POLÍTICAS DE CERTIFICACIÓN Y DECLARACIÓN DE PRÁCTICAS

IDENTITY DEL PERÚ S.A.

RUC Nº 20607123463

Versión 1.3 de 21 de julio de 2025

Clasificación: Público

Ref. DPC_EC_Soluti_Latam-001

INTELLISIGN 2025

Augusto Castañeda

Firmado Digitalmente por:
ROBERTO AUGUSTO CASTAÑEDA CHAVEZ DNI:42811955 RUC:20607123463
Motivo: En señal de conformidad
Cargo: GERENTE GENERAL
Empresa: IDENTITY DEL PERU SOCIEDAD ANONIMA
IP: 38.25.95.82
Fecha: 25/07/2025 - Hora: 14:21

ÍNDICE

1. INTRODUCCIÓN

Esta CPS o DPC (Declaración de Prácticas de Certificación) establece las prácticas que lleva a cabo, nuestra empresa, **IDENTITY DEL PERÚ S.A.** identificada con RUC Nro. 20607123463, también referida técnicamente como **EC SOLUTI LATAM PERU.**, para emitir, gestionar, revocar y renovar certificados digitales, siguiendo el estándar RFC 3647 “Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework”.

IDENTITY DEL PERÚ S.A. declara para todos los efectos que cumple con todos los requisitos establecidos en la Guía de Acreditación y el Anexo 1 del Marco De La Política De Emisión De Certificados Digitales de la IOFE administrada por la INDECOPI.

2. VISIÓN GENERAL

Este documento tiene como objeto la descripción de las operaciones y prácticas que utiliza IDENTITY DEL PERÚ S.A. 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. Asimismo, el presente documento se encuentra en concordancia con la Política de Seguridad de la EC IDENTITY DEL PERU S.A., la cual garantiza que la seguridad de la información que es tratada durante todo el proceso de certificación digital. Todos los procedimientos establecidos e implementados por **EC IDENTITY DEL PERU S.A.** cumplen con la Política de Privacidad y la infraestructura PKI opera de acuerdo con los estándares internacionales establecidos.

3. OBJETO DE LA ACREDITACIÓN

El alcance de la acreditación cubre la infraestructura y procesos de los servicios de certificación digital de **IDENTITY DEL PERÚ S.A.** identificada con RUC Nro. 20607123463, representa todos los aspectos de responsabilidad y mediación entre las personas jurídicas y naturales del Estado Peruano.

4. NOMBRE E IDENTIFICACIÓN DEL DOCUMENTO

- Políticas de Certificación y Declaración de Prácticas de EC IDENTITY DEL PERÚ S.A.
- Código: DPC_EC_Soluti_Latam-001

5. HISTORIAL Y CONTROL DE VERSIONES

Versión	Fecha	Descripción	Cambios
1.0	31/01/2025	Versión inicial	
1.1	30/05/2025	Versión Actualizada	Se organizó la estructura e índice de los contenidos según el lineamiento del Anexo I De Marco De La Política De Emisión De Certificados Digitales.
1.2.	15/07/2025	Corrección de Políticas	Se actualizaron las Políticas de Responsabilidades, Limitaciones y excepciones. Actualización del Perfil de Denominación de Certificados. Re-organización de ítems relacionados a información del usuario suscriptor. Actualización de los perfiles de los certificados digitales. Actualización de información sobre EC raíz Subordinadas.
1.3.	21/07/2025	Actualización Auditorías	Se actualizaron los controles e información referente a los puntos 93, 94 y 95 del Anexo I de la Guía de Acreditación con respecto a los plazos y formas de auditoría de la AAC.

6. PARTICIPANTES

6.1 ENTIDAD DE CERTIFICACIÓN DE IDENTITY DEL PERÚ S.A.

IDENTITY DEL PERÚ S.A. en su papel de Entidad de Certificación Raíz y Entidad de Certificación del Nivel Subsiguiente, es la persona jurídica privada que presta indistintamente servicios de producción, emisión, gestión, cancelación u otros servicios inherentes a la certificación digital.

IDENTITY DEL PERU S.A., como Entidad de Certificación, le corresponderá la realización de todos los trámites y procedimientos administrativos necesarios ante la AAC a fin de poder ingresar a la IOFE.

Asimismo, dentro de sus funciones se encuentran las siguientes:

- Garantizar la seguridad, disponibilidad y calidad de las operaciones de gestión de los certificados digitales de los usuarios finales.
- Garantizar la seguridad de las claves de la EC Raíz y las EC Subordinadas durante todo su ciclo de vida.
- Garantizar la disponibilidad y accesibilidad de los servicios de consulta de estado de revocación de los certificados digitales.
- Garantizar la protección de los datos personales de los usuarios finales.
- Garantizar la continuidad del servicio a los titulares durante todo el tiempo en que se hayan contratado los servicios de certificación digital.

6.2 ENTIDAD DE REGISTRO

ER IDENTITY DEL PERÚ brinda también los servicios de Entidad de Registro, la cual es la encargada de certificar la validez de la información suministrada por el solicitante de un certificado digital, mediante la verificación de su identidad y su registro.

6.3 TITULAR

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

La figura de Titular será diferente dependiendo de los distintos certificados emitidos por IDENTITY DEL PERU S.A., conforme a lo establecido en la Política de Certificación.

Todos los atributos correspondientes a los certificados proporcionados por IDENTITY DEL PERU S.A. se encuentran establecidos en esta Política de Certificación.

6.4 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 del suscriptor recaerá sobre el representante legal designado por esta entidad. Si el certificado está designado para ser usado por un agente automatizado, la titularidad del certificado y de las firmas digitales generadas a partir de dicho certificado corresponderá a la persona jurídica. La atribución de responsabilidad del suscriptor, para tales efectos, corresponde a la misma persona jurídica.

6.5 SOLICITANTE

Se entenderá por Solicitante, la persona natural o jurídica que solicita un certificado emitido bajo el documento CPS/DPC. En el caso de los certificados de persona natural puede coincidir con la figura del Titular.

6.6 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 de IDENTITY DEL PERU S.A., a un titular. El Tercero que confía, a su vez puede ser o no titular.

6.7 ENTIDAD EN 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.

7. ADMINISTRACIÓN DE LA POLÍTICA

La Declaración de Prácticas de Certificación – DPC y de Registro – RPS de IDENTITY DEL PERU S.A., así como la Política de Seguridad, Política y Plan de Privacidad de la Entidad de Certificación y de Registro, y otra documentación relevante son publicadas en: https://soluti.pe/legal/entidad-certificacion

Todas las modificaciones relevantes en la documentación de IDENTITY DEL PERU S.A., 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 IDENTITY DEL PERU S.A. antes de ser publicado, controlando versiones de este, para evitar modificaciones y suplantaciones no autorizadas.

Las modificaciones relativas a la DPC u otra documentación relativa serán publicadas luego de ser aprobadas por el INDECOPI.

7.1 Organización que administra los documentos

IDENTITY DEL PERU S.A. administra los documentos Declaración de Prácticas de Certificación (DPC), Política de Seguridad, Política y Plan de Privacidad, y todos los documentos normativos de la EC de IDENTITY DEL PERU S.A.. El responsable de aprobar estos documentos es:

- Nombres: Eduardo Nascimento de Oliveira
- Correos electrónicos: governanca@soluti.com.br
- Cargo: Supervisor de Compliance

7.2 Formas de contacto

- Razón Social: IDENTITY DEL PERU S.A. (RUC: 20607123463)
- Central telefónica: +51 (01) 5105161
- Correo electrónico: certificacion@solutilatam.atlassian.net – clientes@solutitech.com
- Sitio web: https://soluti.pe/contacto
- Dirección Física y Fiscal: Calle Las Orquídeas 585, Oficina 1207, Piso 12, Edificio Fibra,
- Ciudad/Provincia/País: San Isidro, Lima, Perú.

8. DEFINICIONES Y ACRÓNIMOS

8.1 ACRÓNIMOS

ACRÓNIMO	DESCRIPCIÓN
AAC	Autoridad Administrativa Competente.
DN	(Distinctive Name) Nombre Distintivo.
EC	Entidad de Certificación.
ER	Entidad de Registro.

CPS/DPC	(Certification Practice Statement) Declaración de Prácticas de Certificación.
CRL	Lista de Certificados Revocados
IOFE	Infraestructura Oficial de Firma Electrónica
PC	Política de Certificación
RUC	Registro Único de Contribuyentes
SHA	Secure Hash Algorithm (Algoritmo de seguridad HASH)
CA	Cetification Authority (Autoridad de Certificación)
DSCF	Dispositivo seguro de creación de firma.
FIPS	Federal Information Processing Standards(Estándares Federales de Procesamiento de la Información)
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
PKCS	Public-Key Cryptography Standards
PKI	Infraestructura de llave pública
PSC	Prestador de Servicios de Certificación
RA	Autoridad de Registro
RFC	Request For Comments
RSA	Rivest, Shamir y Adleman
SSL	Secure Sockets Layer
TSA	Time Stamping Authority – Autoridad de Sello de Tiempo
TSU	Time Stamping Unit

8.2 DEFINICIONES

- **Entidad de Certificación – EC**: Entidad que presta servicios de emisión, revocación, re-emisión 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 y que se encarga de custodiar esta misma información.
- **Política de Certificación**: Conjunto de reglas que indican el marco de aplicabilidad de los servicios para una comunidad de usuarios definida.
- **Titular**: Entidad que requiere los servicios provistos por la EC, 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 firmada digitalmente, y que confía en la validez de las transacciones realizadas.
- **Algoritmo**: es un conjunto prescrito de instrucciones o reglas bien definidas, ordenadas y finitas que permite realizar una actividad mediante pasos sucesivos que no generen dudas a quien deba realizar dicha actividad. Dados un estado inicial y siguiendo los pasos sucesivos se llega a un estado final y se obtiene una solución.
- **Certificado digital:** mensaje de datos electrónico firmado por la entidad de certificación digital, el cual identifica tanto a la entidad de certificación que lo expide, como al suscriptor y contiene la llave pública de este último.

