BIT4ID SAC

DECLARACIÓN DE PRÁCTICAS DE VALOR AÑADIDO (DPSVA)

Información general

Control del Documento

Clasificación de seguridad:	**Público**
Versión:	**1.1**
Fecha edición:	**25/06/2022**
Fichero / código:	**BIT4IDSAC_DPSVA_v1.1**
Formato:	**Office**

Estado formal

Preparado por:	Revisado por:	Aprobado por:
Nombre: Alejandro Grande Fecha: 25/06/2022	Nombre: Alejandro Grande Fecha: 01/07/2022	Nombre: Jorge García Fecha: 06/07/2022

Antecedentes del Documento

Versión	Partes que cambian	Descripción del cambio	Autor del cambio	Fecha del cambio
1.0	Original	Creación del documento	AGB/ABD/JGA	02/11/2021
1.1	1.2.2	Contacto	AGB	25/06/2022

Índice

Información general 2
Control del Documento 2
Estado formal 2
Antecedentes del Documento 3
Índice 4
1. Gestión del documento 8
1.1. Introducción 8
1.2. Administración del documento y conformidad 8
1.2.1. Organización que administra el documento y conformidad 8
1.2.2. Contacto 8
1.2.3. Procedimiento de aprobación 9
1.3. Publicación y Registro 9
1.3.1. Publicación de la información sobre certificación 9
1.3.2. Frecuencia de la Publicación 9
1.3.3. Controles de acceso a los registros 9
2. Aplicación del documento 11
2.1. Participantes 11
2.1.1. Autoridad de Sellado de Tiempo 11
2.1.2. Suscriptor 11
2.1.3. Tercero que confía 11
2.1.4. Otros participantes 11
2.2. Aplicabilidad 11
3. Autoridad de Sellado de Tiempo 13
3.1. Responsabilidades 13
3.1.1. Responsabilidades y obligaciones de la TSA. 13
3.1.2. Responsabilidades y obligaciones del suscriptor 13
3.1.3. Responsabilidades de los terceros que confían. 13
3.1.4. Limitaciones de responsabilidad. 14
3.2. Gestión del ciclo de vida de las claves 15
3.2.1. Generación de las claves de TSA. 15
3.2.2. Protección de la clave privada y registro de eventos de la TSU 16

3.2.3. Distribución de la clave pública TSU 16
3.2.4. Término del ciclo de vida de la clave privada del TSU 16
3.3. Gestión del ciclo de vida del módulo criptográfica 16
3.4. Sello de tiempo 17
3.4.1. Tipo y finalidad del certificado de TSA 18
3.4.2. Contenido del sello de tiempo 18
3.4.3. Validación de los certificados de la TSU 19
3.5. Sincronización del reloj 19
4. Gestión de la seguridad y de las operaciones 20
4.1. Gestión de la seguridad 20
4.2. Controles de seguridad física 20
4.2.1. Localización y construcción de las instalaciones 21
4.2.2. Acceso físico 21
4.2.3. Electricidad y aire acondicionado 22
4.2.4. Exposición al agua 22
4.2.5. Prevención y protección de incendios 22
4.2.6. Almacenamiento de soportes 22
4.2.7. Tratamiento de residuos 22
4.2.8. Copia de respaldo fuera de las instalaciones 23
4.3. Controles de procedimientos 23
4.3.1. Funciones fiables 23
4.3.2. Identificación y autenticación para cada función 23
4.4. Controles de personal 23
4.4.1. Requisitos de historial, calificaciones, experiencia y autorización 24
4.4.2. Procedimientos de investigación de historial 24
4.4.3. Requisitos de formación 25
4.4.4. Requisitos y frecuencia de actualización formativa 25
4.4.5. Secuencia y frecuencia de rotación laboral 25
4.4.6. Sanciones para acciones no autorizadas 25
4.4.7. Requisitos de contratación de profesionales 26
4.4.8. Suministro de documentación al personal 26
4.5. Procedimientos de auditoría de seguridad 26
4.5.1. Tipos de eventos registrados 26

4.5.2. Frecuencia de tratamiento de registros de auditoría 27
4.5.3. Período de conservación de registros de auditoría 28
4.5.4. Protección de los registros de auditoría 28
4.5.5. Procedimientos de copia de respaldo 28
4.5.6. Localización del sistema de acumulación de registros de auditoría 29
4.5.7. Notificación del evento de auditoría al causante del evento 29
4.5.8. Análisis de vulnerabilidades 29
4.6. Archivos de informaciones 29
4.6.1. Período de conservación de registros 29
4.6.2. Protección del archivo 30
4.6.3. Procedimientos de copia de respaldo 30
4.6.4. Requisitos de sellado de fecha y hora 30
4.6.5. Localización del sistema de archivo 30
4.6.6. Procedimientos de obtención y verificación de información de archivo 30
4.7. Compromiso de claves y recuperación de desastre 30
4.7.1. Procedimientos de gestión de incidencias y compromisos 31
4.7.2. Corrupción de recursos, aplicaciones o datos 31
4.7.3. Compromiso de la clave privada de la entidad 31
4.8. Terminación del servicio 31
4.8.1. Término de la organización o servicio que administra la TSA 31
4.8.2. Compromiso de los servicios de sellado de tiempo 32
4.9. Controles de seguridad informática 32
4.9.1. Requisitos técnicos específicos de seguridad informática 33
4.9.2. Evaluación del nivel de seguridad informática 33
4.10. Controles técnicos del ciclo de vida 33
4.10.1. Controles de desarrollo de sistemas 34
4.10.2. Controles de gestión de seguridad 34
4.11. Controles de seguridad de red 36
4.12. Fuentes de Tiempo 36
5. Auditoría 37
5.1. Frecuencia y circunstancias de la evaluación 37
5.2. Identidad/Calificaciones de asesores 37
5.3. Relación del auditor con la entidad auditada 37

5.4. Elementos cubiertos por la evaluación 37
5.5. Publicación de Resultados 38
6. Registros y otros aspectos legales 39
6.1. Archivo de informaciones 39
6.2. Cumplimiento normativo 39
6.3. Responsabilidad financiera 39
6.4. Protección de datos personales 39
6.4.1. Acuerdo y notificación 40
ANEXO 1. Acrónimos 41

1. Gestión del documento

1.1. Introducción

Bit4id, S.A.C., en lo sucesivo "BIT4ID" es una sociedad mercantil registrada en el Perú especializada en el desarrollo de sistemas para la gestión de la identidad digital y la firma electrónica, y que presta servicios de Sellado de Tiempo, mediante la explotación de la infraestructura de llave pública (PKI) de Uanataca, S.A., empresa registrada de acuerdo a la legislación española, que tiene por objeto la Prestación de Servicios de Confianza Cualificados conforme a las previsiones del Reglamento Europeo No. 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE (Reglamento eIDAS).

