POLÍTICA DE SEGURIDAD

Bit4id S.A.C. – Autoridad de Sellado de Tiempo

Información general

Control documental

Código	TSU-PS-02
Clasificación de seguridad:	Público
Versión:	1.2
Fecha edición:	04/07/2022
Nombre del documento:	BIT4IDSAC Política de Seguridad TSA_v1.2.docx
Formato:	Office

Estado formal

Preparado por:	Revisado por:	Aprobado por:
Nombre: Alejandro Grande Fecha: 04/07/2022	Nombre: Albert Borrás Fecha: 04/07/2022	Nombre: Jorge Garcia Fecha: 05/07/2022

Control de versiones

Versión	Partes que cambian	Descripción del cambio	Autor del cambio	Fecha del cambio
1.0	Original	Creación del documento	ABD	02/11/2021
1.1	5	Se incluye la recuperación de evidencias	AGB	19/11/2021
1.2	1.3.2	Contacto	AGB	04/07/2022

Índice

INFORMACIÓN GENERAL **2**

CONTROL DOCUMENTAL 2
ESTADO FORMAL 2
CONTROL DE VERSIONES 3

ÍNDICE **4**

1. ASPECTOS GENERALES **6**

1.1. PRESENTACIÓN 6
1.2. OBJETO 6
1.3. ADMINISTRACIÓN DEL DOCUMENTO Y CONFORMIDAD 6
1.3.1. Organización que administra el documento y conformidad *7*
1.3.2. Contacto *7*
1.3.3. Responsabilidad y Conformidad *7*
1.4. ÁMBITO DE APLICACIÓN 8

2. POLÍTICA DE SEGURIDAD **9**

2.1. CUMPLIMIENTO NORMATIVO 9
2.2. CONTROLES DE SEGURIDAD 10
2.2.1. Controles de seguridad *10*
2.2.2. Seguridad física y del entorno *11*
2.2.3. Controles de acceso a la información *11*
2.2.4. De otros entornos y ambientes *12*
2.2.4.1. Seguridad de los servidores de almacenamiento 12
2.2.4.2. Conexiones 12
2.2.4.3. Seguridad 12
2.2.4.4. Entorno controlado 12
2.2.4.5. Certificaciones 13
2.2.4.6. Potencia eléctrica 13
2.2.4.7. Climatización 13
2.2.4.8. Racks 13

3. CONTROLES EN LA GESTIÓN DE LA SEGURIDAD **14**

3.1. AUDITORIAS Y DETECCIÓN DE INTRUSIONES 14
3.2. DE LOS ACTIVOS 14
3.3. CONFIGURACIÓN 14

4. TRATAMIENTO DE LA INFORMACIÓN **15**

4.1. RESIDUOS Y EQUIPOS 15
4.2. CUSTODIA DE LA INFORMACIÓN 15
4.3. DE LA INFORMACIÓN SENSIBLE 16

5. RECUPERACIÓN DE EVIDENCIAS 17

5.1. OBJETIVO 17
5.2. DESCRIPCIÓN 17
5.3. ÁMBITO DE APLICACIÓN 17
5.4. RESPONSABILIDAD 17
5.5. PROCEDIMIENTO 18
5.5.1. Solicitudes 18
5.5.2. Registro de la solicitud 18
5.5.3. Recuperación de evidencias de la infraestructura 18
5.5.4. Recuperación de evidencias de los servicios de confianza 19
5.5.5. Entrega de las evidencias 19

6. OTRAS CONSIDERACIONES 20

6.1. REVISIÓN DEL DOCUMENTO 20

1. Aspectos generales

1.1. Presentación

Bit4id, S.A.C., en lo sucesivo "BIT4ID" es una sociedad mercantil registrada en Perú especializada en el desarrollo de sistemas para la gestión de la identidad digital y la firma electrónica, y que presta servicios de certificación, especialmente aquellos relacionados con la gestión del ciclo de vida de certificados digitales, 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. Objeto

Este documento contiene la Política de Seguridad que Bit4id implementa en la prestación de los servicios de valor añadido para el Sellado de tiempo.

