los requerimientos exigidos por BPO.

28.3.8 DOCUMENTACIÓN PROPORCIONADA AL PERSONAL

BPO, pone a disposición de todo el personal la documentación donde se detallen las funciones encomendadas, en particular la normativa de seguridad y la CPS.

Esta documentación se encuentra en un repositorio interno accesible por cualquier empleado de BPO, en el repositorio existe una lista de documentos de obligado conocimiento y cumplimiento. Adicionalmente se suministrará la documentación que precise el personal en cada momento, al objeto de que pueda desarrollar de forma competente sus funciones.

28.4 PROCEDIMIENTOS DE CONTROL DE SEGURIDAD

BPO, en calidad de prestador de servicios, está sujeta a las validaciones anuales del INDECOPI que regula el establecimiento de procesos adecuados para garantizar una correcta gestión de la seguridad en los servicios como Entidad de Certificación y Autoridad de Sellado de Tiempo.

28.4.1 TIPOS DE EVENTOS REGISTRADOS

Se registran y guarda los registros de auditoría de todos los eventos relativos al sistema de seguridad de la EC.

Se registrarán los siguientes eventos:

- Encendido y apagado del sistema.
- Intentos de accesos no autorizados al sistema de la EC a través de la red.
- Intentos de accesos no autorizados al sistema de archivos.
- Acceso físico a los registros de auditoría.
- Cambios en la configuración y mantenimiento del sistema.
- Registros de las aplicaciones de la EC.
- Encendido y apagado de la aplicación de la EC.
- Intentos de creación, borrado, restablecimiento de contraseñas o cambio de privilegios.
- Intentos de inicio y fin de sesión.
- Cambios en los detalles de la EC y/o sus claves.
- Cambios en la creación de políticas de certificados.
- Generación de claves propias.
- Creación y revocación de certificados.
- Registros de la destrucción de los medios que contienen las claves, datos de Activación.

- Eventos relacionados con el ciclo de vida del módulo criptográfico, como recepción, uso y desinstalación de este.

También se conserva, ya sea manualmente o electrónicamente, la siguiente información:

- La ceremonia de generación de claves y las bases de datos de gestión de claves.
- Registros de acceso físico.
- Mantenimientos y cambios de configuración del sistema.
- Cambios en el personal.
- Informes de compromisos y discrepancias.
- Registros de la destrucción de material que contenga información de claves, datos de activación o información personal del Firmante, en caso de certificados individuales, o del poseedor de claves, en caso de certificados de organización.
- Posesión de datos de activación, para operaciones con clave privada de la Entidad de Certificación.
- Informes completos de los intentos de intrusión física en las infraestructuras que dan soporte a la emisión y gestión de certificados.

BPO revisa sus registros de auditoría cuando se produce una alerta del sistema motivada por la existencia de algún incidente.

28.4.2 PERIODO DE RETENCIÓN DE LOS REGISTROS DE AUDITORÍA

BPO almacena la información de los registros de auditoría al menos durante 10 años.

28.4.3 PROTECCIÓN DE LOS REGISTROS DE AUDITORÍA

Los registros de auditoría de los sistemas son protegidos de su manipulación mediante mecanismos que aseguren su integridad.

Los dispositivos son manejados en todo momento por el personal autorizado.

28.4.4 PROCEDIMIENTOS DE BACKUP DE LOS REGISTROS DE AUDITORÍA

BPO dispone de un procedimiento adecuado de copia de respaldo de manera que, en caso de pérdida o destrucción de archivos relevantes, estén disponibles en un periodo corto de tiempo las correspondientes copias de respaldo de los registros de auditoría.

28.4.5 SISTEMA DE RECOGIDA DE INFORMACIÓN DE AUDITORÍA (INTERNA O EXTERNA)

La información de la auditoría de eventos es recogida internamente y de forma automatizada por el sistema operativo, la red y por el software de gestión de certificados, además de por los datos manualmente generados, que serán almacenados por el personal debidamente autorizado, todo ello compone el sistema de acumulación de registros de auditoría.

28.4.6 ANÁLISIS DE VULNERABILIDADES

En el caso de las plataformas de las CA, se realiza periódicamente una revisión de discrepancias en la información de los logs y actividades sospechosas, así como análisis de vulnerabilidades de direcciones IP internas y externas, de acuerdo al procedimiento interno establecido al efecto en las políticas de seguridad.

28.5 ARCHIVO DE REGISTROS

28.5.1 TIPOS DE EVENTOS ARCHIVADOS

Los siguientes documentos implicados en el ciclo de vida del certificado son almacenados por la EC:

- Todos los datos de auditoría de sistema. PKI, TSA y OCSP.
- Solicitudes de emisión y revocación de certificados.
- Número de identificación único proporcionado por el documento anterior.
- Todos los certificados emitidos o publicados.
- CRLs emitidas o registros del estado de los certificados generados.
- El historial de claves generadas.
- Las comunicaciones entre los elementos de la PKI.
- Políticas y Prácticas de Certificación

BPO es responsable del correcto archivo de todo este material.

28.5.2 PERIODO DE CONSERVACIÓN DE REGISTROS

Todos los datos del sistema relativos al ciclo de vida de los certificados se conservarán durante al menos 10 años desde el momento de la expiración del certificado. En particular:

- Los certificados se conservarán durante al menos 10 años desde su expiración.

- Los contratos con los Titulares, y cualquier información relativa a la identificación y autenticación de los Titulares, de los Solicitantes, y de los Suscriptores o de los Custodios de claves, y a la solicitud, aceptación y entrega de los certificados serán conservados durante al menos 10 años desde el momento de la expiración del certificado por la Entidad de Registro Afiliada.

- En el caso del cese de actividad de la CA de BPO sin transferencia de la gestión de los certificados emitidos a otro PSC, se conservará la última CRL emitida por la CA de BPO, después de realizar una revocación masiva de todos los certificados vigentes emitidos, durante al menos 10 años desde su emisión.

28.5.3 PROTECCIÓN DE ARCHIVOS

BPO asegura la correcta protección de los archivos mediante la asignación de personal calificado para su tratamiento y el almacenamiento en cajas de seguridad ignífugas e instalaciones externas.