- **Cliente**: En los servicios de certificación digital, el término cliente identifica a la persona natural o jurídica con la cual la EC establece una relación comercial.
- **Datos de Creación de Firma (Llave privada o clave privada):** son valores numéricos únicos que, utilizados juntamente con un procedimiento matemático conocido, sirven para generar la firma digital de un mensaje de datos.
- **Declaración de Prácticas de Certificación**: Es el documento en el que consta de manera detallada los procedimientos que aplica la EC para la prestación de sus servicios. Una declaración de las prácticas que una EC emplea para emitir, gestionar, revocar y renovar certificados sin y con cambio de claves.
- **Dispositivo seguro de creación de firma**: Elemento software o hardware empleado por el suscriptor para la generación de firmas digitales, de manera que se realicen las operaciones criptográficas dentro del dispositivo y se garantice su control únicamente por el suscriptor.
- **FIPS**: Federal Information Processing Standards (FIPS, en español Estándares Federales de Procesamiento de la Información) son estándares anunciados públicamente desarrollados por el gobierno de los Estados Unidos para la utilización por parte de todas las agencias del gobierno no militares y por los contratistas del gobierno. Muchos estándares FIPS son versiones modificadas de los estándares usados en las comunidades más amplias (ANSI, IEEE, ISO, etc.)
- **Firma Digital**: Se entenderá como un valor numérico que se adhiere a un mensaje de datos y que, utilizando un procedimiento matemático reconocido, vinculado a la clave del iniciador y al texto del mensaje permite determinar que este valor se ha obtenido exclusivamente con la clave del iniciador y que el mensaje inicial no ha sido modificado después de efectuada la transformación. Función Hash o Hash: es una operación que se realiza sobre un conjunto de datos de cualquier tamaño, de forma que el resultado obtenido es otro conjunto de datos de tamaño fijo, independientemente del tamaño original, y que tiene la propiedad de estar asociado unívocamente a los datos iniciales.
- **Lista de Certificados Digitales Revocados**: es aquella relación que debe incluir todos los certificados revocados por la entidad de certificación digital.
- **Log**: Servicio de registro de eventos del sistema de información, dejando la información anterior y la actual, identifica quién y cuándo se realizó el evento.
- **PKI**: Infraestructura de llave pública (Public key Infraestructure): es el conjunto de hardware, software, políticas, procedimientos y elementos tecnológicos que, mediante la utilización de un par de claves criptográficas, una privada que sólo posee el suscriptor del servicio y una pública, que se incluye en el certificado digital, logran: Identificar al emisor de un mensaje de datos electrónico, impedir que terceras personas puedan observar los mensajes que se envían a través de medios electrónicos, impedir que un tercero pueda alterar la información que es enviada a través de medios electrónicos y evitar que el suscriptor del servicio de certificación digital que envió un mensaje electrónico pueda después negar dicho envío (no repudio).
- **PKCS**: Public-Key Cryptography Standards. Estándares de criptografía de llave pública concebidos y publicados por los laboratorios de RSA. Anexo G
- **Políticas de Certificado**: Es el conjunto de reglas que indica los requisitos de un certificado en una comunidad y/o clase en particular, en el marco de los requisitos legales, reglamentarios, y con requisitos de seguridad comunes.
- **RFC**: Request for Comments son una serie de publicaciones del Internet Engineering Task Force (IETF) que describen diversos aspectos del funcionamiento de Internet y otras redes de computadoras, como protocolos, procedimientos, etc.
- **RSA**: Rivest, Shamir y Adleman. Es un sistema criptográfico de llave pública desarrollado en 1977. Es el primer y más utilizado algoritmo de este tipo y es válido tanto para cifrar como para firmar digitalmente.
- **Servicio de certificación digital**: Conjunto de actividades de certificación que ofrece la EC para certificar el origen e integridad de mensajes de datos, basados en las firmas digitales o electrónicas,

estampado de tiempo, así como en la aplicabilidad de estándares técnicos admitidos y vigentes en infraestructura de llave pública.

- **Solicitante**: persona natural o jurídica que, con el propósito de obtener servicios de certificación digital de una EC, demuestra el cumplimiento de los requisitos establecidos en la DPC y PC de éstas, para acceder al servicio de certificación digital.
- **SSL**: Secure Sockets Layer: capa de conexión segura. Protocolo criptográfico que proporciona comunicaciones seguras por una red, comúnmente Internet.
- **Suscriptor**: persona natural o jurídica a cuyo nombre se expide un certificado digital.
- **Token**: Dispositivo hardware criptográfico suministrado por una EC, el cual contiene el certificado digital y la llave privada del suscriptor.

9. SERVICIOS DE CERTIFICACIÓN DIGITAL

IDENTITY DEL PERU S.A. brinda los servicios de emisión, re-emisión, revocación de certificados digitales.

Los certificados y las prácticas relacionadas a la gestión de su ciclo de vida son descritas en la Declaración de Prácticas y las Políticas de Certificación de IDENTITY DEL PERU S.A., publicadas en: https://soluti.pe/legal/entidad-certificacion

10. PUBLICACIÓN Y RESPONSABILIDADES SOBRE REPOSITORIOS

- Certificado Raíz:
  - http://latam.rep.solutitech.com/cacert/ec-soluti-latam-root.crt
- Certificados Subordinados:
  - http://latam.rep.solutitech.com/cacert/ec-soluti-latam-identity-peru-v1.crt
- Lista Certificados Revocados (CRL):
  - http://latam.rep.solutitech.com/crl/ec-soluti-latam-root.crl
  - http://latam.rep.solutitech.com/crl/ec-soluti-latam-identity-peru-v1.crl
- Declaración de Prácticas de Certificación (DPC): https://soluti.pe/legal/entidad-certificacion
- Política de Certificados (PC): https://soluti.pe/legal/entidad-certificacion

10.1 CONTROL DE ACCESO A LOS REPOSITORIOS

La consulta a los repositorios disponibles en la página Web de La Entidad de Certificación IDENTITY DEL PERU S.A., antes mencionados, es de libre acceso al público en general. La integridad y disponibilidad de la información publicada es responsabilidad de La Entidad de Certificación IDENTITY DEL PERU S.A., 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.

10.2 PUBLICACIÓN DE LA INFORMACIÓN DE CERTIFICACIÓN

El Responsable de la EC de IDENTITY DEL PERU S.A. es el encargado de la autorización de la publicación de la DPC y es responsable de asegurar la integridad y disponibilidad de la información publicada en la página Web: https://soluti.pe/legal/entidad-certificacion

La Lista de Certificados Revocados es publicada en la página web de IDENTITY DEL PERU S.A. y está firmada digitalmente por la Entidad de Certificación EC IDENTITY DEL PERU S.A..

10.3 PLAZO O FRECUENCIA DE LA PUBLICACIÓN

10.1.3 Certificado Raíz

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

10.2.3 Certificado Subordinado

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

10.3.3 Lista de Certificados Revocados (CRL)

La Entidad de Certificación IDENTITY DEL PERU S.A., publicará en la página Web, la lista de certificados revocados en los eventos y con la periodicidad definidas en el numeral.

10.4.3 Declaración de Prácticas de Certificación (DPC)

Con autorización del Responsable de la Entidad de Certificación de IDENTITY DEL PERU S.A. 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 IDENTITY DEL PERU S.A. junto con la nueva versión. La Auditoría anual validará estos cambios y emitirá el informe de cumplimiento.

11. RESPONSABILIDADES

11.1 Responsabilidades de la Entidad de Certificación

Las responsabilidades contractuales, garantías financieras y coberturas del seguro y Póliza de Responsabilidad Civil Profesional son brindadas por la Entidad de Certificación de EC - IDENTITY DEL PERU S.A..

IDENTITY DEL PERU S.A. representa todos los aspectos de ejecución de obligaciones contractuales, responsabilidad y mediación entre las personas jurídicas y naturales usuarios, clientes y vinculados con la Entidad de Certificación.

11.2 Responsabilidades financieras dela EC.

La EC de IDENTITY DEL PERÚ S.A. dispondrá en todo momento de una póliza de seguro en los términos que marque la legislación vigente. 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 Suscriptores y de los terceros que confíen en los certificados.

La EC de IDENTITY DEL PERU S.A. dispone de una póliza de seguro que contempla sus responsabilidades, para indemnizar por daños y perjuicios que se puedan ocasionar a los usuarios de sus servicios, por un monto de hasta US$ 100,000.00 (Cien Mil y 00/100) dólares americanos, monto que supera lo establecido por la normativa vigente. La EC otorga al cliente una garantía de devolución de dinero dentro de acuerdo con nuestras Políticas de Devolución y Reembolso descritas en nuestro sitio web: https://soluti.pe/legal/devolucion-dinero.

11.3 Las obligaciones de la EC de IDENTITY DEL PERÚ S.A:

a. Generar, emitir y distribuir certificados de clave pública con seguridad e idoneidad.
b. Generar y publicar información actualizada del estado del certificado a través de protocolos como CRL o OSCP.
c. Mantener la seguridad, disponibilidad y continuidad de la emisión del certificado sus protocolos de publicidad de certificados revocados o activos (CRL-OSCP).

d. Proporcionar un medio para que los Suscriptores soliciten la revocación de sus certificados digitales.

e. Revocación de certificados de clave pública de acuerdo con las Políticas de Certificación y CPS.

f. Organizar, coordinar y publicitar sus por auditorías internas y externas.

La EC de IDENTITY DEL PERÚ S.A. asume responsabilidad en relación con errores u omisiones en el procesamiento y mantenimiento de directorios y Listas de Certificados Revocados (CRL) y OSCP, así como en la disponibilidad de dichos repositorios.

Para información sobre las responsabilidades de la EC IDENTITY DEL PERÚ S.A. en relación con las operaciones que realiza el repositorio y cualquier otro participante no mencionado previamente, lo invitamos a leer el apartado de “Limitación y Exclusión de Responsabilidades” y de “Indemnizaciones”.

11.4 Responsabilidades de la Entidad de Registro

a. Asimismo, IDENTITY DEL PERU S.A. brinda los servicios de registro y verificación conforme a las Guías de Acreditación del INDECOPI como Entidad de Registro (ER), para realizar la verificación de identidad de los solicitantes de los certificados digitales.

b. Otras Entidades de Registro vinculadas con la EC de IDENTITY DEL PERÚ S.A. serán responsables de la correcta identificación de los titulares (personas naturales y/o jurídicas) y suscriptores (personas naturales) y de la seguridad en la entrega de los certificados digitales, siendo realizada por Operadores de Registro autorizados por la EC de IDENTITY DEL PERÚ S.A.

c. Las peticiones, quejas o reclamos para la atención de suscriptores y terceros debido a consultas relacionadas con el servicio que dispone la EC, son recibidas directamente por IDENTITY DEL PERU S.A. a través de sus canales oficiales de contacto, declarados en el apartado “8. Formas de Contacto” de este documento.

