2024

Política y Plan de Seguridad de la Información de la Autoridad de Sellado de Tiempo

Autoridad de Sellado de Tiempo

Índice

1 INFORMACIÓN DEL DOCUMENTO 4
1.1. NOMBRE Y RESPONSABLE 4
1.2 CONTROL DE VERSIONES 4
2 INTRODUCCIÓN 5
3 OBJETIVO 5
4 OBJETO DE LA ACREDITACIÓN 5
5 DEFINICIONES Y ABREVIACIONES 5
5.1 ABREVIACIONES 5
5.2 DEFINICIONES 7
5.3 PKI PARTICIPANTES 8
5.3.1 ENTIDAD DE CERTIFICACIÓN BPO (EC BPO) 8
5.3.2 ENTIDAD DE REGISTRO BPO 8
5.3.3 AUTORIDAD DE SELLADO DE TIEMPO (TSA BPO) 8
5.3.4 TITULAR 8
5.3.5 SUSCRIPTOR 8
5.3.6 SOLICITANTE 8
5.3.7 TERCERO QUE CONFÍA 9
5.3.8 ENTIDAD A LA CUAL SE ENCUENTRA VINCULADO EL TITULAR 9
6 POLÍTICA DE SEGURIDAD 9
7 PLAN DE SEGURIDAD 9
7.1 CONTROLES FÍSICOS 9
7.1.1 SERVICIOS EN LA SALA DEL DATA CENTER 9
7.1.2 INGRESO PROGRAMADO AL DATA CENTER 9
7.1.3 INGRESO AL DATA CENTER EN CASO DE EMERGENCIA 10
7.1.4 INGRESO AL DATA CENTER CON EQUIPOS 10
7.1.5 OTRAS NORMAS 10
7.2 CONTROLES DE PROCEDIMIENTO 11
7.2.1 ROLES DE CONFIANZA 11
7.2.2 NÚMERO DE PERSONAS REQUERIDAS POR TAREA 13
7.2.3 SEGREGACIÓN DE FUNCIONES 13
7.2.4 IDENTIFICACIÓN Y AUTENTICACIÓN PARA CADA ROL 13
7.3 GESTIÓN DE ACTIVOS 13
7.4 CONTROLES DE PERSONAL 13
7.4.3 REQUISITOS DE FORMACIÓN 14
7.4.4 REQUISITOS Y FRECUENCIA DE ACTUALIZACIÓN DE FORMACIÓN 14
7.4.5 FRECUENCIA Y SECUENCIA DE ROTACIÓN DE TAREAS 14
7.4.6 SANCIONES POR ACTUACIONES NO AUTORIZADAS 14
7.4.7 REQUISITOS DE CONTRATACIÓN DE TERCEROS 14
7.4.8 DOCUMENTACIÓN PROPORCIONADA AL PERSONAL 15
7.5 PROCEDIMIENTOS DE CONTROL DE SEGURIDAD 15