28.5.4 PROCEDIMIENTOS DE BACKUP DEL ARCHIVO DE REGISTROS

BPO dispone de un centro de almacenamiento externo para garantizar la disponibilidad de las copias del archivo de ficheros electrónicos. Los documentos físicos se encuentran almacenados en lugares seguros de acceso restringido sólo a personal autorizado.

28.5.5 REQUISITOS PARA EL SELLADO DE TIEMPO DE LOS REGISTROS

Los registros están fechados con una fuente fiable.

Existe dentro de la documentación técnica y de configuración de la CA un apartado sobre la configuración de tiempos de los equipos utilizados en la emisión de certificados.

28.5.6 SISTEMA DE ARCHIVO DE LA INFORMACIÓN DE AUDITORÍA (INTERNA O EXTERNA)

El sistema de archivo de la información de auditoría de BPO es interno, dispone de un centro de almacenamiento externo para garantizar la disponibilidad de las copias del archivo de ficheros electrónicos.

28.5.7 PROCEDIMIENTOS PARA OBTENER Y VERIFICAR INFORMACIÓN ARCHIVADA.

Los eventos registrados están protegidos contra manipulaciones no autorizadas.

Sólo el personal autorizado para ello tiene acceso a los archivos físicos de soportes y archivos informáticos, para obtener y llevar a cabo verificaciones de integridad de dichos archivos.

28.6 CAMBIO DE CLAVES DE UNA EC

28.6.1 CA RAÍZ

Antes de que expiren todos los certificados autofirmados que contienen la clave pública de la CA Raíz, se generará un nuevo certificado autofirmado de la CA Raíz, pudiendo optar por una de las siguientes posibilidades:

A. Sustitución del certificado de la CA Raíz sin cambio de claves:

- La CA Raíz seguirá usando la misma clave privada y tendrá el nuevo certificado autofirmado, que contendrá la misma clave pública y el mismo DN en el campo subject que su anterior certificado.
- El nuevo certificado de la CA Raíz se publicará en los repositorios de BPO en las mismas URL que su anterior certificado.
- Las nuevas CRL de la CA Raíz (ARL) se publicarán en los repositorios de BPO en las mismas URL que las anteriores CRL.

B. Sustitución del certificado de la CA Raíz con cambio de claves:

- En este caso, se generará una nueva CA Raíz.
- La nueva CA Raíz usará la nueva clave privada y tendrá el nuevo certificado autofirmado, que contendrá la nueva clave pública y un DN en el campo subject distinto al contenido en su anterior certificado de la CA Raíz.
- La clave privada de la anterior CA Raíz sólo se usará para la firma de sus CRL (ARL) mientras existan certificados vigentes emitidos por la anterior CA Raíz y, después, para la firma de una última CRL.
- Cuando se deje de usar la clave privada de la anterior CA Raíz, ésta será destruida.
- El certificado de la nueva CA Raíz se publicará en los repositorios de BPO en URL distintas a las de la anterior CA Raíz.
- Las CRL de la nueva CA Raíz (ARL) se publicarán en los repositorios de BPO en URL distintas a las de la anterior CA Raíz.
- En todos los casos de sustitución del certificado de la CA Raíz, se podrán introducir cambios en su contenido, para que se ajuste mejor a la normativa y la legislación vigentes y/o a la realidad de BPO y del mercado.

28.6.2 CA SUBORDINADA

En el momento en el que BPO lo consideren conveniente y, en todo caso, antes de que expiren o sean revocados todos los certificados emitidos por la CA Raíz que contienen la clave pública de la CA Subordinada de BPO, se emitirá un nuevo certificado de la CA Subordinada de BPO firmado por la CA Raíz, pudiendo optar por una de las siguientes posibilidades:

Se generará un nuevo certificado de EC con una clave privada nueva y un CN (common name) distinto al del certificado de la EC a sustituir.

También se realizará cambio de certificado de una EC cuando el estado del arte criptográfico (algoritmos, tamaño de claves.) lo requiera.

A. Sustitución del certificado de la CA Subordinada de BPO sin cambio de claves

La CA Subordinada de BPO seguirá usando la misma clave privada y tendrá el nuevo certificado firmado por la CA Raíz, que contendrá la misma clave pública y el mismo DN en el campo subject que su anterior certificado.

El nuevo certificado de la CA Subordinada de BPO se publicará en los repositorios, en las mismas URL que su anterior certificado.

Las nuevas CRL de la CA Subordinada de BPO se publicarán en los repositorios, en las mismas URL que las anteriores CRL.

B. Sustitución del certificado de la CA Subordinada de BPO con cambio de claves

La nueva CA Subordinada de BPO usará la nueva clave privada y tendrá el nuevo certificado firmado por la CA Raíz, que contendrá la nueva clave pública y un DN en el campo subject distinto al contenido en su anterior certificado.

La clave privada de la anterior CA Subordinada de BPO sólo se usará para la firma de sus CRL mientras existan certificados vigentes emitidos por dicha CA y, después, para la firma de una última CRL.

Cuando se deje de usar la anterior clave privada de la CA Subordinada de BPO, ésta será destruida.

El certificado de la nueva CA Subordinada de BPO se publicará en los repositorios de BPO en URL distintas a las de la anterior CA Subordinada de BPO.

Las CRL de la nueva CA Subordinada de BPO se publicarán en los repositorios de BPO en URL distintas a las de la anterior CA Subordinada de BPO.

En todos los casos de sustitución del certificado de la CA Subordinada de BPO, se podrán introducir cambios en su contenido, para que se ajuste mejor a la normativa y la legislación vigentes y/o a la realidad de BPO y del mercado.

28.7 RECUPERACIÓN EN CASO DE COMPROMISO DE UNA CLAVE Y DESASTRE NATURAL U OTRO TIPO DE CATÁSTROFE

BPO en calidad de Entidad de Certificación ha desarrollado un plan de continuidad, el cual contempla el compromiso de la clave raíz de la EC como un caso particular.

Cualquier fallo en la consecución de las metas marcadas por este plan de contingencias, será tratado como razonablemente inevitable, a no ser que dicho fallo se deba a un incumplimiento de las obligaciones de BPO para implementar dichos procesos.

