

PLAN DE PRIVACIDAD

Bit4id S.A.C.



Información general

Control documental

| | |
|------------------------------------|---------------------------------|
| Código | RA-PLP-01 |
| Clasificación de seguridad: | Público |
| Versión: | 2.0 |
| Fecha edición: | 11/05/2020 |
| Nombre del documento: | BIT4IDSAC Plan de Privacidad_v2 |
| Formato: | Office |

Estado formal

| Preparado por: | Revisado por: | Aprobado por: |
|---|--|---|
| Nombre: Alejandro Grande Fecha: 11/05/2020 | Nombre: Albert Borrás Fecha: 11/05/2020 | Nombre: Jorge García Fecha: 12/05/2020 |

Control de versiones

| Versión | Partes que cambian | Descripción del cambio | Autor del cambio | Fecha del cambio |
|---------|--------------------|--|------------------|------------------|
| 1.0 | Original | Creación del documento | Albert Borrás | 16/11/2017 |
| 2.0 | Completo | Ajuste de la terminología aplicada en la versión original del documento, así como modificación del formato, para adaptarlo a las necesidades del ente regulador. | Alejandro Grande | 11/05/2020 |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

Índice

| | |
|---|-----------|
| INFORMACIÓN GENERAL..... | 2 |
| CONTROL DOCUMENTAL | 2 |
| ESTADO FORMAL | 2 |
| CONTROL DE VERSIONES | 3 |
| ÍNDICE | 4 |
| INTRODUCCIÓN | 6 |
| PRESENTACIÓN | 6 |
| OBJETO | 6 |
| 1. ÁMBITO DE APLICACIÓN DEL DOCUMENTO | 7 |
| 1.1. PARTICIPANTES | 7 |
| 1.1.1. Entidades de Certificación | 7 |
| 1.1.2. Entidades de Registro..... | 7 |
| 1.1.3. Proveedor de Servicios de Infraestructura de Servicios de Certificación | 8 |
| 1.1.4. Titulares de los certificados | 8 |
| 1.1.5. Tercero que confía (Tercer Usuario)..... | 8 |
| 1.2. DEFINICIONES Y ABREVIATURAS..... | 9 |
| 1.3. ALCANCE..... | 10 |
| 1.4. INFORMACIÓN RECOLECTADA Y PROTEGIDA..... | 10 |
| 1.5. TRATAMIENTO DE DATOS PERSONALES..... | 12 |
| 1.5.1. Determinación de la información..... | 12 |
| 1.5.2. Información privada..... | 13 |
| 1.6. FLUJO TRANSFRONTERIZO DE DATOS PERSONALES..... | 14 |
| 2. IMPLEMENTACIÓN DE LOS PRINCIPIOS DE PRIVACIDAD | 15 |
| 2.1. MEDIDAS PREVENTIVAS..... | 15 |
| 2.2. LIMITACIONES A LA RECOLECCIÓN | 16 |
| 2.3. USO DE LA INFORMACIÓN PERSONAL..... | 16 |
| 2.4. ELECCIÓN | 16 |
| 2.5. INTEGRIDAD DE LA INFORMACIÓN PERSONAL | 17 |
| 2.6. SALVAGUARDAS A LA SEGURIDAD | 17 |
| 2.7. ACCESO Y CORRECCIÓN | 17 |
| 3. FUNCIONES Y OBLIGACIONES DEL PERSONAL | 19 |
| 3.1. CONTROLES DEL PERSONAL | 19 |
| 3.2. RESPONSABILIDADES | 19 |
| 4. PROCEDIMIENTOS..... | 20 |

| | | |
|-----------|---|-----------|
| 4.1. | COPIAS DE RESPALDO | 20 |
| 4.2. | PROCEDIMIENTO DE GESTIÓN DE INCIDENCIAS | 20 |
| 5. | OTRAS CONSIDERACIONES | 21 |
| 5.1. | REVISIÓN DEL PLAN..... | 21 |
| 5.2. | CONFORMIDAD..... | 21 |

Introducción

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.

Objeto

Bit4id ha definido el presente documento como el Plan de Privacidad en complemento a su Declaración de Políticas de Certificación, con el fin de dar 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.

Este Plan de privacidad se realizado teniendo en cuenta que para la gestión de datos personales se utiliza la infraestructura de llave pública (PKI) de UANATACA.

1. Ámbito de aplicación del documento

1.1. Participantes

1.1.1. Entidades de Certificación

La Entidad de Certificación (ER) es la persona, física o jurídica, que expide y gestiona certificados para entidades finales o presta otros servicios relacionados con la certificación digital. Bit4id presta el servicio de certificación digital basado en la infraestructura tecnológica de UANATACA, S.A., identificada al inicio de este documento.