11.5 Responsabilidades de titular, del solicitante, del suscriptor y de terceros que confían.

a. Los usuarios, solicitantes y suscriptores de los servicios de emisión de certificados digitales provistos por IDENTITY DEL PERU S.A. son responsables de revisar la presente CPS/DPC y Políticas de IDENTITY DEL PERU S.A., a fin de estar informados de las características de la plataforma de servicios, infraestructura y procedimientos empleados en la gestión del ciclo de vida de los certificados digitales, certificados Raíz, certificados Intermedios y de usuario final, así como las obligaciones de cada parte.

b. Es responsabilidad del Titular, del Solicitante, y del Suscriptor o del Custodio de claves cumplir con las obligaciones estipuladas en el presente documento y en la PC correspondiente, y en los instrumentos jurídicos vinculantes firmados por los mismos.

c. Es responsabilidad de los terceros que confían y otros participantes, Verificar la validez de los certificados en el momento de realizar cualquier operación basada en los mismos.

d. Es responsabilidad de los terceros que confían y otros participantes conocer y sujetarse a las garantías, límites y responsabilidades aplicables en la aceptación y uso de los certificados en los que confía, y aceptar sujetarse a las mismas.

11.6 Responsabilidades de otros participantes

La EC de IDENTITY DEL PERÚ S.A. no considera para efectos de la validación y verificación de los certificados digitales a ninguna persona responsable distinta a las establecidas en el presente documento. En este sentido, la EC de IDENTITY DEL PERÚ S.A. no considera responsable por cualesquiera acciones/procedimientos realizados por otras Partes, distintos de los perfiles previamente establecidos en esta política, incluso en lo que respecta al acceso y consumo de información prevista en su repositorio.

11.7 Limitación de Responsabilidades

IDENTITY DEL PERÚ S.A. como Entidad de Certificación delega en las Entidades de Registro (ER) vinculadas, los límites de responsabilidades comerciales, técnicas, contractuales y legales, las cuáles deben estar establecidas en cada Contrato de Suscriptor emitidos y administrados por las ER.

IDENTITY DEL PERÚ S.A. no será responsable en ningún caso cuando se encuentre ante cualquiera de estas circunstancias:

a. Desastres naturales, estado de guerra, funcionamiento defectuoso de los servicios eléctricos, las redes telemáticas y/o telefónicas o de los equipos informáticos utilizados por el Titular por el Suscriptor, o por los terceros que confían en los certificados, o cualquier otro caso de fuerza mayor fuera del alcance de la EC.
b. En su caso, por el uso indebido de los repositorios de certificados emitidos por la Entidad de Certificación de IDENTITY DEL PERÚ S.A.
c. Por el uso indebido de la información contenida en el certificado, en la CRL o en el servicio OCSP.
d. Por el contenido de los mensajes o documentos firmados o cifrados mediante los certificados.
e. Por las acciones u omisiones del Solicitante, del Titular, y del Suscriptor claves.
f. Por la falta de veracidad o exactitud de la información suministrada por el Solicitante, del Titular y/o Suscriptor para emitir el certificado.
g. Ausencia de solicitud de revocación del certificado cuando proceda.
h. Negligencia en la conservación de sus datos como claves privadas en la creación de firma digital y en el aseguramiento de su confidencialidad y en la protección de todo acceso o revelación.
i. Uso del certificado digital fuera de su periodo de vigencia.
j. Uso del certificado digital, a pesar de haber recibido la notificación de su revocación o vencimiento.
k. Falta de comprobación de la pérdida de vigencia del certificado publicada en el servicio de consulta sobre la vigencia de los certificados o falta de verificación de la firma digital.
l. Uso no adecuado del certificado digital para los propósitos establecidos en esta CPS-DPC y según lo dispuesto en la normativa vigente y en la presente DPC, en particular, superar los límites que figuren en el certificado en cuanto a sus posibles usos y al importe individualizado de las transacciones que puedan realizarse con él o no utilizarlo conforme a las condiciones establecidas y comunicadas al Titular, y al Suscriptor.
m. Excepciones de garantía: La EC se exceptúa de brindar la garantía del servicio cuando se evidencia que la omisión o error no es atribuible a la EC.

11.8 Exoneración de responsabilidades

La EC de IDENTITY DEL PERU S.A. no será responsable en ningún caso cuando se encuentran ante cualquiera de estas circunstancias:

a. Por el incumplimiento de las obligaciones establecidas por parte del Suscriptor o Terceros que confían en la normativa vigente, la presente DPC o en las Prácticas Correspondientes;
b. Por el perjuicio causado en el periodo de verificación de las causas de revocación/suspensión;
c. Por el contenido de los mensajes o documentos firmados o cifrados digitalmente;
d. Por la no recuperación de documentos cifrados con la clave pública del Suscriptor;

11.9 Indemnizaciones

La EC IDENTITY DEL PERÚ S.A. cuenta con una Póliza de Responsabilidad Civil por un valor de US$100,000.00 (Cien mil y 00/100) dólares americanos, emitida por una Aseguradora de Prestigio en el Perú, la cual se renueva anualmente. Este seguro profesional cubre el límite máximo por los daños y perjuicios que ocasionen servicios defectuosos y la operación no idónea de la EC, la misma que

alcanza a terceros y cualquier otro participante no mencionado que haya sido afectado por los servicios y operaciones de la EC. Para la determinación de daños que resulte legalmente obligado a pagar, se requerirá de un procedimiento judicial en el que pueda establecerse la responsabilidad de la EC IDENTITY DEL PERÚ S.A. y la cobertura con este seguro.

12. REQUISITOS OPERACIONALES DEL CICLO DE VIDA DE LOS CERTIFICADOS

12.1 Certificados Digitales

12.1.1 Tipos de Certificados Digitales

IDENTITY DEL PERU S.A. emite los siguientes tipos de certificados:

a. **Certificado de Persona Natural (1)**

Comercialmente denominado como “Certificado Digital Profesional” o “Certificado Digital de Perfil de Profesional”. Es el tipo de certificado que tiene como propósito permitir a una persona natural acreditarse y ser vinculado con su profesión para firmar digitalmente como tal, asumiendo la responsabilidad de suscriptor y titular de dicho certificado.

b. **Certificado de Persona Jurídica (2):**

Es el tipo de certificado tiene como propósito identificar al firmante como Representante legal, Apoderado o Trabajador de una Organización o Entidad para firmar digitalmente como tal, asumiendo la responsabilidad de suscriptor de dicho certificado. Comercialmente, la EC de IDENTITY DEL PERÚ S.A. emite dos tipos de estos certificados:

- Certificado Digital de Facturación Electrónica SUNAT.
- Certificado Digital de Persona Vinculado a Organización.

c. **Certificado de Agente Automatizado (1)**

Es el tipo de certificado que tiene como propósito identificar a un dispositivo informático perteneciente a una persona jurídica que realiza las operaciones de firma digital o cualificada de forma automática o desatendida, y cuyas acciones se encuentran bajo la responsabilidad del suscriptor del certificado (organización). Dentro de este tipo de certificados, se encuentran los de Operador de Servicios Electrónicos (OSE), de facturación electrónica y certificado de agente automatizado.

12.2 Usos del Certificado Digital

12.1.2 Usos Adecuado Del Certificado Digital

Los Certificados emitidos bajo esta CPS/DPC pueden ser utilizados con los siguientes propósitos:

- **Identificación y Autenticación del Titular:** 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.
- **Integridad del documento firmado:** 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. Se certifica que el mensaje recibido por el Receptor o Destino que confía es el mismo que fue emitido por el Titular.
- **No repudio de origen:** Con el uso de este Certificado también se garantiza que la persona que firma el documento no puede repudiarlo, es decir, el Titular que ha firmado no puede negar la autoría o la integridad de este.

12.2.2 Usos Prohibidos Del Certificado Digital

Los Certificados emitidos bajo esta DPC no pueden ser utilizados para las siguientes circunstancias: Cuando contravengan la Ley de Firmas y Certificados Digitales – Ley 27269, las Guías de Acreditación del INDECOPI o sus anexos.

12.3 Denominación y Nombres de Certificados Digitales

12.1.3 Tipos y Restricciones de Nombres

- Los nombres se distinguen conforme al estándar X.501. La estructura y el contenido de los campos de cada certificado emitido por la EC de IDENTITY DEL PERÚ S.A. se encuentran descritos en la sección Perfiles de Certificado a continuación.
- Las restricciones de nombre están basadas en las políticas del RFC 5280. Los nombres deben ser únicos y en el caso de personas jurídicas, no se podrá volver a asignar un nombre de titular que ya haya sido asignado a un titular diferente.
- En el caso de que exista un conflicto o duplicación del nombre, se establecerá que la entidad que presente información fehaciente y actualizada sobre la titularidad del nombre será atendida para la asignación de esta denominación.

12.2.3 Necesidad de Significado en Nombres

- En casos de emitir varios certificados digitales para una organización, éstos podrán diferenciarse a través de los campos OU, escribiendo como referencia sus roles u propósitos para permitir que los terceros que confían diferencien entre los certificados con los Elementos comunes. En caso se emitan certificados de prueba se colocará como CN “TEST”.

12.3.3 Reglas Para La Interpretación De Varias Formas De Nombres

- IDENTITY DEL PERU S.A. atiende en todo caso a lo marcado por el estándar X.500.

12.4.3 Singularidad De Los Nombres

- IDENTITY DEL PERU S.A. no asigna un nombre a un suscriptor que ya hubiera sido asignado a otro diferente. Para lo cual, la identificación del titular debe estar formada por su nombre y apellidos, además de su documento oficial de identidad.
- Asimismo, cuando aparezcan datos de personas jurídicas, esta identificación se debe realizar por medio de su denominación o razón social y su RUC. Además del nombre y apellidos del suscriptor, más su documento oficial de identidad.

12.5.3 Formato De Nombres

Los certificados información que resulte necesaria para su uso, según determine la correspondiente política de autenticación, firma electrónica, cifrado, evidencia electrónica y/o no repudio.

En general, los certificados digitales emitidos por la EC de IDENTITY DEL PERÚ S.A. contienen la identidad de la persona que los recibe (suscriptor), preferiblemente en los campos Subject Name o Subject Alternative Name, incluyendo los siguientes datos:

- Nombre y Apellidos del Suscriptor, poseedor o representado, en campos separados, o con indicación del algoritmo que permite la separación de forma automática;
- Denominación social de la persona jurídica, cuando corresponda;
- Números y tipo de documentos de identificación correspondientes, de acuerdo con la legislación aplicable al Suscriptor, poseedor o representado, sea persona natural o jurídica.
- Dirección de correo electrónico del suscriptor.
- Otros valores e información podrán ser declarados en los campos OU adicionales.

12.6.3 Limitaciones De Los Nombres

- Se puede utilizar restricciones de nombre (utilizando la extensión del certificado “name constrains”) en aquellos certificados de la EC de IDENTITY DEL PERU S.A. emitidos a terceras partes de forma que solo se pueda emitir por la EC el conjunto de certificados permitido en dicha extensión.
- Para una mejor legibilidad y usabilidad, todos los nombres e información contenida en los certificados digitales podrán ser declarados en MAYÚSCULA y caracteres ASCII estándar, sin símbolos especiales.