1.3. Administración del documento y conformidad

1.3.1. Organización que administra el documento y conformidad

La presente política es administrada por Bit4id, S.A.C., y está basada en las medidas, planes y protocolos de seguridad adoptados por Uanataca, S.A., como responsable de la infraestructura de llave pública (PKI).

La autoridad para la aprobación de las modificaciones que se realicen a este documento, recae sobre la persona responsable de la administración de los servicios, cuyos y datos de contacto se identifican en el siguiente apartado. Igualmente sobre esta persona, recae la autoridad y responsabilidad de la implementación del contenido de esta política.

Se deja constancia de que cualquier modificación que se realice en el documento, se hará con sujeción a lo previsto a la normativa legal y guías de acreditación dictadas por la AAC que resulten aplicables. Se deja constancia de 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 web.uanataca.com/pe/.

1.3.2. Contacto

La persona responsable de la administración de este documento es Jorge García Aliaga, con quien se puede establecer contacto a través del correo electrónico info.pe@uanataca.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, 15074 – Lima
- Correo electrónico: info.pe@uanataca.com
- Página web: https://web.uanataca.com/pe/

1.3.3. Responsabilidad y Conformidad

El responsable será quien autorice los cambios sobre este documento, y de asegurar la implementación de las medidas que resulten pertinentes para su cumplimiento.

1.4. Ámbito de aplicación

La presente política de seguridad se aplicará a la ejecución de los servicios de Sellado de Tiempo que presta BIT4ID, en su condición de Prestador de Servicios de Valor añadido debidamente acreditada. En consecuencia, la misma será de cumplimiento obligatorio para todo el personal de BIT4ID y por cualquier tercero que intervenga o participe en la ejecución de las actividades relacionadas con la prestación de los servicios propios de la Autoridad de Sellado de Tiempo.

2. Política de seguridad

2.1. Cumplimiento normativo

BIT4ID garantiza el cumplimiento de los requisitos de seguridad que resultan pertinentes de acuerdo a la Ley Nº 27269, Ley de Firmas y Certificados Digitales y su Reglamento, así como de los requerimientos establecidos para las Entidades Prestadoras de Servicios de Valor Añadido por la Autoridad Administrativa Competente, el Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual (INDECOPI).

BIT4ID garantiza que la observancia de dichos requisitos de seguridad exigidos por la normativa, se lleva a cabo mediante el cumplimiento de los controles y requisitos de seguridad exigidos a los Prestadores de Servicios de Certificación, los cuales son evaluados por una entidad auditora independiente. Para ello, BIT4ID dispone de informes anuales que certifican el mantenimiento de la evaluación de conformidad y el cumplimiento de los controles exigidos por los estándares internacionales siguientes:

- *ETSI EN 319 411-2 v 2.1.1 Policy and security requirements for Trust Service Providers issuing certificates: Requirements for trust service providers issuing EU qualified certificates.*
- *ETSI EN 319 411-1 v 1.1.1 Policy and security requirements for Trust Service Providers issuing certificates: General requirements.*
- *ETSI EN 319 401 v2.1.1 General Policy Requirements for Trust Service Providers.*
- *ETSI EN 319 411-2 v 2.1.1 Policy and security requirements for Trust Service Providers issuing certificates: Requirements for trust service providers issuing EU qualified certificates.*
- *ETSI EN 319 411-1 v 1.1.1 Policy and security requirements for Trust Service Providers issuing certificates: General requirements.*
- *ETSI EN 319 401 v2.1.1 General Policy Requirements for Trust Service Providers.*
- ETSI EN 319 421 v1.1.1 Policy and Security Requirements for Trust Service Providers issuing Time-Stamps.
- ETSI EN 319 401 v2.1.1 General Policy Requirements for Trust Service Providers.