28.8 CESE DE UNA EC

28.8.1 CESE DE LA EC DE BPO

Antes del cese de su actividad BPO realizará las siguientes actuaciones:

- La EC debe informar al INDECOPI, a los suscriptores, titulares y terceros que confían sobre el cese de sus operaciones con por lo menos treinta (30) días calendario de anticipación.
- Proveerá de los fondos necesarios (mediante seguro de responsabilidad civil) para continuar la finalización de las actividades de revocación.
- Informará a todos Suscriptor/Firmantes, Partes Usuarias y otras ECs con los cuales tenga acuerdos u otro tipo de relación del cese con una anticipación mínima de 6 meses.
- Revocará toda autorización a entidades subcontratadas para actuar en nombre de la EC en el procedimiento de emisión de certificados.
- Transferirá sus obligaciones relativas al mantenimiento de la información de registro y de los registros de auditoría durante el periodo de tiempo indicado a los Firmantes y usuarios.
- Las claves privadas de la EC serán destruidas o deshabilitadas para su uso.
- BPO mantendrá los certificados activos y el sistema de verificación revocación hasta la extinción de todos los certificados emitidos.
- Todas estas actividades estarán recogidas en detalle en el plan de continuidad y disponibilidad de BPO.

29 CONTROLES TÉCNICOS DE SEGURIDAD

29.1 GENERACIÓN E INSTALACIÓN DEL PAR DE CLAVES

29.1.1 GENERACIÓN DEL PAR DE CLAVES DE LA EC

BPO realiza los esfuerzos que razonablemente estén a su alcance para confirmar que las claves de BPO sean generadas de acuerdo a los estándares.

En particular:

a) La generación de la clave de BPO se realizó en un entorno securizado físicamente por el personal adecuado según los roles de confianza y, al menos con un control dual. El personal autorizado para desempeñar estas funciones está limitado a aquellos requerimientos desarrollados en la CPS

b) La generación de la clave de BPO se realizó en un dispositivo que cumple los requerimientos que se detallan en el FIPS 140-2, en su nivel 3.

c) Las claves tendrán una longitud de clave adecuada para los propósitos de la firma electrónica avanzada y para el algoritmo de clave pública empleado.

29.1.2 GENERACIÓN DEL PAR DE CLAVES DEL SUSCRIPTOR

El par de claves ha sido generado por BPO mediante un quórum de seguridad 2 de 3.

Si las claves del Firmante/Suscriptor son generadas por la BPO, ésta deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que las claves son generadas de forma segura y que se mantendrá la privacidad de las mismas. En particular:

a) Las claves serán generadas usando un algoritmo adecuado para los propósitos de la firma electrónica avanzada.

b) Las claves tendrán una longitud de clave adecuada para los propósitos de la firma electrónica avanzada y para el algoritmo de clave pública empleado.

c) Las claves serán generadas y guardadas de forma segura antes de entregárselas al Firmante/Suscriptor.

d) Las claves serán destruidas de forma segura después de su entrega al Firmante/Suscriptor.

29.1.3 ENTREGA DE LA CLAVE PÚBLICA AL SUSCRIPTOR

Cuando la clave privada del Firmante/Suscriptor sea generada por BPO, ésta le será entregada de manera que la confidencialidad de la misma no sea comprometida y sólo el Firmante/Suscriptor tenga acceso a la misma.

La clave privada deberá ser almacenada en todo caso en un dispositivo seguro de almacenamiento de los datos de creación de firma (DSADCF) o en dispositivo seguro de creación de firma (DSCF).

Así mismo, este dispositivo seguro podrá consistir en un medio de almacenamiento externo (p. ej smartcard o key token) o bien en un medio software (p. ej. PKCS12).

Cuando la EC entrega un dispositivo seguro al Firmante/Suscriptor, deberá hacerlo de forma segura. En particular:

a) La preparación del dispositivo seguro, deberá ser controlada de manera segura por la EC.

b) El dispositivo seguro será guardado y distribuido de forma segura.

c) Cuando el dispositivo seguro tenga asociado unos datos de activación de Tercero que confía (p.ej. un código PIN), los datos de activación se deberán preparar de forma segura y distribuirse de manera separada del dispositivo seguro de creación de firma.

29.1.4 ENTREGA DE LA CLAVE PÚBLICA DEL SUSCRIPTOR AL EMISOR DEL CERTIFICADO

Cuando el Suscriptor pueda generar sus propias claves, la clave pública del Suscriptor tiene que ser transferida a la ER o EC, de forma que se asegure que,

- No ha sido cambiado durante el traslado
- El remitente está en posesión de la clave privada que se corresponde con la clave pública transferida y
- El proveedor de la clave pública es el legítimo Tercero que confía que aparece en el certificado.

29.1.5 ENTREGA DE LA CLAVE PÚBLICA DE LA EC A LOS TERCEROS QUE CONFÍAN

La EC deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que la integridad y la autenticidad de la clave pública de BPO y los parámetros a ella asociados son mantenidos durante su distribución a los terceros que confían. En particular:

- La clave pública de la EC estará disponible a los Terceros que confían de manera que se asegure la integridad de la clave y se autentique su origen.
- El certificado de la EC y su fingerprint (huella digital) estarán a disposición de los Terceros que confían a través de su página web.

29.1.6 TAMAÑO Y PERIODO DE VALIDEZ DE LAS CLAVES DEL EMISOR

El emisor deberá usar claves basadas en el algoritmo RSA con una longitud mínima de 2048 bits para firmar certificados, en todo caso estará sujeto en este aspecto a la práctica habitual en esta tecnología.

El periodo de uso de una clave privada será como máximo de 6 años, después del cual deberán cambiarse estas claves.

El periodo de validez del certificado de la EC se establecerá como mínimo en atención a lo siguiente:

- El periodo de uso de la clave privada de la EC
- El periodo máximo de validez de los certificados de los suscriptores firmados con esa clave.

29.1.7 TAMAÑO Y PERIODO DE VALIDEZ DE LAS CLAVES DEL SUSCRIPTOR

El Suscriptor deberá usar claves basadas en el algoritmo RSA con una longitud mínima de 2048 bits, en todo caso estará sujeto en este aspecto a la práctica habitual en esta tecnología.

El periodo de uso de la clave pública y privada del Suscriptor no deberá ser superior a 3 años y no excederá del periodo durante el cual los algoritmos de criptografía aplicada y sus parámetros correspondientes dejan de ser criptográficamente fiables.

