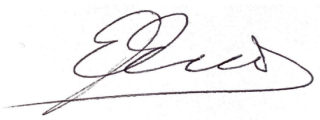
Entidad de Certificación

PSNET

UN MUNDO MEJOR POR LA TECNOLOGÍA



Firmado Digitalmente por
Eduardo J. Escardó de la Fuente

Declaración de Prácticas de Certificación

Información del documento

Nombre	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN
Realizado por	PERU SECURE E NET S.A.C.
Dirigido a	INDECOPI
Versión	1.5
Fecha	18/12/2019

Historial de versiones

Versión	Fecha	Descripción
1.0	28/02/2018	Elaboración de documento inicial.
1.1	25/08/2019	Ampliación de alcance de EC.
1.2	02/09/2019	Cambios menores referente al certificado de TSA
1.3	13/09/2019	Cambios menores en el Anexo B.
1.4	05/12/2019	Se tomaron recomendaciones de Auditoría Externa, se realizaron cambios.
1.5	18/12/2019	Cambios menores

ÍNDICE

1 INTRODUCCIÓN

PERU SECURE E NET S.A.C. (en adelante PERU SECURE) es una empresa peruana dedicada a propiciar el aumento de la productividad y eficiencia de las empresas, instituciones y comunidades del país a través del uso de herramientas tecnológicas de alta confiabilidad en telecomunicaciones y gestión de la información. PERU SECURE aprovecha la capacidad de Internet y las redes de telecomunicación en general, así como modernas técnicas de seguridad informática, para realizar transacciones e intercambio de información a distancia de manera ágil, eficiente y segura.

Para llevar a cabo los servicios de certificación digital, PERU SECURE cuenta con el respaldo de WISEKEY S.A. (en adelante WISEKEY), quien provee los servicios de emisión, re-emisión, distribución y revocación de certificados digitales. WISEKEY ha obtenido la certificación Webtrust for Certification Authorities.

Dentro de los servicios que ofrece PERU SECURE se encuentra la autenticación de sus clientes, tanto en el caso de personas jurídicas como naturales; y el registro de evidencias de dicha verificación.

2 OBJETIVO

Este documento tiene como objetivo la descripción de operaciones y prácticas que utiliza PERU SECURE para la administración de sus servicios como Entidad de Certificación Digital – EC, en el marco del cumplimiento de los requerimientos de la "Guía de Acreditación de Entidades de Certificación Digital (EC)" establecida por el INDECOPI.

3 OBJETO DE LA ACREDITACIÓN

El alcance de la acreditación cubre la infraestructura y procesos de los servicios de certificación digital brindados por PERU SECURE a través de la infraestructura provista y administrada por la empresa WISEKEY, la cual cuenta con la certificación Webtrust for Certification Authorities emitida por AICPA/CICA.

PERU SECURE representa a WISEKEY para todos los aspectos de mediación entre las personas jurídicas y naturales del Estado Peruano y la Entidad de Certificación WISEKEY.

La responsabilidad y garantías por los servicios de certificación digital son asumidos por WISEKEY.

4 DEFINICIONES Y ABREVIACIONES

Entidad de Certificación - EC	Entidad que presta servicios de emisión y revocación de certificados digitales en el marco de la regulación establecida por la IOFE.
Entidad de Registro - ER	Entidad que realiza los procesos de verificación de identidad de los solicitantes de los servicios de certificación digital.
Política de Certificación	Conjunto de reglas que indican el marco de aplicabilidad de los servicios para una comunidad de usuarios definida.
Acreditación	Acto a través del cual la Autoridad Administrativa Competente, previo cumplimiento de las exigencias establecidas en la Ley, en su Reglamento y en las disposiciones dictadas por ella, faculta a las entidades solicitantes reguladas en el Reglamento a prestar los servicios solicitados en el marco de la Infraestructura Oficial de Firma Electrónica.

Agente automatizado	Procesos y equipos programados para atender requerimientos predefinidos y dar una respuesta automática sin intervención humana, en dicha fase.
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.
Infraestructura Oficial de Firma Electrónica (IOFE)	POLÍTICADE CERTIFICACIÓN6Infraestructura 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) ylas Entidades de Registro o Verificación para el Estado Peruano (EREP).
Titular	Entidad que requiere los servicios provistos por la EC de PERU SECURE y que está de acuerdo con los términos y condiciones de los servicios conforme a lo declarado en el presente documento.
Tercero que confía	Persona que recibe un documento, log, o notificación firmado digitalmente, y que confía en la validez de las transacciones realizadas.
Sello de Tiempo	es un mecanismo en línea que permite demostrar que una serie de datos han existido y no han sido alterados desde un instante específico en el tiempo. Este protocolo se describe en el RFC 3161 y está en el registro de estándares de Internet

4.1 PARTICIPANTES

4.1.1 ENTIDAD DE CERTIFICACIÓN PERU SECURE (EC PERU SECURE)

PERU SECURE, en su papel de Entidad de Certificación, es la persona jurídica privada que presta indistintamente servicios de producción, emisión, gestión, cancelación u otros servicios inherentes a la certificación digital.

4.1.2 ENTIDAD DE REGISTRO PERU SECURE (ER PERU SECURE)

PERU SECURE brinda también los servicios de Entidad de Registro, la cual se encarga de certificar la validez de la información suministrada por el solicitante de un certificado digital, mediante la verificación de su identidad y su registro.

4.1.3 PROVEEDOR DE SERVICIOS DE CERTIFICACIÓN DIGITAL (WISEKEY)

Los proveedores de servicios de certificación son terceros que prestan su infraestructura o servicios tecnológicos a la Entidad de Certificación WISEKEY, cuando la Entidad de Certificación así lo requiere y garantizan la continuidad del servicio a los titulares durante todo el tiempo en que se hayan contratado los servicios de certificación digital.

Los servicios de certificación digital que se ofrecen son provistos por WISEKEY.

4.1.4 TITULAR

Titular es la persona natural o jurídica a cuyo nombre se expide un certificado digital y por tanto actúa como responsable del mismo confiando en él, con conocimiento y plena aceptación de los derechos y deberes establecidos y publicados en la CPS de WISEKEY.

La figura de Titular será diferente dependiendo de los distintos certificados emitidos por WISEKEY como prestador de servicios de PERU SECURE.

4.1.5 SUSCRIPTOR

Conforme a la IOFE, el Suscriptor es la persona natural responsable del 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 o por una autoridad de sellado de tiempo, 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.

4.1.6 SOLICITANTE

Se entenderá por Solicitante, la persona natural o jurídica que solicita un Certificado emitido bajo esta CPS.

En el caso de los certificados de persona natural puede coincidir con la figura del Titular.

4.1.7 TERCERO QUE CONFÍA

Tercero que confía son todas aquellas personas naturales o jurídicas que deciden aceptar y confiar en los certificados digitales emitidos por la Entidad de Certificación WISEKEY a un titular. El Tercero que confía, a su vez puede ser o no titular.

4.1.8 ENTIDAD A LA CUAL SE ENCUENTRA VINCULADO EL TITULAR

En su caso, la persona jurídica u organización a la que el Titular se encuentra estrechamente relacionado mediante la vinculación acreditada en el Certificado.

4.1.9 AUTORIDAD DE SELLADO DE TIEMPO

En su caso, la persona jurídica u organización a la que el Titular se encuentra estrechamente relacionado mediante la vinculación acreditada en el Certificado. Esta autoridad está destinada a emitir certificados para la emisión de sellos de tiempo. Un sello de tiempo es un paquete de datos con una estructura estandarizada donde se asocia el código resumen o código hash de un documento o transacción electrónica a una fecha y hora concreta.

La autoridad de sellado de tiempo emite certificados a entidades intermedias llamadas "Unidades de Sellado de Tiempo" TSU. Estas unidades de sellado son las que finalmente emiten los sellos de tiempo ante la recepción de una solicitud estandarizada que siga las especificaciones del RFC 3161. Cada una de estas TSU puede estar asociada, bien a unas características técnicas del servicio específicas, bien a un uso exclusivo de un cliente.

Bajo esta CPS se permite la emisión de certificados de TSU a empresas y organismos que residan fuera de territorio suizo. El procedimiento de emisión del certificado se tratará dentro del documento Solicitud de certificados Peru Secure v1.1 en el apartado 13. EMISIÓN DEL CERTIFICADO DIGITAL DE SELLO DE TIEMPO.

5 SERVICIOS DE CERTIFICACIÓN DIGITAL

PERU SECURE brinda los servicios de emisión, revocación y distribución de los certificados de WISEKEY.

Los certificados y las prácticas relacionadas a la gestión de su ciclo de vida son descritos en la Declaración de Prácticas y la Política de Certificación de WISEKEY:

https://www.wisekey.com/repository/cps_versions/

Los certificados son también descritos en la Política de Certificación de PERU SECURE:

http://www.perusecure.net/ArchivosEC.htm

6 RESPONSABILIDADES DE PERU SECURE

Las responsabilidades contractuales, garantías financieras y coberturas de seguros son brindadas por WISEKEY.

PERU SECURE representa a WISEKEY para todos los aspectos de ejecución de obligaciones contractuales, responsabilidad y mediación entre las personas jurídicas y naturales del Estado Peruano y la Entidad de Certificación.

Asimismo, PERU SECURE brinda los servicios de registro o verificación conforme a las Guías de Acreditación del INDECOPI, para realizar la verificación de identidad de las personas jurídicas y naturales solicitantes de los certificados digitales.

Las peticiones, quejas o reclamos sobre los servicios prestados por WISEKEY, son recibidas directamente por PERU SECURE. La línea telefónica y correo electrónico para la atención a

titulares y terceros para consultas relacionadas con el servicio que brinda PERU SECURE, se indica en la sección Persona de contacto del presente documento.

7 USO DEL CERTIFICADO

La EC de PERU SECURE cuenta con tipos de certificados digitales indicados en el documento "Solicitud de Certificados". Se emiten y revocan los siguientes tipos de certificados digitales:

- Persona Natural
- Profesional
- Persona Jurídica
- Agente Automatizado
- Sello de Tiempo

7.1 USO PERMITIDO DEL CERTIFICADO

El uso adecuado de los Certificados emitidos se encuentra especificado en la Política General de Certificación de WISEKEY, los certificados emitidos bajo esta CPS pueden ser utilizados con los siguientes propósitos:

Autenticación del cliente. El Titular del certificado puede autenticar, frente a otra parte, su identidad, demostrando la asociación de su clave privada con la respectiva clave pública, contenida en el certificado.

Firma digital. La utilización del certificado garantiza que el documento firmado es íntegro, es decir, garantiza que el documento no fue alterado o modificado después de firmado por el Titular, así como la identidad del Titular como firmante del documento. Se certifica que el mensaje recibido por el Receptor o Destino que confía es el mismo que fue emitido por el Titular.Y al vincular de manera inequívoca al titular con el documento firmado, le da características de "No Repudiable", es decir se garantiza que la persona que firma el documento no puede repudiar el documento firmado por el digitalmente. El titular que ha firmado no puede negar la autoría o la integridad del mismo.

Sello de tiempo. Es un certificado que se emite dentro de la Infraestructura Oficial de Firma Electrónica de acuerdo con 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

Uso permitido para personas natural, funcionarios de organización, corporaciones u organizaciones en general y para uso interno.

7.2 USO PROHIBIDO DEL CERTIFICADO

En general, cualquier uso que no esté explicado en la sección Uso Permitido del Certificado o en otra sección de este documento es considerado prohibido.

8 PERSONA DE CONTACTO

Datos de la Entidad de Certificación Digital y de Registro:

Nombre: PERU SECURE E NET S.A.C.
Dirección: Av. Nicolás Arriola 314 Of. 1001-La Victoria. Lima-Perú
Teléfono: +511 2253100

Correo electrónico: informes@perusecure.net
Página Web: www.perusecure.net

Datos de la Entidad Prestadora de Servicios de Certificación Digital:

Nombre: OISTE-WISeKey Global Trust Model (OWGTM)
Responsable: OWGTM Policy Approval Authority
Dirección: route de Pré-Bois,29 Case postale 885
Domicilio: Ginebra
Teléfono: +41 22 594 3000
Fax: +41 22 594 3001
Correo electrónico: cps@wisekey.com
Página Web: www.wisekey.com

9 RESPONSABILIDADES DE LOS TITULARES Y SUSCRIPTORES

Los usuarios y solicitantes de los certificados digitales provistos por PERU SECURE, son responsables de revisar la presente CPS y las Políticas de Certificación, a fin de ser enterados de las características de la plataforma de servicios, infraestructura y procedimientos empleados en la gestión del ciclo de vida de los certificados digitales, Raíz, Intermedios y de usuario final, así como las obligaciones de cada parte.

10 ORGANIZACIÓN QUE ADMINISTRA LOS DOCUMENTOS DE CP Y CPS

PERU SECURE administra los documentos de Declaración de Prácticas, y todos los documentos normativos de la EC de PERU SECURE.

Para cualquier consulta contactar:

- Nombre: Eduardo José Escardó de la Fuente
- Cargo: Gerente General
- Dirección de correo electrónico: informes@perusecure.net

11 PUBLICACIÓN DE LA DECLARACIÓN DE PRÁCTICAS

La Declaración de Prácticas de Certificación Digital– CPS de PERU SECURE, la Política y Plan de Privacidad, así como la Declaración de Prácticas y Política General de Certificación de PERU SECURE y otra documentación relevante son publicados en la siguiente dirección: www.perusecure.net

Todas las modificaciones relevantes serán comunicadas al INDECOPI y las nuevas versiones del documento serán publicadas en el mismo sitio web.

El presente documento es firmado por el responsable de la EC de PERU SECURE antes de ser publicado, y se controlan las versiones del mismo, a fin de evitar modificaciones y suplantaciones no autorizadas.