2.2. Controles de seguridad

De conformidad con lo anterior y con el fin de asegurar los más altos estándares de seguridad y protección, BIT4ID garantiza la implementación de medidas de seguridad para asegurar la información en sus operaciones, así como de la infraestructura que sostiene el servicio, las cuales se encuentran detalladas en los apartados 5 y 6 de la Declaración de Prácticas de Certificación de Bit4id, S.A.C como entidad de certificación, la cual se encuentra disponible en web.uanataca.com/pe/.

2.2.1. Controles de seguridad

Estas medidas resultan aplicables a las instalaciones donde se producen las operaciones vinculadas a la prestación de servicios de valor añadido bajo plena responsabilidad de BIT4ID ,que la presta desde sus instalaciones de alta seguridad, tanto principales como, en su caso, de operación en contingencia, que son debidamente auditadas de forma periódica.

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:

a) Controles de acceso;

b) Clasificación y tratamiento de la información;

c) Seguridad física y del entorno;

d) Aquellas orientadas a los usuarios finales, como:
   i. Uso aceptable de activos.
   ii. Política de pantallas y escritorios despejados.
   iii. Transferencia de información.
   iv. Teletrabajo y dispositivos móviles.
   v. Restricciones en la instalación y el uso del software.

e) Transferencia de información;

f) Copias de seguridad;

g) Protección frente a malware;

h) Gestión de vulnerabilidades técnicas;

i) Controles criptográficos;

j) Seguridad de las comunicaciones;

k) Política de privacidad y de protección de los datos personales; y,

l) Relaciones con los proveedores.

2.2.2. Seguridad física y del entorno

Los equipos y sistemas de la Infraestructura de Clave Pública de Uanataca, se alojarán en un rack/armario aislado físicamente de otras infraestructuras hospedadas en el Data Center.

El Centro de Datos de producción y alta disponibilidad se ubica en instalaciones seguras de un proveedor de servicios de hospedaje para procesamiento de datos.

2.2.3. Controles de acceso a la información

Los equipos informáticos al servicio de la PKI de BIT4ID, se encuentran protegidos con medidas de seguridad que impiden el libre acceso a la información allí contenida. Los documentos electrónicos y registros digitales relativos a las actividades críticas de certificación y registro, se encuentran protegidos contra posible destrucción, alteración de datos, incluyendo especialmente información confidencial y datos personales de los suscriptores y firmantes de los certificados digitales.

Adicionalmente, todo el personal que desarrolle funciones fiables, que le permita acceder a información sensible dentro de los sistemas de información, se autenticará en los sistemas mediante autenticación fuerte con certificado electrónico.

2.2.4. De otros entornos y ambientes

2.2.4.1. Seguridad de los servidores de almacenamiento

La información relacionada con los procesos de la PKI se guarda de manera segura y se dispone de servidores de respaldo con la finalidad de eliminar el riesgo asociado a una única ubicación. Se dispone de copia de respaldo de las claves privadas de la AC fuera de los centros de procesamiento de datos de la PKI en lugares cercanos a sus instalaciones.

2.2.4.2. Conexiones

- Operador neutro de comunicaciones.
- Interconexión entre clientes.
- 2 MMR con acceso al edificio independientes

2.2.4.3. Seguridad

Uanataca protege las infraestructuras físicas relativas a la PKI a través de:

- Vallas anti-trepamiento con sensor de movimientos automatizado y pilones anti alunizajes.
- Seguridad perimetral externa
- Control de acceso biométrico
- Circuito cerrado de CCTV con video análisis
- Sistema de Alarma perimetral
- Personal de seguridad 24x7
- Notificaciones a central receptora de alarmas externa

2.2.4.4. Entorno controlado

- Sistema de alarma y monitorización 24x7 centralizado
- Agente extintor.
- Sistema de detección temprana (VESDA)
- Soporte CSU 24x7

2.2.4.5. Certificaciones

Las instalaciones donde se encuentra alojada la infraestructura PKI de Uanataca, cuentan con las siguientes infraestructuras:

