POLÍTICA DE SEGURIDAD

Bit4id S.A.C. – Entidad de Registro

Información general

Control documental

Clasificación de seguridad:	Público
Versión:	3.2
Fecha edición:	08/07/2020
Nombre del documento:	BIT4IDSAC Política de Seguridad ER_v3.2
Formato:	Office

Estado formal

Preparado por:	Revisado por:	Aprobado por:
Nombre: Alejandro Grande Fecha: 08/07/2020	Nombre: Albert Borrás Fecha: 08/07/2020	Nombre: Jorge García Fecha: 08/07/2020

Control de versiones

Versión	Partes que cambian	Descripción del cambio	Autor del cambio	Fecha del cambio
1.0	Original	Creación del documento	DMP / RLG	11/10/2016
2.0	Capítulo 3	Desagregación del capítulo 3. Detalle de medidas de seguridad físicas.	DMP / RLG	30/11/2016
3.0	Completo	Adaptación del documento de acuerdo a la nueva EC.	ABD/DMP	15/01/2018
3.1	1 y 2.8	Revisión del documento y ajuste al nuevo marco de la política de registro para la emisión de certificados digitales de acuerdo con la última guía de INDECOPI.	ABD	15/07/2019
3.2	Completo	Ajuste de la terminología aplicada en la versión original del documento, así como modificación del formato, para adaptar a las necesidades del ente regulador.	AGB	08/07/2020

Índice

1. Introducción

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 sus servicios como Entidad de Registro (ER) acreditada dentro de la Infraestructura Oficial de Firma Electrónica (IOFE) de la República del Perú, de acuerdo a la regulación aplicable.

Este documento es el resultado del compendio de documentos relativos a los procesos que garantizan la seguridad de los procesos de registro en la ER.

1.3. Nombre e identificación del documento

Este documento se denomina "Política de Seguridad de Bit4id, S.A.C. – Entidad de Registro".

1.4. Participantes

1.4.1. Entidades de Certificación

Bit4id, S.A.C se ha constituido como Entidad de Certificación y lleva a cabo el servicio de certificación digital basado en la infraestructura tecnológica de UANATACA, S.A., identificada al inicio de este documento. Asimismo se encuentra acreditada por la Autoridad Administrativa Competente (AAC), INDECOPI.
Toda la información con respecto los servicios de certificación, incluyendo la Declaración de Prácticas de Certificación se encuentran disponibles en el sitio web www.uanataca.com/pe.

1.4.2. Entidades de Registro

BIT4ID se encuentra acreditada de acuerdo a la Guía de Acreditación de Entidades de Registro (ER) y sus anexos, publicada por la Autoridad Administrativa Competente (AAC), INDECOPI. BIT4ID actúa como registrador de la identidad de los suscriptores de certificados.

BIT4ID publica su Declaración de Prácticas de Registro o Verificación, los convenios que mantiene con entidades de certificación y generadoras de certificados digitales, y en general toda la información relevante sobre la prestación de sus servicios como entidad de registro en su página web www.uanataca.com/pe.

Los servicios de registro se realizan bajo instrucciones y responsabilidad de las entidades de certificación para las cuales se presta el servicio.

1.4.3. Terceros contratistas

Los terceros contratistas son personas naturales o jurídicas que realizan funciones de registro, tales como solicitudes de emisión, revocación, re-emisión, etc. BIT4ID formalizará contractualmente las relaciones entre ella misma y cada uno de los terceros contratistas que realicen funciones de registro.

Los terceros contratistas quedan sujetos al presente documento que rige las medidas de seguridad ante la realización de funciones de registro.

1.5. Administración de la Política de Seguridad

La presente Política de Seguridad es administrada por BIT4ID en su condición de Entidad de Registro.

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 de registro y verificación de BIT4ID como entidad de registro, cuyo titular y datos de contacto se identificarán plenamente en la Declaración de Prácticas de Registro o Verificación. Igualmente, sobre esta persona, recae la autoridad y responsabilidad de la implementación del contenido de esta política.