1.1.2. Entidades de Registro

Una Entidad de Registro (ER) es la entidad encargada de: Tramitar las solicitudes de certificados, Identificar al solicitante y comprobar que cumple con los requisitos necesarios para la solicitud de los certificados, Validar las circunstancias personales de la persona que constará como firmante del certificado, Gestionar la generación de claves y la emisión del certificado, Hacer entrega del certificado al suscriptor o de los medios para su generación Y Custodiar la documentación relativa a la identificación y registro de los firmantes y/o suscriptores y gestión del ciclo de vida de los certificados.

Podrán actuar como Entidad de Registro de Bit4id, cualquier Entidad de Registro debidamente acreditada y registrada ante la Autoridad Administrativa Competente y que cuente con la correspondiente autorización y acuerdo con Bit4id.

Las comunicaciones entre la ER y la EC se realizan vía web de manera ininterrumpida, según los niveles de disponibilidad y recuperación brindados y declarados por cada EC. La ER tiene procedimientos de contingencia para acceder a los sistemas en casos de corte del servicio de Internet. La disponibilidad del servicio web de registro es provisto por cada EC.

1.1.3. Proveedor de Servicios de Infraestructura de Servicios de Certificación

UANATACA, S.A se configura como el Proveedor de Servicios de Certificación Digital por lo que a través de un contrato o acuerdo, presta su infraestructura y/o servicios tecnológicos a BIT4ID para que este pueda llevar a cabo los servicios inherentes a una Entidad de Certificación, garantizando en todo momento la continuidad de los servicios en las condiciones y bajo los requisitos exigidos por la normativa.

1.1.4. Titulares de los certificados

La comunidad de usuarios definidos como titulares de los certificados digitales será definida según lo establecido en la Política de Certificación y Declaración de Prácticas de la Autoridad de Certificación. Como norma general, son las personas naturales o jurídicas destinatarias de los servicios de emisión, gestión y uso de certificados digitales, para los usos de autenticación y firma electrónica.

1.1.5. Tercero que confía (Tercer Usuario)

Los terceros que confían son personas naturales o jurídicas que confían en el contenido y la aplicación de un certificado digital. En este sentido, los terceros que confían pueden ser todas aquellas personas naturales y jurídicas que requieren evaluar la validez de un certificado para proceder con sus respectivas transacciones electrónicas, incluyendo entidades de otras infraestructuras además de la IOFE.

1.2. Definiciones y abreviaturas

| | |
|--|--|
| Entidades 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. |
| Entidades de Registro o Verificación (ER) | Persona jurídica, con excepción de los notarios públicos, encargada del levantamiento de datos, la comprobación de éstos respecto a un solicitante de un certificado digital, la aceptación y autorización de las solicitudes para la emisión de un certificado digital, así como de la aceptación y autorización de las solicitudes de cancelación de certificados digitales. Las personas encargadas de ejercer la citada función serán supervisadas y reguladas por la normatividad vigente. |
| Declaración de Prácticas de Certificación (DPC o CPS) | Documento oficialmente presentado por una entidad de certificación a la Autoridad Administrativa Competente, mediante el cual define sus Prácticas de Certificación. |
| Operador de Registro | Persona responsable de representar a la ER en las actividades de recepción, validación y procesamiento de solicitudes. |
| Roles de confianza | Roles que tienen acceso a la información crítica de las operaciones de Certificación |
| Suscriptor | Es la persona natural responsable de la generación y uso de la clave privada, a quien se le vincula de manera exclusiva con un documento electrónico firmado digitalmente utilizando su clave privada. En el caso que el titular del certificado digital sea una persona natural, sobre ella recaerá la responsabilidad de suscriptor. En el caso que una persona jurídica sea el titular de un certificado digital, la responsabilidad de suscriptor recaerá sobre el representante legal designado por esta entidad. Si el certificado está designado para ser usado por un agente automatizado, la titularidad del certificado y de las firmas digitales generadas a partir de dicho certificado corresponderán a la persona jurídica. La atribución de responsabilidad de suscriptor, para tales efectos, corresponde a la misma persona jurídica. |
| Tercero que | Se refiere a las personas naturales, equipos, servicios o cualquier otro |

| | |
|----------------|--|
| confía | ente que actúa basado en la confianza sobre la validez de un certificado y/o verifica alguna firma digital en la que se utilizó dicho certificado. |
| Titular | Es la persona natural o jurídica a quien se le atribuye de manera exclusiva un certificado digital. |

1.3. Alcance

El presente Plan de Privacidad es de cumplimiento obligatorio para el personal contratado por Bit4id que participa de las operaciones críticas de los servicios propios de una Entidad de Certificación, descritos en la Declaración de Prácticas de Certificación, así como para los servicios de Entidad de Registro de acuerdo con su Declaración de Prácticas de Registro.