La PKI de Uanataca, S.A., se somete a auditorías anuales para la evaluación de la conformidad de prestadores cualificados de servicios de confianza de acuerdo a la normativa aplicable, bajo las normas ISO/IEC 17065:2012, ETSI EN 319 403 V2.2.2., ETSI EN 319 421 v1.1.1, ETSI EN 319 401 v2.1.1, ETSI EN 319 411-2 v 2.1.1, ETSI EN 319 411-1 v 1.1.1., ETSI EN 319 401 v2.1.1, ETSI EN 319 411-2 v 2.1.1 ETSI EN 319 411-1 v 1.1.1, ETSI EN 319 401 v2.1.1.

1.2. Administración del documento y conformidad

1.2.1. Organización que administra el documento y conformidad

La presente Declaración de Prácticas de Valor Añadido (DPSVA) es administrada por BIT4ID. Se deja constancia que cada nueva versión o actualización de este documento se presentará a la Autoridad Administrativa Competente INDECOPI previa a su implementación, y luego de su aprobación, será publicada en el sitio web http://web.uanataca.com/pe/.

1.2.2. Contacto

La persona responsable de la administración de los Servicios de Valor añadido en modalidad de Autoridad de Sellado de Tiempo de BIT4ID como Autoridad de Sellado de Tiempo es Jorge García Aliaga, con quien se puede establecer contacto a través del correo electrónico info.pe@BIT4ID.com, e igualmente a través del teléfono 242 9994. Asimismo para cualquier consulta, pueden dirigirse a:

- Nombre: Bit4id S.A.C
- Dirección: Calle Enrique Palacios N° 360 – Oficina 510

- Miraflores
- 15074 – Lima
- Correo electrónico: info.pe@uanataca.com
- Página web: https://web.uanataca.com/pe/
- Tel: +(51) 1 242 9994

1.2.3. Procedimiento de aprobación

El presente documento se aprueba a través del procedimiento previsto para tal fin de acuerdo a las políticas de BIT4ID, bajo la autoridad del responsable de los servicios de sellado de tiempo identificado en este documento.

1.3. Publicación y Registro

1.3.1. Publicación de la información sobre certificación

BIT4ID pública a través de su sitio web http://www.uanataca.com/pe/ toda la documentación correspondiente a su Declaración de Prácticas de Valor Añadido y cualquier otra documentación relevante en relación a sus servicios como Autoridad de Sellado de Tiempo. BIT4ID mantiene igualmente publicada en el sitio web indicado, todas las versiones anteriores a las actualmente vigentes de la documentación relevante sobre los servicios prestados como Autoridad de Sellado de Tiempo, haciéndolas disponibles a cualquier persona o institución interesada en todo momento. Se publica el certificado (siempre que el suscriptor lo autorice en el contrato del suscriptor) e información de estado de certificados, así como de información en relación a la revocación de un certificado sin revelar la razón de dicha revocación.

1.3.2. Frecuencia de la Publicación

La documentación relativa a la Declaración de Prácticas de Valor Añadido en la modalidad de Autoridad de Sellado de Tiempo de BIT4ID, se publicarán en el día hábil siguiente a su aprobación previo cumplimiento de la notificación respectiva a la AAC. Con igual diligencia se publicarán las eventuales actualizaciones a la documentación que sean aprobadas en el futuro.

1.3.3. Controles de acceso a los registros

BIT4ID no limita el acceso de lectura a las informaciones establecidas anteriormente, pero establece controles para impedir que personas no autorizadas puedan añadir, modificar o borrar registros del mismo, para proteger la integridad

y autenticidad de la información, especialmente la información de estado de revocación.

BIT4ID emplea sistemas fiables, de modo tal que:

- Únicamente personas autorizadas puedan hacer anotaciones y modificaciones.
- Pueda comprobarse la autenticidad de la información.
- Pueda detectarse cualquier cambio técnico que afecte a los requisitos de seguridad.

2. Aplicación del documento

2.1. Participantes

2.1.1. Autoridad de Sellado de Tiempo

BIT4ID se constituye como Prestador de Servicios de Valor Añadido en la modalidad de Autoridad de Sellado del Tiempo y gestionando dichos servicios, los cuales se prestan a través de la infraestructura de llave pública instalada para este propósito.

2.1.2. Suscriptor

De acuerdo a esta declaración el suscriptor se configura como la comunidad de usuarios, personales naturales o jurídicas, que requieren y/o utilizan los servicios provistos por el Prestador de Servicios de Valor Añadido de Sellado de Tiempo y a su vez, aceptan los acuerdos y obligaciones que se describen en el presente documento así como de las políticas inherentes al servicio de sellado de tiempo.

2.1.3. Tercero que confía

Los terceros que confían son personas naturales o jurídicas que confían en el contenido y la aplicación de los sellos de tiempo emitidos en los términos y condiciones previsto en esta declaración de prácticas.

2.1.4. Otros participantes

BIT4ID declara que en la prestación de sus servicios de valor añadido como Autoridad de Sellado de Tiempo, en forma auxiliar o subsidiaria puede pactar, contratar y utilizar servicios de terceros para la ejecución parcial o total de una o varias actividades.

BIT4ID en la contratación de estos servicios a terceros observará apego a Declaración de Prácticas de Valor Añadido, así como de toda aquella documentación relevante y necesaria, y así lo dejará constar expresamente en los acuerdos y contratos que suscriba a tal efecto.

2.2. Aplicabilidad

Los sellos de tiempo limitan su uso en las aplicaciones y/o sistemas de los Suscriptores (personas naturales o jurídicas) que han contratado estos servicios.

No se utilizarán los sellos de tiempo para fines distintos de los especificados anteriormente.

3. Autoridad de Sellado de Tiempo

3.1. Responsabilidades

3.1.1. Responsabilidades y obligaciones de la TSA.

En relación a la prestación del servicio de sellado de tiempo electrónico BIT4ID se obliga a:

a) Emitir, entregar y administrar los sellos, de acuerdo con las instrucciones suministradas por el suscriptor, en los casos y por los motivos descritos en la DPSVA de BIT4ID.
b) Ejecutar los servicios con los medios técnicos y materiales adecuados, y con personal que cumpla las condiciones de cualificación y experiencia establecidas en la DPSVA y cuantos documentos se deriven de la naturaleza de la prestación.
c) Cumplir los niveles de calidad del servicio, en conformidad con lo que se establece en la DPSVA, en los aspectos técnicos, operativos y de seguridad.

3.1.2. Responsabilidades y obligaciones del suscriptor.

El suscriptor se obliga a:

- Realizar las solicitudes de sellos de tiempo de acuerdo con el procedimiento y, si es necesario, los componentes técnicos suministrados por BIT4ID, de conformidad con lo que se establece en la Declaración de Prácticas de Valor Añadido y en la documentación de BIT4ID.
- Seguir las indicaciones especificadas de las políticas inherentes al servicio de sellado de tiempo de UANTACA.
- Verificar las firmas digitales de los sellos de tiempos electrónicos, incluyendo la validez del certificado usado.
- Usar los sellos de tiempo electrónicos dentro de los límites y el ámbito descritos en este documento.