ISO/IEC 27001:2013

2.2.4.6. Potencia eléctrica

- Doble acometida de 2 MW. (Fase I) 4 MW (Fase II)
- Distribución eléctrica modular
- Líneas A+B por Rack protegidas con UPS y Generador en redundancia 2N

2.2.4.7. Climatización

- Pasillo frío confinado
- Pasillo caliente con recuperación del aire
- Free Cooling
- Sistemas de alta eficiencia N+1

2.2.4.8. Racks

- Tamaño: 600x1000x47u
- Potencia: de 16 hasta 64 Amperios por rack (monofásica o trifásica)

3. Controles en la gestión de la seguridad

3.1. Auditorias y Detección de Intrusiones

Se someten a los sistemas a auditorías periódicas en las formas, condiciones y alcance descrito en la Declaración de Prácticas de Certificación, con el fin de verificar su conformidad con el mismo.

Periódicamente se realizan pruebas de la seguridad del sistema en busca de vulnerabilidades basado en el sistema OpenVas, así como pruebas de intrusión para determinar las debilidades de la seguridad de acuerdo con la metodología OSSTM.

3.2. De los Activos

BIT4ID mantiene un inventario sobre los activos que componen la infraestructura, y demás equipos que pueden estar vinculados a las operaciones de los servicios de certificación. En este sentido, BIT4ID documenta la incorporación y desincorporación de cualquier elemento componente de la infraestructura de clave pública que sustenta la prestación de sus servicios de confianza.

3.3. Configuración

BIT4ID revisa periódicamente la configuración y condiciones de sus sistemas para detectar disparidades con sus políticas.

4. Tratamiento de la información

4.1. Residuos y equipos

BIT4ID realiza la eliminación de los soportes de la información en forma segura, asegurando que la información no puede ser recuperada.

En relación a los soportes en papel, BIT4ID utiliza maquinas trituradoras de papel para su posterior desecho, o alternativamente la utilización de papeleras donde la documetación de deposita previa inutilización manual para su posterior desecho controlado. En el caso de soportes magnéticos, es posible su reutilización siempre que hayan sido sometidos a un proceso de borrado permanente o formateo que verifique que la información que estaba allí contenida no puede ser recuperada. En el caso de que estos soportes formen parte de la infraestructura de clave pública a través de la que se prestan servicios electrónicos de confianza los procesos de borrado y manipulación deberán documentarse.

En el caso de que se optase por desechar o eliminar un soporte magnético de información, se procederá a través de su destrucción física a través de múltiples perforaciones, su incineración o inutilización a través de fuerza física, de acuerdo al caso de que se trate.

4.2. Custodia de la información

BIT4ID se asegura de custodiar y preservar los Logs de todos los sistemas de su infraestructura destinada a la prestación de sus servicios de certificación, por un mínimo de 10 años a partir de su generación.

Igualmente, BIT4ID custodia la información relativa al ciclo de vida de los certificados y los suscriptores/firmantes por un período de al menos 15 años o el que establezca la legislación vigente desde su cambio de estado.

4.3. De la información sensible

BIT4ID dispone de una política y un plan de privacidad por el que da cumplimiento a la normativa vigente en concepto de protección de la privacidad de la información, en concreto a las obligaciones que derivan del decreto supremo n° 004-2007-PCM y de la norma marco sobre privacidad APEC.

5. Recuperación de evidencias

5.1. Objetivo

Describir el procedimiento para la recuperación de evidencias, registros y logs relativos a la prestación de servicios de confianza.

5.2. Descripción

Se recogen los procedimientos necesarios para la solicitud, gestión y obtención de las evidencias referentes al Sistema de Gestión de la Seguridad de la Información, así como de la infraestructura de BIT4ID.

En concreto determina todo el circuito de gestión de peticiones, de la tipología de sujetos solicitantes, así como las distintas posibilidades de solicitud y el procedimiento técnico de recuperación de evidencias, atendiendo además a las posibles excepciones que puedan aplicarse como consecuencia del procedimiento.

