

POLÍTICA DE PRIVACIDAD

Bit4id S.A.C.



Información general

Control documental

Clasificación de seguridad:	Público
Versión:	2.0
Fecha edición:	16/11/2017
Nombre del documento:	Bit4id.- Política de Privacidad_v1.docx
Formato:	Office

Estado formal

Preparado por:	Revisado por:	Aprobado por:
Nombre: Albert Borrás Fecha: 16/11/2017	Nombre: David Márquez Fecha: 20/11/2017	Nombre: Rodrigo López Fecha: 22/11/2017

Control de versiones

Versión	Partes que cambian	Descripción del cambio	Autor del cambio	Fecha del cambio
1.0	Original	Creación del documento	DMP	22/11/2016
2.0	Completo	Adaptación total del documento a la acreditación de BIT4ID.	ABD	16/11/2017

Índice

INFORMACIÓN GENERAL	2
CONTROL DOCUMENTAL.....	2
ESTADO FORMAL	2
CONTROL DE VERSIONES.....	3
ÍNDICE	4
1. ASPECTOS GENERALES.....	5
1.1. PRESENTACIÓN.....	5
1.2. OBJETO	5
1.3. NOMBRE E IDENTIFICACIÓN DEL DOCUMENTO.....	5
1.4. PARTICIPANTES	6
1.4.1. <i>Entidades de Certificación</i>	6
1.4.2. <i>Entidades de Registro</i>	6
1.5. ADMINISTRACIÓN DEL DOCUMENTO Y CONFORMIDAD	6
1.5.1. <i>Organización que administra el documento y conformidad</i>	6
1.5.2. <i>Contacto</i>	7
1.5.3. <i>Responsabilidad y Conformidad</i>	7
1.6. ÁMBITO DE APLICACIÓN	7
2. DEFINICIONES	8
3. DE LA PRIVACIDAD DE LOS DATOS PERSONALES	11
3.1. RESPOSNABILIDAD	11
3.2. COMO ENTIDAD DE CERTIFICACIÓN	11
3.3. COMO ENTIDAD DE REGISTRO.....	12
3.4. COMO AUTORIDAD DE SELLADO DE TIEMPO.....	12

1. Aspectos generales

1.1. Presentación

Bit4id, S.A.C., en lo sucesivo “UANATACA” 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 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 Privacidad que UANATACA implementa en la prestación de los servicios de certificación para los que se encuentra acreditada, dentro de la Infraestructura Oficial de Firma Electrónica (IOFE) de la República del Perú, de acuerdo a la regulación aplicable.

1.3. Nombre e identificación del documento

Este documento se denomina “Política de Privacidad de Bit4id, S.A.C.”

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.uanatata.com/pe.

1.4.2. Entidades de Registro

Bit4id, S.A.C., 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 SAC actúa como registrador de la identidad de los suscriptores de certificados.

Bit4id, S.A.C., 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.uanatata.com/pe.

1.5. Administración del documento y conformidad

1.5.1. Organización que administra el documento y conformidad

La presente Política de Privacidad es administrada por Bit4id, S.A.C..

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 www.uanataca.com/pe.

1.5.2. Contacto

La persona responsable de la administración de este documento es Rodrigo López González, 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:

- Bit4id S.A.C.
- Calle Mártir Olaya n°129, oficina 1204 Miraflores, Lima, Perú
- Email: info.pe@uanataca.com
- Tel: +(51) 1 242 9994
- Web: www.uanataca.com/pe

1.5.3. 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.

1.6. Ámbito de aplicación

La presente política de privacidad se aplicará a la ejecución de los servicios de certificación prestará Bit4id S.A.C., para los que se encuentre debidamente acreditada por la AAC.

En consecuencia, la presente política será de cumplimiento obligatorio para todo el personal y/o cualquier tercero que intervenga o participe en la ejecución de las actividades relacionadas con la prestación de los servicios de certificación para los que se encuentre acreditada.

2. 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.

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.

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.

Banco de datos personales: Conjunto organizado de datos personales, automatizado o no, independientemente del soporte, sea este físico, magnético, digital, óptico u otros que se creen, cualquiera fuere la forma o modalidad de su creación, formación, almacenamiento, organización y acceso.

Datos personales: Toda información sobre una persona natural que la identifica o la hace identificable a través de medios que pueden ser razonablemente utilizados.