3.1.3. Responsabilidades de los terceros que confían.

3.1.3.1. Verificación de la firma digital correspondiente al sello de tiempo electrónico

Los terceros que confían tienen la obligación y responsabilidad de verificar el sello de tiempo, para lo cual deberá verificar el estatus del certificado con el que se haya emitido. La comprobación será ejecutada a través del software idóneo para tal verificación bajo la responsabilidad del tercero y, en todo caso, de acuerdo con la DPSVA y cuando documentos se deriven de ésta.

3.1.3.2. Confianza en una firma digital no verificada correspondiente a un sello de tiempo electrónico

Si el tercero confía en una firma digital correspondiente a un sello de tiempo electrónico no verificado, asumirá todos los riesgos derivados de esta actuación. En todo caso el tercero que confía deberá tomar en cuenta las limitaciones en el uso contenidas en este documento y otros documentos relevantes que pueden ser encontrados en www.uanataca.com/pe.

3.1.3.3. Efecto de la verificación

En virtud de la correcta verificación de los certificados de sello de tiempo electrónico, de conformidad con este documento, el tercero puede confiar en la información suministrada.

3.1.3.4. Uso correcto y actividades prohibidas

El tercero que confía se obliga a no utilizar ningún tipo de información de estado de los sellos de tiempo electrónico o de ningún otro tipo que haya sido suministrada por BIT4ID, en la realización de transacción alguna prohibida para la ley aplicable a la citada transacción.

El tercero se obliga a no inspeccionar, interferir o realizar ingeniería inversa de la implantación técnica de los servicios BIT4ID, sin previo consentimiento escrito.

Adicionalmente, el tercero se obliga a no comprometer la seguridad de los servicios de sellado de tiempo de BIT4ID.

Los servicios de valor añadido de sellado de tiempo prestados por BIT4ID no han sido diseñados ni permiten la utilización o reventa, como equipos de control de situaciones peligrosas o para usos que requieran actuaciones a prueba de errores, como la operación de instalaciones nucleares, sistemas de navegación o comunicación aérea, sistemas de control de tráfico aéreo, o sistemas de control de armamento, donde un error podría causar la muerte, daños físicos o daños medioambientales graves.

3.1.4. Limitaciones de responsabilidad.

3.1.4.1. Garantía de BIT4ID por los servicios de valor añadido de sellado de tiempo

BIT4ID garantiza al suscriptor que los sellos de tiempo cumplen con todos los requisitos materiales establecidos en la DPSVA, así como con la regulación peruana establecida por la Autoridad Administrativa Competente, el Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual (INDECOPI).

BIT4ID garantiza al tercero que confía en el sello de tiempo que la información contenida o incorporada por referencia en el sello es correcta, excepto cuando se indique lo contrario.

Adicionalmente, BIT4ID garantiza al suscriptor y al tercero que confía en el sello de tiempo la responsabilidad del Prestador de Servicios de Valor Añadido, con los límites que se establezcan, sin que en ningún caso BIT4ID responda por caso fortuito y en caso de fuerza mayor.

3.1.4.2. Exclusión de la garantía

BIT4ID rechaza toda otra garantía diferente a la anterior que no sea legalmente exigible.

3.1.4.3. Resolución de disputas

BIT4ID establece en el contrato de suscriptor los procedimientos de mediación y resolución de conflictos aplicables. En caso de discrepancia por parte de los suscriptores se intentará una resolución amistosa previa. Si no se llegase a un acuerdo al respecto, el conflicto se someterá a la jurisdicción civil, de conformidad con las normas de competencia aplicables.

3.2. Gestión del ciclo de vida de las claves

3.2.1. Generación de las claves de TSA.

El Prestador de Servicios de Valor Añadido asegurará que las claves criptográficas de TSA son generadas bajo un estricto control.

En particular:

- Las claves de TSA se generan en un ambiente de seguridad..
- La generación de las claves de TSA se generan dentro de un módulo criptográfico que reúna los requisitos FIPS 140-2 nivel 3.
- La generación de las claves de TSU se realiza de acuerdo a las previsiones del estándar ETSI EN 319 421 Policy and Security Requirements for Trust Service Providers issuing Time-Stamps.
- El procedimiento para la generación de las claves criptográficas se documenta.

3.2.2. Protección de la clave privada y registro de eventos de la TSU.

El Prestador de Servicios de Valor Añadido asegura que la clave privada para el sellado de tiempo permanece confidencial y mantiene su integridad. Específicamente la clave privada del sellado de tiempo se mantendrá en un dispositivo criptográfico que cumpla los requerimientos identificados en FIPS 140-2 level 3. Se registran todos los eventos para su análisis y acciones posteriores.

3.2.3. Distribución de la clave pública TSU.

El Prestador de Servicios de Valor Añadido asegura que en la distribución de las claves públicas se garantice su integridad y autenticidad. La clave pública de verificación se pondrá a disposición de los terceros que confían.

3.2.4. Término del ciclo de vida de la clave privada del TSU.

3.2.4.1. Cambio de claves de TSU

El periodo de validez de las claves de sellado de tiempo no será superior al periodo de tiempo que los algoritmos criptográficos elegidos sean adecuados para este uso.

3.2.4.2. Fin del ciclo de vida de la clave de TSA-TSU

El prestador de servicios de valor añadido garantizara que la clave privada de sellado de tiempo no será usada después del final de su ciclo de vida.

En particular:

- Que se utilizaran procedimientos técnicos y operacionales para generar nuevas claves cuando la actual caduca, de acuerdo a lo previsto en este documento.
- La clave privada de sellado de tiempo o cualquier parte de ella, es destruida completamente de tal forma que no pueda ser recuperada.

3.3. Gestión del ciclo de vida del módulo criptográfica

El Prestador de Servicios de Valor Añadido realiza los esfuerzos que razonablemente estén a su alcance para confirmar la seguridad del hardware criptográfico a lo largo de su ciclo de vida. En particular, que:

a) el hardware criptográfico usado para la firma de sellos de tiempo no se manipula durante su transporte ni durante el tiempo que está almacenado;

b) el uso del hardware criptográfico usado para la firma de sellos de tiempo requiere el uso de al menos dos empleados de confianza.
c) el hardware criptográfico usado para la firma de sellos de tiempo está funcionando correctamente y;
d) la clave privada de firma de la TSU almacenada en el hardware criptográfico se eliminará una vez se ha retirado el dispositivo.

Antes de que el uso de la clave privada de sellado de tiempo caduque se deberá realizar un cambio de claves. Los siguientes certificados serán puestos a disposición pública en el directorio:

- Clave pública de la nueva TSA firmada por la clave privada de la vieja TSA
- Clave pública de la vieja TSA firmada con la clave privada de la nueva TSA.

3.4. Sello de tiempo

El servicio de sellado de tiempo electrónico sigue las indicaciones de esta declaración de prácticas de valor añadido, así como las contenidas en el texto divulgativo del Certificado de Sello de tiempo con el OID 1.3.6.1.4.1.47286.2.2.5., publicada BIT4ID en su página web www.uanataca.com/pe.