Los documentos referidos a la Declaración de Prácticas y Políticas de Certificación de los proveedores de PERU SECURE, así como la Declaración de Prácticas de las ER con las que tiene filiación serán publicados en la siguiente dirección: www.perusecure.net

12 RESPONSABILIDADES SOBRE REPOSITORIOS Y PUBLICACIÓN DE INFORMACIÓN

Certificado Raíz OWGTM como prestador de servicios de PERU SECURE

OISTE WISeKey Global Root GA CA

https://www.WISeKey.com/repository/cacertificates/

Certificados Subordinadas OWGTM como prestador de servicios de PERU SECURE

WISeKey CertifyID Advanced G1 CA https://www.WISeKey.com/repository/cacertificates/

- *WISeKey CertifyID Advanced Services CA 2*

https://www.WISeKey.com/repository/cacertificates/

- *WISeKey CertifyID Advanced Services CA 4*

https://www.WISeKey.com/repository/cacertificates/

Lista de Certificados Revocados (CRL)

OISTE WISeKey Global Root GA CA

http://public.WISeKey.com/crl/owgrgaca.crl

WISeKey CertifyID Advanced G1 CA

http://public.WISeKey.com/crl/wcidag1ca.crl

- *WISeKey CertifyID Advanced Services CA 2*

http://public.wisekey.com/crl/wcidasca2.crl

- *WISeKey CertifyID Advanced Services CA 4*

http://public.wisekey.com/crl/wcidasca4.crl

Declaración de Prácticas de Certificación (CPS)

PERU SECURE

http://www.perusecure.net/WISEKEY

https://www.WISeKey.com/repository/

12.1 PUBLICACIÓN DE LA INFORMACIÓN DE CERTIFICACIÓN

El responsable de la EC de PERU SECURE es el encargado de la autorización de la publicación de la CPS y es responsable de asegurar la integridad y disponibilidad de la información publicada en la página Web: www.perusecure.net

12.2 PLAZO O FRECUENCIA DE LA PUBLICACIÓN

Certificado Raíz

El certificado raíz se publicará y permanecerá en la página Web de la Entidad de Certificación PERU SECURE durante todo el tiempo en que se estén prestando servicios de certificación digital.

Certificado Subordinada

El certificado de la EC Subordinada se publicará y permanecerá en la página Web de la Entidad de Certificación PERU SECURE durante todo el tiempo en que se estén prestando servicios de certificación digital.

Lista de Certificados Revocados (CRL)

WISEKEY publicará en la página Web, la lista de certificados revocados en los eventos y con la periodicidad definidas en el numeral Frecuencia de emisión de las CRLs.

Declaración de Prácticas de Certificación (CPS)

Con autorización del responsable de la Entidad de Certificación de PERU SECURE y el INDECOPI, se publicará la versión finalmente aprobada. Los cambios generados en cada nueva versión serán previamente informados al INDECOPI y publicados en la página Web de la Entidad de Certificación de PERU SECURE junto con la nueva versión. La Auditoría anual validará estos cambios y emitirá el informe de cumplimiento.

12.3 CONTROLES DE ACCESO A LOS REPOSITORIOS

La consulta a los repositorios disponibles en la página Web de WISEKEY, antes mencionados, es de libre acceso al público en general. La integridad y disponibilidad de la información publicada es responsabilidad de WISEKEY, que cuenta con los recursos y procedimientos necesarios para restringir el acceso a los repositorios con otros fines diferentes a la consulta y a la página Web por parte de personas ajenas a WISEKEY.

13 IDENTIFICACIÓN Y AUTENTICACIÓN

13.1 NOMBRES

13.1.1 TIPOS DE NOMBRES

A todos los suscriptores se les asigna un Nombre Distintivo (DN) de acuerdo con el estándar X.501. Este DN está compuesto por un Nombre Común (CN), el cual incluye una identificación única del suscriptor como se describe en la sección Certificados del Suscriptor de la Entidad Final, y una estructura de componentes X.501 cómo se define en sección Reglas para la interpretación de varias formas de nombre.

13.1.1.1 Certificado raíz de WISEKEY como prestador de servicios de PERU SECURE

La descripción de cada tipo de certificado cubiertos por esta CPS, está detallada en la sección Perfiles de certificados, CRL y OCSP.

13.1.1.2 Certificados de las Subordinadas de WISEKEY como prestador de servicios de PERUSECURE

La descripción de cada tipo de certificado cubiertos por esta CPS, están detallado en la sección Perfiles de certificados, CRL y OCSP.

13.1.1.3 Certificados de titular de WISEKEY como prestador de servicios de PERU SECURE

La descripción de cada tipo de certificado cubiertos por esta CPS, está detallada en la sección Perfiles de certificados, CRL y OCSP.

13.1.2 NECESIDAD DE QUE LOS NOMBRES TENGAN SIGNIFICADO

Los nombres distintivos (DN) de los certificados emitidos por WISEKEY, como prestador de servicios de PERU SECURE, deben tener significado y la identificación de los atributos asociados al Suscriptor debe encontrase de forma verificable a través de un documento oficial nacional y/o internacional.

13.1.3 REGLAS PARA LA INTERPRETACIÓN DE VARIAS FORMAS DE NOMBRE

Las reglas utilizadas por WISEKEY, como prestador de servicios de PERU SECURE, para interpretar los nombres distintivos del Emisor y de los Titulares de certificados que emite, es el estándar ISO/IEC 9595 (X.500) Nombre Distintivo (DN).

13.1.4 SINGULARIDAD DE LOS NOMBRES

Los DN en WISEKEY, como prestador de servicios de PERU SECURE, deben ser únicos y nunca dar lugar a la ambigüedad entre los suscriptores asociados a una Entidad emisora en particular. Esto se consigue mediante un conjunto de técnicas y procedimientos implementados en varios niveles de la PKI, mediante la verificación de identidad del titular o suscriptor contra la base de datos del Registro Nacional de Identidad u otra entidad oficial pertinente, generalmente mediante la inclusión de una dirección de correo electrónico única, un número serial único de la organización relacionada con este, combinado-con / asociado-a un número serial único (como el # de Registro del Contribuyente).

13.2 RECONOCIMIENTO, AUTENTICACIÓN Y PAPEL DE MARCAS RECONOCIDAS

La inclusión de un nombre en un certificado no implica ningún derecho sobre ese nombre, ni para WISEKEY ni la demandante, ni el suscriptor. WISEKEY se reserva el derecho de rechazar una solicitud de certificado, o revocar una ya existente, si se detecta un conflicto sobre la propiedad de un nombre.

En cualquier caso, WISEKEY no intentará intermediar ni resolver los conflictos respecto a la propiedad de los nombres o marcas.

14 VALIDACIÓN INICIAL DE LA IDENTIDAD

14.1 MÉTODO PARA DEMOSTRAR LA POSESIÓN DE LA CLAVE PRIVADA

Si el par de claves es generado por la entidad final (solicitante o futuro suscriptor), a continuación, se solicita una demostración de la posesión de la clave privada asociada a la clave pública. Los medios aceptados son la generación de una solicitud de Firma de certificado (CSR) vinculado a la clave privada, o cualquier otro método aceptado por WISEKEY.

14.2 AUTENTICACIÓN DE LA IDENTIDAD DE UNA ORGANIZACIÓN (PERSONA JURÍDICA)

Los procedimientos de autenticación de la identidad de personas jurídicas son descritos en el documento de Declaración de Prácticas de Registro o Verificación del PERU SECURE– RPS.

No obstante, lo anterior, PERU SECURE y WISEKEY, se reservan el derecho de no expedir certificados cuando a su juicio se pueda poner en riesgo la credibilidad, valor comercial y/o idoneidad legal o moral de todo el sistema de certificación.

14.3 AUTENTICACIÓN DE UNA IDENTIDAD INDIVIDUAL (PERSONA NATURAL)

Los procedimientos de autenticación de la identidad de los titulares y suscriptores son descritos en el documento de Declaración de Prácticas de Registro o Verificación de PERU SECURE– RPS.

No obstante, lo anterior, PERU SECURE y WISEKEY, se reservan el derecho de no expedir certificados cuando a su juicio se pueda poner en riesgo la credibilidad, valor comercial y/o idoneidad legal o moral de todo el sistema de certificación.

14.4 AUTENTICACIÓN DE LA IDENTIDAD DE SISTEMAS DE INFORMACIÓN

Los procedimientos de autenticación de la identidad de sistemas de información son descritos en el documento de Declaración de Prácticas de Registro o Verificación de PERU SECURE– RPS.

No obstante, lo anterior, PERU SECURE y WISEKEY, se reservan el derecho de no expedir certificados cuando a su juicio se pueda poner en riesgo la credibilidad, valor comercial y/o idoneidad legal o moral de todo el sistema de certificación.

14.5 INFORMACIÓN DE TITULAR NO VERIFICADA

En general, cualquier información de identidad incluida en el componente Nombre comúnen el Certificado “CertifyID Standard Personal” y CertifyID Advanced Services.

Otra información no verificada del suscriptor, si se presenta, se hará relevante como un aviso en un componente de Unidad organizativa (OU) del certificado.

14.6 VALIDACIÓN DE LA AUTORIDAD

Los procedimientos de autenticación de validación son descritos en el documento de Declaración de Prácticas de Registro o Verificación de PERU SECURE– RPS.

14.7 CRITERIOS PARA LA INTEROPERABILIDAD

WISEKEY, como prestador de servicios de PERU SECURE, únicamente emitirá certificados a EC Subordinadas, que estén directamente vinculadas y operadas por WISEKEY.

15 IDENTIFICACIÓN Y AUTENTICACIÓN PARA PETICIONES DE RE-EMISIÓN DE CLAVES

15.1 IDENTIFICACIÓN Y AUTENTICACIÓN PARA RE-EMISIÓN DE RUTINA

Para entidades emisoras, WISKEY no admite la renovación de claves o renovaciones automatizadas. La entidad solicitante debe seguir una ceremonia formal de creación de clave de la EC y un operador designado apropiadamente debe verificar que la información contenida en el certificado de EC es válida.

Para los certificados de entidad final gestionados mediante una interfaz de ER aplicado o proporcionado por WISeKey S.A., el suscriptor o un Operador de registro autorizado puede utilizar sus credenciales de acceso para iniciar y aprobar, respectivamente, un certificado de cambio de la clave o renovación. Para clases distintas del Certificado "CertifyID Standard Personal" y "CertifyID Advanced Services" , el Operador de registro debe validar que los atributos de identidad a ser incluidos en el nuevo certificado siguen siendo válidos antes de aprobar la solicitud.

Los socios de WISEKEY que no utilizan la interfaz de ER proporcionada por WISEKEY, deben implementar los controles de seguridad adecuadas para garantizar que los niveles de seguridad no se ven afectados. Estos controles deben darse a conocer y ser aceptados por WISEKEY antes de que el socio comience sus operaciones.

15.2 IDENTIFICACIÓN Y AUTENTICACIÓN TRAS UNA REVOCACIÓN

WISEKEY, como prestador de servicios de PERU SECURE, no admite la renovación de clave de los certificados después de una revocación. El suscriptor debe solicitar un nuevo certificado digital mediante el uso de los procedimientos para su emisión.

16 IDENTIFICACIÓN Y AUTENTICACIÓN PARA PETICIONES DE REVOCACIÓN

La política de identificación para las solicitudes de revocación es la misma que se estipula para el registro inicial. Las solicitudes telemáticas solo serán aceptadas si estas incluyen una firma digital utilizando el certificado digital diferente al que está solicitando el suscriptor que sea revocado, o el certificado de un tercero que está autorizado a solicitar la revocación en nombre del suscriptor.

PERU SECURE puede definir, que, durante el proceso de inscripción, un suscriptor puede crear una contraseña que se puede utilizar en las solicitudes de revocación remotas, utilizando un procedimiento online comunicado al usuario cuando se expide el certificado.

WISEKEY, como prestador de servicios de PERU SECURE, puede solicitar la revocación de un certificado si hay conocimiento o sospecha fundada de que la clave privada asociada ha sido comprometida, o razones para creer cualquier otro dato que recomienda esta acción.

17 REQUISITOS OPERACIONALES PARA EL TIEMPO DE VIDA DE LOS CERTIFICADOS

17.1 SOLICITUD DEL CERTIFICADO

Las Entidades de registro que operan bajo PERU SECURE son las competentes y responsables de determinar si el tipo de certificado solicitado es adecuado para el solicitante y futuro suscriptor, de conformidad con la Política de Certificación en relación con dicho certificado, y por lo tanto proceder o no con la solicitud del certificado.

17.2 QUIÉN PUEDE SOLICITAR UN CERTIFICADO

Una solicitud de certificado puede ser presentada por el titular del certificado o por un representante autorizado por él.

17.3 PROCESO DE REGISTRO Y RESPONSABILIDADES

El proceso de registro, incluyendo la información verificada y las atribuciones para ejecutar el proceso se detalla en la Declaración de Prácticas de Registro de PERU SECURE (RPS).

18 TRAMITACIÓN DE SOLICITUD DE CERTIFICADOS

18.1 REALIZACIÓN DE LAS FUNCIONES DE IDENTIFICACIÓN Y AUTENTICACIÓN

Este proceso se detalla en la Declaración de Prácticas de Registro de PERU SECURE (RPS).

18.2 APROBACIÓN O RECHAZO DE LAS SOLICITUDES DE CERTIFICADO

Este proceso se detalla en la Declaración de Prácticas de Registro de PERU SECURE (RPS).

18.3 PLAZO PARA PROCESAR LAS SOLICITUDES DE CERTIFICADO

Este proceso se detalla en la Declaración de Prácticas de Registro de PERU SECURE(RPS).

19 EMISIÓN DE CERTIFICADOS

19.1 ACTUACIONES DE LA EC DURANTE LA EMISIÓN DE CERTIFICADOS

La EC de PERU SECURE adherida a WISEKEY procede a emitir un certificado solo después de la ejecución de las medidas necesarias para verificar que la petición recibida por la Entidad de Registro de PERU SECURE es genuina. Los controles específicos son la verificación de identidad del suscriptor, firma de la solicitud-contrato y cumplimiento de la RPS de PERU SECURE.

19.2 NOTIFICACIÓN AL SOLICITANTE POR LA EC DE LA EMISIÓN DEL CERTIFICADO

Después de ser emitido un certificado, la EC notifica a la ER de la emisión y la disponibilidad del certificado, y el nuevo certificado se publica en el repositorio de certificados.

El mecanismo de notificación puede ser acordado específicamente con el suscriptor. En general, para los certificados personales, la ER es responsable de notificar al suscriptor de la disponibilidad de su certificado, enviándole una copia o mediante la especificación de cómo se puede obtener el certificado.

Las notificaciones electrónicas pueden ser firmadas digitalmente por la ER o representante habilitado.

20 ACEPTACIÓN DEL CERTIFICADO

20.1 FORMA EN LA QUE SE ACEPTA EL CERTIFICADO

La aceptación del certificado queda entendida después de que el suscriptor o su representante lleva a cabo uno o más de los siguientes puntos:

- Se firma el "Acuerdo del suscriptor o titular", que incluye los términos y condiciones asociadas con la política de certificado, y que constituye la aceptación formal de los términos;

- Se descarga y/o instala el certificado, por lo que es técnicamente disponible para el uso;

- No se rechaza explícitamente el certificado una vez que la disponibilidad de la notificación ha sido enviada.