Datos sensibles: Datos personales constituidos por los datos biométricos que por sí mismos pueden identificar al titular; datos referidos al origen racial y étnico; ingresos económicos, opiniones o convicciones políticas, religiosas, filosóficas o morales; afiliación sindical; e información relacionada a la salud o a la vida sexual.

Encargado del banco de datos personales: Toda persona natural, persona jurídica de derecho privado o entidad pública que sola o actuando conjuntamente con otra realiza el tratamiento de los datos personales por encargo del titular del banco de datos personales.

Flujo transfronterizo de datos personales: Transferencia internacional de datos personales a un destinatario situado en un país distinto al país de origen de los datos personales, sin importar el soporte en que estos se encuentren, los medios por los cuales se efectuó la transferencia ni el tratamiento que reciban.

Fuentes accesibles para el público: Bancos de datos personales de administración pública o privada, que pueden ser consultados por cualquier persona, previo abono de la

contraprestación correspondiente, de ser el caso. Las fuentes accesibles para el público son determinadas en el reglamento.

Nivel suficiente de protección para los datos personales: Nivel de protección que abarca por lo menos la consignación y el respeto de los principios rectores de esta Ley, así como medidas técnicas de seguridad y confidencialidad, apropiadas según la categoría de datos de que se trate.

Procedimiento de anonimización: Tratamiento de datos personales que impide la identificación o que no hace identificable al titular de estos. El procedimiento es irreversible.

Procedimiento de disociación: Tratamiento de datos personales que impide la identificación o que no hace identificable al titular de estos. El procedimiento es reversible.

Titular de datos personales: Persona natural a quien corresponde los datos personales.

Titular del banco de datos personales: Persona natural, persona jurídica de derecho privado o entidad pública que determina la finalidad y contenido del banco de datos personales, el tratamiento de estos y las medidas de seguridad.

Transferencia de datos personales: Toda transmisión, suministro o manifestación de datos personales, de carácter nacional o internacional, a una persona jurídica de derecho privado, a una entidad pública o a una persona natural distinta del titular de datos personales.

Tratamiento de datos personales: Cualquier operación o procedimiento técnico, automatizado o no, que permite la recopilación, registro, organización, almacenamiento, conservación, elaboración, modificación, extracción, consulta, utilización, bloqueo, supresión, comunicación por transferencia o por difusión o cualquier otra forma de procesamiento que facilite el acceso, correlación o interconexión de los datos personales.

3. De la Privacidad de los Datos Personales

3.1. Responsabilidad

UANATACA se obliga a cumplir con la normativa sobre protección de datos personales, y con las medidas de seguridad que resulten pertinentes de acuerdo a la Ley N° 29733 de Protección de Datos Personales y su Reglamento.

UANATACA declara obtener los datos personales que figuran en los ficheros y formularios, recolectando los datos del suscriptor, quien debe haberlos obtenido legalmente de quien corresponda en las condiciones legales aplicables.

La información confidencial de acuerdo con la normativa en protección de datos personales se protege de su pérdida, destrucción, daño, falsificación y procesamiento ilícito o no autorizado, de conformidad con las prescripciones establecidas en la Declaración de Prácticas de Registro.

3.2. Como Entidad de Certificación

UANATACA para la prestación de servicios como Entidad de Certificación, ha definido un Plan de Privacidad como complemento a su Declaración de Políticas de Certificación y la presente política de privacidad, con el fin de dar cumplimiento a la normativa vigente en concepto de protección de la privacidad de la información y de la norma marco sobre privacidad APEC.

Dicho Plan de Privacidad es de cumplimiento obligatorio para el personal contratado y 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 también será de aplicación a todo el personal externo de UANATACA, siempre que colabore directa o indirectamente en la prestación de servicios de certificación, independientemente del título, modo o relación que les una.

3.3. Como Entidad de Registro

En el supuesto que UANATACA actúe como Entidad de Registro de terceras EC, tendrá la condición de encargado del banco de datos personales en tanto que no decidirá sobre la finalidad, contenido y uso del tratamiento de dichos datos de carácter personal. No obstante, a que la EC de la que se trate tendrá el carácter de Titular del banco de datos personales, los datos personales contenidos en los ficheros podrán ser utilizados única y exclusivamente para los fines que figuran en esta Declaración de Prácticas respectiva.

3.4. Como Autoridad de Sellado de Tiempo

UANATACA, en el desarrollo de la prestación de servicio de Sellado de Tiempo, no recoge 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.