29.1.8 HARDWARE/SOFTWARE DE GENERACIÓN DE CLAVES

Las claves de la EC deberán ser generadas en un módulo criptográfico validado al menos por el nivel 2 de FIPS 140-2 o por un nivel de funcionalidad y seguridad equivalente.

El par de claves y las claves simétricas para los Suscriptores serán generadas en un módulo de software y / o hardware criptográfico.

29.1.9 FINES DEL USO DE LA CLAVE

La EC deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que las claves de firma de la EC son usadas sólo para los propósitos de generación de certificados y para la firma de CRLs.

La clave privada del Suscriptor deberá ser usada únicamente para la generación de firmas electrónicas avanzadas, de acuerdo con el apartado Ámbito de aplicación y usos.

29.2 PROTECCIÓN DE LA CLAVE PRIVADA

La EC deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que las claves privadas de BPO continúan siendo confidenciales y mantienen su integridad. En particular:

a) La clave privada de firma de BPO será mantenida y usada en un dispositivo criptográfico seguro, el cual cumple los requerimientos que se detallan en el FIPS 140-2, en su nivel 2 o superior.

b) Cuando la clave privada de BPO esté fuera del módulo criptográfico esta deberá estar cifrada

c) Se deberá hacer un back up de la clave privada de firma de BPO, que deberá ser almacenada y recuperada sólo por el personal autorizado según los roles de confianza, usando, al menos un control dual en un medio físico seguro. El personal autorizado para desempeñar estas funciones estará limitado a aquellos requerimientos desarrollados en la CPS

d) Las copias de back up de la clave privada de firma de BPO se regirán por el mismo o más alto nivel de controles de seguridad que las claves que se usen en ese momento.

Del Firmante/Suscriptor:

La EC deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que la clave privada está protegida de forma que:

- El Firmante/Suscriptor pueda mantener la clave privada bajo su exclusivo control.
- Su secreto está razonablemente asegurado.
- La clave privada puede ser efectivamente protegida por el Firmante/Suscriptor contra un uso ajeno.

29.3 ESTÁNDARES PARA MÓDULOS CRIPTOGRÁFICOS

Todas las operaciones criptográficas deben ser desarrolladas en un módulo validado por al menos el nivel 2 de FIPS 140-2 o por un nivel de funcionalidad y seguridad equivalente.

29.3.1 CONTROL MULTIPERSONA (N DE M) DE LA CLAVE PRIVADA

Se requerirá un control multipersona para la activación de la clave privada de la EC. Este control deberá ser definido adecuadamente por la CPS en la medida en que no se trate de información confidencial o pueda comprometer de algún modo la seguridad del sistema.

29.3.2 CUSTODIA DE LA CLAVE PRIVADA

La clave privada de BPO debe ser almacenada en un medio seguro protegido criptográficamente y al menos bajo un control dual.

Las claves de los Suscriptores estarán custodiadas por este ya sea en dispositivos software como en tarjeta criptográfica tal como se describe en el certificado digital asociados a estas.

29.3.3 BACKUP DE LA CLAVE PRIVADA

La EC deberá realizar una copia de back up de su propia clave privada que haga posible su recuperación en caso de desastre o de pérdida o deterioro de la misma de acuerdo con el apartado anterior.

Las copias de las claves privadas de los Suscriptores se regirán por lo dispuesto en el punto anterior.

29.3.4 ARCHIVO DE LA CLAVE PRIVADA

La clave privada de la EC no podrá ser archivada una vez finalizado su ciclo de vida. Las claves privadas de Suscriptor no pueden ser archivadas por la EC salvo aquellas usadas para cifrado de datos.

29.3.5 INTRODUCCIÓN DE LA CLAVE PRIVADA EN EL MÓDULO CRIPTOGRÁFICO

La clave privada de la EC debe crearse en el propio dispositivo. La recuperación de la clave privada en el módulo criptográfico debe realizarse al menos con el concurso de dos operadores autorizados.

29.3.6 MÉTODO DE ACTIVACIÓN DE LA CLAVE PRIVADA

Se deberá proteger el acceso a la clave privada del Suscriptor por medio de una contraseña, PIN, u otros métodos de activación equivalentes. Si estos datos de activación deben ser entregados al Suscriptor, esta entrega deberá realizarse por medio de un canal seguro.

Estos datos de activación deberán tener una longitud de al menos 4 dígitos en el caso de custodia en un dispositivo hardware y de 8 en el caso de dispositivo software.

Los datos de activación deben ser memorizados por el Suscriptor y no deben ser anotados en un lugar de fácil acceso ni compartidos.

29.3.7 MÉTODO DE DESACTIVACIÓN DE LA CLAVE PRIVADA

La clave privada de BPO quedará desactivada mediante el borrado del contenido del dispositivo criptográfico que la contiene siguiendo estrictamente los manuales de administrador de dicho dispositivo.

La clave privada del Firmante/Suscriptor quedará inaccesible después de sucesivos intentos en la introducción del código de activación.

29.3.8 MÉTODO PARA DESTRUIR LA CLAVE PRIVADA

La EC realiza los esfuerzos que razonablemente estén a su alcance para confirmar que la clave privada de BPO no será usada una vez finalizado su ciclo de vida.

Todas las copias de la clave privada de firma de la EC deberán ser destruidas o deshabilitadas de forma que la clave privada no pueda ser recuperada.

La destrucción o deshabilitación de las claves se detallará en un documento creado al efecto.

Las claves privadas de los Suscriptores deberán ser destruidas o hacerlas inservibles después del fin de su ciclo de vida por el propio Suscriptor.

29.4 OTROS ASPECTOS DE LA GESTIÓN DEL PAR DE CLAVES

29.4.1 ARCHIVO DE LA CLAVE PÚBLICA

La EC deberá conservar todas las claves públicas de verificación.

29.4.2 PERIODO DE USO PARA EL PAR DE CLAVES

El periodo operativo de un certificado y el periodo de uso de su par de claves estarán determinados por el periodo de validez o por la revocación del certificado.

La clave privada no debe ser usada después del periodo de validez o la revocación del certificado.

La clave pública no debe ser usada después del periodo de validez o la revocación del certificado, excepto por los Terceros que confían en los certificados para verificar datos históricos.