12.7.3 Extensión Con Las Facultades De Representación Especial

El certificado, emitido bajo la Política de Certificación de IDENTITY DEL PERU S.A., incluirá una extensión en la que el solicitante detallará las facultades que le han sido otorgadas mediante poder notarial especial para la realización de determinados trámites en nombre y representación de la entidad.

12.8.3 Extensiones Específicas

El certificado, emitido bajo la presente Política, podrá incluir por petición del suscriptor extensiones adicionales con información específica de su propiedad. Esta información estará bajo la exclusiva responsabilidad del suscriptor. Dichas extensiones no se marcarán como críticas y sean reconocibles como tales.

12.4 Perfiles De Certificados Digitales

Todos los certificados emitidos por la EC IDENTITY DEL PERÚ S.A. bajo la Política de Certificación declarada, serán conformes al estándar X.509 versión 3 y al RFC 3039 "Internet X.509 Public Key Infrastructure Qualified Certificates Profile". La EC IDENTITY DEL PERÚ S.A. emite certificados X.509 Versión 3.

12.1.4 Identificadores y Políticas de Identificación

La PKI de la EC de IDENTITY DEL PERÚ S.A. está identificada con el OID: 1.3.6.1.4.1.41061.6.1.1

EC de IDENTITY DEL PERÚ S.A. cuenta con un OID para cada tipo certificado, tal y como se describe a continuación.

En este apartado se establecen los OID para los perfiles de certificados emitidos por la EC IDENTITY DEL PERÚ S.A.

NOMBRE	OID
Política de Certificado de Persona Natural (Certificado Dig. Profesional)	1.3.6.1.4.1.41061.6.1.1.2
Política de Certificado de Persona Jurídica (Cert. Pers. Vinc. Org.)	1.3.6.1.4.1.41061.6.1.1.3
Política de Certificado de Agente Automatizado	1.3.6.1.4.1.41061.6.1.1.4
Política de Certificado de Persona Jurídica (Cert. Dig. Fact. Elec. SUNAT)	1.3.6.1.4.1.41061.6.1.1.1

12.5 Perfil y Extensiones del CRL y OSCP

Todos los certificados emitidos bajo la Política de Certificación de IDENTITY DEL PERU S.A. serán conformes al estándar X.509 versión 3 y al RFC 3039 "Internet X.509 Public Key Infrastructure Qualified Certificates Profile".

- IDENTITY DEL PERU S.A. emite certificados X.509 Versión 3.
- Se soporta y se utilizan CRLs conformes al estándar X.509.
- El perfil del certificado de CRL está redactado en un documento independiente. Dicho documento debe estar a disposición de cualquier tercero que lo solicite bajo demanda.
- El perfil OCSP está redactado en un documento independiente. Dicho documento debe estar a disposición de cualquier tercero que lo solicite bajo demanda.

12.6 VALIDACIÓN INICIAL DE LA IDENTIDAD

12.1.6 Métodos para demostrar la posesión de la clave privada

El modelo de generación de claves utilizado se indica a continuación:

Si el par de claves es generado por el 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 la EC de IDENTITY DEL PERÚ S.A..

Si el par de claves es generado por la ER, la EC de IDENTITY DEL PERÚ S.A. define y hace cumplir procedimientos aprobados para transferir de forma segura la clave privada para el suscriptor (es decir, enviar archivos PFX y contraseñas por diferentes canales y eliminar cualquier clave privada de firma una vez que la transferencia es efectiva).

12.2.6 Generación de Claves por parte de la EC.

- **En Software:** Se entrega al Suscriptor mediante correo a través ficheros protegidos utilizando el Standard PKCS#12. La seguridad del proceso queda garantizada debido a que el código de acceso PKCS#12 que posibilita la instalación de este en las aplicaciones, es entregada por un medio distinto al utilizado en la recepción inicial.
- **En hardware:** La generación de claves se realiza en un dispositivo que cumple el estándar FIPS 140-2 nivel 2 el cual es realizado por personal de IDENTITY DEL PERU S.A. con un rol de confianza del correspondiente o personal de la empresa autorizada para realizar dicha actividad.
- **DSCF**: Los certificados pueden ser emitidos en formato DSCF.

12.3.6 Generación de las claves por el Suscriptor

- El Suscriptor dispone de un mecanismo de generación de claves en software. La prueba de posesión de la clave privada en estos casos es la petición recibida por la EC en formato PKCS#10.
- Las claves privadas serán provistas directamente al suscriptor o al módulo criptográfico del mismo sin generar copias de estas.

12.4.6 Autenticación de la identidad de una organización (certificado de persona jurídica)

La RPS o Declaración de Prácticas de la ER de IDENTITY DEL PERU S.A. describe específicamente los procedimientos de autenticación, documentación requerida y validación de la identidad de personas jurídicas.

12.5.6 Autenticación de la identidad de una identidad individual (certificado de persona natural)

La RPS o Declaración de Prácticas de la ER de IDENTITY DEL PERU S.A. describe específicamente los procedimientos de autenticación, documentación requerida y validación de la identidad de la persona natural profesional.

12.6.6 Autenticación de la identidad de una organización (certificado de agente automatizado)

La RPS o Declaración de Prácticas de la ER de IDENTITY DEL PERU S.A. describe específicamente los procedimientos de autenticación, documentación requerida y validación de la identidad para certificados de agente automatizado.

12.7.6 Información de titular No verificada

En ninguna circunstancia IDENTITY DEL PERU S.A. omitirá las labores de verificación que conduzcan a la identificación del Suscriptor y que se traduce en la solicitud de exhibición de los documentos mencionados para organizaciones y personas naturales.

12.8.6 Validación de la autoridad

- La validación de la Entidad de Certificación IDENTITY DEL PERU S.A. respecto a la propiedad de un dominio, se realiza a través de la comprobación de la existencia de un correo que contiene la dirección del dominio en cuestión y/o verificación de datos de registro de dominio respectivo.
- Los procedimientos de autenticación y de validación son descritos en el documento de Declaración y Política de Registro de IDENTITY DEL PERU S.A..

12.9.6 Criterios para la interoperabilidad

La Entidad de Certificación IDENTITY DEL PERU S.A., únicamente emitirá certificados a ER Subordinadas, que estén directamente vinculadas o terceros con vínculo contractual los cuales se someten al cumplimiento de las CPS/DPC de la EC de IDENTITY DEL PERU S.A..

12.7 Titulares de Certificados Digitales e Información de Atributos

Atributos de nombre por tipos de certificados digitales:

El certificado de firma digital de una persona natural para la obtención de un Certificado Digital Profesional, debe contener lo siguiente:

- Nombre completo;
- Tipo de Documento;
- Número de documento de identidad;
- Dirección de Correo Electrónico;

- Código o Número de Escuela Profesional.

El certificado de firma digital de una persona jurídica debe contener lo siguiente:

- Razón Social de la organización;
- Número Único de Registro Tributario (RUC).
- Tipo de documento de identidad de suscriptor;
- Número de Documento de Identidad del suscriptor;
- Dirección de Correo Electrónico del Suscriptor;
- Cargo del Suscriptor en la organización;
- Área o Departamento de la organización.

El certificado de firma digital de agente automatizado debe contener lo siguiente:

- Razón Social de la organización;
- Número Único de Registro Tributario (RUC).
- Tipo de documento de identidad de suscriptor;
- Número de Documento de Identidad del suscriptor;
- Dirección de Correo Electrónico del Suscriptor;
- Área o Departamento de la organización.

12.8 Identificación y Autenticación

12.1.8 Anonimato y Pseudo Anonimato De Los Titulares

La EC de IDENTITY DEL PERU S.A. puede emitir Certificados anónimos o seudónimos de entidad final, siempre que dichos códigos no estén prohibidos por la política aplicable y, si es posible, se conserva la singularidad del espacio de nombres.

En el certificado del representante legal quedarán registrados sus atributos, los cuales le permitirán utilizar el certificado para realizar transacciones en nombre de la persona jurídica. Tratándose de certificados digitales solicitados por personas jurídicas para su utilización a través de agentes automatizados, la titularidad de certificados y de las firmas digitales generadas a partir de dicho certificado corresponderá a la persona jurídica. La atribución de responsabilidad, para tales efectos, corresponde al representante legal, que en nombre de la persona jurídica solicita el certificado digital.

12.2.8 Reconocimiento, Autenticación Y Papel De Las Marcas Reconocidas

IDENTITY DEL PERU S.A. no podrá volver a asignar un nombre de titular que ya haya sido asignado a un titular diferente.

No obstante, IDENTITY DEL PERU S.A. no se compromete a buscar evidencias acerca de los derechos de uso sobre marcas registradas u otros signos distintivos con anterioridad a la emisión de los certificados.

12.9 Identificación y autenticación para peticiones de re-emisión de claves

IDENTITY DEL PERU S.A. realiza en todos los eventos del proceso de autenticación del solicitante incluso en los de re-emisión y con base en ello emite los certificados digitales.

Los procedimientos de autenticación son descritos en el documento de Declaración y Política de Registro de IDENTITY DEL PERU S.A..

12.10 Identificación y Autenticación tras Una Revocación

Debido a que una revocación implica la expedición de un nuevo certificado, IDENTITY DEL PERU S.A. realiza un nuevo proceso de autenticación del solicitante.

Los procedimientos de autenticación son descritos en el documento de Declaración y Política de Registro de IDENTITY DEL PERU S.A.

12.11 Identificación y autenticación para peticiones de revocación

IDENTITY DEL PERU S.A. atiende las peticiones de revocación de conformidad con las causales de revocación especificadas en el documento de Declaración y Política de Registro de IDENTITY DEL PERU S.A., y autentica la identidad de quien solicita la revocación de certificado.

Los procedimientos de autenticación de la identidad de los titulares y suscriptores son descritos en la RPS o Declaración de Prácticas como ER de IDENTITY DEL PERU S.A.

13. TRAMITACIÓN DE SOLICITUD DE CERTIFICADOS

13.1 Solicitud del certificado digital

Dicho procedimiento le compete a la Entidad de Registro (ER) y por lo tanto se describe en el documento Declaración y Política de Registro de la ER de IDENTITY DEL PERU S.A.

13.2 Quién puede solicitar un certificado digital

Los procedimientos relativos a la Entidad de Registro son descritos en el documento de Declaración y Política de Registro de la ER de IDENTITY DEL PERU S.A.

13.3 Proceso de registro y responsabilidades

Los procedimientos relativos a la Entidad de Registro son descritos en el documento de Declaración y Política de Registro de la ER de IDENTITY DEL PERU S.A..