7.5.1 TIPOS DE EVENTOS REGISTRADOS 15
7.5.2 PERIODO DE RETENCIÓN DE LOS REGISTROS DE AUDITORÍA 16
7.5.3 PROTECCIÓN DE LOS REGISTROS DE AUDITORÍA 16
7.5.4 PROCEDIMIENTOS DE BACKUP DE LOS REGISTROS DE AUDITORÍA 16
7.5.5 SISTEMA DE RECOGIDA DE INFORMACIÓN DE AUDITORÍA (INTERNA O EXTERNA) 16
7.5.6 ANÁLISIS DE VULNERABILIDADES 16
7.5 ARCHIVO DE REGISTROS 16
7.5.1 TIPOS DE EVENTOS ARCHIVADOS 16
7.5.2 PERIODO DE CONSERVACIÓN 17
7.5.3 PROTECCIÓN DE ARCHIVOS 17
7.5.4 PROCEDIMIENTOS DE BACKUP DEL ARCHIVO DE REGISTROS 17
7.5.5 REQUISITOS PARA EL SELLADO DE TIEMPO DE LOS REGISTROS 17
7.5.6 SISTEMA DE ARCHIVO DE LA INFORMACIÓN DE AUDITORÍA (INTERNA O EXTERNA) 17
7.5.7 PROCEDIMIENTOS PARA OBTENER Y VERIFICAR INFORMACIÓN ARCHIVADA. 17
7.6 GESTIÓN DE OPERACIONES 18
7.7 CONTROLES TÉCNICOS DEL CICLO DE VIDA 18
7.7.1 CONTROLES DE DESARROLLO DE SISTEMAS 18
7.7.2 CONTROLES DE GESTIÓN DE SEGURIDAD 18
7.7.3 CONTROLES DE SEGURIDAD DEL CICLO DE VIDA 18
7.8 CONTROLES DE SEGURIDAD DE LA RED 19
7.9 SELLADO DE TIEMPO 19
7.10 GESTIÓN DE RIESGOS 19
7.11 GESTIÓN DE ACCESOS 19
7.12 DESARROLLO Y MANTENIMIENTO DE SISTEMAS CONFIABLES 20
7.13 ADMINISTRACIÓN DE LOS SERVICIOS DE SELLADO DE TIEMPO 20
7.14 RECUPERACIÓN EN CASO DE COMPROMISO DE LOS SERVICIOS DE LA TSU 20
7.15 SEGUIMIENTO Y MONITOREO 20
7.16 ADMINISTRACIÓN DE INCIDENTES DE SEGURIDAD 21
8 OFICIAL DE SEGURIDAD Y PRIVACIDAD 21
9 CONFORMIDAD CON LA LEY APLICABLE 21
10 BIBLIOGRAFÍA 21

1 INFORMACIÓN DEL DOCUMENTO

1.1. NOMBRE Y RESPONSABLE

Nombre del documento	Política y Plan de Seguridad de Información TSA 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	Febrero 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 a Prestador de Servicios de Valor Añadido como Autoridad de Sellado de Tiempo, en el marco del cumplimiento de los requerimientos de la “Guía de Acreditación de Prestadores de Servicios de Valor Añadido (SVA)” establecida por el INDECOPI.

4 OBJETO DE LA ACREDITACIÓN

El alcance de la acreditación cubre la infraestructura y procesos de los servicios de sellos de tiempo brindados por BPO como Prestadores de Servicios de Valor Añadido como Autoridad de Sellado de Tiempo 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 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 HAS
CA	Certification Authority (Autoridad de Certificación)
DSCF	Dispositivo seguro de creación de firma
FIPS	Federal Information Processing Standards(Estánda 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 Política y Declaración de Prácticas SVA 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 Política y Declaración de Prácticas SVA 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 POLÍTICA DE SEGURIDAD

Es compromiso de la dirección de la TSA de BPO, el garantizar la autenticidad e integridad de los servicios de sellado de tiempo que proporciona, mediante la gestión de riesgos de seguridad y la aplicación de políticas y estándares que regulen las actividades críticas de las operaciones de sellado de tiempo, por parte del personal y terceros subcontratados, en cumplimiento de las obligaciones de la TSU, en los ámbitos legales, regulatorios y contractuales.

7 PLAN DE SEGURIDAD

7.1 CONTROLES FÍSICOS

El acceso físico a BPO dispone de un esquema de control de acceso. Asimismo, el acceso físico a los sistemas del servicio de valor añadido 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.

7.1.1 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.

7.1.2 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.

7.1.3 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.

7.1.4 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.

7.1.5 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.

7.2 CONTROLES DE PROCEDIMIENTO

7.2.1 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

7.2.2 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.

7.2.3 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.

7.2.4 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

7.3 GESTIÓN DE ACTIVOS

El servicio de administración de infraestructura de BPO protege sus activos, de acuerdo a la clasificación y controles especificados por el Oficial de Seguridad y Privacidad de la TSA.

