BIT4ID SAC

POLÍTICA DE REGISTRO

Información general

Control documental

Clasificación de seguridad:	Público
Entidad de destino:	BIT4ID SAC
Versión:	4.0
Fecha edición:	15/01/2018
Fichero:	BIT4IDSAC_Política de registro_v4.docx
Formato:	Office

Estado formal

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

Control de versiones

Versión	Partes que cambian	Descripción del cambio	Autor del cambio	Fecha del cambio
1.0	Original	Creación del documento	DMP/RLG	23/09/2016
2.0	General	Adecuación del documento según las guías de INDECOPI.	RLG	18/01/2017
3.0	General	Adecuación del documento según las guías de INDECOPI.	RLG	03/05/2017
3.1	General	Corrección de errores.	RLG	04/05/2017
4.0	Completo	Adaptación completa del documento de acuerdo a la EC vinculada	ABD/DMP	15/01/2018

Índice

1. Introducción

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.

2. PARTICIPANTES

Son considerados como participantes, para efectos del presente documento, la entidad de certificación, la entidad de registro, los titulares y/o suscriptores, los terceros de confianza y los proveedores de servicios de valor añadido dentro de la IOFE.

Entidad de Certificación (EC): Es la 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.

Titulares y/o Suscriptores: 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. UANATACA brinda servicios solamente a personas naturales o jurídicas. En el caso de personas naturales, los servicios de validación serán brindados a personas sin impedimento legal de nacionalidad peruana

Terceros de confianza: 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.

3. DEFINICIONES Y ABREVIACIONES

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 Registro (RPS)	Conjunto de declaraciones sobre políticas y prácticas de la Entidad de Registro, que sirve para comunicar el cumplimiento legal y regulatorio a los suscriptores y terceros que confían.
Operador de Registro	Persona responsable de representar a la ER en las actividades de recepción, validación y procesamiento de solicitudes.
Prácticas de Registro	Son las prácticas que establecen las actividades y requerimientos de seguridad y privacidad correspondientes al Sistema de Registro o Verificación de una Entidad de Registro o Verificación.
Roles de confianza	Roles que tienen acceso a la información crítica de las operaciones de registro.
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 confía	Se refiere a las personas naturales, equipos, servicios o cualquier otro 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.

4. USO APROPIADO DEL CERTIFICADO

Los criterios para definir el uso apropiado, rango de acción o aplicabilidad de un certificado digital solicitado a UANATACA en calidad de ER, dependerán de lo establecido en las Políticas y Prácticas de Certificación de cada EC para las que UANATACA brinda el servicio de ER.

5. ADMINISTRACIÓN DE POLÍTICAS

5.1. Organización que administra los documentos de RPS

UANATACA es la organización responsable de administrar esta política de certificación, de acuerdo a la RPS.

5.2. Protección de integridad del documento

La presente y sucesivas versiones de las Políticas de Registro administradas por UANATACA, se encontrarán firmadas a nombre de la persona que determina la conformidad de la RPS. El formato del documento firmado será en PDF usando un certificado emitido por una EC reconocida por el IOFE.

5.3. Procedimiento de aprobación de política de registro

La presente Política de Registro es administrada y verificada por UANATACA, cada nueva versión será presentada a la AAC y luego de su aprobación, será debidamente publicada en la siguiente dirección url: https://www.uanataca.com/pe.

5.4. Persona de contacto

La persona responsable de la administración de los servicios de certificación digital, es ubicable mediante la siguiente información de contacto:

- Nombre: RODRIGO LOPEZ GONZALEZ
- Cargo: Responsable de BIT4ID S.A.C. en calidad de ER
- Dirección de correo electrónico: info.pe@uanataca.com

5.5. Persona de contacto

La política de Registro de UANATACA y toda la documentación pertinente y relevante vigente de la Entidad de Registro, así como sus versiones anteriores, son publicadas en la siguiente dirección web: https://www.uanataca.com/pe.

Frente a cada modificación sobre el RPS de UANATACA se publicará tan pronto como razonablemente sea posible.

6. PROCEDIMIENTOS DE REGISTRO

6.1. Identificación y autenticación

UANATACA establece procedimientos seguros para el aseguramiento de la posesión de la clave privada, conformes con los estándares de seguridad Common Criteria EAL 4+ y/o FIPS 140-2 de acuerdo a la guía de acreditación de la ACC. En este sentido, UANATACA implementa procedimientos conformes a la legislación aplicable en la República del Perú para la autenticación de la identidad de personas físicas y representantes de personas jurídicas, en la solicitud de emisión y remisión de certificados, estableciendo procedimientos análogos que les permita la suspensión y revocación de los mismos. UANATACA declara verificar documental y/o telemáticamente todos los datos que incluye en los certificados emitidos.