Asimismo será de aplicación a todo el personal externo de Bit4id, siempre que colabore directa o indirectamente en la prestación de servicios de certificación, independientemente del título, modo o relación que les una.

El sometimiento al mismo será obligatorio y con carácter previo al inicio de la actividad. En este sentido, el Personal Externo, mediante la forma que considere oportuna, debe acogerse y aceptar dicho Plan de Privacidad.

1.4. Información recolectada y protegida

Bit4id por sí mismo y/o a través de los terceros autorizados, recolecta y almacena en su banco de datos personales, información de suscriptores y titulares del siguiente tipo:

- Datos de identificación personal, incluyendo una copia de documentos de identidad.
- Datos de la persona jurídica, incluyendo copia de los documentos que acrediten la existencia y vigencia de la persona jurídica.
- Datos del Representante Legal y el tipo de facultades que ostenta, incluyendo copia de documento que garantice dichas facultades.
- Contrato de solicitud de servicios.

Asimismo, en cumplimiento con las medidas de seguridad de la normativa que le es de aplicación, gestiona ficheros que contienen datos de carácter personal, incluyendo los sistemas de información, soportes y equipos empleados para el tratamiento de datos de carácter personal, los cuales son protegidos de acuerdo con lo dispuesto en normativa vigente, las personas que intervienen en el tratamiento y los locales en los que se ubican.

Bit4id incorpora todos los datos de carácter personal, que se deriven de la actividad propia de la prestación de servicios de certificación electrónica, en ficheros, creados, declarados y mantenidos bajo la responsabilidad de Bit4id.

Descripción de los datos almacenados

| | |
|-------------------------------------|---|
| <u>Datos personales incluidos</u> | <ul style="list-style-type: none">• D.N.I./N.I.F.• NOMBRE Y APELLIDOS.• DIRECCIÓN.• FIRMA.• FIRMA ELECTRÓNICA.• CORREO ELECTRÓNICO. |
| <u>Otros tipos de datos</u> | <ul style="list-style-type: none">• ACADÉMICOS Y PROFESIONALES.• DETALLES DEL EMPLEO. |
| <u>Tipificación de la finalidad</u> | <ul style="list-style-type: none">• PRESTACIÓN DE SERVICIOS DE CERTIFICACIÓN ELECTRÓNICA. |
| <u>Origen de los datos</u> | <ul style="list-style-type: none">• Facilitados por el propio interesado o su representante legal.• Solicitudes de certificados, aprobadas o denegadas, así como toda otra información personal obtenida para la expedición y mantenimiento de certificados. |

1.5. Tratamiento de datos personales

1.5.1. Determinación de la información

De acuerdo con la Declaración de Práctica de Certificación de Bit4id, la información siguiente es considerada como confidencial:

- Solicitudes de certificados, aprobadas o denegadas, así como toda otra información personal obtenida para la expedición y mantenimiento de certificados, excepto las informaciones indicadas en la sección siguiente.
- Claves privadas generadas y/o almacenadas por el prestador de servicios de certificación.
- Registros de transacciones, incluyendo los registros completos y los registros de auditoría de las transacciones.
- Registros de auditoría interna y externa, creados y/o mantenidos por la Entidad de Certificación y sus auditores.
- Planes de continuidad de negocio y de emergencia.
- Política y planes de seguridad.
- Documentación de operaciones, archivo, monitorización y otros análogos.
- Toda otra información identificada como “Confidencial”.

De acuerdo con la Declaración de Prácticas de Certificación de Bit4id, la información siguiente es considerada como no confidencial:

- Los certificados emitidos o en trámite de emisión.
- La vinculación del suscriptor a un certificado emitido por la Entidad de Certificación.
- El nombre y los apellidos de la persona física identificada en el certificado, así como cualquiera otra circunstancia o dato personal del titular, en el supuesto de que sea significativa en función de la finalidad del certificado.
- La dirección de correo electrónico de la persona física identificada en el certificado, o la dirección de correo electrónico asignada por el suscriptor, en el supuesto de que sea significativa en función de la finalidad del certificado.
- Los usos y límites económicos reseñados en el certificado.
- El periodo de validez del certificado, así como la fecha de emisión del certificado y la fecha de caducidad.
- El número de serie del certificado.