El servicio suministrado por BIT4ID es conforme a la política Best Practices Policy for Time-Stamp (BTSP) definida en ETSI 319 421, identificado con el OID 0.4.0.2023.1.1.

itu-t(0) identified-organization(4) etsi(0) time-stamp-policy(2023) policy-identifiers(1) baseline-ts-policy (1)	0.4.0.2023.1.1.

Los clientes que reciben este servicio de sellado electrónico están obligados a cumplir con lo dispuesto por la normativa vigente, a respetar lo indicado en los respectivos acuerdos de servicios, verificar la corrección de la firma del sello de tiempo, la validez del certificado de la TSU, así como verificar que el hash del sello de tiempo coincide con el que se envió.

Los servicios de valor añadido de sellado de tiempo se regulan técnicamente y operativamente a través de la presente Declaración de Prácticas de Valor Añadido, por sus actualizaciones posteriores, así como por documentación complementaria.

La DPSVA y la documentación de operaciones se modifica periódicamente en el Registro y se puede consultar en la página de Internet: https://www.uanataca.com/pe.

3.4.1. Tipo y finalidad del certificado de TSA

Este certificado dispone del OID 1.3.6.1.4.1.47286.2.2.5. Es un certificado que se emite dentro de la Infraestructura Oficial de Firma Electrónica de acuerdo a la Ley de Firmas y Certificados Digitales y su Reglamento, para la firma de evidencias digitales de tiempo electrónico para la identificación y firma de entidades u organizaciones.

La información de usos en el perfil de certificado indica lo siguiente:

a) El campo "key usage" tiene activadas, y por tanto permite realizar, las siguientes funciones:
   a. Compromiso con el contenido (Content commitment, para realizar la función de firma digital)

b) En el campo "extKeyUsage" se dispone de forma activada de la indicación:
   a. "timeStamping" para realizar la función de sellado de tiempo electrónico.

El campo "User Notice" describe el uso de este certificado

3.4.2. Contenido del sello de tiempo

Cada sello de tiempo emitido por BIT4ID contiene toda la documentación que requiere la normativa, de manera orientativa pero no limitativa:

1. El número de serie del sello de tiempo.
2. El algoritmo de firma de sello de tiempo. En este caso el algoritmo utilizado es el RSA (SHA256rsa 1.2.840.113549.1.1.11).
3. El identificador del certificado relativo a la clave pública de la TSU.
4. La fecha y hora del sello de tiempo.
5. La exactitud de la fuente de tiempo en comparación con el UTC. En este caso es un de un segundo o mejor (punto 1.4.1 del presente documento).
6. El identificador del algoritmo de hash utilizado para generar la huella de la evidencia. Este caso el algoritmo usado es SHA-256 (hash seguro ALGORITM 256-bit OID: 2.16.840.1.101.3.4.2.1).
7. El valor de la huella de la evidencia informática.

8. El identificado del país en la cual la TSA es establecida.

3.4.3. Validación de los certificados de la TSU

La comprobación del estado de los certificados se realiza desde:

- Accesos al servicio de OCSP en:

  http://ocsp1.uanataca.com/public/pki/ocsp/

  http://ocsp2.uanataca.com/public/pki/ocsp/

- Descarga de las CRL desde el web https://www.uanataca.com/pe/

3.5. Sincronización del reloj

El servicio de Sellado de Tiempo de BIT4ID se basa en el uso del protocolo TSP sobre HTTP, definido en la norma RFC 3161 "*Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)".*

La fuente de tiempo se obtiene mediante un servidor NTP (INACAL)

La exactitud del servicio de sellado de tiempo de BIT4ID es de 1 segundo respecto a UTC.

Si el tiempo provisto se encuentra fuera de la exactitud de acuerdo lo definido en la sincronización del reloj, el sello de tiempo no se emitirá.

Se registran todos los eventos de sincronización los cuales son analizados y gestionados para mantener el servicio ofrecido con apoyo de la gestión de incidentes.

4. Gestión de la seguridad y de las operaciones

4.1. Gestión de la seguridad

El Prestador Servicios de Valor Añadido garantiza la implementación de medidas de seguridad para asegurar la información en sus operaciones, así como de la infraestructura que sostiene el servicio, para ello hace un análisis de todos los requerimientos de seguridad que luego pasan a la etapa de diseño, las pruebas, implementación y su constante monitoreo para gestionar los riesgos.

BIT4ID evalúa los riesgos periódicamente así como los controles implementados, que responden a dicha evaluación de riesgos y amenazas detectadas. En este sentido, ha establecido los siguientes controles para gestionar la seguridad y las operaciones.

Todos los procedimientos operativos del Prestador de Servicios de Valor Añadido, así como procedimientos de seguridad se encuentran documentados, de acuerdo con la Política de Seguridad de BIT4ID.

4.2. Controles de seguridad física

El Prestador Servicios de Valor Añadido a través de la infraestructura de llave pública presta sus servicios de valor añadido, la cual ha establecido controles de seguridad física y ambiental para proteger los recursos de las instalaciones donde se encuentran los propios sistemas y los equipamientos empleados para las operaciones para la prestación de los servicios electrónicos de confianza.

En concreto, la política de seguridad digital establece prescripciones sobre lo siguiente:

- Controles de acceso físico.
- Protección frente a desastres naturales.
- Medidas de protección frente a incendios.
- Fallo de los sistemas de apoyo (energía electrónica, telecomunicaciones, etc.)
- Derrumbamiento de la estructura.
- Inundaciones.
- Protección antirrobo.
- Salida no autorizada de equipamientos, informaciones, soportes y aplicaciones relativos a componentes empleados para los servicios del prestador de servicios de certificación.

Estas medidas resultan aplicables a las instalaciones desde donde se prestan los servicios, en sus entornos de producción y contingencia.

Las instalaciones cuentan con sistemas de mantenimiento preventivo y correctivo con asistencia 24h-365 días al año con asistencia en las 24 horas siguientes al aviso.

4.2.1. Localización y construcción de las instalaciones

La protección física se logra mediante la creación de perímetros de seguridad claramente definidos en torno a los servicios. La calidad y solidez de los materiales de construcción de las instalaciones garantiza unos adecuados niveles de protección frente a intrusiones por la fuerza bruta y ubicada en una zona de bajo riesgo de desastres y permite un rápido acceso.

La sala donde se realizan las operaciones en el Centro de Proceso de Datos cuenta con redundancia en sus infraestructuras, así como varias fuentes alternativas de electricidad y refrigeración en caso de emergencia.

Se dispone de instalaciones que protegen físicamente la prestación de los servicios de aprobación de solicitudes de certificados y de gestión de revocación, del compromiso causado por acceso no autorizado a los sistemas o a los datos, así como a la divulgación de los mismos.

4.2.2. Acceso físico

Se dispone de tres niveles de seguridad física (Entrada del Edificio donde se ubica el CPD, acceso a la sala del CPD y acceso al Rack) para la protección del servicio, debiendo accederse desde los niveles inferiores a los niveles superiores.

