2024

Política y Plan de Seguridad de la Información de la Entidad de Certificación

Índice

1 INFORMACIÓN DEL DOCUMENTO

1.1. NOMBRE Y RESPONSABLE

Nombre del documento	Política y Plan de Seguridad de Información EC 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

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 operaciones y prácticas de seguridad de la información que cumple 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 BPO a través de 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 de 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 de 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
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.

La figura de Titular será diferente dependiendo de los distintos certificados emitidos por 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 POLÍTICA DE SEGURIDAD

BPO protege la información que es relevante para los servicios de certificación digital que brinda durante todo su ciclo de vida, siguiendo un ciclo de mejora continua.

Esta política tiene como objetivos:

- Proteger la información que sirve para garantizar y dar fe de la autenticidad de los credenciales de identidad otorgados por la EC de BPO. En particular de las claves privadas de las Autoridades de Certificación Raíz y Subordinadas.
- Adoptar los controles de seguridad exigidos por la Autoridad Administrativa Competente respecto de los servicios de certificación brindados.
- Proteger los datos personales recogidos durante las operaciones de certificación digital de BPO conforme a la regulación vigente.

- Garantizar la correcta identificación de los suscriptores de los certificados digitales emitidos por BPO.

9 PLAN DE SEGURIDAD

9.1 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.

9.1.1 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.

9.1.2 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.

9.1.3 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.

9.1.4 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.

9.1.5 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 de personal del Centro de Datos.

9.2 CONTROLES DE PROCEDIMIENTO

9.2.1 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

9.2.2 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.

9.2.3 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.

9.2.4 IDENTIFICACIÓN Y AUTENTICACIÓN PARA CADA ROL

Cada persona solo 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 tarjetas criptográficas y códigos de activación

9.3 CONTROLES DE PERSONAL

9.3.1 REQUISITOS SOBRE LA CUALIFICACIÓN, 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

9.3.2 PROCEDIMIENTO DE COMPROBACIÓN DE ANTECEDENTES

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

9.3.3 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.

9.3.4 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.

9.3.5 FRECUENCIA Y SECUENCIA DE ROTACIÓN DE TAREAS

No está estipulado.

9.3.6 SANCIONES POR ACTUACIONES NO AUTORIZADAS

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

9.3.7 REQUISITOS DE CONTRATACIÓN DE TERCEROS

Los empleados contratados para realizar tareas confiables firman anteriormente 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.

9.3.8 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.

9.4 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.

9.4.1 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.

9.4.2 PERIODO DE RETENCIÓN DE LOS REGISTROS DE AUDITORÍA

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

9.4.3 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.

9.4.4 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.

9.4.5 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.

9.4.6 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.

9.5 ARCHIVO DE REGISTROS

9.5.1 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, EC, 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.

9.5.2 PERIODO DE CONSERVACIÓN

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.

9.5.3 PROTECCIÓN DE ARCHIVOS

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

9.5.4 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.

9.5.5 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.

9.5.6 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.

9.5.7 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.

9.6 CAMBIO DE CLAVES DE UNA EC

9.6.1 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.

9.6.2 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.

9.7 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.

9.8 CESE DE UNA EC

9.8.1 CESE DE LA EC DE BPO

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

- 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, apartado “Plan de Cierre”.

10 CONTROLES TÉCNICOS DE SEGURIDAD

10.1 GENERACIÓN E INSTALACIÓN DEL PAR DE CLAVES

10.1.1 GENERACIÓN DEL PAR DE CLAVES DE LA EC

BPO deberá realizar 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 la BPO se realizará 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 estará limitado a aquellos requerimientos desarrollados en la CPS

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

10.1.2 GENERACIÓN DEL PAR DE CLAVES DEL SUSCRIPTOR

El par de claves será generado por el emisor o bajo su control.

Si las claves del Firmante/Suscriptor son generadas por 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.

10.1.3 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.

10.1.4 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.

10.1.5 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.

10.1.6 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.

10.1.7 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 4 años y no excederá del periodo durante el cual los algoritmos de criptografía aplicada y sus parámetros correspondientes dejan de ser criptográficamente fiables.

10.1.8 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.

10.1.9 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.

10.2 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.

10.3 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.

10.3.1 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.

10.3.2 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.

10.3.3 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.

10.3.4 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.

10.3.5 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.

10.3.6 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.

10.3.7 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.

10.3.8 MÉTODO PARA DESTRUIR LA CLAVE PRIVADA

La EC deberá realizar 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 detalla 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.

10.4 OTROS ASPECTOS DE LA GESTIÓN DEL PAR DE CLAVES

10.4.1 ARCHIVO DE LA CLAVE PÚBLICA

La EC deberá conservar todas las claves públicas de verificación.

10.4.2 PERIODO DE USO PARA EL PAR DE CLAVES

Ya visto.