29.4.3 FINALIZACIÓN DE LA SUSCRIPCIÓN

La EC describe los procedimientos que pueden ser utilizados por el suscriptor para terminar la suscripción a los servicios de la EC, incluyendo: La revocación de los certificados al final de la suscripción (que pueden ser diferentes, dependiendo de si el final de la suscripción se debió a la expiración del certificado o resolución del servicio). La finalización de la suscripción puede darse cuando un suscriptor elija realizar su suscripción como parte de la IOFE o la EC termine su suscripción al mismo, por fallecimiento del suscriptor o extinción de la persona jurídica que es titular del certificado.

29.5 DATOS DE ACTIVACIÓN

29.5.1 GENERACIÓN E INSTALACIÓN DE LOS DATOS DE ACTIVACIÓN

Los datos de activación de las EC se generan y se almacenan en smart cards criptográficas únicamente en posesión de personal autorizado de confianza.

29.5.2 PROTECCIÓN DE LOS DATOS DE ACTIVACIÓN

Solo el personal autorizado conoce los PINs y contraseñas para acceder a los datos de activación y estos se encuentran en cajas ignífugas dentro de las oficinas de BPO.

29.5.3 OTROS ASPECTOS DE LOS DATOS DE ACTIVACIÓN

No estipulados.

29.6 GESTIÓN DEL CICLO DE VIDA DEL MÓDULO CRIPTOGRÁFICO

La EC de BPO debe proteger el módulo criptográfico donde se almacena la clave privada, a fin de evitar su compromiso.

- El módulo criptográfico no será manipulado durante su transporte, ya sea hacia el centro de datos, su importación, o algún otro sitio autorizado por el responsable de la EC; para lo cual se mantendrá en su caja y sellada con cinta adhesiva de seguridad “VOID/OPEN” de transferencia total.

- El módulo criptográfico no será manipulado durante su almacenamiento, con excepción del equipo designado para ponerlo en su rack en el centro de datos con supervisión del responsable de la EC ó CISO de BPO.
- La instalación y activación de la clave de firma de BPO en el módulo criptográfico será realizada sólo por personal que ocupa roles de confianza (Titulares de las claves), usando al menos un control de acceso de dos personas.
- Por medio de enlaces web como el Nagios, BPO verifica que el módulo criptográfico funcione correctamente.
- Las claves de firma de la EC que son almacenadas en un módulo criptográfico deben ser borradas antes de que el dispositivo sea retirado

29.7 CONTROLES DE SEGURIDAD INFORMÁTICA Y OPERACIONALES

BPO emplea sistemas fiables para ofrecer sus servicios de certificación. BPO ha realizado controles y auditorías informáticas a fin de establecer una gestión de sus activos informáticos adecuados con el nivel de seguridad requerido en la gestión de sistemas de certificación electrónica.

Los equipos usados son inicialmente configurados con los perfiles de seguridad adecuados por parte del personal de sistemas de BPO, en los siguientes aspectos:

1. Configuración de seguridad del sistema operativo.
2. Configuración de seguridad de las aplicaciones.
3. Dimensionamiento correcto del sistema.
4. Configuración de Usuarios y permisos.
5. Configuración de eventos de registros de auditoría.
6. Plan de copia de respaldo y recuperación.
7. Configuración antivirus
8. Requerimientos de tráfico de red.

29.7.1 REQUISITOS TÉCNICOS DE SEGURIDAD ESPECÍFICOS

Cada servidor de BPO incluye las siguientes funcionalidades:

- Control de acceso a los servicios de EC y gestión de privilegios.
- Imposición de separación de tareas para la gestión de privilegios.
- Identificación y autenticación de roles asociados a identidades.
- Archivo del historial del Firmante y la EC y datos de auditoría.
- Auditoría de eventos relativos a la seguridad .
- Auto-diagnóstico de seguridad relacionado con los servicios de la EC.
- Mecanismos de recuperación de claves y del sistema de EC Las funcionalidades expuestas son realizadas mediante una combinación de sistema operativo, software de PKI, protección física y procedimientos.

29.7.2 EVALUACIÓN DE LA SEGURIDAD INFORMÁTICA

La seguridad de los equipos viene reflejada por un análisis de riesgos iniciales de tal forma que las medidas de seguridad implantadas son respuesta a la probabilidad e impacto producido cuando un grupo de amenazas definidas puedan aprovechar brechas de seguridad.

29.7.3 CONTROLES DE GESTIÓN DE SEGURIDAD

BPO desarrolla las actividades precisas para la formación y concienciación de los empleados en materia de seguridad. Los materiales empleados para la formación y los documentos descriptivos de los procesos son actualizados después de su aprobación por un grupo para la gestión de la seguridad. Para realizar esta función dispone de un plan de formación anual.

BPO exige mediante contrato, las medidas de seguridad equivalentes a cualquier proveedor externo implicado en las labores de certificación.

29.7.4 CONTROLES DE SEGURIDAD DEL CICLO DE VIDA

Para proteger la gestión del ciclo de vida de las claves de la EC, BPO cuenta con roles de confianza que se mencionan en la Política y Plan de Seguridad.

29.8 CONTROLES DE SEGURIDAD DE LA RED

BPO protege el acceso físico a los dispositivos de gestión de red y dispone de una arquitectura que ordena el tráfico generado basándose en sus características de seguridad creando secciones de red claramente definidas. Esta división se realiza mediante el uso de cortafuegos.

La información que se transfiere por redes no seguras se realiza de forma cifrada mediante uso de protocolos SSL.

29.9 SELLADO DE TIEMPO

BPO obtiene mediante un hardware específico con reloj atómico del átomo de rubidio, sincronización GPS y consulta al Real Observatorio de la Armada, siguiendo el protocolo NTP a través de Internet. La descripción del protocolo NTP se puede encontrar en la RFC 5905 “Network Time Protocol”.