El acceso físico a las dependencias donde se llevan a cabo procesos está limitado y protegido mediante una combinación de medidas físicas y procedimentales. Así:

- Está limitado a personal expresamente autorizado, con identificación en el momento del acceso y registro del mismo, incluyendo filmación por circuito cerrado de televisión y su archivo.
- El acceso a las salas se realiza con lectores de tarjeta de identificación y gestionado por un sistema informático que mantiene un log de entradas y salidas automático.
- Para el acceso al rack donde se ubican los procesos del PSVA es necesario la autorización previa de BIT4ID a los administradores del servicio de hospedaje que disponen de la llave para abrir la jaula.

4.2.3. Electricidad y aire acondicionado

Las instalaciones disponen de equipos estabilizadores de corriente y un sistema de alimentación eléctrica de equipos duplicado con un grupo electrógeno.

Las salas que albergan equipos informáticos cuentan con sistemas de control de temperatura con equipos de aire acondicionado.

4.2.4. Exposición al agua

Las instalaciones están ubicadas en una zona de bajo riesgo de inundación.

Las salas donde se albergan equipos informáticos disponen de un sistema de detección de humedad.

4.2.5. Prevención y protección de incendios

Las instalaciones y activos cuentan con sistemas automáticos de detección y extinción de incendios.

4.2.6. Almacenamiento de soportes

Únicamente personal autorizado tiene acceso a los medios de almacenamiento.

La información de más alto nivel de clasificación se guarda en una caja de seguridad fuera de las instalaciones del Centro de Proceso de Datos.

4.2.7. Tratamiento de residuos

La eliminación de soportes, tanto papel como magnéticos, se realizan mediante mecanismos que garantizan la imposibilidad de recuperación de la información.

En el caso de soportes magnéticos, se desechan en cuyo caso se destruyen físicamente, o se reutilizan previo proceso de borrado permanente o formateo. En el caso de documentación en papel, mediante trituradoras o en papeleras dispuestas al efecto para posteriormente ser destruidos, bajo control.

4.2.8. Copia de respaldo fuera de las instalaciones

Se utiliza un almacén externo seguro para la custodia de documentos, dispositivos magnéticos y electrónicos que son independientes del centro de operaciones.

4.3. Controles de procedimientos

Se garantiza que los sistemas de la infraestructura tecnológica se operan de forma segura, para lo cual cuenta con procedimientos para las funciones que afectan a la provisión de sus servicios.

El personal encargado de la prestación del servicio ejecuta los procedimientos administrativos y de gestión de acuerdo con la política de seguridad.

4.3.1. Funciones fiables

Para la prestación de los servicios y administración de la infraestructura se han identificado, las siguientes funciones o roles con la condición de fiables, las cuales se encuentran detalladas en el apartado 5.2.1de la Declaración de Prácticas de Certificación de BIT4ID.

Las personas que ocupan los puestos anteriores se encuentran sometidas a procedimientos de investigación y control específicos. Adicionalmente, se han implementado criterios en sus políticas para la segregación de las funciones, como medida de prevención de actividades fraudulentas.

4.3.2. Identificación y autenticación para cada función

Las personas asignadas para cada rol son identificadas por el auditor interno que se asegurará que cada persona realiza las operaciones para las que está asignado.

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 usuario/contraseña, certificado digital, tarjeta de acceso físico y/o llaves.

4.4. Controles de personal

4.4.1. Requisitos de historial, calificaciones, experiencia y autorización

Todo el personal está cualificado y/o ha sido instruido convenientemente para realizar las operaciones que le han sido asignadas.

El personal en puestos de confianza no tiene intereses personales que entran en conflicto con el desarrollo de la función que tenga encomendada.

En general, se retirará de sus funciones de confianza a una persona, cuando se tenga conocimiento de la existencia de conflictos de interés y/o la comisión de algún hecho delictivo que pudiera afectar al desempeño de sus funciones.

No se asignará a un sitio confiable o de gestión a una persona que no sea idónea para el puesto, especialmente por una falta que afecte su capacidad para el mismo. Por este motivo, previamente se realiza una investigación en el marco de la legislación aplicable, relativa a los siguientes aspectos:

- Estudios, incluyendo titulación alegada.
- Trabajos anteriores, hasta cinco años, incluyendo referencias profesionales.
- Referencias profesionales.

4.4.2. Procedimientos de investigación de historial

Con carácter previo a la asignación de una persona o de que ésta acceda al puesto de trabajo, se realizan las siguientes comprobaciones:

- Referencias de los trabajos de los últimos años.
- Referencias profesionales.
- Estudios, incluyendo titulación alegada.

Dicha investigación se realiza siempre previo consentimiento inequívoco del afectado, y se procesa y protege todos sus datos personales de acuerdo con la normativa de Protección de Datos aplicable a cada caso.

Todas las comprobaciones se realizan hasta donde lo permite la legislación vigente aplicable. Los motivos que pueden dar lugar a rechazar al candidato a un puesto fiable son los siguientes:

- Falsedades en la solicitud de trabajo, realizadas por el candidato.
- Referencias profesionales muy negativas o muy poco fiables en relación con el candidato.

4.4.3. Requisitos de formación

El personal que ocupa puestos fiables y de gestión, recibe formación hasta que alcanzan la cualificación necesaria para el desempeño de sus funciones, manteniendo archivo de dicha formación.

Los programas de formación son revisados periódicamente, y son actualizados y mejorados de forma periódica.

La formación incluye, al menos, los siguientes contenidos:

- Principios y mecanismos de seguridad del PSVA, así como el entorno de usuario de la persona a formar.
- Tareas que debe realizar la persona.
- Políticas y procedimientos de seguridad correspondientes. Uso y operación de maquinaria y aplicaciones instaladas.
- Gestión y tramitación de incidentes y compromisos de seguridad.
- Procedimientos de continuidad de negocio y emergencia.
- Procedimiento de gestión y de seguridad en relación con el tratamiento de los datos de carácter personal.

4.4.4. Requisitos y frecuencia de actualización formativa

La formación del personal se actualiza de acuerdo con las necesidades, y con la frecuencia suficiente para cumplir sus funciones de forma competente y satisfactoria, especialmente cuando se realicen modificaciones sustanciales en las tareas de certificación.

4.4.5. Secuencia y frecuencia de rotación laboral

No aplicable.

4.4.6. Sanciones para acciones no autorizadas

Se dispone de un sistema sancionador, para depurar las responsabilidades derivadas de acciones no autorizadas, adecuado a la legislación laboral aplicable.

Las acciones disciplinarias incluyen la suspensión, separación de las funciones y hasta el despido de la persona responsable de la acción dañina, de forma proporcionada a la gravedad de la acción no autorizada.