10.5 DATOS DE ACTIVACIÓN

10.5.1 GENERACIÓN E INSTALACIÓN DE LOS DATOS DE ACTIVACIÓN

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

10.5.2 PROTECCIÓN DE LOS DATOS DE ACTIVACIÓN

Solo el personal autorizado conoce los PINs y contraseñas para acceder a los datos de activación.

10.5.3 OTROS ASPECTOS DE LOS DATOS DE ACTIVACIÓN

No estipulados.

10.6 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.

Respecto a la seguridad de la información se sigue el esquema de certificación sobre sistemas de gestión de la información ISO 270001.

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.

10.6.1 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.

10.6.2 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.

10.7 CONTROLES TÉCNICOS DEL CICLO DE VIDA

10.7.1 CONTROLES DE DESARROLLO DE SISTEMAS

BPO posee un procedimiento de control de cambios en las versiones de sistemas operativos y aplicaciones que impliquen una mejora en sus funciones de seguridad o que corrijan cualquier vulnerabilidad detectada. Como respuesta a los análisis de intrusión y vulnerabilidades se realizan las adaptaciones de los sistemas y aplicaciones que pueden tener problemas de seguridad y a las alertas de seguridad recibidas desde los servicios de seguridad gestionadas contratados con terceros, se realizan ejecutan los RFC (Request for Changes) correspondientes para la incorporación de los parches de seguridad o la actualización de las versiones con problemas.

En el RFC se incorporan y se documentan las medidas tomadas para la aceptación, ejecución o la denegación de dicho cambio. En los casos que la ejecución de la actualización o corrección de un problema incorpore una situación de vulnerabilidad o un riesgo importante se incorpora en el análisis de riesgos y se ejecutan controles alternativos hasta que el nivel de riesgo sea asumible.

10.7.2 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

10.7.3 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.

10.8 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.

10.9 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".

11 AUDITORÍA DE CONFORMIDAD Y OTROS CONTROLES

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

11.1 FRECUENCIA O CIRCUNSTANCIAS DE LOS CONTROLES

Se realizarán auditorías periódicas, generalmente con carácter anual.

BPO se compromete a realizar las auditorías necesarias.

11.2 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.

11.3 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.

11.4 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.

11.5 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.

Si la Entidad auditada es incapaz de desarrollar y / o ejecutar dicho plan en el plazo de tiempo solicitado, o si las deficiencias encontradas suponen una amenaza inmediata para la seguridad o integridad del sistema, deberá comunicar inmediatamente la autoridad de políticas, que podrá ejecutar las siguientes acciones:

- Cesar las operaciones transitoriamente.
- Revocar el certificado correspondiente, y regenerar la infraestructura.
- Terminar el servicio a la Entidad.
- Otras acciones complementarias que resulten necesarias.

12 CLÁUSULAS FINALES

12.1 OBLIGACIONES

12.1.1 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.

12.1.2 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 vinculada 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.

12.1.3 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.

12.1.4 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.

12.1.5 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.

12.1.6 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.

12.2 RESPONSABILIDAD

La EC dispondrá en todo momento de un seguro de responsabilidad civil en los términos que marque la legislación vigente. La EC actuará en la cobertura de sus responsabilidades por sí o a través de la entidad aseguradora, satisfaciendo los requerimientos de los solicitantes de los certificados, de los Suscriptores y de los terceros que confíen en los certificados.

Las responsabilidades de la EC incluyen las establecidas por la presente Política de Certificación, así como las que resulten de aplicación como consecuencia de la normativa peruana e internacional.

La EC será responsable del daño causado ante el Suscriptor o cualquier persona que de buena fe confíe en el certificado, siempre que exista dolo o culpa grave, respecto de:

1. la exactitud de toda la información contenida en el certificado en la fecha de su emisión

2. la garantía de que, en el momento de la entrega del certificado, obra en poder del Suscriptor o servicio electrónico, la clave privada correspondiente a la clave pública dada o identificada en el certificado

3. la garantía de que la clave pública y privada funcionan conjunta y complementariamente

4. la correspondencia entre el certificado solicitado y el certificado entregado

5. Cualquier responsabilidad que se establezca por la legislación vigente.

12.2.1 EXONERACIÓN DE RESPONSABILIDAD

La EC de BPO no serán responsables 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 Política de Certificación 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

12.2.2 LÍMITE DE RESPONSABILIDAD EN CASO DE PÉRDIDAS POR TRANSACCIONES

La EC de BPO no aplicará límites de cantidad a las transacciones que se realicen con el certificado. Podrán establecerse garantías particulares a través de seguros específicos que se negociarán individualmente. Esta garantía será de aplicación a efectos de lo dispuesto en legislación vigente.

12.3 RESPONSABILIDAD FINANCIERA

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.

13 OFICIAL DE SEGURIDAD Y PRIVACIDAD

El Oficial de Seguridad y Privacidad de BPO, gestiona la implementación y vela por el cumplimiento de la presente política, así como de su revisión periódica, actualización, difusión y concientización y capacitación al personal y terceros para su adecuado cumplimiento.

14 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.

15 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