20.2 PUBLICACIÓN DEL CERTIFICADO POR LA EC

Las entidades emisoras que operan bajo WISEKEY publican todos los certificados emitidos.

20.3 NOTIFICACIÓN DE LA EMISIÓN DEL CERTIFICADO POR LA EC A OTRAS ENTIDADES

No aplica.

21 USO DE LA CLAVE PRIVADA Y DEL CERTIFICADO

21.1 USO DE LA CLAVE PRIVADA Y DEL CERTIFICADO POR EL TITULAR POR TERCEROS QUE CONFIAN

Los usos específicos permitidos para una clave privada asociada a un tipo de certificado expedido en WISEKEY son tal y como se detalla en la sección Uso permitido del certificado del presente documento.

21.2 USO DE LA CLAVE PÚBLICA Y DEL CERTIFICADO POR TERCEROS QUE CONFÍAN

El tercero que confía debe acceder y utilizar la clave pública y certificado conforme a lo estipulado en la presente CPS y tal como se indica en el documento "Acuerdo del tercero que confía", hecho público en la página web http://www.wisekey.com/repository.

22 MODIFICACIÓN DE CERTIFICADOS

WISEKEY, como prestador de servicios de PERU SECURE, no permite la modificación de los certificados durante su periodo de validez. Si la información contenida en un certificado deja de

ser válido, o las circunstancias del suscriptor cambian de manera tal que las condiciones expresadas en la CPS o CP no se cumplen, entonces el único procedimiento aceptado es la revocación del certificado digital.

23 REVOCACIÓN DE CERTIFICADOS

23.1 CIRCUNSTANCIAS PARA LA REVOCACIÓN DE UN CERTIFICADO

La EC que opere bajo WISEKEY debe revocar un certificado que ha emitido, sobre la ocurrencia de cualquiera de los siguientes eventos:

1. El suscriptor solicita la revocación de su certificado.

2. El suscriptor indica que el certificado original no estaba autorizado y no le concede retroactivamente la autorización.

3. La EC obtiene evidencia razonable de que la clave privada del suscriptor (correspondiente a la clave pública en el certificado) ha sido comprometida o se sospecha de compromiso, o de lo contrario el certificado ha sido mal utilizado.

4. La EC recibe aviso o caso contrario se da cuenta de que un suscriptor ha violado una o más de sus obligaciones fundamentales bajo el contrato de suscriptor o condiciones de uso.

5. La EC recibe aviso o caso contrario se da cuenta de que un tribunal o árbitro ha revocado el derecho de un suscriptor para utilizar un nombre (por ejemplo, un nombre de dominio) que aparece en el certificado, o que el suscriptor no ha logrado renovar su derecho a utilizar ese nombre.

6. La EC recibe aviso o de lo contrario se da cuenta de un cambio sustancial en la información contenida en el certificado.

7. Una determinación, a la sola discreción de la autoridad competente, de que el certificado no ha sido emitido de conformidad con los términos y condiciones derivadas de la política de certificación apropiada

8. La EC determina que alguna de la información que aparece en el certificado no es exacta.

9. La EC cesa su actividad por cualquier razón y no ha dispuesto otra EC bajo WISeKey para proporcionar soporte de revocación del certificado.

10. El derecho de la EC de emitir certificados para una política de certificado expira o es revocado o terminado, a menos que la EC haga los arreglos para seguir manteniendo el repositorio CRL/OCSP.

11. La clave privada de cualquier EC en el curso de certificación se sospecha que ha sido comprometida.

12. El suscriptor es un participante en el PKI (por ejemplo, Registro Operador) y pierde su derecho de acceso para seguir actuando como tal.

13. La EC recibe aviso o de lo contrario se da cuenta de que un suscriptor se ha añadido como una parte denegada o persona prohibida de una lista negra, o está operando desde un lugar o de una manera que está prohibida en virtud de las leyes y la jurisdicción del país de operación de la EC.

23.2 QUIÉN PUEDE SOLICITAR UNA REVOCACIÓN

El suscriptor o representante legal pueden solicitar la revocación de un certificado individual u organizacional.

La ER autorizada o representante titulado pueden solicitar la revocación de un certificado si se presenta alguna de las circunstancias expresadas en el apartado anterior.

23.3 PROCEDIMIENTO DE SOLICITUD DE REVOCACIÓN

El procedimiento que se utiliza para las solicitudes de revocación de certificados se detalla en la "Solicitud-Contrato".

Los usuarios individuales podrán encontrar el contacto adecuado e información del procedimiento en el URL

http://www.wisekey.com/repository

La práctica común para todos los certificados emitidos bajo el Modelo de confianza (Trust Model) de WISeKey es para las solicitudes de revocación sean aceptadas de forma automática y produzcan una revocación inmediata en el caso de:

- Solicitudes remotas enviadas por correo electrónico o a través de una página web o servicio, debidamente autenticados por el suscriptor o su representante.

- Las solicitudes presenciales dirigidas a un representante de la ER operador y la identidad del solicitante se demuestran por el mismo medio que el utilizado para el registro de certificados.

- Las solicitudes de revocación enviados por un representante operador de registro o certificación que opere bajo el Modelo de confianza (Trust Model) de WISeKey.

Las solicitudes de revocación comunicadas por otros medios (es decir, por no firmar mensajes electrónicos o por teléfono), que no se autentican de manera inequívoca al solicitante va a producir la revocación del certificado., tal como se define en las secciones relativas a la Suspensión del certificado.

23.4 PERIODO DE GRACIA DE SOLICITUD DE REVOCACIÓN

No se estipula un periodo de gracia para las solicitudes de revocación. El proceso de revocación se iniciará inmediatamente después de la recepción de dicha solicitud por la ER o EC.

23.5 PLAZO EN EL QUE LA EC DEBE RESOLVER LA SOLICITUD DE REVOCACIÓN

Las solicitudes de revocación son procesadas por la EC en un periodo no mayor a 24 horas.

23.6 REQUISITOS DE VERIFICACIÓN DE LAS REVOCACIONES POR LOS TERCEROS QUE CONFÍAN

WISEKEY, como prestador de servicios de PERU SECURE, requiere que todos los terceros que confían en los certificados expedidos de conformidad con el Modelo de confianza (Trust Model), comprueben el estado de estos certificados en cada solicitud de verificación de firmay autenticación digital utilizando el certificado. Este requisito puede cumplirse mediante la consulta de la CRL más reciente de la EC que emitió el certificado o mediante el servidor Online Certificate Status Protocol de WISeKey (referido como WISeKey OCSP).

La información necesaria para localizar estos servicios de revocación, se incluye en todos los certificados WISeKey, utilizando el estándar CDP y/o extensiones AFP.

23.7 FRECUENCIA DE EMISIÓN DE LAS CRLS

Las frecuencias estipuladas son:

- La EC Raíz de WISEKEY emite una CRL completa todos los años, con un periodo de latencia de una semana. Esta CRL contendrá los certificados revocados por la Política de EC de WISEKEY o ECs emisoras, según corresponda a la jerarquía. Las nuevas CRLs se publican inmediatamente si una nueva EC subordinada se revoca.

- La Política de EC de WISEKEY emite una CRL completa todos los meses, con un periodo de latencia de 1 hora. Esta CRL contendrá los certificados, en su caso, revocados para las ECs emisoras de WISEKEY. La nueva CRL se publica inmediatamente si una nueva EC subordinada se revoca.

- La Política de ECs emisoras de WISEKEY emite una CRL completa cada 24 horas, con una latencia máxima de 1 hora en caso de interrupción del servicio. Esta CRL contendrá los certificados, en su caso, revocados para los usuarios finales/suscriptores de WISEKEY.

23.8 TIEMPO MÁXIMO DE LATENCIA DE LAS CRLS

El tiempo entre la generación y publicación de la CRL es mínimo debido a que la publicación es automática, menor a una hora como lo establece el INDECOPI.

23.9 REVOCACIÓN ON-LINE/DISPONIBILIDAD DE VERIFICACIÓN DEL ESTADO

WISEKEY, como prestador de servicios de PERU SECURE, publicará tanto la CRL como el estado de los certificados revocados en repositorios de libre acceso y fácil consulta, con disponibilidad 7X24 durante todos los días del año. La disponibilidad del servicio OCSP no es obligatorio para los certificados de garantía bajos, como el Certificado “CertifyID Standard Personal”.

La URL utilizada para acceder a este servicio está incluido en la "extensión AIA" en todos los certificados emitidos.

Para ciertos Certificados de la EC emisora se podría publicar en servicios online, web-based u otros.

Estos servicios adicionales están estipulados en el “Contrato de suscriptor/titular”.

23.10 REQUISITOS DE COMPROBACIÓN DE LA REVOCACIÓN ON- LINE

La comprobación de la revocación online se ofrece abiertamente sin restricción a todos los participantes en la PKI.

Se solicita a los terceros que confían verificar siempre la validez del certificado en la que se basan, según lo estipulado en el apartado *Requisitos de verificación de las revocaciones por los terceros que confían.*

23.11 OTRAS FORMAS DISPONIBLES DE DIVULGACIÓN DE INFORMACIÓN DE REVOCACIÓN

No se estipula.

23.12 REQUISITOS ESPECIALES DE RENOVACIÓN DE CLAVES COMPROMETIDAS

Cualquier tercero que detecte un compromiso de la clave en cualquier nivel del Modelo de confianza (Trust Model) es requerido para comunicar inmediatamente esto a la Entidad de Registro o a la Entidad de Certificación.

24 SERVICIOS DE INFORMACIÓN DEL ESTADO DE CERTIFICADOS

24.1 CARACTERÍSTICAS OPERACIONALES

Los servicios de estado de certificados son accesibles a través de servidores HTTP pertenecientes a las EC de WISEKEY. Se puede acceder a los servicios mediante la descarga de listas de revocación (CRL) o mediante el envío de solicitudes a los servidores OCSP.

Las direcciones URL de servicios de información de revocación de certificados apropiados se incluyen en las extensiones estándar dentro de los certificados emitidos.

Otros servicios podrían estar disponibles, según lo estipulado en el "Contrato de suscriptor/titular" correspondiente.

24.2 DISPONIBILIDAD DEL SERVICIO

El servicio de consulta del estado de certificados digitales tiene una disponibilidad mínima de 99% anual, con un tiempo programado de inactividad máximo de 1% y con una frecuencia mínima de actualización de 24 horas.

24.3 CARACTERÍSTICAS OPCIONALES

No se estipula.

24.4 FINALIZACIÓN DE LA SUSCRIPCIÓN

La finalización de la suscripción se produce después de la expiración de un certificado, y es solo en ese caso, que no afecta a las suscripciones adicionales (si las hay) que la entidad final puede llevar a cabo dentro de WISEKEY. También, cuando un suscriptor elija finalizar su suscripción como parte de la IOFE o la EC termine su suscripción al mismo, por fallecimiento del suscriptor o extinción de la persona jurídica que es titular del certificado

25 CUSTODIA Y RECUPERACIÓN DE CLAVES

25.1 ALMACENAMIENTO DE LA CLAVE PRIVADA DEL TITULAR

Solo se permite el depósito de garantía de los certificados de suscriptor/titular. Para los certificados de infraestructura, como EC, ER o de otros, las políticas de copia de seguridad apropiadas deben ser implementadas, según la sección *Backup de la clave privada*.

25.2 PRÁCTICAS Y POLÍTICAS DE CUSTODIA Y RECUPERACIÓN DE CLAVES

WISEKEY, como prestador de servicios de PERU SECURE, no ofrece el servicio de custodia y recuperación de claves en ningún caso. Las ECs o ERs emisoras con el acceso a través de una interfaz de "Managed PKI", pueden aplicar diferentes procedimientos para el depósito de claves, siendo obligatoria en tal caso una comunicación explícita de tales características al suscriptor del certificado.

En particular, WISEKEY no recomienda ningún tipo de depósito en garantía o respaldo de las claves privadas habilitadas para las firmas digitales, siempre y cuando el usuario final sea la única entidad que tiene acceso efectivo a esta información.

25.3 PRÁCTICAS Y POLÍTICAS DE CUSTODIA Y RECUPERACIÓN DE LA CLAVE DE SESIÓN

Si se implementa el depósito de claves, de acuerdo con las consideraciones anteriores, cualquier clave de sesión que permite el descifrado de una clave privada debe mantenerse bajo el control exclusivo del suscriptor del certificado o representante autorizado.

26 CONTROLES FÍSICOS DE LA INSTALACIÓN, GESTIÓN Y OPERACIONALES

26.1 CONTROLES FÍSICOS DE LA INFRAESTRUCTURA TECNOLÓGICA A TRAVÉS DE WISEKEY COMO PRESTADOR DE SERVICIOS DE PERU SECURE

26.1.1 UBICACIÓN FÍSICA Y CONSTRUCCIÓN

Los sistemas de información WISEKEY, como prestador de servicios de PERU SECURE, se encuentran en el Centro de Datos Seguros que proporcionan niveles de seguridad adecuados y bajo vigilancia las 24 horas del día, los 7 días a la semana. Este Centro de Datos está construido de tal manera que los riesgos físicos críticos correspondientes estén controlados.

26.1.2 ACCESO FÍSICO

El Centro de Datos Seguros de WISEKEY, como prestador de servicios de PERU SECURE, implementa diversos perímetros de seguridad. El acceso desde un externo hacia un perímetro interno requiere diferentes controles de seguridad y autorización. Entre estos controles se implementan la puerta de acceso biométrico, sistemas de video vigilancia y detección de intrusos.

26.1.3 ALIMENTACIÓN ELÉCTRICA Y AIRE ACONDICIONADO

Las instalaciones de WISEKEY, como prestador de servicios de PERU SECURE, están equipadas con sistemas de alimentación ininterrumpida (SAI) con capacidad suficiente para mantener de forma autónoma los sistemas WISEKEY durante los cortes de energía eléctrica y proteger estos sistemas de los daños que puedan deberse a fluctuaciones de energía.

Los sistemas de aire acondicionado utilizados en WISEKEY se componen de un equipo independiente que asegura los márgenes operativos de temperatura y humedad en el interior del Centro de Datos Seguros.

26.1.4 EXPOSICIÓN AL AGUA

Las instalaciones de WISEKEY, como prestador de servicios de PERU SECURE, están ubicadas en un lugar donde se controlan los riesgos de inundación naturales, además de encontrarse equipadas con sensores de inundación y alarmas.