4.4.7. Requisitos de contratación de profesionales

Los empleados contratados para realizar tareas confiables firman con anterioridad las cláusulas de confidencialidad y los requerimientos operacionales empleados para llevar a cabo la prestación de servicios de certificación correspondientes. Cualquier acción que comprometa la seguridad de los procesos aceptados podría, una vez evaluados, dar lugar al cese de la designación para el rol fiable.

En el caso de que todos o parte de los servicios sean operados por un tercero, los controles y previsiones realizadas en esta sección, o en otras partes de la DPVA, serán aplicados y cumplidos por el tercero que realice las funciones de operación de los servicios de certificación, no obstante, BIT4ID 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 un tercero.

4.4.8. Suministro de documentación al personal

Todo el personal recibirá la documentación que estrictamente precise en cada momento, al objeto de realizar su trabajo de forma competente y satisfactoria.

4.5. Procedimientos de auditoría de seguridad

4.5.1. Tipos de eventos registrados

Se producen y guardan registro, al menos, de los siguientes eventos relacionados con la seguridad de la entidad:

- Encendido y apagado del sistema.
- Intentos de creación, borrado, establecimiento de contraseñas o cambio de privilegios.
- Intentos de inicio y fin de sesión.
- Intentos de accesos no autorizados al sistema de la TSA a través de la red.
- Intentos de accesos no autorizados al sistema de archivos.
- Acceso físico a los logs.
- Cambios en la configuración y mantenimiento del sistema.
- Registros de las aplicaciones de la TSA.
- Encendido y apagado de la aplicación de la TSA.

- Cambios en los detalles de la TSA 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 éste.
- 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 suscriptor, en caso de certificados individuales, o de la persona natural identificada en el certificado, en caso de certificados de organización.
- Informes completos de los intentos de intrusión física en las infraestructuras que dan soporte a la emisión y gestión de certificados.

Las entradas del registro incluyen los siguientes elementos:

- Fecha y hora de la entrada.
- Número de serie o secuencia de la entrada, en los registros automáticos.
- Identidad de la entidad que entra el registro.
- Tipo de entrada.

4.5.2. Frecuencia de tratamiento de registros de auditoría

BIT4ID revisa sus logs cuando se produce una alerta del sistema motivada por la existencia de algún incidente.

El procesamiento de los registros de auditoría consiste en una revisión de los registros que incluye la verificación de que éstos no han sido manipulados, una breve inspección de todas las entradas de registro y una investigación más profunda de cualquier alerta o irregularidad en los registros. Las acciones realizadas a partir de la revisión de auditoría están documentadas.

Se mantiene un sistema que permite garantizar:

- Espacio suficiente para el almacenamiento de logs.
- Que los ficheros de logs no se reescriben.
- Que la información que se guarda incluye como mínimo: tipo de evento, fecha y hora, usuario que ejecuta el evento y resultado de la operación.
- Los ficheros de logs se guardarán en ficheros estructurados susceptibles de incorporar en una BBDD para su posterior exploración.

4.5.3. Período de conservación de registros de auditoría

BIT4ID almacena la información de los logs durante un periodo de entre 10 años.

4.5.4. Protección de los registros de auditoría

Los logs de los sistemas:

- Están protegidos de manipulación mediante la firma de los ficheros que los contienen.
- Son almacenados en dispositivos ignífugos.
- Se protege su disponibilidad mediante su almacenamiento en instalaciones externas al centro donde se ubica la EC.

El acceso a los ficheros de logs está reservado solo a las personas autorizadas. Asimismo, los dispositivos son manejados en todo momento por personal autorizado.

Existe un procedimiento interno donde se detallan los procesos de gestión de los dispositivos que contienen datos de logs de auditoría.

4.5.5. Procedimientos de copia de respaldo

BIT4ID dispone de un procedimiento adecuado de backup de manera que, en caso de pérdida o destrucción de archivos relevantes, estén disponibles en un periodo corto de tiempo las correspondientes copias de backup de los logs.

BIT4ID tiene implementado un procedimiento de backup seguro de los logs de auditoría, realizando semanalmente una copia de todos los logs en un medio externo. Adicionalmente se mantiene copia en centro de custodia externo.

4.5.6. Localización del sistema de acumulación de registros de auditoría

La información de la auditoria de eventos es recogida internamente y de forma automatizada por el sistema operativo, las comunicaciones de 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.

4.5.7. Notificación del evento de auditoría al causante del evento

Cuando el sistema de acumulación de registros de auditoría registre un evento, no es preciso enviar una notificación al individuo, organización, dispositivo o aplicación que causó el evento.

4.5.8. Análisis de vulnerabilidades

El análisis de vulnerabilidades queda cubierto por los procesos de auditoría.

Los análisis de vulnerabilidad deben ser ejecutados, repasadas y revisadas por medio de un examen de estos acontecimientos monitorizados. Estos análisis deben ser ejecutados periódicamente de acuerdo al procedimiento interno que previsto para este fin.

Los datos de auditoría de los sistemas son almacenados con el fin de ser utilizados en la investigación de cualquier incidencia y localizar vulnerabilidades.

4.6. Archivos de informaciones

BIT4ID garantiza que toda la información relativa a los servicios de TSA, se conserva durante un período de tiempo apropiado, según lo establecido en este documento.

4.6.1. Período de conservación de registros

Los registros especificados anteriormente se archivan durante al menos 10 años, o el período que establezca la legislación vigente.

4.6.2. Protección del archivo

El archivo se protege de forma que sólo personas debidamente autorizadas puedan obtener acceso al mismo. El archivo es protegido contra visualización, modificación, borrado o cualquier otra manipulación mediante su almacenamiento en un sistema fiable.

Asimismo se asegura la correcta protección de los archivos mediante la asignación de personal cualificado para su tratamiento y el almacenamiento en instalaciones seguras externas.

4.6.3. Procedimientos de copia de respaldo

Se 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 solo a personal autorizado.

Como mínimo se realizan copias de respaldo incrementales diarias de todos sus documentos electrónicos y copias de respaldo completas semanalmente para casos de recuperación de datos.

4.6.4. Requisitos de sellado de fecha y hora

Los registros están fechados con una fuente fiable vía NTP.

No es necesario que esta información se encuentre firmada digitalmente.

4.6.5. Localización del sistema de archivo

Se dispone de un sistema centralizado de recogida de información de la actividad de los equipos implicados en el servicio de gestión de certificados.

4.6.6. Procedimientos de obtención y verificación de información de archivo

Se dispone de un procedimiento donde se describe el proceso para verificar que la información archivada es correcta y accesible. Asimismo proporciona la información y medios de verificación al auditor.

4.7. Compromiso de claves y recuperación de desastre

4.7.1. Procedimientos de gestión de incidencias y compromisos

Se prevé políticas de seguridad y continuidad del negocio que le permiten la gestión y recuperación de los sistemas en caso de incidentes y compromiso de sus operaciones, asegurando los servicios críticos de revocación y publicación del estado de los certificados.

