BIT4ID SAC

DECLARACIÓN DE PRÁCTICAS DE VALOR AÑADIDO (DPSVA)

Información general

Control del Documento

Clasificación de seguridad:	**Público**
Versión:	**1.0**
Fecha edición:	**15/01/2018**
Fichero / código:	**BIT4IDSAC_DPSVA_v1.docx**
Formato:	**Office**

Estado formal

Preparado por:	**Revisado por:**	**Aprobado por:**
Nombre: Albert Borrás Fecha: 15/01/2018	Nombre: David Márquez Fecha: 29/01/2018	Nombre: Rodrigo López Fecha: 22/01/2018

Antecedentes del Documento

Versión	Partes que cambian	Descripción del cambio	Autor del cambio	Fecha del cambio
1.0	Original	Creación del documento	ABD/DMP	15/01/2018

Índice

1. Gestión del documento

1.1. Introducción

Bit4id, S.A.C., en lo sucesivo "UANATACA" 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 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 UANATACA. 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://www.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 UANATACA como Autoridad de Sellado de Tiempo 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 nº129, oficina 1204 Miraflores, Lima, Perú

- Email: info.pe@uanataca.com
- Tel: +(51) 1 242 9994
- Web: www.uanataca.com/pe

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 UANATACA, 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

UANATACA 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. UANATACA 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.

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 UANATACA, 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

UANATACA 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.

UANATACA 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

UANATACA 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 del de UANATACA, S.A., identificada al inicio de este documento.

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

UANATACA 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.

UANATACA 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 UANATACA 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 UANATACA.
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 UANATACA, de conformidad con lo que se establece en la Declaración de Prácticas de Valor Añadido y en la documentación de UANATACA.
- 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 UANATACA, 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 UANATACA, sin previo consentimiento escrito.

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

Los servicios de valor añadido de sellado de tiempo prestados por UANATACA 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

UANATACA 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).

UANATACA 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, UANATACA 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 UANATACA responda por caso fortuito y en caso de fuerza mayor.

3.1.4.2. Exclusión de la garantía

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

3.1.4.3. Resolución de disputas.

UANATACA establece, en el contrato de suscriptor y otra documentación relevante que puede encontrarse en www.uanataca.com/pe, los procedimientos de mediación y resolución de conflictos 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, directamente controlado por personal confiable de Uanataca.
- 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 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 o superior.

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 UANATACA en su página web www.uanataca.com/pe.

El servicio suministrado por UANATACA 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 UANATACA contiene toda la documentación que requiere la normativa, como por ejemplo:

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.

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 UANATACA 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)*".

UANATACA dispone de una fuente fiable de tiempo en alta disponibilidad que permite un nivel de confianza de STRATUM 3, vía NTP, con el CSUC.

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

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, las cuales se encuentran detalladas en los apartados 5 y 6 de la Declaración de Prácticas de Certificación de BIT4ID SAC como EC y que concretamente prevén:

CONTROLES DE SEGURIDAD FÍSICA, DE GESTIÓN Y DE OPERACIONES

- Controles de seguridad física
- controles de procedimientos
- controles de personal
- procedimientos de auditoría de seguridad
- archivos de informaciones
- renovación de claves
- compromiso de claves y recuperación de desastre
- terminación del servicio

CONTROLES DE SEGURIDAD TÉCNICA

- Generación e instalación del par de clave
- protección de la clave privada
- otros aspectos de gestión del par de claves
- datos de activación
- controles de seguridad informática
- controles técnicos del ciclo de vida
- controles de seguridad de red
- controles de ingeniería de módulos criptográficos
- fuentes de tiempo
- cambio de estado de un dispositivo seguro de creación de firma

La Declaración de Prácticas de Certificación de BIT4ID, SAC como EC se encuentra disponible al público en www.uanataca.com/pe.

Asimismo, UANATACA cuenta con una Política de Seguridad que da cumplimiento a la regulación establecida por la Autoridad Administrativa Competente, el Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual (INDECOPI).

4.2. **Compromiso de los servicios de sellado de tiempo**

UANATACA 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.

4.3. **Término de la organización que administra la TSA**

UANATACA ante un eventual cese de actividad, 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. Revocación de las autorizaciones de las entidades subcontratadas o aquellas que actúen en nombre del PSVA.
3. Posibilidad de la transferencia de la actividad a otro Prestador siempre y cuando asegurando que se cumplen las condiciones legales exigidas.
4. Custodia y archivo para asegurar el mantenimiento continuo de los registros, conservando toda la documentación e información que un PSVA debe mantener.
5. Destrucción o inhabilitación de las claves privadas de la TSA.
6. Dotación de una provisión de fondos para continuar la finalización de las actividades requeridas para la terminación.

5. Auditoría

UANATACA 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 UANATACA se somete una vez al año a auditorías de conformidad respecto del marco de la IOFE.

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 UANATACA.

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 UANATACA, la cual se encuentra detallada en la Declaración de Prácticas de Certificación de BIT4ID, SAC.

En este sentido, el PSVA archiva los registros especificados por un periodo de al menos 10 años, o bien el periodo que establezca la legislación vigente.

6.2. Cumplimiento normativo

UANATACA 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

UANATACA 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.

6.4. Protección de datos personales

UANATACA cumple 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, 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, UANATACA 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