Para lo anterior, UANATACA desarrolla su respectiva Declaración de Prácticas de Registro basada en los procedimientos mencionados en el párrafo precedente, siempre de conforma coherente con la normativa de aplicación, y la Declaración de Prácticas de Certificación de la Entidad de Certificación a la cual se encuentra vinculada.

6.2. Solicitud del certificado, re emisión, suspensión y revocación

Los procedimientos de solicitud, re emisión y revocación dependerán de lo establecido en la CP y CPS de cada EC a la que UANATACA se encuentra vinculada.

7. GESTIÓN DE LA SEGURIDAD

7.1. Controles de las instalaciones, de la gestión y controles operacionales

Los controles a las instalaciones y la gestión operacional dentro de la ER se definen en la Política de Seguridad de Entidad de Registro de UANATACA.

7.2. Controles de seguridad tecnica

Los módulos criptográficos usados por la ER de UANATACA o eventuales Proveedores de servicios de repositorio acreditados (si fuesen requeridos) deben cumplir los requerimientos o ser equivalentes a los requerimientos de FIPS 140-2 nivel de seguridad 2 como mínimo.

Los módulos criptográficos usados por los titulares o suscriptores bajo el marco de la IOFE deben cumplir los requerimientos o ser equivalentes a los requerimientos de FIPS 140-2 nivel 1.

NOTA: Los requerimientos exigidos en esta sección se aplican tanto al hardware como al firmware (“sistema operativo”) de los módulos criptográficos.

8. AUDITORIAS DE COMPATIBILIDAD Y OTRAS EVALUACIONES

Se debe estar sometido a auditoría de compatibilidad independiente en relación a las operaciones que realiza. La frecuencia de auditorías externas o evaluaciones de compatibilidad y el proceso de publicación de los resultados debe ser de una vez al año o cuando AAC así lo establezca.

La auditoría de compatibilidad o los procesos de evaluación requeridos para obtener y mantener la acreditación debe asimismo estar establecidos en la RPS u otra documentación relevante.

9. OTRAS MATERIAS DE NEGOCIO Y LEGALES

9.1. Tarifas

Las ER de UANATACA, en convenio con las ECs vinculadas, establecen el monto de sus tarifas. En particular, las tarifas deben ser referenciadas en los contratos de suscriptores y terceros que confían.

9.2. Responsabilidad financiera

9.2.1. Cobertura de seguro

El monto mínimo de la póliza es fijado por la AAC. UANATACA mantiene la cobertura de acuerdo al marco regulatorio aplicable.

9.2.2. Cobertura de seguro o garantía para entidades finales

En el caso que exista cobertura de seguro o garantía disponibles para los suscriptores, la UANATACA establecerá en sus RPS los tipos correspondientes, lo cual deberá se referenciará en el contrato de suscriptor, incluyendo los términos y condiciones de dicha cobertura.

En el caso que exista cobertura de seguro o garantía disponibles para los terceros que confían, esto deberá encontrarse referenciado en la CPS, en donde deben incluirse los términos y condiciones de la cobertura para el tercero que confía.

9.3. Confidencialidad de la información del negocio

El uso apropiado y confidencialidad de la información está referida en la Política de Privacidad de la Información definida por UANATACA como ER.

9.4. Exención de garantías

La ER establece en su RPS y otra documentación relevante, cualquier exención de responsabilidad que pudiera aplicársele.

Asimismo, se debe asegurar que estas provisiones sean incluidas en cualquier contrato de suscriptor o tercero que confía.

No cabe exención de responsabilidad para aquellas garantías establecidas por la legislación vigente.

9.5. Materia de negocios y legal

La ER identifica en su RPS y otra documentación relevante la ley aplicable a sus operaciones de acuerdo a la Ley N° 27269 y el Reglamento de Ley de Firmas y Certificados Digitales, aprobado por el D.S. 004-2007-PCM.

Los requerimientos legalmente significativos deben de estar establecidos o referenciados en los contratos de suscriptores y terceros que confían.

9.6. Finalizacion de UANATACA en calidad de ER

Antes de su finalización, UANATACA en calidad de ER informará a la AAC, a los suscriptores, titulares y terceros que confían sobre el cese de sus operaciones con por lo menos treinta (30) días calendario de anticipación.

Todas las solicitudes y contratos de suscriptores y titulares serán transferidos a la AAC o a otro PSC designado por éste.

En caso de una operación de transferencia de titularidad, los nuevos dueños u operadores solicitarán la evaluación de cumplimiento a la AAC para garantizar que se mantienen los requisitos de acreditación.

Anexo I.- 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
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
TCP/IP	Transmission Control. Protocol/Internet Protocol