26.1.5 PREVENCIÓN Y PROTECCIÓN DE INCENDIOS

Las instalaciones de WISEKEY, como prestador de servicios de PERU SECURE, implementan controles de detección de incendios, prevención y protección

26.1.6 SISTEMA DE ALMACENAMIENTO

Los medios de información confidencial se almacenan de forma segura en contenedores a prueba de fuego y cajas fuertes de alta seguridad, en función del tipo de soporte y la clasificación de la información que contienen.

Estos contenedores y cajas fuertes se encuentran en ubicaciones redundantes, con el fin de eliminar los riesgos del uso en una sola ubicación (es decir, en caso de incendio o daño por agua).

El acceso a estos lugares de almacenamiento y los artículos está restringido a personas autorizadas y regulada por procedimientos de seguridad.

26.1.7 ELIMINACIÓN DEL MATERIAL DE ALMACENAMIENTO DE LA INFORMACIÓN

La eliminación de desechos de papel y medios de comunicación ópticos o magnéticos que contienen cualquier información generada durante las operaciones WISEKEY, se ejecuta siguiendo los procedimientos establecidos para tales fines, incluyendo los procesos de destrucción y/o de desmagnetización, dependiendo del tipo de medio a ser eliminado.

26.1.8 BACKUP FUERA DE LA INSTALACIÓN

Diariamente WISEKEY, en calidad de prestador de servicios de PERU SECURE, realiza una copia de seguridad de toda la información necesaria para promover un centro de datos secundario al estado operativo en el caso de un desastre.

De forma periódica, se hace una copia de seguridad remota y se almacena de manera tal que se requiere un control de acceso doble para restaurar las copias de seguridad.

26.2 CONTROLES DE PROCEDIMIENTO

26.2.1 ROLES DE CONFIANZA

WISEKEY establece y hace cumplir una política de seguridad estricta para controlar todas las operaciones realizadas en cualquier nivel del Modelo de confianza (Trust Model). Esto incluye la identificación y el control de las personas que realicen estas operaciones. Estas personas se consideran "Roles de confianza" e incluyen, pero no se limitan a:

- Director de la Entidad de Certificación
- Administrador de la Entidad de Certificación
- Operador de la Entidad de Certificación
- Director de la Entidad de Registro
- Administrador de la Entidad de Registro
- Operador de la Entidad de Registro
- Operador del Punto de Registro
- Director de Soporte, Capacitación y Comunicación
- Consejero legal
- Director de la documentación
- Administrador de sistemas
- Gerente de seguridad
- Administrador de Seguridad y del operador
- Autoridad de Aprobación de Políticas

Las personas que quieran obtener dichos Roles de confianza deben completar con éxito los requisitos de selección establecidos en la presente CPS, sección *Controles de personal.*

26.2.2 NÚMERO DE PERSONAS REQUERIDAS POR TAREA

WISEKEY, como prestador de servicios de PERU SECURE, establece la necesidad de segregar funciones en base a la responsabilidad del trabajo con el fin de garantizar el número adecuado de Roles de confianza para realizar tareas confidenciales.

Las funciones que requieren la separación de funciones se estipula en la sección *Roles que requieren segregación de funciones*.

26.2.3 IDENTIFICACIÓN Y AUTENTICACIÓN PARA CADA ROL

Todas las personas que asuman un rol en los sistemas de WISEKEY siguen un proceso de autorización que les da derecho a acceder a la información y los sistemas apropiados para su función.

El control de acceso físico para todas las personas autorizadas que acceden a los sistemas y servicios de sistemas de WISEKEY típicamente se ve impuesto mediante la autenticación de dos factores que por lo general incluye la biometría.

26.2.4 ROLES QUE REQUIEREN SEGREGACIÓN DE FUNCIONES

Los roles que requieren separación de funciones incluyen al menos los siguientes:

- La habilitación de una EC en un estado de producción (Ceremonia de procedimientos EC)

- La emisión o revocación de certificados de la EC

- Validación de la información y la emisión de certificados de alta seguridad del suscriptor

26.3 CONTROLES DE PERSONAL

26.3.1 REQUISITOS SOBRE LA CUALIFICACIÓN, EXPERIENCIA Y CONOCIMIENTO PROFESIONALES

Se requiere que el personal que actúa directa o indirectamente para la WISEKEY posea la titulación requerida y/o experiencia demostrada en relación a la prestación de servicios de certificación. Además, se requiere que todo el personal involucrado actúe de acuerdo con la Política de Seguridad de WISEKEY y poseer lo siguiente:

- El conocimiento y la formación (de acuerdo con el papel asignado a la persona) en Infraestructuras de Clave Pública.

- El conocimiento y la formación (de acuerdo con el papel) en Sistemas de Información de Seguridad.

- El conocimiento y la formación específica de las responsabilidades asignadas.

26.3.2 PROCEDIMIENTO DE COMPROBACIÓN DE ANTECEDENTES

El Departamento de Recursos Humanos realiza las comprobaciones de verificación en el personal permanente en el momento de las solicitudes de empleo, y se asegura de que todo el personal con acceso a información confidencial es digno de confianza y comprende sus responsabilidades; esto incluye, como mínimo, lo siguiente:

- Disponibilidad y verificación de referencias satisfactorias;

- La confirmación de las calificaciones académicas y profesionales reivindicadas;
- Los controles de identidad de pasaporte o documento similar.

26.3.3 REQUISITOS DE FORMACIÓN

El personal implicado en WISEKEY, incluyendo las ECs emisoras operadas por terceros y las ER, seguirán un plan de formación interna adaptada a sus atribuciones asignadas. Esta formación será compatible con las normas de la industria, como el EC/Línea Base del Foro Internacional y/o requisitos de Validación extendida, según sea el caso.

26.3.4 REQUISITOS Y FRECUENCIA DE ACTUALIZACIÓN DE FORMACIÓN

Se requieren sesiones de actualización para todo el personal involucrado en el caso del medio ambiente, la tecnología y/o cambios operativos. Los cambios en las prácticas y/o políticas se comunican a todo el personal involucrado.

26.3.5 FRECUENCIA Y SECUENCIA DE ROTACIÓN DE TAREAS

No se estipula.

26.3.6 SANCIONES POR ACTUACIONES NO AUTORIZADAS

En caso WISEKEY, como proveedor de servicios de PERU SECURE, detecte una acción no autorizada, emprenderá las acciones disciplinarias necesarias. Cualquier acción que (intencionalmente o no) contraviene la Declaración de Prácticas de Certificación.

Tras la detección de una acción no autorizada, WISEKEY iniciará un proceso de investigación. Durante este proceso se evitará que las personas involucradas obtengan acceso a los sistemas e información de WISEKEY.

Las medidas disciplinarias serán tomadas después de la investigación determine la gravedad y la intención de la acción.

26.3.7 REQUISITOS DE CONTRATACIÓN DE TERCEROS

Se requiere que los contratistas externos estén de acuerdo con las Políticas de seguridad de la información de WISEKEY, y el personal temporal no amparado por un acuerdo de confidencialidad existente también estará obligado a firmar el acuerdo de confidencialidad antes de concederse el acceso a los recursos de información.

El acuerdo se examina cuando existen cambios en las condiciones de empleo o contratos.

26.3.8 DOCUMENTACIÓN PROPORCIONADA AL PERSONAL

A todo el personal incorporado dentro de WISEKEY se le proporciona el acceso a por lo menos la siguiente información:

- Declaración de Prácticas de Certificación
- Políticas de Certificación
- Política de Privacidad
- Política de Seguridad

- Organigrama y funciones y responsabilidades asignadas

- Procedimientos operacionales

- Procedimientos de respuesta a incidentes

26.3.9 FIN DEL CONTRATO Y PROCEDIMIENTO DE CAMBIO DE ROLES ASIGNADOS

En el caso de que un contrato finalice o se cambie el papel asignado a una persona, WISEKEY se asegura de que se ejecute el procedimiento correspondiente. Este procedimiento incluye al menos los cambios necesarios en los privilegios concedidos a las instalaciones de acceso, sistemas de información y documentación.

El material asignado (tarjetas inteligentes, ordenadores, etc.) será devuelto o reasignado como sea necesario.

El cambio o terminación será notificado a todas las partes involucradas.

26.4 PROCEDIMIENTOS DE AUDITORÍA DE SEGURIDAD

26.4.1 TIPOS DE EVENTOS REGISTRADOS

WISEKEY, en calidad de prestador de servicios de PERU SECURE, registra en sus servidores todos los eventos relacionados a:

- Eventos de administración con relación al ciclo de vida del par de claves de la EC, que incluyen:

  a. La generación de claves, copia de seguridad, almacenamiento, recuperación, archivo y destrucción tal como se expone en la documentación de procedimiento

  b. Eventos de administración de ciclo de vida del dispositivo criptográfico tal como se expone en la documentación de procedimiento

- Eventos de administración con relación al ciclo de vida del Certificado del Suscriptor, entre otros:

  a. Las solicitudes de revocación de certificados tal como se expone en los registros de la EC

  b. Las actividades de verificación

  c. Fecha, hora, número de teléfono utilizado, personas con las que se habló, y los resultados finales de las llamadas telefónicas de verificación tal como lo exponen los Operador de registro

  d. La aceptación y el rechazo de las solicitudes de certificados tal como se expone en los registros de la EC

  e. La emisión de certificados tal como se expone en los registros de la EC

  f. Generación de listas de certificados revocados tal como se expone en los registros de la EC (NB CRL no se conservan, solo el registro de su generación)

  g. Generación de entradas OCSP que pueda ser capturado por los registros del servidor OCSP disponibles (entradas NB OCSP no se conservan, solo el registro de su generación si es registrado por el servidor OCSP)

- Los eventos de seguridad, incluyendo:

a. Los intentos de acceso al sistema PKI exitosos y no exitosos, tal como se expone en los registros del sistema operativo

b. Las principales acciones de PKI y del sistema de seguridad llevadas a cabo, tal como se expone en los registros del sistema operativo

c. Cambios en el perfil de seguridad, tal como se expone en los registros del sistema operativo

d. Los fallos del sistema, fallos de hardware y otras anomalías en los registros del servidor

e. Actividades de firewalls y routers, tal como se expone en los registros del dispositivo

f. Las entradas y salidas de la instalación de la EC, tal como se expone en los registrosde control de acceso.

26.4.2 FRECUENCIA DE PROCESADO DE REGISTROS DE AUDITORÍA (LOG)

La revisión de los logs se realiza cuando se detecte una alerta de seguridad o existan indicios de un funcionamiento no usual de los sistemas.

Los registros son procesados y auditados de forma regular.

Para los sistemas que se mantienen fuera de línea, como la EC Raíz, los registros de auditoría se recogen solamente cuando se ejecuta una operación.

26.4.3 PERIODO DE RETENCIÓN DE LOS REGISTROS DE AUDITORÍA

WISEKEY y las partes implicadas conservan todos los registros de auditoría como se especifica en la sección *Periodo de conservación*.

26.4.4 PROTECCIÓN DE LOS REGISTROS DE AUDITORÍA

Todos los registros de auditoría y los archivos se guardan en armarios a prueba de fuego, y solo es accesible para personas autorizadas.

La destrucción de un registro de auditoría solo puede ejecutarse después de la autorización firmada por el auditor de WISEKEY y el Administrador de seguridad de la información de WISEKEY. Un rastro de los materiales destruidos se mantiene para futuras referencias.

26.4.5 PROCEDIMIENTOS DE BACKUP DE LOS REGISTROS DE AUDITORÍA

Los registros de auditoría están respaldados mediante procedimientos graduales y remotos.

26.4.6 SISTEMA DE RECOGIDA DE INFORMACIÓN DE AUDITORÍA (INTERNA O EXTERNA)

El sistema de recogida de registros de auditoría en WISEKEY es una combinación de procesos automáticos y manuales, y es ejecutado por los sistemas operativos adecuados, aplicaciones de software, y el personal de operación de estos sistemas.

26.4.7 NOTIFICACIÓN AL SUJETO CAUSA DEL EVENTO

No se estipula.

26.4.8 ANÁLISIS DE VULNERABILIDADES

WISEKEY, como prestador de servicios de PERU SECURE, realiza una evaluación periódica de la vulnerabilidad mediante el control de los registros de actividad. Las evaluaciones a profundidad y los controles se realizan sobre una base anual, incluyendo la conformidad con los planes de recuperación de desastres. En el caso de que una evaluación no logre realizarseo se retrase, WISEKEY informará a las partes involucradas los registros de tal evento y su causa se mantendrá para futuras consultas.

Este análisis de la seguridad implica la identificación de las tareas necesarias para corregir las vulnerabilidades detectadas.

26.5 ARCHIVO DE REGISTROS

26.5.1 TIPOS DE EVENTOS ARCHIVADOS

La información y los eventos archivados son:

- La información generada (en la EC y ER) durante el ciclo de vida de todos los certificados WISEKEY,
- Los contratos y acuerdos,
- Los registros de auditoría estipulados en la sección *Procedimientos de auditoría de seguridad* de la presente CPS.

26.5.2 PERIODO DE CONSERVACIÓN

Los registros archivados y los registros de auditoría se mantienen registros y se conservarán al menos durante diez (10) años luego de su expiración o revocación.

26.5.3 PROTECCIÓN DE ARCHIVOS

El acceso a los materiales de archivo está restringido a personas autorizadas para se haga garantizar la integridad del archivo.

26.5.4 PROCEDIMIENTOS DE BACKUP DEL ARCHIVO DE REGISTROS

Las copias de seguridad se ejecutan diariamente. La copia principal se mantiene en el centro principal de WISEKEY y se almacena dentro de una zona protegida. Las copias son encriptadas periódicamente y de forma remotamente almacenadas fuera del sitio.

26.5.5 REQUISITOS PARA EL SELLADO DE TIEMPO DE LOS REGISTROS

Además de las estipulaciones mencionadas en el apartado *Protección de archivos*, el sellado de tiempo está incluido en los registros firmados digitalmente. El sellado de tiempo no tiene por qué ser de la naturaleza criptográfica.

26.5.6 SISTEMA DE ARCHIVO DE LA INFORMACIÓN DE AUDITORÍA (INTERNA O EXTERNA)

El sistema de archivo es una tarea interna en WISEKEY que no puede ser encargada a terceros.

Con la única excepción de puntos de Entidad de Registro autorizados, a los cuales se les permite archivar la información recogida durante el ciclo de vida de los certificados. En ese caso, esta información debe mantenerse de forma segura, accesible solo para personas autorizadas, y estará disponible para cualquier entidad de auditoría interna o externa exigida por WISEKEY.