30 PERFILES DE CERTIFICADOS, CRL Y OCSP

30.1 TAMAÑO DE LAS CLAVES Y VALIDEZ DE LOS CERTIFICADOS

Certificado	Tamaño claves RSA	Función HASH	Validez del certificado
CA Raíz	4096 bits	SHA 384	Hasta 6 años
CA Subordinada	4096 bits	SHA 384	Hasta 6 años
CA TSA	4096 bits	SHA 384	Hasta 6 años

Entidad final	2048 bits	SHA 384	1 año hasta 2025, a partir del 2025 el tamaño de claves debe ser 3072
Operador de registro	2048 bits	SHA 384	1 año hasta 2025, a partir del 2025 el tamaño de claves debe ser 3072

30.2 PERFIL DE CERTIFICADO

Todos los certificados emitidos bajo esta política serán conformes al estándar X.509 versión 3 y al RFC 3739 "Internet X.509 Public Key Infrastructure Qualified Certificates Profile".

El perfil común a todos los certificados es el siguiente:

Campo del certificado	Nombre	Descripción
Versión	N° de versión	V3 (versión del estándar X509)
Serial	Número de serie	Código aleatorio único con respecto al DN del emisor
Signature	Algoritmo de firma	OID Y parámetros del algoritmo de firma
Issuer	Emisor	DN (Nombre Distinguido) de la ECD que emite el certificado (BPO)
notBefore	Válido desde	Fecha de inicio de validez, tiempo UTC
notAfter	Válido hasta	Fecha de fin de validez, tiempo UTC
Subject	Sujeto	Nombre distinguido del suscriptor
SubjectPublicKeyInfo	Clave pública	Valor de la clave pública
Extensions	Extensiones	Extensiones de los certificados

30.2.1 NÚMERO DE VERSIÓN

BPO emite certificados X.509 Versión 3.

30.2.2 EXTENSIONES DEL CERTIFICADO

Campo del DN	Nombre	Descripción
Authority key Identifier	Identificador de Clave de la Entidad	Identificador de la Clave Pública del certificado de BPO SHA256 Standard CA
Subject Key Identifier	Identificador de Clave del Sujeto	Identificador de la clave pública del certificado.

Key Usage	Uso de Clave	Firma Digital Sin Repudio.
Certificate Policies	Directivas del Certificado	OID 1.3.6.1.4.1.50718.0.1.0.1.1 URL de la DPC://bpo/repository/
Subject Alternative Name	Nombre Alternativo del sujeto	RFC822name:correo electrónico del suscriptor
Basic Contraints	Restricciones Básicas	Tipo de Asunto: Entidad Final Restricción de Longitud de ruta: Ninguno
Extended Key Usage	Uso mejorado de las claves	Autenticación del cliente (1.3.6.1.5.5.7.3.2) Correo Seguro (1.3.6.1.5.5.7.3.4)
CRL Distribution Points	CRL Puntos de distribución	URL de la CRL http://crl.bpo/bpostandardca.crl
Authority Information Access	Acceso a la información de la Autoridad	URL del certificado de BPO SHA256 Standard CA URL del servicio OCSP de BPO SHA256 Standard CA

30.2.3 IDENTIFICADORES DE OBJETOS DE ALGORITMO

El identificador de objeto del algoritmo de firma será 1.2.840.113549.1.1.5

El identificador de objeto del algoritmo de la clave pública será rsaEncryption 1.2.840.113549.1.1.1

30.2.4 FORMATO DE NOMBRES

Los certificados deberán contener las informaciones que resulten necesarias para su uso, según determine la correspondiente política de autenticación, firma electrónica, cifrado o evidencia electrónica.

Campo del DN	Nombre	Descripción
CN, Common Name	Nombre	Nombre completo del suscriptor
SN, Serial Number	Número de serie	Tipo y número de documento del suscriptor
E, E-mail	E-mail	Correo electrónico del suscriptor
C, Country Name	País	Código de país de dos dígitos según ISO 3166-1. Por defecto “PE”.

L, Locality	Localidad	Lima

30.2.5 LIMITACIONES DE LOS NOMBRES

Se puede utilizar restricciones de nombre (utilizando la extensión del certificado "name constrains") en aquellos certificados de la EC de BPO emitidos a terceras partes de forma que solo se pueda emitir por la EC el conjunto de certificados permitido en dicha extensión.

30.3 PERFIL DE CRL

El perfil de la CRL es conforme al estándar RFC 5280 "internet X.509 public key infraestructura certificate and certificate revocation list (CRL)

Campo de la CRL	Nombre	Descripción
Versión	N° de versión	V2
Signature	Algoritmo de firma	Sha256WithRSAEncryption
Issuer	Emisor	DN (Nombre Distinguido) de la ECD que emite la CRL (BPO)
ThisUpdate	Fecha y hora de emisión de esta CRL	(fecha y hora de emisión de la CRL, tiempo UTC)
NextUpdate	Fecha y hora de emisión de la próxima CRL	Fecha de fin de validez de la CRL, tiempo UTC
RevokedCertificates	Entradas de la CRL	Nº de serie del certificado revocado Fecha y hora de revocación del certificado Código de razón de revocación del certificado

30.3.1 NÚMERO DE VERSIÓN

El formato de las CRLs utilizadas es el especificado en la versión 2 (X509 v2).

30.3.2 CRL Y EXTENSIONES CRL

Se soporta y se utilizan CRLs conformes al estándar X.509.

30.4 PERFIL OCSP

El Servicio de Validación de Certificados se basa en el uso del protocolo OCSP sobre HTTP, definido en la norma RFC 6960 "Online Certificate Status Protocol – OCSP".

Los servicios OCSP cumplen con con la norma IETF RFC 6960

Campo del DN	Nombre	Descripción
CN, Common Name	Nombre	BPO SHA256 Standard CA OCSP signer 1 La SubCA emite el certificado para OCSP

30.4.1 CAMPO ISSUER DEL CERTIFICADO

Campo del DN	Nombre	Descripción
CN, Common Name	Nombre	BPO SHA256 Standard CA
O, Organization Name	Nombre de la Empresa	BPO
C, Country Name	País	Código de país de dos dígitos según ISO 3166-1. Por defecto “PE”.

31 AUDITORÍA DE CONFORMIDAD Y OTROS CONTROLES

BPO se somete a auditorías anuales como se describe en los apartados siguientes.

31.1 FRECUENCIA O CIRCUNSTANCIAS DE LOS CONTROLES

Se realizarán auditorías periódicas, generalmente con carácter anual.

BPO se compromete a realizar las auditorías necesarias.