BIT4ID deja constancia de que cualquier modificación que se realice en el documento se realizará 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 www.uanataca.com/pe.

1.6. Definiciones

Autoridad Administrativa Competente (AAC): organismo público responsable de acreditar a las entidades de certificación y a las entidades de registro o verificación, de reconocer los estándares tecnológicos aplicables en la Infraestructura Oficial de Firma

Electrónica, de supervisar dicha Infraestructura y las otras funciones señaladas en el Reglamento o aquellas que requiera en el transcurso de sus operaciones. Dicha responsabilidad recae en el Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual – INDECOPI.

Certificado digital: documento electrónico generado y firmado digitalmente por una entidad de certificación el cual vincula un par de claves con una persona natural o jurídica confirmando su identidad.

Clave privada: es una de las claves de un sistema de criptografía asimétrica que se emplea para generar una firma digital sobre un mensaje de datos y es mantenida en reserva por el titular de la firma digital.

Declaración de prácticas de certificación (CPS): documento oficialmente presentado por una entidad de certificación a la Autoridad Administrativa Competente, mediante el cual define sus Prácticas de Certificación.

Declaración de prácticas de registro o verificación (RPS): documento oficialmente presentado por una entidad de Registro o Verificación a la Autoridad Administrativa Competente, mediante el cual define sus Prácticas de Registro o Verificación.

Entidad de certificación (EC): persona jurídica pública o privada que presta indistintamente servicios de producción, emisión, gestión, cancelación u otros servicios inherentes a la certificación digital. Asimismo, puede asumir las funciones de registro o verificación.

Entidad de Registro o Verificación (ER): persona jurídica, con excepción de los notarios públicos, encargada del levantamiento de datos, comprobación de éstos respecto a un solicitante de un mecanismo de firma electrónica o certificación digital, la aceptación y autorización de las solicitudes para la emisión de un mecanismo de firma electrónica o certificados digitales, así como de la aceptación y autorización de las solicitudes de cancelación de mecanismos de firma electrónica o certificados digitales. Las personas encargadas de ejercer la citada función serán supervisadas y reguladas por la normatividad vigente.

Estándares técnicos internacionales: requisitos de orden técnico y de uso internacional que deben observarse en la emisión de firmas electrónicas y en las prácticas de certificación.

Infraestructura Oficial de Firma Electrónica (IOFE): sistema confiable, acreditado, regulado y supervisado por la Autoridad Administrativa Competente, provisto de instrumentos legales y técnicos que permiten generar firmas electrónicas y proporcionar diversos niveles de seguridad respecto a: 1) la integridad de los mensajes de datos y documentos electrónicos; 2) la identidad de su autor, lo que es regulado conforme a la Ley. El sistema incluye la generación de firmas electrónicas, en la que participan entidades de certificación y entidades de registro o verificación acreditadas ante la Autoridad Administrativa Competente, incluyendo a la Entidad de Certificación Nacional para el Estado Peruano (ECERNEP), las Entidades de Certificación para el Estado Peruano (ECEP) y las Entidades de Registro o Verificación para el Estado Peruano (EREP).

Medios telemáticos: conjunto de bienes y elementos técnicos informáticos que en unión con las telecomunicaciones permiten la generación, procesamiento, transmisión, comunicación y archivo de datos e información.

Políticas de Certificación (CP): documento oficialmente presentado por una entidad de certificación a la Autoridad Administrativa Competente, mediante el cual establece, entre otras cosas, los tipos de certificados digitales que podrán ser emitidos, cómo se deben emitir y gestionar los certificados, y los respectivos derechos y responsabilidades de las Entidades de Certificación. Para el caso de una EC Raíz, la CP incluye las directrices para la gestión del Sistema de Certificación de las ECs vinculadas.

Suscriptor o titular de la firma digital: persona natural responsable de la generación y uso de la clave privada, a quien se le vincula de manera exclusiva con un mensaje de datos firmado digitalmente utilizando su clave privada. En el caso que el titular del certificado sea una persona natural, sobre la misma recaerá la responsabilidad de suscriptor.