26.5.7 PROCEDIMIENTOS PARA OBTENER Y VERIFICAR INFORMACIÓN ARCHIVADA

Solo personal autorizado puede obtener acceso a los medios físicos que contienen archivos, copias de seguridad y otra información registrada.

Las comprobaciones de integridad se realizan automáticamente si el archivo incluye una firma digital.

26.6 CAMBIO DE CLAVES DE UNA EC

WISEKEY, como prestador de servicios de PERU SECURE, requiere cambio de claves para la EC que necesite renovar su certificado. Solo en casos excepcionales se puede aceptar repetir la ceremonia de creación de claves de la EC manteniendo las mismas claves creadas en un HSM para una ceremonia previa, en orden de enmendar cualquier error en el proceso.

Cuando se crea un nuevo certificado para una entidad, el periodo de validez aplicadoa este certificado se verá limitado a la validez de las claves de las EC que lo emita.

26.7 RECUPERACIÓN EN CASO DE COMPROMISO DE UNA CLAVE Y DESASTRE NATURAL U OTRO TIPO DE CATÁSTROFE

WISEKEY, como prestador de servicios de PERU SECURE, establece una serie de circunstancias en que los sistemas y servicios de la EC se vean interrumpidos o comprometidos en su normal funcionamiento seguro, y el Plan de Continuidad de servicios que debe activarse en esos casos.

El CPS de WISEKEY, que rige a la EC de PERU SECURE y forma parte de su CPS, resume, en la sección correspondiente, situaciones específicas de este tipo y la reacción establecida de la organización de WISEKEY, para reactivar los servicios en el más breve plazo. El Plan de Continuidad detallado es un documento confidencial.

El CPS vigente de WISEKEY se encuentra en el Repositorio documental de WISEKEY:

https://www.wisekey.com/repository/

26.7.1 PROCEDIMIENTOS DE GESTIÓN DE INCIDENTES Y VULNERABILIDADES

Las ECs y/o ERs que operen bajo WISEKEY están obligadas a hacer cumplir los controles necesarios para comprobar y demostrar que los procedimientos de gestión de incidentes y vulnerabilidades son eficaces. Las personas involucradas deben ser convenientemente entrenadas en sus roles y responsabilidades en el ejercicio de sus funciones.

26.7.2 ALTERACIÓN DE LOS RECURSOS HARDWARE, SOFTWARE Y/O DATOS

Si los recursos de hardware o de software se ven alterados o se sospecha que han sido alterados, WISEKEY detendrá las operaciones normales hasta que se establezca un entorno seguro. De forma paralela, una auditoría se llevará a cabo con el fin de identificar la causa y disponer las medidas necesarias para evitar futuras repeticiones.

En el caso de que los certificados digitales se emitan durante el periodo de incertidumbre y existe el riesgo de que estos certificados podrían verse comprometidas, a continuación, estos certificados serán revocados y los suscriptores serán notificados de la necesidad de volver a emitir sus certificados.

26.7.3 PROCEDIMIENTO DE ACTUACIÓN ANTE LA VULNERABILIDAD DE LA CLAVE PRIVADA DE UNA AUTORIDAD

En el caso de que una clave privada se vea comprometida en la arquitectura de WISEKEY y además de las estipulaciones en la sección Alteración de los recursos hardware, software y/o datos, las entidades subordinadas en función de la clave privada comprometida serán notificadas de este evento y se llevará a cabo las acciones necesarias. Así mismo, no se emitirán certificados hasta que se supere el incidente.

Todos los certificados emitidos por entidades de subordinación a la clave comprometida desde el momento de compromiso de la clave y la revocación del certificado serán revocados, y las partes involucradas serán notificadas tal como lo dispone la presente CPS. Además, se tomarán medidas para volver a emitir los certificados necesarios.

26.7.4 CAPACIDAD DE RECUPERACIÓN DESPUÉS DE UN DESASTRE NATURAL U OTRO TIPO DE CATÁSTROFE

En el caso de un desastre (independientemente de su naturaleza) que afecte a las instalaciones principales de WISEKEY, y cualquiera de los servicios que se proporcionan a partir de estos, el Plan de Continuidad de Servicio WISEKEY se activará, asegurando que los servicios identificados como "críticos" están disponibles en menos de 72 horas después de la activación del plan. El resto de los servicios estaría disponible en los términos razonables, según se juzga adecuado para su importancia y nivel de criticidad.

26.8 CESE DE UNA EC O ER

26.8.1 ENTIDAD DE CERTIFICACIÓN

En el caso de que una EC bajo WISEKEY se vea obligada a poner fin a sus actividades,las acciones mínimas que deben ejecutarse son:

- Notificar a todos los suscriptores de certificados y revocar todos los certificados en el marco de la EC.
- Informar a todas las partes de confianza que tienen una relación directa registrada con esa EC sobre la terminación de la prestación del servicio certificado. Esto también terminará la acreditación otorgada a la EC para operar bajo WISEKEY.
- Realizar un aviso público de la terminación dentro de la sección de repositorio del sitio web de la EC afectada, y llevar a cabo otras comunicaciones públicas que se consideren necesarias para informar a la comunidad del tercero que confía.
- La EC deberá transferir sus obligaciones a una parte confiable para mantener los archivos de los log de eventos y registros de auditorías necesarios para demostrar la correcta operación de la EC por un periodo razonable.
- La EC deberá transferir sus obligaciones a una parte confiable para mantener disponible su clave pública o sus certificados a los terceros que confían por un periodo razonable de tiempo.
- Las claves privadas de EC incluyendo las copias de respaldo deberán ser destruidos de tal manera que la clave privada no pueda ser recuperada.
- Todos los datos necesarios para la continuación de las operaciones bajo el marco de la IOFE, en particular los certificados raíz, las listas de certificados revocados, son transferidas al propio INDECOPI o a otro PSC designado por éste.
- Cuando se trata de una operación de transferencia de titularidad, se debe asegurar que los nuevos dueños u operadores cumplan con los requisitos de acreditación del INDECOPI.

- La EC deberá notificar al INDECOPI, con un periodo no menor al de treinta (30) días calendarios de anticipación.

En el caso de cese de una EC Raíz de WISEKEY, esto implicará la terminación de toda la jerarquía que depende de esa CA raíz.

27 CONTROLES TÉCNICOS DE SEGURIDAD

27.1 GENERACIÓN E INSTALACIÓN DEL PAR DE CLAVES

27.1.1 GENERACIÓN DEL PAR DE CLAVES

Los pares de claves de las EC que operan en WISEKEY, se generan y se instalan en un procedimiento que cumple con las regulaciones aplicables. Los detalles de este procedimiento son:

- La generación del par de claves de la EC Raíz es auditado por un evaluador externo calificado.

- Las ECs Subordinadas se generan bajo la supervisión directa de los auditores internos de WISEKEY.

- Las ceremonias de las ECs son ejecutados por personal de confianza designados.

- Hay una secuencia de comandos de ejecución pre-definido que se debe seguir durante la ceremonia.

- Durante la ceremonia, es la auditoría es grabada lo suficiente en orden de probar que la ceremonia se realizó sin ningún riesgo de seguridad.

- Después de la ceremonia, un informe de la ceremonia se genera y debidamente archivada para referencia futura

El par de claves de la EC Raíz de la WISEKEY se generan en los módulos de seguridad de hardware (HSM) acreditada en virtud de las normas especificadas en la sección *Controles y estándares para los módulos criptográficos*.

El par de claves para la Política de las ECs emisoras en WISEKEY pueden ser generados en los módulos de seguridad de hardware (HSM) acreditada en virtud de las normas especificadas en la sección *Controles y estándares para los módulos criptográficos*.

El par de claves para la Política de las ECs emisoras en WISEKEY pueden ser generados en forma “escrowable” y protegidos según lo dispuesto en los requisitos de WebTrust, e importado y operado dentro de los módulos de seguridad de hardware (HSM) en virtud de las normas especificadas en la sección *Controles y estándares para los módulos criptográficos*.

Otro par de claves distinto de los asignados a las Entidades de certificación pueden ser generados por componentes de software, excepto el "Certify ID calificado" y los certificados de "Certify ID URA Admin", que deben generarse en dispositivos seguros de firma (FIPS 140-2 Nivel 2 y equivalentes, o más altos).

27.1.2 ENTREGA DE LA CLAVE PRIVADA A LOS TITULARES

En el Modelo de confianza (Trust Model) de WISEKEY, los perfiles específicos de certificados de entidad final permiten la generación de la clave privada de la ER o por el Suscriptor usuario final. Si las claves son generadas por la ER, FIPS 140-2 Nivel 1, o superior, se deben usar contenedores. En particular, se acepta el uso de archivos protegidos con contraseñas cifradas o software, tarjetas inteligentes u otros cripto-tokens válidos.

27.1.3 ENTREGA DE LA CLAVE PÚBLICA AL EMISOR DELCERTIFICADO

Las claves públicas generadas por, o para, las entidades finales se envían a la EC por medio de canales seguros a través de las ERs de WISEKEY, como parte de una solicitud de certificado en formatos aceptables, tales como PKCS # 10 u otros estándares de RSC.

27.1.4 ENTREGA DE LA CLAVE PÚBLICA DE LA EC A TERCEROSACEPTANTES

Las claves públicas de todas las ECs que operan bajo el Modelo de confianza (Trust Model) de WISEKEY se publican y se pueden descargar libremente desde su repositorio que se encuentra en

http://www.wisekey.com/repository

Los certificados raíz de confianza se pueden obtener directamente de los repositorios apropiados en la mayoría de navegadores y sistemas operativos.

27.1.5 TAMAÑO DE LAS CLAVES

WISEKEY, como prestador de servicios de PERU SECURE, impone el uso de un mínimo de longitud de 2048 bits RSA y ECC NIST P-256, P-384, o P- 521 pares de claves en todos los niveles de la jerarquía.

El algoritmo hash soportado es SHA-2, dependiendo de la jerarquía a la que pertenece el certificado de entidad final.

27.1.6 PARÁMETROS DE GENERACIÓN DE LA CLAVE PÚBLICA Y VERIFICACIÓN DE LA CALIDAD

El algoritmo utilizado en WISEKEY para la generación de claves es RSA o ECC.

27.1.7 USOS PERMITIDOS DE LA CLAVE (SEGÚN EL CAMPO KEYUSAGE DE LA X.509)

Todos los certificados emitidos en WISEKEY contienen los atributos "uso de la clave" y "uso extendido de la clave", como se define en el estándar X.509v3. Más información disponible en la CPS de WISeKey.

27.2 PROTECCIÓN DE LA CLAVE PRIVADA Y CONTROLES DE INGENIERÍA DE LOS MÓDULOS CRIPTOGRÁFICOS

WISEKEY, como prestador de servicios de PERU SECURE, ha establecido controles para asegurar que los riesgos derivados de un compromiso de la clave privada, se gestionan y se mantienen en niveles razonables. Estos controles son diferentes para los componentes principales (ECs) y las claves de usuario final.

27.2.1 CONTROLES Y ESTÁNDARES PARA LOS MÓDULOSCRIPTOGRÁFICOS

Se requiere que las ECs de WISEKEY utilicen módulos de seguridad de hardware, por lo menos compatible con FIPS 140-2 Nivel 3 para los componentes de PKI.

Los requisitos para los dispositivos criptográficos de usuario final (si los hay) pueden variar en términos del nivel de seguridad esperado.

27.2.2 CONTROL MULTIPERSONA (N DE M) DE LA CLAVE PRIVADA

Las claves privadas de las ECs siempre están bajo el control multipersona. Los datos de activación necesarios para permitir a una Entidad de certificación, serán compartidos de tal manera que se necesiten al menos dos personas autorizadas para realizar cualquier operación delicada en una EC, excepto cuando se activa el reinicio de funcionamiento sin supervisión de ECs emisoras.

Las claves privadas para entidades finales están bajo el control exclusivo del suscriptor o del representante autorizado

27.2.3 CUSTODIA DE LA CLAVE PRIVADA

La clave privada de los certificados digitales de usuario final está bajo el exclusivo control y custodia del titular. Bajo ninguna circunstancia WISEKEY como prestador de servicios de PERU SECURE guarda copia de la clave privada del titular ya que esta es generada por el mismo titular y no es posible tener acceso a ella por WISEKEY o por PERU SECURE.

27.2.4 BACKUP DE LA CLAVE PRIVADA

Las copias de backup de las claves privadas de las ECs para todas las Entidades de Certificación bajo el Modelo de confianza (Trust Model) de WISEKEY se mantienen con fines de recuperación de rutina y recuperación de desastres. Dichas claves se almacenan normalmente en forma encriptada dentro de los módulos criptográficos de hardware y dispositivos de almacenamiento de claves relacionadas. Los módulos criptográficos utilizados para el almacenamiento de claves privadas de la EC cumplen con los requisitos de esta CPS.

27.2.5 ARCHIVO DE LA CLAVE PRIVADA

Las claves privadas no se archivan para cualquier participante PKI.

27.2.6 TRANSFERENCIA DE LA CLAVE PRIVADA A/DESDE EL MÓDULO CRIPTOGRÁFICO

El proceso de descarga de las claves privadas se realiza según procedimiento del dispositivo criptográfico y se almacenan de forma segura protegidas por claves criptográficas con control dual.

Para la EC que opere bajo el Modelo de confianza (Trust Model) de WISEKEY, es obligatorio que los pares de claves se operen en los Módulos de seguridad de hardware como se define en la sección *Controles y estándares para los módulos criptográficos*. Las claves privadas se pueden transferir a los módulos de seguridad de hardware adecuados para las operaciones de copia de seguridad y recuperación.

No hay ninguna estipulación para las llaves pertenecientes a otros participantes de PKI.

27.2.7 ALMACENAMIENTO DE LAS CLAVES PRIVADAS EN UN MÓDULO CRIPTOGRÁFICO

Las claves privadas de la EC o ER mantenidas en los módulos criptográficos de hardware se almacenan en un formato cifrado apoyado por el proveedor de HSM.

Las claves privadas de entidad final deben utilizar contenedores cifrados que cumplen al menos con FIPS 140-2 Nivel 2.

27.2.8 MÉTODO DE ACTIVACIÓN DE LA CLAVE PRIVADA

La clave privada de la EC en WISEKEY se activa al iniciar el software de PKI y activando el HSM donde se almacena la clave. Este proceso requiere al menos un control dual-persona, a excepción de una EC emisora donde se permite la activación automática de claves en caso de fallo del sistema o reinicio.

La activación de la clave privada del suscriptor se estipula en la sección *Datos de Activación*.