13.4 Realización de las funciones de identificación y autenticación

Los procedimientos relativos a la Entidad de Registro son descritos en el documento de Declaración y Política de Registro IDENTITY DEL PERU S.A..

13.5 Aprobación o rechazo de las solicitudes de certificados

Los procedimientos relativos a la Entidad de Registro son descritos en el documento de Declaración y Política de Registro de la ER de IDENTITY DEL PERU S.A..

13.6 Plazo para procesar las solicitudes de certificados

Los procedimientos relativos a la Entidad de Registro son descritos en el documento de Declaración y Política de Registro de la ER de IDENTITY DEL PERU S.A..

14. EMISIÓN DE CERTIFICADOS DIGITALES

14.1 Actuaciones de la EC durante la emisión de certificados

Una vez aprobada la solicitud se procederá a la emisión del certificado, que deberá ser entregado de forma segura al Suscriptor. Contamos con 3 casos en los que un certificado digital puede ser emitido:

14.1.1 Emisión de certificado mediante software (.pfx. O .p12)

- La Entidad de Certificación recibe la solicitud de la Entidad de Registro asociada una vez que la validación de identidad fue completada correctamente.
- El Operador de Registro aprueba la solicitud usando su firma digital.
- El solicitante recibe el enlace de descarga del certificado en el correo electrónico indicado en el pedido.

14.2.1 Emisión de certificado mediante hardware (token criptográfico o smartcard)

- La Entidad de Certificación recibe la solicitud de la Entidad de Registro asociada una vez que la validación de identidad fue completada correctamente.
- El Operador de Registro aprueba la solicitud usando su firma digital.

- El certificado se instala directamente en el dispositivo criptográfico del solicitante usando Internet Explorer mediante el formato PKCS#10.

14.3.1 Notificación al suscriptor por la EC de la emisión del certificado

La EC de IDENTITY DEL PERU S.A. notificará al Suscriptor la emisión del certificado y el método de descarga si es necesario.

15. ACEPTACIÓN DEL CERTIFICADO

15.1 Forma en la que se acepta el certificado

El certificado se considera aceptado una vez que es descargado. La EC de IDENTITY DEL PERU S.A. cuenta con un mecanismo para saber cuándo el certificado digital es descargado a fin de dar la conformidad correspondiente.

Por otro lado, el titular/suscriptor puede dar a conocer su inconformidad con algún dato del perfil del certificado digital a través de un medio no repudiable como un correo electrónico o documentos firmados digitalmente, por ejemplo.

15.2 Publicación del certificado por la EC

Los procedimientos relativos a la Entidad de Registro son descritos en el documento de Declaración y Política de Registro de IDENTITY DEL PERU S.A..

15.3 Notificación de la emisión del certificado por la EC a otras entidades

La EC de IDENTITY DEL PERU S.A. notifica sobre la emisión de un certificado digital a través de la plataforma de la ER de IDENTITY DEL PERU S.A..

16. USO DEL PAR DE CLAVES Y DEL CERTIFICADO

16.1 Uso de la clave privada y del certificado por el titular/suscriptor

Los suscriptores deben proteger su clave privada teniendo cuidado de evitar la divulgación a terceros. El contrato de Suscriptor identifica las obligaciones del Suscriptor con respecto a la Protección de Clave Privada (para más información, revisar el documento: (DECLARACIÓN Y POLÍTICA DE REGISTRO DE LA ER DE IDENTITY DEL PERÚ S.A.). Las claves privadas sólo se deben utilizar como se especifica en los campos de uso de clave y de uso extendido de clave como se indica en el Certificado correspondiente. Donde es posible hacer una copia de seguridad de una clave privada, los suscriptores deben utilizar el mismo nivel de cuidado y protección atribuido a la clave privada en vivo. Al final de la vida útil de una clave privada, los suscriptores deben eliminar de forma segura la clave privada y los fragmentos que se han dividido para fines de copia de seguridad.

16.2 Uso de la clave privada y del certificado por terceros que confían

Es responsabilidad de los terceros que confían, verificar el estado del certificado. Asimismo, podrán utilizar los certificados para aquello que establece la presente DPC y la Política de Certificación.

17. RE-EMISIONES DEL CERTIFICADO DIGITAL

17.1 Re-emisión del certificado Sin cambio de claves

La EC de IDENTITY DEL PERU S.A. no permite la re-emisión de certificados sin renovación de claves.

17.2 Re-emisión del certificado con cambio de claves

Para la Entidad de Certificación de IDENTITY DEL PERU S.A. un requerimiento de re-emisión de un certificado con cambio de claves es un requerimiento normal de solicitud de un certificado digital como si fuera uno nuevo y por consiguiente implica el cambio de claves y así lo reconoce y acepta el solicitante y suscriptor.

La EC de IDENTITY DEL PERU S.A. comunicará al suscriptor, con una anticipación de al menos 30 días antes de la expiración del certificado, para que pueda renovar a tiempo dicho certificado. Si el suscriptor no solicita la re-emisión de certificado, el certificado expirará. Luego de ello, el suscriptor deberá realizar el proceso de validación de identidad desde la etapa inicial.

17.3 Circunstancias para la re-emisión de certificados con cambio de claves

Las circunstancias son definidas en la Declaración y Política de Registro de IDENTITY DEL PERU S.A. como Entidad de Registro.

17.4 Quién puede solicitar una re-emisión con cambio de claves

Las precisiones sobre quién puede solicitar una re-emisión son definidas en la Declaración y Política de Registro de IDENTITY DEL PERU S.A. como Entidad de Registro.

17.5 Trámites para la solicitud de re-emisión de certificados con cambio de claves

El procedimiento para re-emisión de certificados digitales es definido en la Declaración y Política de Registro de IDENTITY DEL PERU S.A. como Entidad de Registro.

17.6 Notificación al titular de la emisión de un nuevo certificado con cambio de claves

El procedimiento para re-emisión de certificados digitales es definido en la Declaración y Política de Registro de IDENTITY DEL PERU S.A. como Entidad de Registro.

17.7 Forma en la que se acepta la re-emisión de un certificado

El procedimiento para re-emisión de certificados digitales es definido en la Declaración y Política de Registro de IDENTITY DEL PERU S.A. como Entidad de Registro.

17.8 Publicación del certificado re-emitido por la EC

El procedimiento para re-emisión de certificados digitales es definido en la Declaración y Política de Registro de IDENTITY DEL PERU S.A. como Entidad de Registro.

17.9 Notificación de la emisión de un certificado re-emitido por la EC a otras entidades

El procedimiento para re-emisión de certificados digitales es definido en la Declaración y Política de Registro de IDENTITY DEL PERU S.A. como Entidad de Registro.

18. MODIFICACIÓN DE CERTIFICADOS

La modificación del certificado se define como la producción de un nuevo certificado que tiene detalles que difieren de un certificado previamente emitido. La EC IDENTITY DEL PERU S.A. trata la modificación de la misma manera que la emisión de un nuevo certificado.

19. REVOCACIÓN Y SUSPENSIÓN DE CERTIFICADOS

19.1 Circunstancias para la revocación de un certificado

Como mínimo, las causas de revocación de un certificado son debido a:

- Exposición, puesta en peligro o uso indebido de la clave privada.

- Deterioro, alteración o cualquier otro hecho u acto que afecte la clave privada.
- Revocación de las facultades de representación y/o poderes de sus representantes legales o apoderados. Cuando la información contenida en el certificado ya no resulte correcta.
- Cuando el suscriptor deja de ser trabajador(a) o miembro de la comunidad de interés o se sustrae de aquellos intereses relativos al titular.
- Cuando el suscriptor o titular incumple las obligaciones a las que se encuentra comprometido dentro de la IOFE a través de lo estipulado en el contrato del suscriptor y/o titular.
- Cuando la información contenida en el certificado ya no resulte correcta.
- Por decisión de la legislación respectiva.
- Falta de pago del certificado.
- La incapacidad sobrevenida o la muerte del suscriptor o responsable del certificado. Resolución de la autoridad administrativa o judicial competente.

19.2 Quién puede solicitar una revocación

La revocación de un certificado podrá solicitarse por:

- El Suscriptor.
- La Entidad u Organización Titular (a través de un representante de esta).
- La ER o la EC que registró y emitió el certificado digital.
- Adicionalmente las que marquen las políticas de certificación concretas.
- Otro tercero que tenga evidencia de alguna circunstancia de revocación previamente mencionada.
- Por mandato judicial o un juez que de acuerdo con la Ley decida revocar el certificado.

19.3 Procedimiento de solicitud de revocación

Los procedimientos principales para revocación de certificados digitales son definidos en la Declaración de Prácticas de Registro de la ER de IDENTITY DEL PERU S.A. o de otra ER vinculada en el futuro. Estos procedimientos tienen que establecer como mínimo algunos de los siguientes requisitos:

- Un mensaje de la ER firmado digitalmente o una comunicación formal de la ER.
- Un mensaje firmado digitalmente por parte del suscriptor.
- El suscriptor y el titular pueden solicitar a la EC o ER la revocación de su certificado utilizando un medio que garantice el no repudio o que sea aceptado por ambas partes.
- Los terceros que deseen realizar la revocación del certificado deben poseer una orden judicial y deben presentarte personalmente o mediante un representante legalmente autorizado en las instalaciones de la EC o ER. Dicha documentación y el proceso de validación de identidad del solicitante se encuentra especificado en la RPS de cada ER.
- Se facilitará a cada ER y por intermedio de ellas al usuario suscriptor, un acceso web/online para que la solicitud de revocación pueda hacerse en línea, las 24 horas y 365 días del año de forma automática, después de las validaciones anteriores, por medio del portal denominado “Centro de Certificación Digital (CCD) - Soluti” en la dirección web: https://certificacion.soluti.pe/

19.4 Periodo de gracia de solicitud de revocación

La EC IDENTITY DEL PERÚ S.A. se compromete a atender validaciones y solicitudes de revocación dentro de las 24 horas siguientes a la realización de la solicitud en la ER o en la EC, o en caso de existir, a la expiración del periodo de gracia de esta.

19.5 Plazo en el que la EC debe resolver la solicitud de revocación

Los procedimientos relativos a la Entidad de Certificación son descritos en el documento de Declaración y Política de Registro de la ER de IDENTITY DEL PERU S.A. Sin prejuicio de ello se establece que:

a. La EC IDENTITY DEL PERÚ S.A. se compromete a atender validaciones y solicitudes de revocación dentro de las 24 horas siguientes a la realización de la solicitud en la ER o en la EC, o en caso de existir, a la expiración del periodo de gracia de esta.
b. Los terceros que confían pueden verificar la vigencia y comprobar el estado de cada certificado digital por medio de los servicios de CRL y OSCP que serán servicios y mecanismos oficiales de comprobación, los cuales serán publicados y actualizados cada 24 horas para la CRL y de forma online para OSCP.