Terceros contratistas: Los terceros contratistas son personas naturales o jurídicas que realizan funciones de registro, tales como solicitudes de emisión, revocación, re-emisión, etc. BIT4ID formalizará contractualmente las relaciones entre ella misma y cada uno de los terceros contratistas que realicen funciones de registro.

1.7. Del ámbito de aplicación

La presente política de seguridad se aplicará a la ejecución de los servicios de registro y verificación que prestará BIT4ID así como los terceros contratistas, en su condición de Entidad de Registro debidamente acreditada por la AAC. En consecuencia, la presente política será de cumplimiento obligatorio para todo el personal de BIT4ID o cualquier tercero que intervenga o participe en la ejecución de las actividades relacionadas con la prestación de los servicios de la ER.

BIT4ID se asegurará de poner a disposición de sus empleados y terceros que participen en la ejecución de servicios de registro y verificación, la presente política, los cuales la deberán suscribir.

2. Gestión de la seguridad

2.1. Evaluación de los Riesgos

La evaluación de riesgos se trata en un documento específico de carácter confidencial.

2.2. Política de Control de Acceso

2.2.1. Controles de acceso a la información sensible

Los equipos informáticos al servicio de las actividades de registro y verificación, 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 la ER, se encuentra protegidos contra posible destrucción, alteración de datos, incluyendo especialmente información confidencial y datos personales de los suscriptores y titulares de los certificados digitales.

2.2.2. Controles de acceso a los ambientes donde se encuentra la información sensible

Además de lo anterior, BIT4ID dispone de un espacio físico, con medidas de control de acceso, donde almacena los documentos físicos contentivos de la información crítica de los servicios de verificación y registro. El acceso a este espacio físico se encuentra restringido con medidas físicas además de contar con video vigilancia a través de circuito cerrado.

2.3. Seguridad del Personal

2.3.1. Métodos de verificación de datos y antecedentes.

El personal que realiza actividades de registro recibe formación de preparación directamente por parte de las EC con las que la ER se vincula para la realización de las tareas de validación de las peticiones, hasta que adquiere el perfil necesario para desempeñar la labor respectiva. La ER para la verificación de los datos y antecedentes del

personal relacionado con sus actividades de registro y verificación utiliza los siguientes métodos:

En relación a la titulación acreditativa de la formación académica, BIT4ID mantiene expediente del personal, iniciándose con su resumen curricular. En este expediente se archivarán las copias de los títulos que alegue poseer, conjuntamente con copia de los certificados de la formación recibida por las ECs. El responsable de los servicios de la ER o una persona designada por este, contrastará dichas copias contras los respectivos originales para verificar la fidelidad y no alteración de los datos.

En relación a sus trabajos anteriores, BIT4ID. requiere constancias de antiguos empleadores que evidencien la prestación de los servicios o antecedentes laborales alegados por el personal. Estás evidencias son archivadas en el respectivo expediente del personal.

En relación a los antecedentes personales, BIT4ID solicita a su personal constancia de antecedentes penales emitido por la autoridad competente. Este certificado es agregado al expediente del personal.

2.3.2. Detalle de las responsabilidades del personal.

El personal de BIT4ID relacionado con sus servicios como ER, recibe por escrito sus obligaciones y responsabilidades, de acuerdo a las labores que presta. Las responsabilidades se establecen de conformidad con los roles determinados por cada EC. Los empleados contratados para realizar tareas confiables firman con anterioridad las cláusulas de confidencialidad y los requerimientos operacionales empleados por la ER.
En todo caso, todos los empleados cuyos medios de acceso a los sistemas de la ER se vean comprometidos, serán notificados de su obligación de reportarlo tan pronto como tengan conocimiento, en cuyo caso BIT4ID procederá a la inutilización de estos.