27.2.9 MÉTODO DE DESACTIVACIÓN DE LA CLAVE PRIVADA

En las EC, la clave privada se desactiva por el apagado del servidor asociado o por terminar el software PKI o mediante la extracción o la puesta fuera de servicio el HSM que contiene la clave. Esta tarea puede ser realizada por un administrador del sistema y, previamente, tiene que ser notificado y autorizado a/por la EC responsable.

Por otro lado, la desactivación de las claves privadas de las ER o de los usuarios finales basados en hardware, se realiza mediante la extracción del dispositivo de seguridad (tarjeta inteligente u otros cripto-tokens aceptados) de la estación de trabajo donde es utilizada.

La desactivación de otras claves privadas del usuario final, mientras que no se encuentran basadas en el hardware, se lleva a cabo mediante el apagado del dispositivo en el que se almacena la clave privada. El suscriptor debe tomar todas las medidas razonables para evitar el uso no autorizado del dispositivo.

27.2.10 MÉTODO PARA DESTRUIR LA CLAVE PRIVADA

El procedimiento para destruir una clave privada se realiza en los siguientes casos:

- La clave privada ya no se utiliza.

- El token o HSM contiene la clave que se ha deteriorado hasta el punto que impide el uso normal.

- El token se encuentra perdido o ha sido robado, y se sospecha que las teclas que contenía se ven comprometidas.

Asimismo, una clave privada puede ser destruida por el propietario de la clave o un representante legal. En tales casos, el certificado correspondiente será revocado y se le notificará a la comunidad. El procedimiento utilizado para destruir la clave privada depende del contenedor en cuestión, siendo responsabilidad del individuo la ejecución de la destrucción, haciéndolo de una manera apropiada. En particular, para las claves privadas asociadas a las ECs, esta tarea debe ejecutarse bajo control dual y debe ser registrando un seguimiento apropiado de la información por WISeKey.

27.2.11 EVALUACIÓN DEL MÓDULO CRIPTOGRÁFICO

Esta evaluación está bajo la supervisión de WISeKey. Sin estipulación adicional a la sección *Controles y estándares para los módulos criptográficos*.

27.3 OTROS ASPECTOS DE LA GESTIÓN DEL PAR DE CLAVES

27.3.1 ARCHIVO DE LA CLAVE PÚBLICA

Las claves públicas en el Modelo de confianza (Trust Model) WISEKEY son archivados por un período de siete (7) años después de la expiración o revocación del certificado digital correspondiente.

27.3.2 PERIODOS OPERATIVOS DE LOS CERTIFICADOS Y PERIODO DE USO DEL PAR DE CLAVES

El periodo plenamente operativo de un certificado comienza en la emisión y termina con la expiración o revocación del certificado.

El periodo de validez para los pares de claves se establece en la siguiente tabla:

Tipo de certificado	Periodo de validez
OWGTM EC Raíz GA (SHA-1)	32 años
OWGTM EC Raíz GB (SHA-2)	25 años
Política de la EC	Todo el tiempo de vida de la EC Raíz desde el momento de su emisión
EC emisora	Hasta 10 años
Certificado de Entidad final	Hasta 3 años

Se debe entender que el periodo de validez de un certificado puede estar limitado por la propia validez de la EC emisora, ya que no se permite que una entidad subordinada extienda su validez más allá del emisor.

Los certificados son operativos para la validación de la firma y el descifrado desde la emisión hasta el final del periodo de archivo, tal como se indica en el apartado *Archivo de la clave pública*.

27.4 DATOS DE ACTIVACIÓN

27.4.1 GENERACIÓN E INSTALACIÓN DE LOS DATOS DE ACTIVACIÓN

Los datos de activación para las ECs se generan y almacenan en tokens criptográficos y/o tarjetas inteligentes y son utilizados por personas autorizadas. Además, estos tokens requieren una contraseña o PIN con el fin de permitir el proceso de activación.

Las activaciones que requieran el control multi-perona, serán impuestas por la división de los datos de activación de varios tokens.

Los datos de activación de la entidad final, solo se establecen para claves privadas basadas en hardware. En particular:

- Claves privadas para la ER y Certificados reconocidos, requerirán el uso de un código PIN o contraseña de ocho o más caracteres con el fin de activar el dispositivo de hardware en el que se almacena la clave.

- Claves privadas para Certificados "CertifyID Standard Personal" se pueden generar e instalar sin el uso de una contraseña, aunque no es recomendable.

- Claves privadas para otros tipos de certificados deben ser generadas después de que el suscriptor es autenticado correctamente en el sistema en el que se crean las claves. Un método aceptado es el uso de contraseñas razonablemente seguras para acceder a la interfaz de usuario de la ER.

27.4.2 PROTECCIÓN DE LOS DATOS DE ACTIVACIÓN

Solo las personas autorizadas deben conocer la contraseña o PIN para activar las claves privadas. En el caso de entidades finales, solo el suscriptor del certificado tiene derecho a conocer esta información.

En todos los casos, se requiere que el propietario sea el encargado de salvaguardar los datos de activación para la confidencialidad de esta información.

27.4.3 OTROS ASPECTOS DE LOS DATOS DE ACTIVACIÓN

Sin estipulación.

27.5 CONTROLES DE SEGURIDAD INFORMÁTICA

Los detalles de esta información se clasifican y por lo tanto no se hacen públicos. Los documentos que describen los Controles de seguridad informática solo están disponibles para las personas involucradas en WISEKEY y solo son revelados a partes externas acreditadas para fines de auditoría.

Se requiere que Las ECs y ERs que operen bajo el Modelo de confianza (Trust Model) de WISEKEY, cumplan con estos controles de seguridad. El cumplimiento se aplica periódicamente por un procedimiento de auditoría.

27.5.1 REQUISITOS TÉCNICOS DE SEGURIDAD ESPECÍFICOS

WISEKEY, en calidad de prestador de servicios de PERU SECURE, exige el uso de adecuados procedimientos, además de medidas y sistemas técnicos con el fin de controlar eficazmente los riesgos de seguridad. Estos incluyen, pero no se limitan a:

- Políticas de contraseñas fuertes

- La mejora continua de los procedimientos administrativos y operativos

- El aislamiento físico de los sistemas confidenciales y

- Protección antivirus y sistemas de detección de antivirus

- Revisiones periódicas de seguridad interna

En particular, se garantiza el cumplimiento de la Línea de base y los requisitos de Validación extendida por el Foro Internacional de la EC, si es el caso.

27.5.2 EVALUACIÓN DE LA SEGURIDAD INFORMÁTICA

WISEKEY, como prestador de servicios de PERU SECURE, establece que las evaluaciones del ordenador cumplan con las ECs y ERs que operen bajo el Modelo de confianza (Trust Model). El cumplimiento de estas clasificaciones se garantiza mediante periódicas auditorías internas.

27.6 CONTROLES TÉCNICOS DEL CICLO DE VIDA

27.6.1 CONTROLES DE DESARROLLO DE SISTEMAS

Los sistemas se han desarrollado utilizando la Metodología Key Steps WISeKey, que garantiza la seguridad y la calidad mediante el establecimiento de una serie de políticas y procedimientos operativos y técnicos que controlan la construcción de los componentes PKIdurante todas las fases del proyecto.

La autenticidad e integridad de los componentes de software críticos deben ser comprobadas antes de que estén activadas en un entorno de producción, mediante el uso de firma de código u otros métodos aceptables.

27.6.2 CONTROLES DE GESTIÓN DE SEGURIDAD

WISEKEY, como prestador de servicios de PERU SECURE, recomienda seguir el enfoque de gestión de seguridad del certificado ISO 27000. En particular WISEKEY, como operador principal del Modelo de confianza (Trust Model) sigue una adopción no operador de tales normas de seguridad.

27.6.3 CONTROLES DE SEGURIDAD DEL CICLO DE VIDA

Los controles de seguridad del ciclo de vida y cambios relacionados están garantizados por la Metodología WISeKey KeySteps.

27.7 CONTROLES DE SEGURIDAD DE LA RED

WISEKEY, como prestador de servicios de PERU SECURE, impone la adopción de controles efectivos para minimizar cualquier riesgo relacionado con seguridad de la red.

La información detallada acerca de estos controles se clasifica y solo se pone a disposición de los auditores externos después del proceso de autorización correspondiente.

En particular, el servidor utilizado para la EC Raíz de WISEKEY son sistemas off-line, desconectados físicamente de cualquier red de ordenadores, y toda comunicación de información sensible está protegida mediante técnicas de firma digital y cifrado.

27.8 SELLADO DE TIEMPO

WISEKEY, como prestador de servicios de PERU SECURE, proporciona una Política de sellado de tiempo (Certify ID TSP) que regula el funcionamiento de las Entidades de sellado de tiempo según RFC3161. Este servicio está disponible por WISEKEY como operador principal y otras entidades autorizadas que se adhieren a la TSP. Más información sobre los servicios y normas de sellado de tiempo se publica en:

http://www.wisekey.com/repository

Para otros datos que requieren tiempo e información de datos, como certificados y CRL, no es obligatorio estar basados en criptografía.

28 PERFILES DE CERTIFICADOS, CRL Y OCSP

28.1 PERFIL DE CERTIFICADO

Todos los certificados emitidos bajo el Modelo de confianza (Trust Model) de WISeKey cumplen con:

- Recomendación UIT-T X.509 (1997): Tecnología de la Información - Interconexión de sistemas abiertos - El directorio: Marco de autenticación, junio de 1997

- RFC 5280: Internet certificado de infraestructura de clave pública X.509 y CRL Perfil, abril de 2002 ("RFC 5280").

Esta sección de la CPS se proporciona para estipulación general y como una referencia a la Política de certificación específica para cada tipo de certificado, disponible en el anexo B: Políticas y perfiles de certificados aprobados.

28.1.1 NÚMERO DE VERSIÓN

Los certificados emitidos por la Entidad de Certificación WISeKey cumplen con el estándar X.509 Versión 3.

28.1.2 EXTENSIONES DEL CERTIFICADO

Las extensiones de certificado se describen en las tablas disponibles en el anexo A.

28.1.3 KEY USAGE

El "key usage" se describe en las tablas disponibles en el anexo A.

28.1.4 IDENTIFICADORES DE OBJETO (OID) DE LOS ALGORITMOS

Los certificados emitidos bajo WISeKey pueden utilizar SHA-2. Los identificadores de objeto de los algoritmos son:

- Sha256withRSAEncryption: identificador de objeto :: = {iso(1) member-body(2) us(840)

RSADSI (113549) PKCS (1) pkcs-1 (1) 11}

28.1.5 FORMATOS DE NOMBRES

Los certificados emitidos bajo WISeKey contienen el "nombre completo", en formato X.500, para el emisor y el suscriptor, situado en los campos "Nombre del emisor" y "Nombre de sujeto", respectivamente, y se forman como se define en la sección Tipos de nombre.

28.1.6 RESTRICCIONES DE LOS NOMBRES

Las Entidades de Certificación no operadas por WISeKey se verán limitadas en cuanto a la emisión de certificados bajo un conjunto de nombres predefinidos y acordados. Para los casos excepcionales en los que no se aplican estas restricciones, estas ECs se incluirán en la auditoría externa para la garantía del cumplimiento en contra de cualquier requisito aplicable (incluyendo la Línea base y los Requerimientos de validación extendida de la EC / Foro internacional).

Las restricciones de nombres de dominio pueden ser también aplicadas al utilizar la Interfaz de RA MPK de solicitudes de certificados para las empresas que tienen acceso a una ER dedicada.

28.1.7 IDENTIFICADOR DE OBJETO DE LA POLÍTICA DE CERTIFICACIÓN

La Política OID específica para cada modelo de certificado, está documentada en el anexo A.

28.1.8 USO DE LA EXTENSIÓN POLICY CONSTRAINS

Las Entidades de Certificación emisoras no operadas por WISeKey se ven propiamente limitadas a cumplir con los Requerimientos de validación extendida de la EC / Foro internacional. Estas ECs tendrán dificultades por no permitir la emisión de sus propias ECs subordinadas y mediante el control de los usos de la clave permitidos en los certificados de usuario final. La exactitud de esta información está garantizada por las tareas de auditoría ejecutadas durante la ceremonia de Creación de clave de la EC.

28.1.9 TRATAMIENTO SEMÁNTICO PARA LA EXTENSIÓN CERTIFICATE POLICIES

La extensión "Política de Certificación" identifica la Política de WISeKey asignada explícitamente con una Política de certificados. Las aplicaciones de software que requieren un modelo de certificado específico para procesar una firma digital debe comprobar esta extensión con el fin de verificar la idoneidad del certificado para el fin previsto.

28.2 PERFIL DE CRL

Las CRLs emitidas por la Entidad de Certificación WISeKey cumplen con el RFC 5280 (Internet X.509 Public Key Infrastructure Certificate and CRL Profile, Abril 2002) y contienen los siguientes elementos básicos:

28.2.1 NÚMERO DE VERSIÓN

Las CRLs emitidas por WISeKey como prestador de servicios de PERU SECURE cumplen con el estándar X.509 versión 1 y 2.

28.2.2 CRL Y EXTENSIONES CRL

El perfil genérico CRL se especifica en la siguiente tabla:

Versión	1 (i.e. X.509 version 2 CRL)
Número de serie	Los números de serie únicos son asignados por la EC
Algoritmo de firma	SHA 2- RSA
Nombe del Issuer Distinguished	
Nombre Común (CN)	<CA-NAME>
Organisational Unit (OU)	Como lo define la EC
Organisational Unit (OU)	Como lo define la EC
Organisation (O)	Como lo define la EC
País (C)	Como lo define la EC
Reciente actualización	Fecha/Hora de emisión
Próxima actualización	(Según sea apropiado para la EC, previsto en el apartado *Frecuencia de emisión de la CRLs*)
Certificados revocados	
Número de serie	<Número de serie del certificado del suscriptor>
Fecha de revocación	<Hora/fecha del certificado revocado>
Código de razón de CRL	<In accordance with RFC3280>

Número de CRL	Número único para cada CRL emitida por una EC
Autoridad Key Identifier	Extensión marcada NO critica
Key Identifier	<CA-KeyID>

Si hay alguna consideración específica debe ser estipulada en la Política de certificación.

28.3 PERFIL OCSP

En general, el estado de todos los certificados en WISeKey, excepto el Certificado "CertifyID Standard Personal" cumple con lo estipulado en el RFC5280/6960 "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP".

WISeKey garantiza el cumplimiento de los demás requisitos aplicables de la EC / Foro Internacional en términos de implementaciones de OCSP.