19.6 Requisitos de verificación de las revocaciones por los terceros que confían

Los procedimientos relativos a la Entidad de Certificación son descritos en el documento de Declaración y Política de Registro de la ER de IDENTITY DEL PERU S.A.. Sin prejuicio de ello se establece que:

a. Como requisito de uso del servicio de comprobación para terceros que confían se establecen: Conexión a Internet de al menos 5 MB para acceder al servicio de OSCP o descargar la CRL, así como la clave pública y/o fingerprint del certificado digital.

20. SERVICIOS DE ESTADOS DE CERTIFICADOS

20.1 Características operacionales

A fin de contar con un servicio que permita validar si un certificado digital se encuentra revocado, IDENTITY DEL PERU S.A. cuenta con una CRL que publica desde su página web, sin restricciones de acceso.

20.2 Disponibilidad de servicio

IDENTITY DEL PERU S.A. cuenta con una disponibilidad de la CRL con un mínimo de 99.95% anual y un tiempo programado de inactividad máximo de 0.05% anual.

20.3 Frecuencia de emisión de las CRLs

La frecuencia de actualización de la CRL es diaria (cada 24 horas).

20.4 Frecuencia de actualización de OCSP

El servicio de OSCP es un servicio online, se actualiza automáticamente.

20.5 Tiempo máximo de latencia de las CRLs

El tiempo entre la generación y publicación de la CRL es menor a una (1) hora, tal como lo establece el INDECOPI.

20.6 Disponibilidad de verificación del estado

La información relativa a la CRL estará disponible en línea con un mínimo de 99.95% anual y un tiempo programado de inactividad máximo de 0.05% anual.

20.7 Requisitos de comprobación de la revocación on-line

Para el uso de servicio de la CRL de IDENTITY DEL PERU S.A., se debe tener en cuenta que esta Lista se encuentre firmada por IDENTITY DEL PERU S.A. y que sea la última Lista emitida.

20.8 Otras formas disponibles de divulgación de información de revocación

Además del servicio de CRL y OSCP no se ofrecen otras formas de divulgación.

20.9 Notificación de la revocación de un certificado

La notificación de la revocación de un certificado digital es enviada directamente al correo electrónico brindado por el solicitante y suscriptor.

21. SUSPENSIÓN DE CERTIFICADOS DIGITALES

IDENTITY DEL PERU S.A. no brinda el servicio de suspensión de certificados digitales, únicamente revocación.

21.1 Quién puede solicitar la suspensión

IDENTITY DEL PERU S.A. no brinda el servicio de suspensión de certificados digitales, únicamente revocación.

21.2 Procedimiento de solicitud de suspensión

IDENTITY DEL PERU S.A. no brinda el servicio de suspensión de certificados digitales, únicamente revocación.

21.3 Límites del periodo de suspensión

IDENTITY DEL PERU S.A. no brinda el servicio de suspensión de certificados digitales, únicamente revocación.

22. FINALIZACIÓN DE SUSCRIPCIÓN

La EC describe los procedimientos que pueden ser utilizados por el suscriptor o titular para terminar la suscripción a los servicios de la EC, incluyendo:

- Por expiración de la licencia y tiempo del certificado digital lo que indica vencimiento del periodo para el cual un titular contrato la vigencia del certificado.
- Pérdida de validez por la revocación de los certificados. Ver apartado de Revocación de Certificados Digitales.
- Cuando un suscriptor elija finalizar su suscripción y acceda a la revocación.
- Cuando la EC termine su suscripción al mismo, por fallecimiento del suscriptor o extinción de la persona jurídica que es titular del certificado.
- Por mandato judicial.

23. REGISTRO DE TIEMPO

23.1 Fuente de tiempo confiable

Los registros de solicitudes, emisiones y revocaciones de los certificados digitales de la EC de IDENTITY DEL PERÚ S.A. se encuentran fechados con una fuente de tiempo confiable.

La fuente de tiempo que utiliza EC de IDENTITY DEL PERÚ S.A. es el horario GMT Greenwich Mean Time, plenamente reconocida la Oficina Internacional de Pesas y Medidas (BIPM). Así mismo el protocolo para la sincronización se gestiona en menos de un segundo de acuerdo con las políticas del RFC 5905 “Network Time Protocol”.

24. SEGURIDAD Y GESTIÓN DEL CICLO DE VIDA DE LAS CLAVES

24.1 Generación del par de claves de la EC.

La EC de IDENTITY DEL PERÚ S.A. realizará los esfuerzos que razonablemente estén a su alcance para confirmar que las claves de la EC sean generadas de acuerdo con los estándares.

En particular:

- La generación de la clave de la EC se realizará en un entorno asegurado físicamente por el personal adecuado según los roles de confianza y, al menos, con un control dual. El personal autorizado para desempeñar estas funciones estará limitado a aquellos requerimientos desarrollados en la CPS/DPC
- La generación del par de claves de la EC se realizará en un dispositivo que cumpla los requerimientos que se detallan en el FIPS 140-2.
- La generación del par de claves de la EC se llevará a cabo mediante una ceremonia de llaves, donde participan las más altas autoridades del holding de negocios y directores.
- Se utilizan los parámetros recomendados en el documento de especificaciones técnicas de la ETSI TS 119.
- Parámetros usados para la generación de las claves públicas

Signature suite	Hash function	Signature algorithm
ha256-with-rsa	SHA-256	RSA-PKCSv1_5

24.2 Distribución de la Clave Pública

La EC de IDENTITY DEL PERÚ S.A. mantiene controles para garantizar la integridad y autenticidad de las claves públicas de la EC y cualquier parámetro asociado durante su generación y su subsecuente distribución para:

- Los certificados auto-firmados, como es el caso de las raíces.
- La EC de IDENTITY DEL PERÚ S.A. posee un mecanismo para verificar la autenticidad e integridad del certificado auto-firmado.
- Los certificados de las EC intermedias son firmados por los certificados raíz.
- La distribución de la clave pública de la EC es realizada en concordancia con las prácticas declaradas en la CPS.

24.1.2 Entrega de la Clave Pública al Emisor del Certificado

El envío de la clave pública a la EC de IDENTITY DEL PERÚ S.A. para la generación del certificado se realiza mediante el formato autofirmado PKCS #10, utilizando un canal seguro para la transmisión.

24.2.2 Entrega de la Clave Pública a los Terceros que confían

Los certificados de la EC Raiz y la EC Subordinada, así como su identificación de fingerprint están a disposición en la página web: https://soluti.pe/legal/entidad-certificacion

24.3.2 Tamaño de las claves

Certificado	Tamaño de Clave	Validez
CA Raíz	4096 bits RSA	10 años
CA Subordinada	4096 bits RSA	10 años

24.3 Cambio de claves de una EC

El cambio de claves de entidad final es realizado mediante la realización de un nuevo proceso de emisión y ceremonia de llaves., previamente comunicada a la Autoridad Administrativa Competente.

24.4 Recuperación en caso de compromiso de una clave y desastre natural u otro tipo de catástrofe

La EC de IDENTITY DEL PERU S.A. ha desarrollado un Plan de continuidad, el cual contempla la continuidad de las operaciones en caso ocurra un compromiso de seguridad de la clave raíz de la EC como un caso particular.

24.5 Generación del par de claves del suscriptor

El par de claves será generado por el emisor o bajo su control.

Si las claves del suscriptor/titular son generadas por la EC, ésta deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que las claves son generadas de forma segura y que se mantendrá la privacidad de estas. En particular:

- Las claves serán generadas usando un algoritmo adecuado para los propósitos de la firma electrónica cualificada;
- Las claves tendrán una longitud de clave adecuada para los propósitos de la firma electrónica cualificada y para el algoritmo de clave pública empleado;
- Las claves serán generadas y guardadas de forma segura antes de entregárselas al suscriptor/titular;
- Las claves serán destruidas de forma segura después de su entrega al suscriptor/titular.

24.6 Entrega de la clave privada al suscriptor

Cuando la clave privada del suscriptor/titular sea generada por la EC, ésta le será entregada de manera que la confidencialidad de esta no sea comprometida y sólo el suscriptor/titular tenga acceso a la misma.

La clave privada deberá ser almacenada en todo caso en un dispositivo seguro de almacenamiento de los datos de creación de firma. Así mismo, este dispositivo seguro podrá consistir en un medio de almacenamiento externo (p. ej. Smartcard, Token criptográfico o HSM) o bien en un medio software (p. ej. PKCS10).

Cuando la EC entrega un dispositivo seguro al suscriptor/titular, deberá hacerlo de forma segura. En particular:

- La preparación del dispositivo seguro deberá ser controlada de manera segura por la EC.
- El dispositivo seguro será guardado y distribuido de forma segura.
- Cuando el dispositivo seguro tenga asociado unos datos de activación de Tercero que confía (p.ej. un código PIN), los datos de activación se deberán preparar de forma segura y distribuirse de manera separada del dispositivo seguro de creación de firma.

24.7 Entrega de la clave pública del suscriptor al emisor del certificado

Cuando el Suscriptor pueda generar sus propias claves, la clave pública del Suscriptor tiene que ser transferida a la ER o EC, de forma que se asegure que:

- No ha sido cambiado durante el traslado;
- El remitente está en posesión de la clave privada que se corresponde con la clave pública transferida; y
- El proveedor de la clave pública es el legítimo Tercero que confía que aparece en el certificado.

24.8 Entrega de la clave pública de la EC a los terceros que confían

La EC deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que la integridad y la autenticidad de la clave pública de la EC y los parámetros a ella asociados son mantenidos durante su distribución a los Terceros que confían. En particular:

- La clave pública de la EC estará disponible a los Terceros que confían de manera que se asegure la integridad de la clave y se autentique su origen;
- El certificado de la EC y su Fingerprint (huella digital) estarán a disposición de los Terceros que confían a través de su página web;

24.9 Tamaño y periodo de validez de las claves del emisor

El emisor deberá usar claves basadas en el algoritmo RSA con una longitud mínima de 2048 bits para firmar certificados, en todo caso estará sujeto en este aspecto a la práctica habitual en esta tecnología.

El periodo de uso de una clave privada será como mínimo de un (01) año calendario y máximo de tres (3) años, después del cual deberán cambiarse estas claves. El periodo de validez del certificado de la EC se establecerá como mínimo en atención a lo siguiente:

- El periodo de uso de la clave privada de la EC,
- El periodo máximo de validez de los certificados de los Suscriptores firmados con esa clave.