2.4. Seguridad Física

BIT4ID ha establecido controles de seguridad física y ambiental para proteger los recursos de las instalaciones donde se encuentran los sistemas, los propios sistemas y los

equipamientos empleados para las operaciones de registro. BIT4ID 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. Específicamente la ER cuenta con:

- Controles de acceso físico.
- Sistema de video grabación y monitoreo.
- Medidas de protección frente a incendios.
- Redundancia frente a fallo de los sistemas de apoyo (energía electrónica y telecomunicaciones).
- Control para evitar la salida no autorizada de equipamientos, informaciones, soportes y aplicaciones relativos a componentes empleados para los servicios del prestador de servicios de certificación.
- Control de acceso a las instalaciones mediante seguridad con guardias a la entrada que anuncian a los visitantes al ingresar.
- Señalización de zonas seguras.
- Provisión de extinguidores contra incendios
- Uso de estabilizadores y supresores de picos.

2.5. Control de Cambios y Configuración

El responsable de los servicios de registro y verificación cuyos datos de identificación se encuentran en la declaración de prácticas de registro o verificación será el responsable de autorizar los cambios en los sistemas.

Los cambios que se realicen sobre servicios críticos de las actividades de registro se registrarán.

2.6. Planificación de Contingencias

BIT4ID alinea la prestación de sus servicios con los planes de contingencia mínimos de las Entidades de Certificación con las que se vincula. En cualquier caso, prevé una serie de acciones, para el mantenimiento de los servicios mínimos requeridos por la normativa

legalmente aplicable, en el caso de producirse una contingencia que pueda inutilizar total o parcialmente sus servicios.

BIT4ID declara que la disponibilidad de los servicios prestados por las ECs con las que se vincula, será responsabilidad de las entidades de certificación, sin relevarle de su responsabilidad de notificar a los usuarios en la medida que sea necesario.

2.7. Auditorias y Detección de Intrusiones

BIT4ID somete sus sistemas a auditorias regulares de acuerdo a las políticas de seguridad de las ECs con las cuales se vincula, sobre los sistemas que se encuentran directamente vinculados con las actividades de registro, con el fin de verificar la integrar de los sistemas.

Igualmente se somete a las auditorias en las formas, condiciones y frecuencia que establecen las guías de acreditación publicadas por la AAC, con el fin de verificar conformidad con la normativa legalmente aplicable.

2.8. Medios de Almacenamiento

En relación con el almacenamiento de la información contenida en documentos físicos, la misma se resguarda en un un espacio físico, con las medidas de seguridad previstas en el punto 2.2.2., de esta política. Toda la documentación se almacena en la sede principal de Bit4id SAC debiendo los terceros contratistas que realicen funciones de registro remitirla de manera de segura a BIT4ID.

Los medios de seguridad de dicho espacio físico son verificados mensualmente para asegurar su integridad y pleno funcionamiento.

En relación a la información almacenada en medios digitales, ésta viene respaldada mediante un backup local semanal, un backup local mensual, y un backup en cloud en tiempo real, lo que permite su respaldo y recuperación.

3. Tratamiento de la información

3.1. 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, se utilizan máquinas trituradoras de papel para su posterior desecho, o alternativamente la utilización de papeleras donde la documentación 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 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.

3.2. Custodia de la información

La protección de los archivos se realiza conforme a lo establecido en la presente política. Los datos archivados contienen la fecha y hora, y se encuentran firmados digitalmente, debidamente secuenciados para generar evidencias de su cronología.

El periodo de conservación de los archivos es de diez (10) años, así como de las aplicaciones requeridas para su acceso.

3.3. De la información sensible

La información sensible será clasificada confidencial, de acuerdo a las previsiones de la Declaración de Prácticas de Registro de BIT4ID. Cuando contenga datos personales, la misma estará sujeta a la política y plan de privacidad aprobado por BIT4ID.

La clasificación de la información se especificará en cada política o manual de procedimientos aprobados, los cuales describirán la forma y condición del manejo de la información.

4. Otras consideraciones

4.1. Revisión del plan

BIT4ID revisará la presente política de seguridad al menos una vez al año. Asimismo si sucede cualquier evento o incidente que pudiera comprometer los sistemas de protección o controles contemplados en la misma, se procederá a su revisión con el fin de adoptar las medidas que sean necesarias para que la incidencia no se vuelva a repetir.