28.3.1 NÚMERO DE VERSIÓN

WISeKey proporciona soporte para la versión 1 del RFC 5280 / 6960.

28.3.2 EXTENSIONES OCSP

Si una Política de certificación exige el apoyo de OCSP, la extensión AIA apropiada será incluida en los certificados afectados, especificando la dirección URL del servidor OCSP.

Si hay alguna consideración específica debe ser estipulada en la Política de certificación.

29 AUDITORÍA DE CONFORMIDAD Y OTROS CONTROLES

WISEKEY monitorea y asegura el cumplimiento de los requisitos legales, de seguridad y de la industria, en todos los niveles del Modelo de confianza (Trust Model), a través de auditorías internas y externas.

Esas auditorías de conformidad externa e interna se ejecutan según lo definido por la EC / Foro Internacional en su Línea de base y los Requerimientos de validación extendida. Si se da el caso, otros requerimientos de evaluación nacionales y/o industriales pueden ser cumplidos. Dentro de estos requerimientos se incluye la disponibilidad de acceso a los registros concernientes a la operación de los servicios de certificación digital para proveer evidencia de su correcta operación, si es requerida para propósitos legales.

29.1 FRECUENCIA O CIRCUNSTANCIAS DE LOS CONTROLES

Todas las ECs y ERs dependientes deben seguir el Programa de evaluación adecuado (como se estipula en la sección *Aspectos cubiertos por los controles*) en una frecuencia anual.

29.2 IDENTIDAD/CUALIFICACIÓN DEL AUDITOR

El evaluador se seleccionará cuando se requiera una auditoría o evaluación. A cualquier empresa o profesional cuyos servicios son contratados como auditor o asesor, debe de cumplir los siguientes requisitos:

- Capacidad y experiencia suficiente y acreditada para realizar los servicios requeridos (PKI de auditoría, evaluación de seguridad, etc.). En particular, para las auditorías externas, se requiere acreditación adecuada para llevar a cabo auditorías WebTrust.

- En el caso de las auditorías externas, debe ser independiente de WISEKEY a un nivel de organización.

29.3 RELACIÓN ENTRE EL AUDITOR Y LA ENTIDAD AUDITADA

La política de auditoría de WISEKEY no permite ningún tipo de relación jurídica, organizativa o de otro tipo con el auditor externo que daría lugar a un conflicto de intereses.

29.4 ASPECTOS CUBIERTOS POR LOS CONTROLES

WISEKEY establece dos niveles de auditoría y acreditación.

- La EC raíz, la Política de las ECs y ECs emisoras pertenecientes u operados por WISEKEY. Estos servicios son auditados según los criterios WebTrust y estándares de acreditación industrial comúnmente aceptados.

Entidades emisoras gestionadas por terceros que no hacen cumplir las restricciones de nombres deben ser incluidos en esta evaluación.

- Las ECs emisoras pertenecientes y / o gestionados por terceros hacer cumplir las restricciones de nombres. Estos servicios deben cumplir con las prácticas estipuladas en la presente CPS y las CP que tienen derecho a emitir, y son auditados y acreditados por WISEKEY por medio de una auditoría interna realizada por WISEKEY u otro auditor autorizado.

29.5 ACCIONES A TOMAR COMO RESULTADO DE LA DETECCIÓN DE DEFICIENCIAS

En el caso de identificar una deficiencia, WISEKEY adoptará y será responsable de todas las medidas correctivas necesarias.

En el caso de una deficiencia grave que afecte al funcionamiento fiable de una EC o ER, WISEKEY podría decidir suspender temporalmente las actividades de los sistemas o servicios afectados hasta que se resuelva la deficiencia.

29.6 COMUNICACIÓN DE RESULTADOS

Todos los resultados de la evaluación estarán conformados por:

- Reporte detallado. Este documento incluye todos los temas que componen el programa de evaluación ejecutado en detalle. El informe detallado se considera privado y solo se encuentra disponible para el propietario de la Entidad de Certificación y la Entidad Aprobadora de la Política de WISEKEY.

- Declaración del informe de auditoría. Este documento solo incluye una declaración formal por parte del auditor y refleja el resultado de la evaluación, una lista de los temas tratados y el resultado global. El informe resumido se considera público y solo se publica en el repositorio WISEKEY.

30 OTROS ASUNTOS LEGALES Y COMERCIALES

30.1 TARIFAS

30.1.1 TARIFAS DE EMISIÓN O RENOVACIÓN DE CERTIFICADOS

La emisión de certificados en WISEKEY se considera un servicio comercial y por lo tanto sujeto a tarifas. Los honorarios dependen del certificado y del proyecto y se acordarán antes de ponerla a disposición de los suscriptores.

30.1.2 TARIFAS DE ACCESO A LOS CERTIFICADOS

En general, WISEKEY no aplica tasa para el acceso a la información del certificado hecho público en los diferentes repositorios.

30.1.3 TARIFAS DE REVOCACIÓN O ACCESO A LA INFORMACIÓN DE ESTADO

En general, WISEKEY no aplica tasa para el acceso a la información del certificado hecho público en los diferentes repositorios.

30.1.4 TARIFAS DE OTROS SERVICIOS

WISEKEY, como operador de la WISEKEY puede fijar tarifas para los diferentes servicios comerciales prestados a las partes que deseen participar en el Modelo de confianza (Trust Model). Esto incluye, pero no se limita a:

- Servicios de Managed PKI
- Servicios de firma de la EC
- Servicios de hosting y operación de la EC

30.1.5 POLÍTICA DE REEMBOLSO

La política de reembolso aplicable a los servicios comerciales prestados por WISEKEY está incluida en el "Acuerdo del suscriptor" comunicado al usuario final al prestar el servicio. Otras políticas de devolución pueden ser establecidas y en estos casos se deben comunicar de manera efectiva a todas las partes afectadas.

30.2 RESPONSABILIDAD

La EC dispondrá en todo momento de un seguro de responsabilidad civil en los términos que marque la legislación vigente en Perú.

La EC actuará en la cobertura de sus responsabilidades por sí o a través de la entidad aseguradora, satisfaciendo los requerimientos de los solicitantes de los certificados, de los Firmante/Titulares y de los terceros que confíen en los certificados.

Las responsabilidades de la EC incluyen las establecidas por la presente CPS, así como las que resulten de aplicación como consecuencia de la normativa colombiana, peruana e internacional.

La EC será responsable del daño causado ante el Titular o cualquier persona que de buena fe confíe en el certificado, siempre que exista dolo o culpa grave, respecto de:

- La exactitud de toda la información contenida en el certificado en la fecha de su emisión.
- La garantía de que, en el momento de la entrega del certificado, obra en poder del Titular, la clave privada correspondiente a la clave pública dada o identificada en el certificado.

- La garantía de que la clave pública y privada funcionan conjunta y complementariamente.
- La correspondencia entre el certificado solicitado y el certificado entregado.
- Cualquier responsabilidad que se establezca por la legislación vigente.

30.3 EXONERACIÓN DE RESPONSABILIDAD

La EC no será responsable en ningún caso cuando se encuentran ante cualquiera de estas circunstancias:

- Estado de Guerra, desastres naturales o cualquier otro caso de Fuerza Mayor.
- Por el uso de los certificados siempre y cuando exceda de lo dispuesto en la normativa vigente y la presente CPS y sus Anexos.
- Por el uso indebido o fraudulento de los certificados o CRL's emitidos por la Entidad de Certificación.
- Por el uso de la información contenida en el Certificado o en la CRL.
- Por el incumplimiento de las obligaciones establecidas para el Titular o Terceros que confían en la normativa vigente, la presente CPS y sus Anexos.
- Por el perjuicio causado en el periodo de verificación de las causas de revocación.
- Por el contenido de los mensajes o documentos firmados o cifrados digitalmente.
- Por la no recuperación de documentos cifrados con la clave pública del Titular.
- Fraude en la documentación presentada por el solicitante.

30.4 RESPONSABILIDADES FINANCIERAS

WISEKEY establece los controles adecuados para garantizar que los diferentes niveles de responsabilidad financiera son recibidos por los diferentes participantes, de acuerdo con su impacto en el Modelo de confianza (Trust Model).

30.4.1 COBERTURA DEL SEGURO

Para la EC Raíz, ECs emisoras y los servicios de certificación prestados directamente por WISEKEY, se mantiene un contrato de seguro que cubra la responsabilidad expresada en la sección *Obligaciones*.

Para los afiliados y clientes corporativos que actúan como ECs o ERs, las condiciones contractuales acordadas entre las partes garantizan las responsabilidades asumidas por cada parte y transfieren los requisitos a favor del correspondiente seguro para las obligaciones transferidas.

30.4.2 OTROS BIENES

Sin estipulación.

30.4.3 SEGURO O GARANTÍA DE COBERTURA PARA LAS ENTIDADES FINALES

La responsabilidad máxima por certificado de la Raíz OISTE WISeKey PKI o cualquier otra entidad dentro de la Raíz OISTE WISeKey PKI se establecerá en la Política de certificación. Dicho límite de responsabilidad por certificado se aplicará con independencia del número de transacciones, firmas digitales, o causas de acción que surjan de ello o esté relacionada con dicho certificado o cualquier servicio proporcionado en relación con dicho certificado y en forma acumulada.

30.5 CONFIDENCIALIDAD DE LA INFORMACIÓN COMERCIAL

En general, una EC bajo WISEKEY no puede revelar la información confidencial de un suscriptor, o utilizar dicha información para cualquier propósito, excepto:

- Para el personal que requiera la información para los fines de la presente CPS o para la prestación de los servicios.

- Con el consentimiento explícito del suscriptor.

- Si es necesario hacerlo por cualquier ley o un acuerdo aplicable.

30.5.1 ÁMBITO DE LA INFORMACIÓN CONFIDENCIAL

La información revelada al suscriptor o al tercero que confía mediante la EC emisora puede ser considerada confidencial.

Toda EC bajo WISEKEY mantendrá los siguientes tipos de información confidencial y mantendrá controles razonables para evitar la exposición de dichos registros para personal no confiable.

- Todas las claves privadas

- Los datos de activación utilizados para acceder a las claves privadas o lograr acceso al sistema de la EC

- Cualquier plan de continuidad de negocio, de respuesta a incidentes, de contingencia y recuperación de desastres

- Cualquier otra práctica de seguridad, medidas, mecanismos, planes o procedimientos utilizados para proteger la confidencialidad, integridad o disponibilidad de la información

- Cualquier información en poder de la EC emisora de conformidad con la sección *Protección de la información personal*

- Cualquier transaccional, registro de auditoría y registro de archivo identificado en la sección *Procedimientos de auditoría de seguridad* o *Archivo de registros*, incluidos los registros de solicitud de certificado y la documentación presentada en apoyo de la solicitud de certificado ya sea aceptada o rechazada.

- Los registros de transacciones, registros de auditoría financiera y registros de seguimiento de auditoría externa o interna y los informes de auditoría (con la excepción de la carta de un auditor que confirma la eficacia de los controles establecidos en la presente CPS)

- Toda la información clasificada explícitamente como "PRIVADA", "CONFIDENCIAL" o "ESTRICTAMENTE CONFIDENCIAL" cuando se genera o intercambia entre las partes involucradas.

30.5.2 INFORMACIÓN NO CONFIDENCIAL

La siguiente información se considerará como no confidencial:

- Toda la información contenida en los certificados emitidos y listas de revocación de certificados (CRL), incluyendo toda la información que se pueda obtener de este tipo.

- Toda la información clasificada expresamente como "PÚBLICA".

30.5.3 DEBER DE PROTEGER LA INFORMACIÓN CONFIDENCIAL

Las ECs emisoras de WISEKEY son responsables de la protección de la información confidencial generada o comunicada durante todas las operaciones. Las partes delegadas, como las entidades que gestionan las ECs subordinadas, emisoras o ERs, son responsables de proteger la información confidencial que se ha generado o almacenado por sus propios medios.

Para las entidades finales, los suscriptores de certificados son responsables de proteger su propia clave privada y toda la información de activación (es decir, contraseñas o PIN) necesarios para acceder o utilizar la clave privada.

30.6 PROTECCIÓN DE LA INFORMACIÓN PERSONAL

La política de privacidad de WISEKEY se publica en el URL:

http://www.wisekey.com/repository

Esta política cumple con los requisitos aplicables a los servicios comerciales internacionales,y específicamente con los requisitos aplicables de la EC / Foro Internacional.

30.6.1 POLÍTICA DE PRIVACIDAD

La información personal comunicada a WISEKEY por los suscriptores de certificados se almacena en una base de datos propia del operador de la EC o ER. Esta base de datos está convenientemente protegida para evitar cualquier acceso o modificación no autorizada.

Los suscriptores tendrán derecho a acceder a su información y solicitar su modificación o cancelación.

Estos derechos pueden hacerse efectivos mediante solicitud por escrito a la dirección de correo electrónico publicado en la sección *Persona de contacto* de este documento.

En el curso de sus funciones, las ECs emisoras de WISEKEY operados por WISEKEY necesitan almacenar y procesar los datos personales electrónicamente. Todas estas acciones deben llevarse a cabo de conformidad con las leyes suizas relacionadas con la seguridad de los datosy la privacidad y Firma Electrónica. Por otra parte, se aplican todas las disposiciones del apartado *Confidencialidad de la información comercial*.

30.6.2 INFORMACIÓN TRATADA COMO PRIVADA

La información personal acerca de un individuo que no está disponible públicamente enel contenido de un certificado o del CRL se considera privada.

30.6.3 INFORMACIÓN NO CALIFICADA COMO PRIVADA

Para mayor información personal, las disposiciones de la sección *Información no confidencial* se aplican respectivamente.

30.6.4 RESPONSABILIDAD DE LA PROTECCIÓN DE LOS DATOS DE CARÁCTER PERSONAL

WISEKEY garantiza el cumplimiento de las obligaciones legales para las ECs, ERs y otras entidades que operen bajo el Modelo de confianza (Trust Model) de WISEKEY. Cada uno de estos participantes es responsable de proteger la información privada que ha sido proporcionada por los suscriptores u otros participantes en la emisión y mantenimiento de certificados digitales.

30.6.5 NOTIFICACIÓN Y CONSENTIMIENTO PARA USAR DATOS DE CARÁCTER PERSONAL

Para llevar a cabo el servicio de proveer certificación, se requiere que WISEKEY obtenga el consentimiento para utilizar la información personal del suscriptor.