24.10 Tamaño y periodo de validez de las claves del suscriptor

El Suscriptor deberá usar claves basadas en el algoritmo RSA con una longitud mínima de 2048 bits, en todo caso estará sujeto en este aspecto a la práctica habitual en esta tecnología.

El periodo de uso de una clave privada será como mínimo de un (01) año calendario y máximo de tres (3) años y no excederá del periodo durante el cual los algoritmos de criptografía aplicada y sus parámetros correspondientes dejan de ser criptográficamente fiables.

24.11 Hardware/software de generación de claves

Las claves de la EC deberán ser generadas en un módulo criptográfico validado al menos por el nivel 2 de FIPS 140-1 o por un nivel de funcionalidad y seguridad equivalente.

El par de claves simétricas para los Suscriptores serán generadas en un módulo de software y / o hardware criptográfico.

24.12 Fines del uso de la clave

La EC deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que las claves de firma de la EC son usadas sólo para los propósitos de generación de certificados y para la firma de CRLs.

La clave privada del Suscriptor deberá ser usada únicamente para la generación de firmas electrónicas avanzadas, de acuerdo con el apartado Ámbito de aplicación y usos.

24.13 Protección de la clave privada

La EC deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que las claves privadas de la EC continúan siendo confidenciales y mantienen su integridad. En particular:

- La clave privada de firma de la EC será almacenada y usada en un dispositivo criptográfico seguro, el cual cumple los requerimientos que se detallan en el FIPS 140-2, en su nivel 2.
- Cuando la clave privada de la EC esté fuera del módulo criptográfico esta deberá estar cifrada.
- Se deberá hacer un backup o respaldo de la clave privada de firma de la EC, que deberá ser almacenada y recuperada sólo por el personal autorizado según los roles de confianza, usando, al menos un control dual en un medio físico seguro. El personal autorizado para

desempeñar estas funciones estará limitado a aquellos requerimientos desarrollados en la DPC.

- Las copias de backup de la clave privada de firma de la EC se regirán por el mismo o más alto nivel de controles de seguridad que las claves que se usen en ese momento.

24.14 Del suscriptor/titular

La EC deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que la clave privada está protegida de forma que:

- El suscriptor/titular pueda mantener la clave privada bajo su exclusivo control;
- Su secreto está razonablemente asegurado;
- La clave privada puede ser efectivamente protegida por el suscriptor/titular contra un uso ajeno.

24.15 Estándares para módulos criptográficos

Todas las operaciones criptográficas deben ser desarrolladas en un módulo validado por al menos el nivel 2 de FIPS 140-2 o por un nivel de funcionalidad y seguridad equivalente.

24.16 Control multipersona (N de M) de la clave privada

Se requerirá un control multipersona para la activación de la clave privada de la EC. Este control deberá ser definido adecuadamente por la DPC en la medida en que no se trate de información confidencial o pueda comprometer de algún modo la seguridad del sistema.

24.17 Custodia de la clave privada

La clave privada de la EC debe ser almacenada en un medio seguro protegido criptográficamente y al menos bajo un control dual.

Las claves de los Suscriptores estarán custodiadas por este en dispositivos software.

24.18 Backup de la clave privada

La EC deberá realizar una copia de backup o respaldo de su propia clave privada que haga posible su recuperación en caso de desastre o de pérdida o deterioro de esta de acuerdo con el apartado anterior.

Las copias de las claves privadas de los Suscriptores se regirán por lo dispuesto en el punto anterior.

24.19 Archivo de la clave privada

La clave privada de la EC no podrá ser archivada una vez finalizado su ciclo de vida. Las claves privadas de Suscriptor no pueden ser archivadas por la EC salvo aquellas usadas para cifrado de datos.

24.20 Introducción de la clave privada en el módulo criptográfico

La clave privada de la EC será creada en el propio dispositivo. La recuperación de la clave privada en el módulo criptográfico se realizará con la participación de al menos dos operadores autorizados.

24.21 Método de activación de la clave privada

Se protegerá el acceso a la clave privada del Suscriptor por medio de una contraseña, PIN, u otros métodos de activación equivalentes. Si estos datos de activación deben ser entregados al Suscriptor, esta entrega deberá realizarse por medio de un canal seguro.

Estos datos de activación tendrán una longitud de al menos 4 dígitos en el caso de custodia en un dispositivo hardware y de 8 en el caso de dispositivo software.

Los datos de activación deben ser memorizados por el Suscriptor y no deben ser anotados en un lugar de fácil acceso ni compartidos.

24.22 Método de desactivación de la clave privada

La clave privada de la EC quedará desactivada mediante el borrado del contenido del dispositivo criptográfico que la contiene siguiendo estrictamente los manuales de administrador de dicho dispositivo.

La clave privada del suscriptor/titular quedará inaccesible después de más de tres sucesivos intentos en la introducción del código de activación de forma errada.

24.23 Método para destruir la clave privada

La EC de IDENTITY DEL PERÚ S.A., realizará los esfuerzos que razonablemente estén a su alcance para confirmar que la clave privada de la EC no será usada una vez finalizado su ciclo de vida.

Todas las copias de la clave privada de firma de la EC serán destruidas o deshabilitadas de forma que la clave privada no pueda ser recuperada.

La destrucción o inhabilitación de las claves se detallará en un documento creado al efecto.

Las claves privadas de los Suscriptores serán destruidas e inservibles después del fin de su ciclo de vida por el propio Suscriptor.

24.24 Requisitos especiales de comunicación de claves comprometidas

La EC de IDENTITY DEL PERU S.A. utilizará métodos comercialmente razonables para informar a los suscriptores de que su Clave Privada puede haber sido comprometida. Esto incluye los casos en los que se pudieran descubrir nuevas vulnerabilidades. En situaciones como estas, todos los usuarios deben ser debidamente notificados y guiados para adoptar todas las medidas necesarias para mitigar los impactos.

25. GESTIÓN DEL CICLO DE VIDA DEL MÓDULO CRIPTOGRÁFICO

IDENTITY DEL PERU S.A. protegerá el módulo criptográfico donde se almacena la clave privada, a fin de evitar su compromiso.

- El módulo criptográfico no será manipulado durante su transporte, ese sea hacia el centro de datos, su importación, o algún otro sitio autorizado por el responsable de la EC; para lo cual se mantendrá en su caja y sellada con cinta adhesiva de seguridad “VOID/OPEN” de transferencia total;
- El módulo criptográfico no será manipulado durante su almacenamiento, con excepción del equipo designado para ponerlo en su rack en el centro de datos con supervisión del responsable de la EC, Gerente Oficial de Seguridad Digital y PKI o un miembro del Comité de Seguridad de IDENTITY DEL PERU S.A. asignado por el responsable de la EC;
- Procedimientos y controles deben proteger para restringir el acceso físico a sólo personal autorizado;
- La instalación y activación de la clave de firma de IDENTITY DEL PERU S.A. en el módulo criptográfico será realizada sólo por personal que ocupa roles de confianza (Titulares de las claves), usando al menos un control de acceso de dos personas;
- IDENTITY DEL PERU S.A. verificará que el módulo criptográfico funcione correctamente;
- Las claves de firma de la EC que son almacenadas en un módulo criptográfico serán borradas antes de que el dispositivo sea retirado.

26. CONTROLES FÍSICOS DE LA INSTALACIÓN, GESTIÓN Y OPERACIONAL

26.1 Controles del Ciclo de Vida de EC Subordinadas

IDENTITY DEL PERU S.A., mantiene políticas de seguridad física y lógica para los sistemas utilizados para la emisión y gestión de certificados que abarcan el control de acceso físico, protección contra desastres naturales, factores de seguridad contra incendios, fallas en las utilidades de apoyo (por ejemplo, energía, telecomunicaciones), colapso de estructuras y la recuperación de desastres. Los controles deben ser implementados para evitar la pérdida, daño o compromiso de los activos y la interrupción de las actividades empresariales y el robo de la información y las instalaciones de procesamiento de la información. Asimismo, asegura que la infraestructura tecnológica será escalable de acuerdo con el crecimiento del volumen de los aplicativos de sus clientes.

El proceso de gestión de la Autoridad de Certificación Subordinada es responsabilidad primaria de la Autoridad de Certificación Raíz, junto con el Proveedor de Servicios de Soporte y comprende, en forma macro, el siguiente flujo:

- Emisión, aprobación y distribución de certificados de CA del nivel inmediatamente posterior al suyo;
- Publicación de los certificados emitidos por ella;
- Revocación de los certificados emitidos por ella;
- Emisión, gestión y publicación de su Lista de Certificados de Revocación – LCR;
- Adopción de medidas de seguridad y control, previstas en la normativa vigente, como la Declaración de Prácticas de Certificación y la Política de Seguridad, que están directamente relacionadas con los procesos, procedimientos y actividades de la Autoridad de Certificación;
- Mantenimiento de procesos, procedimientos y actividades de acuerdo con la legislación vigente y con las normas, prácticas y reglas establecidas por el organismo regulador.

26.1.1 Hipótesis de revocación del certificado de EC Subordinada

El certificado de EC del nivel inmediatamente posterior al de EC raíz podrá ser revocado en cualquier momento, a solicitud del titular del certificado de EC o por decisión motivada de EC raíz, con sujeción a los principios de contradicción y defensa amplia.

Un certificado de CA subordinada debe revocarse en cualquiera de las situaciones que se enumeran a continuación:

a. Cuando se compruebe una emisión inadecuada o defectuosa de la misma;
b. Cuando sea necesario cambiar cualquier información contenida en el mismo;
c. En caso de disolución de la EC titular del certificado; o
d. En caso de compromiso de la clave privada de la EC o de sus medios de almacenamiento.

26.2.1 Aspectos Generales - Proceso de Evaluación y Aprobación para la Emisión del Certificado de EC Subordinada

Consideramos, dentro del alcance de la Certificación Digital, algunos aspectos como promocionales, para garantizar la emisión de manera asertiva, así como la gestión de las claves EC Subordinadas, entre los que destacamos:

- EC raíz realiza las funciones de identificación y autenticación previstas en su CPS/DPC;
- La EC raíz debe garantizar que se cumplan todos los aspectos técnicos y procesales para la emisión del certificado de EC Posterior, bajo el riesgo de no proceder con la emisión, en caso de cualquier incumplimiento;

- Se debe seguir el procedimiento de ceremonia de emisión del certificado de la EC subordinada, denominada “Ceremonia de EC”.

26.3.1 Ceremonia de emisión del certificado de EC subordinada

La emisión de un certificado por parte de EC raíz se realiza en una ceremonia específica, con la presencia de un representante de EC raíz, de la EC subordinada y, en su caso, auditor(es), en la que se registran todos los procedimientos realizados.