31.2 IDENTIDAD/CALIFICACIÓN DEL AUDITOR

En BPO, las auditorías pueden ser de carácter tanto interno como externo. En este segundo caso se realizan por empresas de reconocido prestigio en el ámbito de las auditorías.

- Para las auditorías internas / EC , SVA , TSA
- En relación a BPO, la selección de auditores depende del INDECOPI.

31.3 RELACIÓN ENTRE EL AUDITOR Y LA ENTIDAD AUDITADA

Las empresas que realizan auditorías externas nunca presentan conflictos de intereses que puedan desvirtuar su actuación en su relación con BPO.

31.4 ASPECTOS CUBIERTOS POR LOS CONTROLES

En líneas generales, las auditorías verifican:

a) Que la EC tiene un sistema que garantice la calidad del servicio prestado.

b) Que la EC cumple con los requerimientos de las Políticas de Certificación que gobiernan la emisión de los distintos certificados digitales.

c) Que la CPS, se ajusta a lo establecido en las Políticas, con lo acordado por la Autoridad aprobadora de la Política y con lo establecido en la normativa vigente.

d) Que la EC gestiona de forma adecuada la seguridad de sus sistemas de información.

31.5 TRATAMIENTOS DE LOS INFORMES DE AUDITORÍA

Una vez recibido el informe de la auditoría de cumplimiento llevada a cabo, BPO discutirá, con la entidad que ha ejecutado la auditoría, las deficiencias encontradas y desarrollarán y ejecutarán un plan correctivo con objeto de solucionar las deficiencias.

32 OTROS ASUNTOS LEGALES Y COMERCIALES

32.1 TARIFAS

32.1.1 TARIFAS DE EMISIÓN DE CERTIFICADOS Y RENOVACIÓN

Los precios de los servicios de certificación o cualquiera otros servicios relacionados estarán disponibles en la página web de BPO ó en sus respectivos contratos..

32.1.2 TARIFAS DE ACCESO A LA INFORMACIÓN RELATIVA AL ESTADO DE LOS CERTIFICADOS O LOS CERTIFICADOS REVOCADOS

La EC proveerá de un acceso a la información relativa al estado de los certificados libre y gratuita.

32.1.3 TARIFAS POR EL ACCESO AL CONTENIDO DE ESTAS POLÍTICAS DE CERTIFICACIÓN

El acceso al contenido de la presente Política de Certificación será gratuito.

32.1.4 POLÍTICA DE REEMBOLSO

La EC dispondrá de una política de reembolso que se encuentra descrita en los contratos con los suscriptores.

32.2 RESPONSABILIDADES ECONÓMICAS DE BPO

BPO, en su actividad como Entidad de Certificación dispone de recursos económicos suficientes para afrontar el riesgo de la responsabilidad por daños y perjuicios ante los usuarios de sus servicios y a terceros, garantizando sus responsabilidades en su actividad de PSC tal como se define en la legislación vigente.

La garantía citada se establece mediante un Seguro de Responsabilidad Civil con una cobertura igual o superior a la mínima establecida por la Guía de Acreditación de Entidades de Certificación del INDECOPI.

32.2.1 EXONERACIÓN DE RESPONSABILIDAD

La EC de BPO no será responsable en ningún caso cuando se encuentran ante cualquiera de estas circunstancias:

1. Estado de guerra, desastres naturales o cualquier otro caso de fuerza mayor

2. Por el uso de los certificados siempre y cuando exceda de lo dispuesto en la normativa vigente y la presente política de certificación

3. Por el uso indebido o fraudulento de los certificados o CRL´S emitidos por la autoridad de certificación

4. Por el uso de la información contenida en el certificado o en la crl.

5. Por el incumplimiento de las obligaciones establecidas para el suscriptor o terceros que confían en la normativa vigente, la presente CPS o en las prácticas correspondientes.

6. Por el perjuicio causado en el periodo de verificación de las causas de revocación /suspensión.

7. Por el contenido de los mensajes o documentos firmados o cifrados digitalmente.

8. Por la no recuperación de documentos cifrados con la clave pública del suscriptor.

9. Fraude en la documentación presentada por el solicitante.

32.3 RESPONSABILIDADES FINANCIERAS

La EC de BPO dispone de un seguro de responsabilidad civil que contempla sus responsabilidades, para indemnizar por daños y perjuicios que se puedan ocasionar a los usuarios de sus servicios, por un monto que supera lo establecido por la normativa vigente.

32.4 CONFIDENCIALIDAD DE LA INFORMACIÓN COMERCIAL

32.4.1 TIPO DE INFORMACIÓN A MANTENER CONFIDENCIAL

Se considerará confidencial toda la información que no esté catalogada expresamente como pública. No se difunde información declarada como confidencial sin el consentimiento expreso por escrito de la entidad u organización que la haya otorgado el carácter confidencial a dicha información, a no ser que exista una imposición legal.

BPO, dispone de una adecuada política de tratamiento de la información y de los modelos de acuerdo de confidencialidad que deberán firmar todas las personas que tengan acceso a información confidencial.

Asimismo, cumple en todo caso con la normativa vigente en cada momento en materia de protección de datos.

32.4.2 TIPO DE INFORMACIÓN CONSIDERADA NO CONFIDENCIAL

Se considera como información no confidencial:

- La contenida en la presente CPS y en las Políticas.
- La información contenida en los certificados.
- Cualquier información cuya accesibilidad sea prohibida por la normativa vigente.

32.5 DERECHOS DE PROPIEDAD INTELECTUAL

La EC de BPO es titular de los derechos de propiedad intelectual, que puedan derivarse del sistema de certificación que regula esta CPS y sus políticas. Se prohíbe por tanto, cualquier acto de reproducción, distribución, comunicación pública y transformación de cualquiera de los elementos que son titularidad exclusiva de la EC sin la autorización expresa por su parte.

No obstante, no necesitará autorización de la EC para la reproducción del Certificado cuando la misma sea necesaria para su utilización por parte del Tercero que confía legítimo y con arreglo a la finalidad del Certificado, de acuerdo con los términos de esta CPS y sus Políticas.