Todos los activos que sean relevantes para garantizar la correcta operación y autenticidad de los servicios de sellado de tiempo brindados por la TSU de BPO son identificados, clasificados e inventariados de acuerdo a su relevancia.

7.4 CONTROLES DE PERSONAL

7.4.1 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

7.4.2 PROCEDIMIENTO DE COMPROBACIÓN DE ANTECEDENTES

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

7.4.3 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.

7.4.4 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.

7.4.5 FRECUENCIA Y SECUENCIA DE ROTACIÓN DE TAREAS

No está estipulado.

7.4.6 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.

7.4.7 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.

7.4.8 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.

7.5 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.

7.5.1 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.

7.5.2 PERIODO DE RETENCIÓN DE LOS REGISTROS DE AUDITORÍA

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

7.5.3 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.

7.5.4 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.

7.5.5 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.

7.5.6 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.

7.5 ARCHIVO DE REGISTROS

7.5.1 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.

7.5.2 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.

7.5.3 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.

7.5.4 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.

7.5.5 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.

7.5.6 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.

7.5.7 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.

7.6 GESTIÓN DE OPERACIONES

Los sistemas de bases de datos que se interconectan a los servidores de sellado de tiempo son protegidos mediante los siguientes controles:

- Todos los servidores tienen protección antivirus
- La instalación y desinstalaciones de aplicaciones de software es controlada
- Se elimina de manera segura la información sensible antes de que los equipos de la TSU sean desechados.
- Se monitorean las demandas de capacidad de memoria, procesamiento y almacenamiento

Implementar medidas para que los componentes sean operados de manera segura y correcta, con mínimos riesgos de falla:

- La operación de los roles críticos de confianza y administrativos que impactan en la entrega de los servicios de sellado de tiempo están documentados y establecidos, y son mejorados de acuerdo a las evaluaciones de riesgo.
- Las operaciones de administración de la TSU deberán son separadas de otras operaciones, como la administración de infraestructura

- Las operaciones de administración de la TSU deben son gestionadas por personal de confianza

7.7 CONTROLES TÉCNICOS DEL CICLO DE VIDA

7.7.1 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.

7.7.2 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

7.7.3 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.

7.8 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.

7.9 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”.

7.10 GESTIÓN DE RIESGOS

El alcance de las medidas de seguridad de la información adoptadas por BPO para la protección de los servicios que brinda su TSU ha sido determinado en función de los resultados de evaluaciones de seguridad periódicas. Mediante la evaluación de riesgos se identifican las potenciales amenazas relacionadas a los servicios de sellado de tiempo y los controles requeridos para impedir o limitar los efectos de estas amenazas.

Se realizan análisis de riesgos anuales a fin de mantener el control de los riesgos.

7.11 GESTIÓN DE ACCESOS

Los accesos a los sistemas de la TSU son restringidos mediante controles de seguridad perimetral de redes:

- Se utilizan firewalls configurados para prevenir todos los protocolos y accesos no autorizados para la operación de la TSU
- Se utilizan sistemas IPS para inspeccionar y bloquear el ingreso de código malicioso
- Se monitorean los equipos de comunicaciones

Se gestionan las cuentas de usuario, respecto de la generación, modificación periódica o remoción de acceso.

Los accesos a la administración de los sistemas de sellado de tiempo son asignados al personal de confianza y son retirados o modificados cuando el personal se retira de la entidad de manera definitiva o temporalmente.

Los sellos de tiempo emitidos son registrados, así como las transacciones principales de gestión de las claves. Estos registros serán auditados durante los procesos anuales de auditoría interna.

Las funciones de administración y protección de logs son separadas de las de monitoreo.

7.12 DESARROLLO Y MANTENIMIENTO DE SISTEMAS CONFIABLES

No se brindan servicios de desarrollo.