Este consentimiento se entiende por la aceptación de las "Condiciones Generales" y / o "Contrato de usuario final" por el suscriptor. Esta aceptación es reconocida por la aceptación del suscriptor para obtener e instalar el certificado.

30.6.6 REVELACIÓN EN EL MARCO DE UN PROCESOADMINISTRATIVO O JUDICIAL

Los participantes en WISEKEY divulgarán información personal de los participantes si es requerido por un proceso judicial o administrativo, previa presentación de las órdenes apropiadas de conformidad con las leyes aplicables del país en el que opera la EC.

30.6.7 OTRAS CIRCUNSTANCIAS DE REVELACIÓN DE INFORMACIÓN

No se estipula.

30.7 DERECHOS DE PROPIEDAD INTELECTUAL

Todos los derechos de propiedad intelectual, incluidos los certificados digitales y las CRL emitidas bajo WISEKEY, identificadores de objetos, los CPS y los diferentes CP son propiedad de WISEKEY.

Las claves privadas y públicas son propiedad de sus respectivos dueños.

Cualquier marca comercial o respaldada incluida en el Nombre Distintivo de un certificado está bajo la responsabilidad del suscriptor del certificado.

30.8 OBLIGACIONES

En esta sección se incluyen estipulaciones generales, términos específicos pueden ser establecidos en la Política de certificación apropiada para una comunidad de usuarios y tipo de certificado dado. Si tal es el caso, el suscriptor específico, el tercero que confía y otros acuerdos serán distribuidos entre las partes.

30.8.1 OBLIGACIONES DE LA EC

La EC Raíz de WISEKEY hará lo siguiente:

- Establecer una cadena de confianza mediante la emisión de un certificado, que es un certificado autofirmado
- Asegurarse de que la Raíz firma cualquier EC subordinada emitida bajo la jerarquía de WISEKEY - Llevar a cabo correctamente el proceso de verificación se describe en la sección *Validación inicial de la identidad*
- Asegurar la exactitud e integridad de cualquier parte de la información del certificado que se genera o recopila por WISEKEY, de acuerdo con la Política de certificación aplicable
- Asegurarse de que toda la información pertinente relativa a un certificado se registra (por medios electrónicos o de otro tipo) por un periodo de tiempo adecuado, y en particular, con el fin de proporcionar pruebas de los efectos de los procedimientos legales
- Utilizar sistemas fiables, procedimientos y recursos humanos en el desempeño de sus servicios
- Cumplir con cualesquiera otras disposiciones pertinentes de la CP o CPS pertinente, y otros documentos aprobados.

Todas las ECs de WISEKEY deben:

- Operar de acuerdo con los requisitos de esta CPS y cualquier nivel de servicio aplicable.
- Asegurarse que, en el momento de emitir un certificado, este contenga todos los elementos requeridos por la CP o el PDS.
- Administrar sus claves de acuerdo con la sección *Protección de la clave privada y controles de ingeniería de los módulos criptográficos.*
- Asegurar la disponibilidad de un directorio de certificados y CRL
- Revocar inmediatamente un certificado si es necesario
- En particular, sea el caso, la EC respetará las garantías y obligaciones establecidas por la EC / Línea Base del Foro Internacional.

30.8.2 OBLIGACIONES DE LA ER

Las ERs que operan bajo la orden de WISEKEY deberán velar por:

- Funcionar de acuerdo con los requisitos de esta CPS.
- Sus certificados cumplan con todos los requisitos materiales de la presente CPS.
- No haya errores introducidos en la información del certificado por las entidades que aprueban la Solicitud de Certificado como resultado de un fallo en la gestión de la Solicitud de Certificado.
- No haya declaraciones falsas de hechos en el Certificado en las entidades que aprueban la Solicitud de Certificado o expide el certificado.
- La disponibilidad de los servicios de revocación (en su caso) y el uso de un depósito conforme con el CPS aplicable en todos los aspectos materiales.

Los contratos y acuerdos comerciales de la ER podrían incluir garantías adicionales.

30.8.3 OBLIGACIONES DEL TITULAR

Los suscriptores de los certificados emitidos bajo WISEKEY deben garantizar que:

- Toda la información suministrada por el suscriptor y contenida en el Certificado es verdadera y válida.
- Todas las representaciones hechas por el Suscriptor en la Solicitud de Certificado presentados son verdaderos y válidos.
- Su clave privada está protegida y que ninguna persona no autorizada ha tenido nunca acceso a la clave privada del suscriptor.
- La obligación y garantía de no instalar y utilizar el certificado o los certificados hasta que se haya revisado y verificado la exactitud de los datos de cada certificado.
- La obligación y garantía de instalar el certificado solo en el servidor accesible en el nombre de dominio que aparece en el certificado, y para utilizar el certificado únicamente en cumplimiento con todas las leyes aplicables, exclusivamente para el negocio autorizado de la empresa, y únicamente de conformidad con el "Acuerdo del suscriptor".
- El certificado se utiliza exclusivamente para los fines autorizados y legales, de conformidad con la presente CPS.
- Cada firma digital creada utilizando la clave privada correspondiente a la clave pública contenida en el certificado, es la firma digital del Suscriptor y el Certificado ha sido aceptado y es operativo (no caducado o revocado) en el momento de crear la firma digital.
- El Suscriptor es un Suscriptor usuario final y no una EC, y no está utilizando la clave privada correspondiente a cualquier clave pública contenida en el certificado a efectos de firmar digitalmente cualquier Certificado (o cualquier otro formato de clave pública certificada) o CRL, como una EC o de otra manera.
- La obligación y la garantía de que cesen de inmediato el uso de un certificado y su clave privada asociada, y la solicitud de inmediato que la entidad emisora de certificados revoca el certificado, en caso de que: (a) toda la información en el certificado es o se vuelve incorrecta o inexacta, o (b) existe cualquier mal uso o sospecha del compromiso de la clave privada del suscriptor asociado a la clave pública contenida en el certificado.

- La obligación y garantía de que cesen de inmediato todo el uso de la clave privada correspondiente a la clave pública contenida en un certificado al vencimiento o revocación de dicho certificado.
  El "Acuerdo del suscriptor" podría incluir garantías adicionales.

30.8.4 OBLIGACIONES DE LOS TERCEROS QUE CONFÍAN

Antes de confiar en un certificado o una firma digital, el tercero que confía debe:

- Validar el certificado y la firma digital (en particular comprobando si es que no se ha revocado, caducado o suspendido)
- Determinar y cumplir con los fines para los cuales se expidió el certificado y cualesquiera otras limitaciones de la dependencia o el uso del certificado que se especifican en la presente CPS.

Si el tercero que confía se basa en una firma digital o certificado, en circunstancias en que no ha sido validado, asume todos los riesgos con respecto a ella (a excepción de aquellas que hubieran surgido si la parte que confía valida el certificado), y no tiene derecho a cualquier presunción de que la firma digital es efectiva a partir de la firma del suscriptor o que el certificado es válido.

El tercero que confía también debe cumplir con las demás obligaciones pertinentes especificados en la presente CPS incluyendo las impuestas a la entidad cuando se está actuando como suscriptor.

Además, el tercero que confía debe considerar el tipo de certificado. La decisión final sobre si confía o no en una firma digital verificada, es exclusivamente del tercero que confía.

El "Acuerdo del tercero que confía" podría incluir garantías adicionales.

30.8.5 OBLIGACIONES DE LA ENTIDAD

Conforme lo establecido en las Políticas de Certificación anexadas a este documento, en el caso de los certificados donde se acredite la vinculación del Titular con la misma será obligación de la Entidad solicitar a la ER la revocación del certificado cuando cese o se modifique dicha vinculación.

30.8.6 OBLIGACIONES DE OTROS PARTICIPANTES.

No se estipula.

30.9 VIGENCIA Y CONCLUSIÓN

La CPS de PERU SECURE, se mantiene vigente mínimo durante el año en curso de publicación a menos de que se haya hecho algún cambio mayor, lo cual dejaría sin efecto o terminada la aplicabilidad de la versión anterior. Dicho esto, si el suscriptor ha firmado la solicitud contrato en el periodo de modificación de versiones, deberá regirse por la versión vigente en la fecha de suscripción y no por la última versión a publicar por la EC, dado que es una etapa de transición.

31 CONFORMIDAD CON LA LEY APLICABLE

PERU SECURE es afecta y cumple con las obligaciones establecidas por la IOFE, a los requerimientos de la Guía de Acreditación de Entidades Prestadoras de Servicios de Valor Añadido, al Reglamento de la Ley de Certificados Digitales, y a la Ley de Firmas y Certificados Digitales -Ley27269, para el reconocimiento legal de los servicios de valor añadido emitidos bajo las directrices definidas en el presente documento.

32 BIBLIOGRAFÍA

a) Guía de Acreditación de Prestadores de Servicios de Valor Añadido, INDECOPI
b) Ley de Firmas y Certificados Digitales –Ley 27269
c) Decreto Supremo 052-2008
d) Decreto Supremo 070-2011
e) Decreto Supremo 105-2012
f) Decreto Supremo 026-2016
g) Declaración de Prácticas de WISeKey v2.5

33 ANEXO A: PERFIL DE CERTIFICADO PERSONAL CERTIFYID ADVANCE

Los OID (Object IDentifier) de las Políticas de Certificación de Peru Secure e Net son administrados por la OGTM (matriz de WISEKEY) y están listados en el Anexo B de la CPS publicada por la fundación OISTE, "Annex B: OID Inventory" (Inventario de OIDs), en https://oiste.org/repository/ .

Nota:

- OISTE = International Organization for Secure Electronic Transactions, de Suiza
- OGTM = OISTE Global Trust Model

Versión 2	(i.e. X.509 versión 3)
Único número de serie	Los números de serie son asignados por la EC
Algoritmo de firma	SHA-2 RSA
Nombre Distintivo delemisor	
Nombre Común (CN)	<Nombre de la EC emisora>
Unidad Organizativa (OU)	<Opcional>
Unidad Organizativa (OU)	<Opcional>
Organización (O)	<Organización que emite>
País (C)	<País que emite>
Validez	
No antes de	Hora de emisión
No después de	1 – 3 años f
Asunto	

Email (E)	<Email del suscriptor> m/e
Nombre Común (CN)	<Nombre Común del suscriptor, persona jurídica autorizada> m/e
Localidad (L)	<Localidad del suscriptor> o/e
Nombre del Estado o Provincia (ST)	<Estado del suscriptor> o/e
Unidad Organizativa (OU)	<Opcional> "Usuario de CertifyID Advanced" o/f
Unidad Organizativa (OU)	<Opcional> o/e
Unidad Organizativa (OU)	<Opcional> Validado por [Appointed ER] – CertifyID ER o/f vía de emisión [Nombre del suscriptor cliente MPKI]
Unidad Organizativa (OU)	<Opcional, Unidad Organizativa del suscriptor> o/e
Organización (O)	<Opcional, Organización del suscriptor> o/e
País (C)	<Código del país del suscriptor> m/e
Información del asunto dela Clave pública	2048 bit RSA f

Extensiones x.509

Autoridad del Key Identifier	Extensión marcada como NO-crítica
Key Identifier	<KeyID>
Asunto del Key Identifier	Extensión marcada como NO-crítica
Key Identifier	The Subject Key Identifier of the Subject of this certificate.
Capacidades del SMIME (opcional)	[1] Capacidades del SMIME Object ID=1.2.840.113549.3.2 Parámetros=02 02 00 80 [2] Capacidades del SMIME Object ID=1.2.840.113549.3.4 Parámetros=02 02 00 80 [3] Capacidades del SMIME Object ID=1.3.14.3.2.7

	[4] Capacidades del SMIME Object ID=1.2.840.113549.3.7
Punto de distribución del CRL	Extensión marcada como NO-crítica
Nombre completo	[1]CRL Distribución Distribution Point Name: Full Name: URL=<URL-TO-CRL>
Authority Information Access	Extension marked non-critical.
Extensiones	[1]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=<URL- TO-ISSUER-CERT>
Key Usage	Extension marked critical.
Key Usages Permitidas	Digital Signature, Non Repudiation
Allowed Enhanced Key Usages	Document Signing (1.3.6.1.4.1.311.10.3.12) Smart Card Logon (1.3.6.1.4.1.311.20.2.2) Client Authentication (1.3.6.1.5.5.7.3.2) SecureEmail (1.3.6.1.5.5.7.3.4)

34 ANEXO B: PERFIL DE CERTIFICADO TSA CERTIFYID ADVANCED

Versión 2	2 (i.e. X.509 version 3)
OID	2.16.756.5.14.7.6
Único número de serie	Los números de serie son asignados por la EC

Algoritmo de firma	SHA-2 RSA	f
Nombre Distintivo delemisor		
Nombre Común (CN)	WISeKey CertifyID Advanced Services CA 4	f
Unidad Organizativa (OU)	International	f
Unidad Organizativa (OU)	Copyright (c) 2006 WISeKey SA	f
Organización (O)	WISeKey	f
País (C)	CH	f
Validez		
No antes de	Hora de emisión	
No después de	No después de la fecha de expiración de la EC emisora	f
Sujeto		
Nombre Común (CN)	<Nombre Común del suscriptor >	m/e
Unidad Organizativa (OU)	<Copyright notice>	m/f
Unidad Organizativa (OU)	CertifyID Advanced TSA Server	m/f
Unidad Organizativa (OU)	Validated by [Appointed RA] -CertifyID RA Issued via [Client MPKI subscriber name]	m/e
Organización (O)	<Opcional, Organización del suscriptor>	m/e
Locality (L)	<Localidad del suscriptor>	o/e
Nombre del Estado o Provincia (S)	<Estado del suscriptor> o/e	
País (C)	<Código del país del suscriptor> m/e	
Información del asunto dela Clave pública	2048 bit RSA	f

Extensiones x.509

Autoridad del Key Identifier	Extensión marcada como NO-crítica

Key Identifier	<KeyID>
Subject Key Identifier	Extensión marcada como NO-crítica
Key Identifier	Identificador o Asunto del ceritifcado
Punto de distribución del CRL	Extensión marcada como NO-crítica
Full name	[1]CRL Distribution PointDistribution PointName:Full Name:URL=<URL-TO-CRL>
Authority Information Access	Extension marked non-critical.
Extensions	[1]Authority Info AccessAccess Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2)Alternative Name:URL=<URL- TO-ISSUER-CERT>
Key Usage	Extension marked critical.
Value	Firma digital, cifrado de clave (a0) (Usos opcionales)
Allowed ExtendedKey Usages	Time Stamping (1.3.6.1.5.5.7.3.8) (Uso único obligatorio /crítica)