4.7.2. Corrupción de recursos, aplicaciones o datos

Cuando acontezca un evento de corrupción de recursos, aplicaciones o datos, se seguirán los procedimientos de gestión oportunos de acuerdo a las políticas de seguridad y gestión de incidentes de BIT4ID, que contemplan escalado, investigación y respuesta al incidente. Si resulta necesario, se iniciarán los procedimientos de compromiso de claves o de recuperación de desastres de BIT4ID y se dejara de emitir sello de tiempo, haciendo de conocimiento de todos los interesados.

4.7.3. Compromiso de la clave privada de la entidad

En caso de sospecha o conocimiento del compromiso, se activarán los procedimientos de compromiso de claves de acuerdo a las políticas de seguridad, gestión de incidencias y continuidad del negocio, que permita la recuperación de los sistemas críticos, si fuera necesario en un centro de datos alternativo.

4.8. Terminación del servicio

4.8.1. Término de la organización o servicio que administra la TSA

BIT4ID ante un eventual cese de actividad o del servicio contratado, ha establecido un plan de cese con el objetivo de minimizar los posibles perjuicios que pudieran producirse a terceros y suscriptores. Dicho plan prevé las siguientes medidas:

1. Publicación y notificación del cese de manera efectiva y con antelación suficiente a todos los suscriptores, usuarios, y en general a cualquier tercero con quien tenga algún tipo de acuerdo o relación.
2. Posibilidad de la transferencia de la actividad a otro Prestador siempre y cuando asegurando que se cumplen las condiciones legales exigidas.

3. Custodia y archivo para asegurar el mantenimiento continuo de los registros, conservando toda la documentación e información que un PSVA debe mantener.
4. Destrucción o inhabilitación de las claves privadas de la TSA.
5. Dotación de una provisión de fondos para continuar la finalización de las actividades requeridas para la terminación.
6. Reembolso de acuerdo a las cláusulas de contrato y a las políticas establecidas por BIT4ID.

4.8.2. Compromiso de los servicios de sellado de tiempo

BIT4ID asegura que ha establecido las medidas de seguridad adecuadas con el fin de evitar el compromiso de los servicios de sellado de tiempo. No obstante lo anterior, de acuerdo a la regulación operativa y técnica contenida en la Declaración de Prácticas de Certificación de Bit4id S.A.C. antes identificada, dispone de un plan de continuidad de negocio, para que en un eventual caso de desastre permita al negocio responder ante los incidentes e interrupciones del servicio, para ofrecer una operación continua de los procesos críticos para el negocio y poder así restablecer el servicio tan pronto como sea posible.

En caso de compromiso, acorde con el mencionado plan, el Prestador de Servicios de Valor Añadido adoptará las, entre otras, las siguientes medidas:

- Activación del Plan de Contingencia, establecimiento del equipo de planificación y gestión del proceso.
- Procedimientos de gestión y comunicación para el caso de compromiso del algoritmo, de la clave, etc.

4.9. Controles de seguridad informática

Se emplea sistemas fiables para ofrecer sus servicios. El Prestador de Servicios de Valor Añadido ha realizado controles y auditorias 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 aplica controles del esquema de certificación sobre sistemas de gestión de la información ISO 27001.

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

- Configuración de seguridad del sistema operativo.
- Configuración de seguridad de las aplicaciones.
- Dimensionamiento correcto del sistema.
- Configuración de Usuarios y permisos.
- Configuración de eventos de Log.
- Plan de backup y recuperación.
- Configuración antivirus.
- Requerimientos de tráfico de red.

4.9.1. Requisitos técnicos específicos de seguridad informática

Los requerimientos de seguridad son analizados para luego pasar a la etapa de diseño, implementación y monitoreo para asegurar su correcta implementación y uso. Cada servidor incluye las siguientes funcionalidades:

- Control de acceso a los servicios de las Autoridades de Certificación subordinadas 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 suscriptor, de las Autoridades de Certificación subordinadas y datos de auditoria.
- Auditoria de eventos relativos a la seguridad.
- Auto-diagnóstico de seguridad relacionado con los servicios de las Autoridades de Certificación subordinadas.
- Mecanismos de recuperación de claves y del sistema de las Autoridades de Certificación subordinadas.

Las funcionalidades expuestas son realizadas mediante una combinación de sistema operativo, software de PKI, protección física y procedimientos.

4.9.2. Evaluación del nivel de seguridad informática

Las aplicaciones de autoridad de certificación y de registro empleadas son fiables.

4.10. Controles técnicos del ciclo de vida

4.10.1. Controles de desarrollo de sistemas

Las aplicaciones son desarrolladas e implementadas por de acuerdo con estándares de desarrollo y control de cambios.

Las aplicaciones disponen de métodos para la verificación de la integridad y autenticidad, así como de la corrección de la versión a emplear.

4.10.2. Controles de gestión de seguridad

Se desarrollan las actividades precisas para la formación y concienciación en materia de seguridad de las personas encargadas de prestar los servicios. 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. En la realización de esta función dispone de un plan de formación anual.

Se exige mediante contrato, las medidas de seguridad equivalentes a cualquier proveedor externo implicado en las labores de servicios electrónicos de confianza.

4.10.2.1. Clasificación y gestión de información y bienes

Se mantiene un inventario de activos, documentación; y un procedimiento para asegurar la adecuada gestión de activos y de nuevos sistemas a fin de evitar incompatibilidades con otros sistemas y vulnerabilidades de seguridad.

La política de seguridad de información detalla los procedimientos de gestión de la información donde se clasifica según su nivel de confidencialidad.

Los documentos están catalogados en tres niveles: SIN CLASIFICAR, USO INTERNO y CONFIDENCIAL.

4.10.2.2. Gestión de operaciones

Se dispone de un adecuado procedimiento de gestión y respuesta de incidencias, mediante la implementación de un sistema de alertas y la generación de reportes periódicos.

En el documento de seguridad de se desarrolla en detalle el proceso de gestión de incidencias.

Se tiene documentado todo el procedimiento relativo a las funciones y responsabilidades del personal implicado en el control y manipulación de elementos contenidos en el proceso de certificación.

4.10.2.3. Tratamiento de los soportes y seguridad

Todos los soportes son tratados de forma segura de acuerdo con los requisitos de la clasificación de la información. Los soportes que contengan datos sensibles son destruidos de manera segura si no van a volver a ser requeridos.

a) Planificación del sistema
Se mantiene un registro de las capacidades de los equipos. Conjuntamente con la aplicación de control de recursos de cada sistema se puede prever un posible redimensionamiento.

b) Reportes de incidencias y respuesta
Se dispone de un procedimiento para el seguimiento de incidencias y su resolución donde se registran las respuestas y una evaluación económica que supone la resolución de la incidencia.

c) Procedimientos operacionales y responsabilidades
Se definen actividades, asignadas a personas con un rol de confianza, distintas de las personas encargadas de realizar las operaciones cotidianas que no tienen carácter de confidencialidad.

4.10.2.4. Gestión del sistema de acceso

Se realizan todos los esfuerzos que razonablemente están a su alcance para confirmar que el sistema de acceso está limitado a las personas autorizadas.