7.13 ADMINISTRACIÓN DE LOS SERVICIOS DE SELLADO DE TIEMPO

Los responsables de las operaciones de la TSU deberán asegurar que en el caso de eventos que puedan afectar la seguridad de los servicios de sellado de tiempo, incluyendo compromisos de la clave de la TSU o pérdidas detectadas de calibración, la información relevante sea comunicada a los suscriptores y terceros que confían.

7.14 RECUPERACIÓN EN CASO DE COMPROMISO DE LOS SERVICIOS DE LA TSU

El plan de recuperación de desastres deberá considerar los casos de compromiso o sospecha de compromiso de la clave privada de la TSU o pérdida de calibración del reloj, que puede afectar los sellos de tiempo emitidos.

En el caso de compromiso, o sospecha de compromiso o pérdida de calibración, se deberá comunicar a todos los suscriptores y terceros que confían una descripción del hecho ocurrido.

En el caso de compromiso, o sospecha de compromiso o pérdida de calibración, no se deberán emitir sellos de tiempo hasta que se hayan tomado las medidas de recuperación.

En el caso de compromiso, o sospecha de compromiso o pérdida de calibración, se debe poner a disposición de los suscriptores y terceros que confían la información que permita identificar los sellos de tiempo afectados, a menos que esto viole la privacidad de los usuarios o la seguridad de los servicios de la TSU.

7.15 SEGUIMIENTO Y MONITOREO

- Se realiza monitoreo del funcionamiento de los servidores de sellado de tiempo y de los servidores de tiempo.
- Los eventos y datos específicos de la generación de los sellos de tiempo y de la gestión del certificado de la TSU y las claves privadas serán registrados
- Se deberá proteger la confidencialidad e integridad de los registros concernientes a la operación de los servicios de sellado de tiempo, durante todo su ciclo de vida
- Los registros concernientes a la operación de los servicios de sellado de tiempo deberán estar disponibles si son requeridos para propósitos de proveer evidencia de la operación correcta de los servicios de sellado de tiempo para propósitos de procesos legales.
- Los registros concernientes a los servicios de sellado de tiempo deberán ser protegidos y almacenados por un periodo de tiempo de un año después de la expiración de la validez del certificado digital de la TSU para proveer la evidencia legal necesaria.
- Se deben registrar los eventos relacionados a la sincronización de los relojes de los TSU, incluyendo la información de la re-calibración o sincronización de relojes
- Se deben registrar los eventos relacionados para detectar la pérdida de la sincronización del reloj de los TSU

7.16 ADMINISTRACIÓN DE INCIDENTES DE SEGURIDAD

Se gestionan los incidentes relacionados a la administración de los controles de acceso físico, la provisión del suministro de energía, los controles ambientales y los de seguridad perimetral de redes y comunicaciones.

Los eventos que puedan alterar el correcto funcionamiento de los servicios de sellado de tiempo respecto de los niveles de disponibilidad establecidos y de los requerimientos de autenticidad de los clientes a los que se debe brindar el servicio, así como a la integridad de las configuraciones de los sistemas y de la información que procesan estos servicios, deben ser detectados y reportados por canales de comunicación eficientes que permitan la reacción oportuna, de acuerdo a una clasificación establecida según el impacto de los incidentes sobre los servicios y a la complejidad de su solución (estimación en latencia). Estos incidentes deben ser escalados hasta su solución tomando registro de los eventos y de las soluciones de los mismos en una base centralizada de conocimiento que permita la pronta solución de eventos similares. El problema fuente de los incidentes recurrentes debe ser investigado a fin de encontrar su solución definitiva.

8 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.

9 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 de valor añadido emitidos bajo las directrices definidas en el presente documento.

10 BIBLIOGRAFÍA

1 Guía de Acreditación para Entidades de Certificación Digital EC, INDECOPI
2 Ley de Firmas y Certificados Digitales – Ley 27269
3 Decreto Supremo 052-2008
4 Decreto Supremo 070-2011
5 Decreto Supremo 105-2012