5.3. Ámbito de aplicación

El presente procedimiento tiene como alcance todos los servicios de confianza ofrecidos por BIT4ID, así como el sistema de seguridad de la información que los sustenta.

5.4. Responsabilidad

Se identifican las siguientes responsabilidades en la aplicación de este procedimiento:

- Responsable de Seguridad:
    - Gestionar las solicitudes de solicitud de petición de evidencias.
    - Aprobar y/o denegar las solicitudes.
- Responsable de la infraestructura PKI:
    - Gestionar el equipo técnico encargado de realizar las actividades técnicas para la recopilación de las evidencias.
- Responsable de Operaciones:
    - Gestionar las actividades en el CMS para la recopilación de las evidencias.

5.5. Procedimiento

Las peticiones de recuperación de evidencias se realizarán a través de la herramienta de ticketing, https://bit4id.mantishub.io/my_view_page.php

5.5.1. Solicitudes

Las solicitudes para la recuperación de evidencias podrán ser:

- Por requisito legal: procedentes de procedimientos judiciales, legales, policiales o administrativos, en general por cualquier organismo de acuerdo con lo establecido con la normativa actual.
- Por petición externa: procedentes de entidades o personas ajenas BIT4ID.
- Por petición interna: procedentes de empleados terceros vinculados a BIT4ID.

5.5.2. Registro de la solicitud

- El responsable de seguridad analizará la procedencia de las solicitudes y las registrará en la herramienta de ticketing.
- Realizado el análisis aprobará o denegará la solicitud, notificándolo a través de la herramienta de ticketing.
- Aprobada la solicitud, se asignará al equipo técnico y/o responsable para que se proceda a su preparación.

5.5.3. Recuperación de evidencias de la infraestructura

- El equipo técnico gestionará la solicitud a través de la herramienta de ticketing.
- El equipo técnico accederá a los sistemas de la infraestructura.
- Se accederá al sistema de logs, que se encuentra encriptado con la clave maestra del HSM, de tal manera que para realizar dicho acceso se requerirá al administrador de la CA y/o de Sistemas por tal de proveer el acceso necesario a dicho sistema de logs.
- Una vez se ha introducido la clave maestra del HSM, y se dispone del acceso a los logs, se descifra el data blob referente a los logs a los que se quiere acceder.

- Descifrado el data blob, se procede a la recolección de la información requerida, en un formato comprensible, para dar cumplimiento a la solicitud presentada debiendo remitirse con la mayor celeridad posible la información reclamada.

5.5.4. Recuperación de evidencias de los servicios de confianza

- El responsable de operaciones gestionará la solicitud a través de la herramienta de ticketing.
- El responsable accederá al CMS de BIT4ID.
- Se procederá a la obtención de los registros mediante consulta al apartado de registro de auditoría propio de la aplicación.
- Se extraerá en un formato legible y comprensible la información solicitada.
- Si fuese necesario por motivo de la solicitud, el responsable de operaciones accederá a los registros físicos de BIT4ID con el fin de justificar los registros.

5.5.5. Entrega de las evidencias

- Los registros se extraerán en un formato legible y comprensible.
- Los mismos serán cifrados o se procederá a su protección para que únicamente el solicitante tenga acceso.
- La notificación y envío se realizará por las vías ordinarias en función de la solicitud, asegurando que las credenciales y/o acceso se entregue una por una vía distinta, cuyo único conocedor sea el solicitante.

6. Otras consideraciones

6.1. Revisión del documento

BIT4ID revisará la presente política de seguridad anualmente, así como la debida observancia de sus disposiciones en sus operaciones y controles con respecto de su propio personal, de BIT4ID y de cualquier tercero que intervenga o participe en la ejecución de las actividades relacionadas con la prestación de los servicios propios de la Autoridad de Sellado de Tiempo.