- Los diferentes estados o situaciones del certificado y la fecha del inicio de cada uno de ellos, en concreto: pendiente de generación y/o entrega, válido, revocado, suspendido o caducado y el motivo que provocó el cambio de estado.
- Las listas de revocación de certificados (LRCs), así como las restantes informaciones de estado de revocación.
- La información contenida en los depósitos de certificados.
- Cualquier otra información que no esté indicada en la sección anterior.

1.5.2. Información privada

Deberá considerarse como información no privada, la siguiente:

- Información personal públicamente disponible.

En estos casos no será requerida autorización del usuario para dar publicidad a esta información.

Deberá considerarse como información privada, la siguiente:

- De conformidad con lo establecido por la Norma Marco sobre privacidad del APEC, se considera información personal, cualquier información relativa a un individuo identificado o identificable.
- Información que pueda permitir a personas no autorizadas la construcción de un perfil de las actividades de los usuarios de los servicios de certificación.
- En todos los casos, deberá ser suscrita por el mismo, su consentimiento para el tratamiento y almacenamiento de estos datos.

Bit4id no divulga ni cede datos personales, excepto en los casos previstos por la normativa. La información del banco de datos personales considerada como privada únicamente será divulgada en caso de que exista consentimiento previo y por escrito firmado para tales efectos por el titular de dicha información o medie una orden judicial o administrativa que así lo determine. Cualquier violación a la privacidad de esta información por parte del personal de Bit4id o de los terceros subcontratados, será sujeto de sanción.

Sin perjuicio de lo anterior, la información confidencial se protege de su pérdida, destrucción, daño, falsificación y procesamiento ilícito o no autorizado, de conformidad con las prescripciones establecidas en este documento y según la Declaración de Prácticas de Certificación de Bit4id, mediante las medidas de seguridad y protocolos adoptados por ésta.

1.6. Flujo transfronterizo de datos personales

Los contratos de los suscriptores contendrán cláusulas que soliciten el consentimiento del suscriptor y titular para transferir los datos personales recolectados a los países donde se encuentre ubicada la EC, todo ello a través de las ER vinculadas a Bit4id.

2. Implementación de los principios de privacidad

Bit4id establece las medidas de seguridad necesarias para garantizar la protección de los datos de carácter personales contenidos en sus bases de datos. En este sentido, el presente documento adopta lo establecido por el APEC a través de la Norma Marco sobre Privacidad respecto de los principios que deben ser observados siempre que se realice algún tipo de labor o función que involucre la recolección, posesión, procesamiento, uso, transferencia o revelación de información personal.

Asimismo, se deja constancia que los datos se almacenan y gestionan bajo la cobertura de la infraestructura de UANATACA, S.A., para ello se ha elaborado una Política de Seguridad (PSI) en la que se regula la seguridad de las instalaciones o centro de tratamiento de datos, los servidores o entornos automatizados, así como el archivo de documentación o tratamiento de documentación no automatizada.

2.1. Medidas preventivas

- Se restringirá el acceso a los datos personales.
- Estos datos serán protegidos contra acceso no autorizado.
- Se concientizará al personal para no divulgar o exponer de manera accidental datos personales de los usuarios.
- Se implementarán procedimientos para documentar las prácticas en lo que respecta a la información personal que se recolecta durante las actividades de operación o comercialización de los servicios de certificación digital, las mismas que deben informar sobre:
 - El hecho de que se está recolectando información personal;
 - Los propósitos para los cuales se recolecta dicha información personal;
 - Los tipos de personas u organizaciones a las que dicha información podría ser revelada;
 - La identidad y ubicación del responsable de la información personal, Incluyendo información respecto a la forma de contactarlo en razón a sus prácticas y manejo de la información personal;

- Las opciones y medios que ofrece el responsable de la información personal a los individuos para limitar el uso y revelación, así como los mecanismos para el acceso y corrección de su información.

Deben tomarse todos los pasos razonablemente necesarios, a fin de asegurar que se provee tal información, sea antes o en el mismo momento en que se está efectuando la recolección de la información personal. Caso contrario, deberá proveerse esta información tan pronto como sea factible.

2.2. Limitaciones a la recolección

La recolección de información personal debe encontrarse limitada a la información que es relevante para el propósito para el cual se está recolectando y esta información deberá ser obtenida de manera legal y apropiada, y, en la medida de lo posible, con la debida información o consentimiento del individuo al cual pertenece.