- Se dispone de controles basados en firewalls, antivirus e IDS en alta disponibilidad.
- Los datos sensibles son protegidos mediante técnicas criptográficas o controles de acceso con identificación fuerte.
- Se dispone de un procedimiento documentado de gestión de altas y bajas de usuarios y política de acceso detallado en su política de seguridad.
- Se dispone de procedimientos para asegurar que las operaciones se realizan respetando la política de roles.
- Cada persona tiene asociado un rol para realizar las operaciones.
- El personal es responsable de sus actos mediante el compromiso de confidencialidad firmado con la empresa.

4.11. Controles de seguridad de red

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

La información confidencial que se trasfiere por redes no seguras, se realiza de forma cifrada mediante uso de protocolos SSL o del sistema VPN con autenticación por doble factor.

4.12. Fuentes de Tiempo

BIT4ID tiene un procedimiento de sincronización de tiempo coordinado vía NTP, que accede al siguiente servicico:

- Sincronización vía NTP, con el Instituto Nacional de Calidad (INACAL).

5. Auditoría

BIT4ID se somete a auditorías de compatibilidad de acuerdo a las previsiones de esta DPSVA.

5.1. Frecuencia y circunstancias de la evaluación

La ER de BIT4ID se somete una vez al año a auditorías de conformidad respecto del marco de la IOFE y como consecuencia hay una revisión y actualización de la documentación.

5.2. Identidad/Calificaciones de asesores

El equipo de auditoría que evalúa la conformidad de sus operaciones cuenta con personas con experiencia significativa en tecnologías de la información, seguridad y tecnologías de PKI y criptográficas, aprobadas previamente por INDECOPI.

5.3. Relación del auditor con la entidad auditada

Los auditores o asesores son independientes de la organización de la ER de BIT4ID.

5.4. Elementos cubiertos por la evaluación

La auditoría deberá verificar en todo caso:

a) Auditoría de los registros.
b) Auditoría del archivo.
c) Auditoría de procedimientos y controles.

Todo ello con el fin de comprobar que los mismos se ajustan a los establecido en el presente documento y en general en cumplimiento de la regulación peruana establecida por la Autoridad Administrativa Competente, el Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual (INDECOPI).

5.5. Publicación de Resultados

Los resultados de las auditorías o evaluaciones de compatibilidad deben ser publicados como parte de la información de estado, la cual es publicada por INDECOPI.

6. Registros y otros aspectos legales

6.1. Archivo de informaciones

Toda la información relativa a la prestación de servicios de Sellado de Tiempo se conserva durante un período de tiempo apropiado de acuerdo a la política de registro de BIT4ID, la cual se encuentra detallada en la Declaración de Prácticas de Certificación de BIT4ID, SAC.

En este sentido, el PSVA archiva todos los registros referido al servicio y a los sellos de tiempo, serán mantenidos por un periodo de al menos 10 años, o bien el periodo que establezca la legislación vigente.

6.2. Cumplimiento normativo

BIT4ID en su condición de Prestador de Servicios de Valor Añadido cumple con los requisitos establecidos por el Reglamento y la Ley de Firmas y Certificados Digitales (Ley 27269) y con la regulación peruana establecida por la Autoridad Administrativa Competente, el Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual (INDECOPI).

6.3. Responsabilidad financiera

BIT4ID cuenta con suficientes garantías financieras que cubran las responsabilidades que se deriven de sus operaciones, en los términos y condiciones establecidos por la normativa de aplicación.

BIT4ID dispone de una garantía de cobertura de su responsabilidad civil suficiente, mediante un seguro de responsabilidad civil profesional, que mantiene de acuerdo a la normativa vigente aplicable.

6.4. Protección de datos personales

BIT4ID cumple con la normativa sobre protección de datos personales y con las medidas de seguridad que resulten pertinentes de acuerdo a la Ley Nº 29733 de Protección de Datos Personales y su Reglamento, así como de los requerimientos establecidos por la Autoridad Administrativa Competente, el Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual (INDECOPI).

No obstante lo anterior, BIT4ID en el desarrollo de la prestación de servicio de sellado de tiempo, no recogen datos personales de los usuarios (personas naturales), ya que de la propia naturaleza del servicio no se desprende ni implica el uso de firma digital por parte del usuario final.

6.4.1. Acuerdo y notificación

La invalidez de una cláusula no afectará al resto de los acuerdos, políticas, textos divulgativos aplicables a la regulación del servicios de sellado de tiempo.

Cualquier notificación con respecto a la presente política se realizará por medio del correo electrónico indicado en el apartado 1.2. de la misma.

ANEXO 1. Acrónimos

AAC	Autoridad Administrativa Competente
AC	Autoridad de Certificación
CA	Certification Authority. Autoridad de Certificación
CP	Certificate Policy. Políticas de Certificación
CPD	Centro de Procesacimiento de Datos.
CPS	Certification Practice Statement. Declaración de Prácticas de Certificación
CRL	Certificate Revocation List. Lista de certificados revocados
CSR	Certificate Signing Request. Petición de firma de certificado
DCCF	Dispositivo Cualificado de Creación de Firma
DES	Data Encryption Standard. Estándar de cifrado de datos
DN	Distinguished Name. Nombre distintivo dentro del certificado digital
DPSVA	Declaración de Prácticas de Valor Añadido
DSA	Digital Signature Algorithm. Estándar de algoritmo de firma
EC	Entidad de certificación
ER	Entidad de Registro o Verificación
ERC	Código de Revocación
FIPS	Federal Information Processing Standard Publication
HSM	Hardware Security Module. Módulo de Seguridad Hardware
IOFE	Infraestructura Oficial de Firma Electrónica
ISO	International Organization for Standardization. Organismo Internacional de Estandarización
LDAP	Lightweight Directory Access Protocol. Protocolo de acceso a directorios
LRC	Listas de revocación de certificados
NTP	Network Time Protocol (NTP
OCSP	On-line Certificate Status Protocol. Protocolo de acceso al estado de los certificados

OID	Object Identifier. Identificador de objeto
PA	Policy Authority. Autoridad de Políticas
PC	Política de Certificación
PDS	Policy Disclosure Statements. Textos de divulgación
PIN	Personal Identification Number. Número de identificación personal
PKI	Public Key Infrastructure. Infraestructura de llave pública
QSCD	Qualified Signature Creation Device. Dispositivo Cualificado de Creación de Firma
RA	Autoridad de Registro
ROA	Real Instituto y Observatorio de la Armada
RPS	Declaración de prácticas de registro o verificación
RSA	Rivest-Shimar-Adleman. Tipo de algoritmo de cifrado
RUC	Registro Único de Contribuyentes
SHA	Secure Hash Algorithm. Algoritmo seguro de Hash
SSL	Secure Sockets Layer
SVA	Servicios de Valor Añadido
TCP/IP	Transmission Control. Protocol/Internet Protocol
TSA	Autoridad de Sellado de Tiempo
TSU	Unidad de Sellado de Tiempo