32.6 OBLIGACIONES

32.6.1 ENTIDAD DE CERTIFICACIÓN BPO

BPO se encuentra obligada a cumplir con lo dispuesto por la normativa vigente y además a:

1. Respetar lo dispuesto en esta Política.

2. Proteger sus claves privadas de forma segura.

3. Emitir certificados conforme a esta Política y a los estándares de aplicación.

4. Emitir certificados según la información que obra en su poder y libres de errores de entrada de datos

5. Emitir certificados cuyo contenido mínimo sea el definido por la normativa vigente para los certificados cualificados.

6. Publicar los certificados emitidos en un directorio, respetando en todo caso lo dispuesto en materia de protección de datos por la normativa vigente.

7. Suspender y revocar los certificados según lo dispuesto en esta Política y publicar las mencionadas revocaciones en la CRL

8. Informar a los Suscriptores de la revocación o suspensión de sus certificados, en tiempo y forma de acuerdo con la legislación vigente.

9. Publicar esta Política y las Prácticas correspondientes en su página web.

10. Informar sobre las modificaciones de la Política y Declaración Prácticas de Certificación de BPO, a los Suscriptores y a la ER vinculada.

11. No almacenar ni copiar los datos de creación de firma del Suscriptor.

12. Proteger, con el debido cuidado, los datos de creación de firma mientras estén bajo su custodia, en su caso.

13. Establecer los mecanismos de generación y custodia de la información relevante en las actividades descritas, protegiéndolas ante pérdida o destrucción o falsificación

14. Conservar la información sobre el certificado emitido por el período mínimo exigido por la normativa vigente.

32.6.2 ENTIDADES DE REGISTRO ANEXAS A LA EC DE BPO

Las ER anexas se encuentran obligadas a cumplir con los dispuestos por la normativa vigente y además a:

- Proteger sus claves privadas
- Comprobar la identidad de los solicitantes de certificados
- Verificar con exactitud y autenticidad la información suministrada por el Suscriptor solicitante
- Archivar, por periodo dispuesto en la legislación vigente, los documentos suministrados por el Suscriptor Pasar por una auditoría de parte de BPO EC una vez al año
- Respetar los dispuesto en los contratos firmados con la EC de BPO y con el suscriptor
- Informar a la EC las causas de revocación siempre y cuando tomen conocimiento

El Administrador y el Responsable de la ER anexa son los que gestionan el IP de su personal con el fin de que puedan acceder a la plataforma de certificados. Además del certificado digital de cada operador que ingresa a la plataforma, es necesario que se habilite su IP para que puedan acceder.

Para la verificación de antecedentes de los operadores de registro de las entidades de registro anexas a la EC se solicitarán los siguientes documentos:

- Antecedentes crediticios
- Antecedentes penales y policiales
- Documentación (solicitud de alta)
- Constancia de capacitación como Operador de Registro
- Constancia de aprobación del examen de OR otorgado por la EC de BPO

32.6.3 SOLICITANTE

El solicitante de un Certificado estará obligado a cumplir con lo dispuesto por la normativa aplicable y además a:

1. Suministrar a la ER la información necesaria para realizar una correcta identificación.

2. Confirmar la exactitud y veracidad de la información suministrada.

3. Notificar cualquier cambio en los datos aportados para la creación del certificado durante su periodo de validez.

32.6.4 SUSCRIPTOR

El Suscriptor (ya sea persona natural o jurídica a través de un representante suficiente) de un certificado estará obligado a cumplir con lo dispuesto por la normativa vigente y además a:

1. Custodiar su clave privada de manera diligente

2. Usar el certificado según lo establecido en la presente Política de Certificación

3. Respetar lo dispuesto en el contrato firmado con la EC de BPO.

4. En el caso de los certificados con alguna vinculación empresarial, informar de la existencia de alguna causa de suspensión /revocación como, por ejemplo, el cese o la modificación de su vinculación con la Entidad.

5. En el caso de los certificados con alguna vinculación empresarial, notificar cualquier cambio en los datos aportados para la creación del certificado durante su período de validez, como el cese o la modificación de su vinculación con la Entidad.

32.6.5 TERCERO QUE CONFÍA

Será obligación de los Terceros que confían cumplir con lo dispuesto por la normativa vigente y además:

1. Verificar la validez de los certificados en el momento de realizar cualquier operación basada en los mismos.

2. Conocer y sujetarse a las garantías, límites y responsabilidades aplicables en la aceptación y uso de los certificados en los que confía, y aceptar sujetarse a las mismas.

32.6.6 EMPRESAS

En el caso de que el certificado exprese alguna vinculación empresarial será obligación de la Empresa solicitar a la ER la suspensión/revocación del certificado cuando cese o se modifique la vinculación del Suscriptor o el servicio electrónico con la Empresa.

32.6.7 REPOSITORIO

La información relativa a la publicación y revocación /suspensión de los certificados se mantendrá accesible al público en los términos establecidos en la normativa vigente. La EC deberá mantener un sistema seguro de almacén y recuperación de certificados y un repositorio de certificados revocados, pudiendo delegar estas funciones en una tercera entidad.

33 RESOLUCIÓN DE DISPUTAS

Para la resolución de disputas el titular/suscriptor escribe desde el correo electrónico que brindó a la Entidad de Registro afiliada con los argumentos de la disputa en mención al correo electrónico de la ENTIDAD teresa.prado@bpo-advisors.net para su revisión y del ser del ámbito será atendido brindando respuesta al titular/suscriptor.

De llegar a alguna disputa o incumplimiento entre las partes, los costos incluido el honorario de abogados será asumida por cada parte.

34 CONFORMIDAD CON LA LEY APLICABLE

BPO es afecta y cumple con las obligaciones establecidas por la IOFE, a los requerimientos de la Guía de Acreditación para Entidades de Certificación Digital EC, al Reglamento de la Ley de Certificados Digitales, y a la Ley de Firmas y Certificados Digitales - Ley 27269, para el reconocimiento legal de los servicios como prestador de servicios de certificación emitidos bajo las directrices definidas en el presente documento.

35 BIBLIOGRAFÍA

a) Guía de Acreditación para Entidades de Certificación Digital EC, INDECOPI
b) Ley de Firmas y Certificados Digitales – Ley 27269
c) Decreto Supremo 052-2008
d) Decreto Supremo 070-2011
e) Decreto Supremo 105-2012