2.3. Uso de la información personal

La información personal recolectada será usada en estricto cumplimiento de los propósitos de la recolección o aspectos relativos a los mismos, excepto:

- que exista consentimiento del individuo al que pertenece la información personal recolectada;
- que esta información fuera necesaria para la provisión de un servicio o producto solicitado por el individuo; o
- que la recolección fuera permitida por mandato de ley u otros instrumentos legales o exista algún tipo de pronunciamiento con efectos legales que lo autorizara.

2.4. Elección

Cuando sea apropiado, se proveerá a los individuos mecanismos claros, pertinentes, fáciles de entender, accesibles y económicos a fin que puedan decidir respecto a la recolección, uso y revelación de su información personal. Puede no resultar necesario

que los responsables de la información provean estos mecanismos en los casos de recolección de información que sea públicamente disponible.

2.5. Integridad de la información personal

La información personal deberá ser exacta, completa y mantenerse actualizada en el extremo que fuere necesario para los propósitos de su empleo.

2.6. Salvaguardas a la seguridad

Los responsables de la información personal deberán proteger la información personal que mantienen, a través de salvaguardas apropiadas contra riesgos tales como pérdida de la información o acceso indebido a la misma, así como contra la destrucción, uso, modificación o revelación no autorizada o cualquier otro abuso. Estas salvaguardas deberán ser proporcionales a la naturaleza y gravedad del daño potencial, la sensibilidad de la información y el contexto en que ésta es mantenida, y deberán ser sometidas a revisiones y reevaluaciones periódicas.

2.7. Acceso y corrección

Los individuos deben ser capaces de:

- obtener del responsable de la información personal, la confirmación respecto a si mantiene o no información personal que les concierne;
- comunicar su información personal, luego de haber probado suficientemente su identidad, dentro de un periodo de tiempo razonable; por una tarifa, si es que la hubiera, la cual no debe ser excesiva; de una manera razonable; de un formato que sea razonablemente comprensible; y
- cuestionar la exactitud de la información que les concierne y de ser posible y apropiado, hacer que la información sea rectificada, completada, enmendada o borrada.

Debe proveerse acceso y oportunidad para la corrección de la información, salvo cuando:

- La carga o costo de hacerlo sea indebido o desproporcional a los riesgos de la privacidad individual en el caso en cuestión;
- la información no pueda ser divulgada por razones legales o de seguridad o para proteger información comercial de carácter confidencial; o
- se podría violar la privacidad de la información de personas diferentes al individuo.

Si una solicitud bajo alguno de los supuestos descritos o un cuestionamiento es denegada, se debe informar al individuo las razones en las que se basa dicha denegatoria y se le debe informar respecto a los mecanismos para cuestionar dicha decisión.

3. Funciones y obligaciones del personal

3.1. Controles del personal

Bit4id declara que el personal sólo accederá a aquellos datos y recursos que precise para el desarrollo de sus funciones. Para ello se garantiza la segregación de funciones y el establecimiento de los mínimos privilegios, asegurando el control y vigilancia.

Bajo la infraestructura de llave pública (PKI) de UANATACA, S.A., se ha definido una Política de Recursos Humanos donde se establecen los controles del personal así como la descripción de los puestos de trabajo, para garantizar que todas aquellas funciones relacionadas con la prestación de los servicios propios de una Entidad de Certificación y Entidad de Registro, cumplan con lo legalmente exigido.

3.2. Responsabilidades

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

4. Procedimientos

4.1. Copias de respaldo

En cuanto a los procedimientos de realización de copias de respaldo y de recuperación de los datos de las bases de datos, Bit4id custodia esta documentación bajo la cobertura de la infraestructura de llave pública (PKI) de UANATACA, S.A., el cual dispone de un Plan de Continuidad de Negocio a través del cual se regula la gestión de copias de seguridad, así como el plan de recuperación de datos.

4.2. Procedimiento de gestión de incidencias

Bajo la infraestructura de llave pública (PKI) de UANATACA, S.A., como custodio de las bases de datos, se dispone de un Protocolo de actuación, previsto en el documento de gestión de incidencias, para el caso de brechas de seguridad o pérdida de integridad de sus sistemas que impliquen una afectación a la prestación de servicios de certificación y a los datos personales que se deriven de éstos.

5. Otras consideraciones

5.1. Revisión del plan

Bit4id revisará el presente Plan de Privacidad de manera anual.

5.2. Conformidad

Este documento ha sido aprobado por el Responsable de Bit4id y cualquier incumplimiento por parte de los empleados, contratistas y terceros mencionados en el alcance de este documento, será revisado por ésta para la ejecución, si procede, de las sanciones oportunas.