Como resultado de la ceremonia, las claves públicas de los certificados de las EC Subordinadas deberán ser debidamente publicadas, en el repositorio debidamente indicado. La emisión de certificados de EC raíz y EC de nivel inmediatamente posterior se realiza utilizando equipos de EC raíz, debidamente homologados y declarados.

26.4.1 Conducta al aceptar el certificado de EC subordinada

Cuando la CA Raíz emite un certificado a una EC del nivel inmediatamente posterior al suyo, garantiza que la información contenida en ese certificado ha sido verificada.

Al momento de la entrega del certificado, durante la ceremonia de su emisión por parte de EC raíz, la EC certifica su recepción mediante la firma del Término de Ceremonia de Emisión del Certificado, Término de Ceremonia de Entrega de Clave Pública y Término de Acuerdo por parte de su representante legal.

El certificado se acepta cuando los datos contenidos en el mismo son verificados por la EC o cuando se utiliza por primera vez la clave privada correspondiente.

26.2 Ubicación física y construcción

Las instalaciones subcontratadas por IDENTITY DEL PERU S.A. están construidas en un local lo suficientemente alejado donde no pueda ser afectado por amenazas de aniego, incendio, disturbios o atentados terroristas. La estructura es de concreto armado, reforzado con material de atenuación a ondas expansivas.

- **Ubicación Física:** Centro de Datos EQUINIX RJ1, cito en Rua Voluntários da Pátria 360, Rio de Janeiro, CEP 22270-010, República Federativa de Brasil.

26.3 Acceso físico

El acceso físico a las dependencias de IDENTITY DEL PERU S.A. donde se llevan a cabo procesos de certificación, cuenta con un sistema de control de ingreso, mediante tarjetas de proximidad, también mantiene un registro detallado de acceso al Centro de Datos por personal autorizado, asimismo, cuenta con cámaras de video vigilancia en las áreas de acceso al Data Center, y por último, cuenta con un servicio de seguridad que opera las 24 horas del día para el control de acceso a las instalaciones y monitoreo de las cámaras de video-vigilancia.

26.4 Alimentación eléctrica y aire acondicionado

El control de acceso físico a las dependencias subcontratadas por IDENTITY DEL PERU S.A. es a través de tarjetas de proximidad y es administrado de forma local. Se controlan todos los accesos tanto de ingresos como de salidas de los empleados, clientes, contratistas y visitantes.

26.5 Exposición al agua

Las instalaciones subcontratadas por IDENTITY DEL PERU S.A. cuentan con un edificio seco, es decir, no cuenta con sistemas de agua ni desagüe para servicios generales. Cuenta con cañerías y drenajes exclusivos para el sistema de Aire Acondicionado de precisión, asimismo es importante mencionar que no cuenta con baños, tanque elevado de agua ni torre de agua de refrigeración de los sistemas de AA de confort de las instalaciones del edificio Administrativo.

26.6 Prevención y protección de incendios

Todas las paredes de las instalaciones subcontratadas por IDENTITY DEL PERU S.A., fueron diseñadas y construidas para retardar la propagación del fuego.

26.7 Sistema de almacenamiento

Cada medio de almacenamiento se mantiene solo al alcance de personal autorizado.

26.8 Eliminación del material de almacenamiento de la información

Cuando deje de ser útil, la información sensible es destruida en la forma más adecuada al soporte que la contenga. Todos los medios que alguna vez almacenaron información como claves o certificados digitales serán manejados de manera segura conforme a la clasificación de activos que administra la EC. Los medios de almacenamiento que contienen datos sensibles serán eliminados de manera segura cuando ya no sean requeridos. La EC gestiona una política de gestión de residuos que permite la destrucción de cualquier tipo de material (físico o papel) que pudiera contener información, garantizando la imposibilidad de recuperación de esta información.

26.9 Backup fuera de la instalación

IDENTITY DEL PERU S.A. realiza una copia de seguridad de las claves de la EC, manteniendo en todo momento el alcance a personal autorizado y con controles de seguridad.

27. CERTIFICACIÓN CRUZADA

Para efectos de la validación de certificados digitales, IDENTITY DEL PERÚ S.A. actualmente no considera la ejecución de procedimientos de validación/emisión de certificados cruzados - Certificación Cruzada.

28. CONTROLES DE SEGURIDAD

A fin de garantizar una correcta gestión de la seguridad en los sistemas de información, IDENTITY DEL PERU S.A. lleva a cabo los controles descritos a continuación.

28.1 Roles de confianza

IDENTITY DEL PERU S.A., garantiza que todo el personal de confianza es el descrito a continuación y que garantiza una segregación de funciones que disemina el control y limita el fraude interno, no permitiendo que una sola persona controle de principio a fin todas las funciones de certificación, y con una concesión de mínimo privilegio, cuando sea posible.

Los roles de confianza que intervienen en el ciclo de vida de IDENTITY DEL PERU S.A. son los siguientes:

- Responsable de la EC;
- Jefe de Servicios de Certificación Digital;
- Jefe de Tecnología y Soporte;
- Titulares de las claves;
- Gerente Oficial de Seguridad Digital y PKI.
- Supervisor de Compliance.

28.2 Responsable de la Seguridad de la Información

- Nombres: Alexandre Dias da Fonseca
- Correos electrónicos: alexandre.fonseca@acsoluti.com.br
- Cargo: Gerente Oficial de Seguridad Digital y PKI

28.3 Documentación de Operaciones

IDENTITY DEL PERÚ S.A. ha documentado y mantiene actualizado todos los procedimientos operativos y de seguridad de las operaciones y actividades lógicas y físicas de la EC.

28.4 Número de personas requeridas por tarea

IDENTITY DEL PERU S.A. garantiza al menos dos personas para realizar las tareas clasificadas como sensibles. Principalmente en la manipulación del dispositivo de custodia de las claves de EC Raíz y EC Subordinadas.

Las personas asignadas para cada rol son identificadas por el Gerente Oficial de seguridad que se asegurará que cada persona realiza las operaciones para las que está asignado. Cada persona solo controla los activos necesarios para su rol, asegurando así que ninguna persona accede a recursos no asignados. El acceso a recursos se realiza dependiendo del activo mediante tarjetas criptográficas y PINs.

28.5 Controles de personal

28.1.5 Requisitos sobre la cualificación, experiencia y conocimiento profesionales

Todo el personal que realiza tareas calificadas como confiables lleva al menos un año trabajando para la EC y tiene contratos laborales fijos. Todo el personal está cualificado y ha sido instruido convenientemente para realizar las operaciones que le han sido asignadas. El personal en puestos de confianza se encuentra libre de intereses personales que entran en conflicto con el desarrollo de la función que tenga encomendada.

28.2.5 Procedimiento de comprobación de antecedentes

El área encargada de Recursos Humanos de IDENTITY DEL PERU S.A. se encarga de realizar las investigaciones pertinentes antes de la contratación de cualquier persona. IDENTITY DEL PERU S.A. nunca asigna tareas confiables a personal con al menos una antigüedad de un año.

Asimismo, el personal de confianza ha sido sometido a verificación de antecedentes penales y policiales.

28.3.5 Requisitos de formación

El personal encargado de tareas de confianza ha sido y será formado de acuerdo con el plan de formación. El plan de formación incluye los siguientes contenidos:

- Principios y mecanismos de seguridad de la jerarquía pública de certificación;
- Versiones de hardware y aplicaciones en uso;
- Tareas que debe realizar la persona;
- Gestión y tramitación de incidentes y compromisos de seguridad;
- Procedimientos de continuidad de negocio y emergencia;
- Procedimiento de gestión y de seguridad en relación con el tratamiento de los datos de carácter personal.

28.4.5 Requisitos y frecuencia de actualización de formación

IDENTITY DEL PERU S.A. realiza los cursos de actualización necesarios para asegurarse de la correcta realización de las tareas de certificación, especialmente cuando se realicen modificaciones sustanciales en las mismas.

28.5.5 Frecuencia y secuencia de rotación de tareas

Se establece que la rotación de tareas será de cada tres años calendario.

28.6.5 Sanciones por actuaciones no autorizadas

Cuando un empleado realice acciones no autorizadas, IDENTITY DEL PERU S.A. tiene la potestad de sancionarlo o incluso ser retirado de la empresa. La decisión será tomada por el Responsable de la EC de IDENTITY DEL PERU S.A.

28.6 Requisitos de contratación de terceros

Los empleados contratados para realizar tareas confiables firman anteriormente las cláusulas de confidencialidad y los requerimientos operacionales empleados por IDENTITY DEL PERU S.A.. Cualquier acción que comprometa la seguridad de los procesos aceptados podría una vez evaluados dar lugar al cese del contrato laboral. En el caso de que todos o parte de los servicios de certificación sean operados por un tercero, los controles y previsiones realizadas en esta sección, o en otras partes de la DPC, serán aplicados y cumplidos por el tercero que realice las funciones de operación de los servicios de certificación, la entidad de certificación será responsable en todo caso de la efectiva ejecución. Estos aspectos quedan concretados en el instrumento jurídico utilizado para acordar la prestación de los servicios de certificación por tercero distinto de IDENTITY DEL PERU S.A. debiendo obligarse los terceros a cumplir con los requerimientos exigidos por IDENTITY DEL PERU S.A..

28.7 Documentación proporcionada al personal

IDENTITY DEL PERU S.A., pone a disposición de todo el personal la documentación donde se detallen las funciones encomendadas, en particular la normativa de seguridad y la DPC.

Esta documentación se encuentra en un repositorio interno accesible por cualquier empleado de IDENTITY DEL PERU S.A., en el repositorio existe una lista de documentos de obligado conocimiento y cumplimiento. Adicionalmente se suministrará la documentación que precise el personal en cada momento, al objeto de que pueda desarrollar de forma competente sus funciones.

28.8 Tipos de eventos registrados

Se registra y guarda los registros de auditoría de todos los eventos relativos al sistema de seguridad de la EC. Se registrarán los siguientes eventos:

- Encendido y apagado del sistema;
- Intentos de creación, borrado, establecimiento de contraseñas o cambio de privilegios;
- Intentos de inicio y fin de sesión;
- Intentos de accesos no autorizados al sistema de la EC a través de la red;
- Intentos de accesos no autorizados al sistema de archivo;
- Acceso físico a los registros de auditoría;
- Cambios en la configuración y mantenimiento del sistema;
- Registros de las aplicaciones de la EC;
- Encendido y apagado de la aplicación de la EC;
- Cambios en los detalles de la EC y/o sus claves;
- Cambios en la creación de políticas de certificados;
- Generación de claves propias;
- Creación y revocación de certificados;
- Registros de la destrucción de los medios que contienen las claves, datos de Activación;
- Eventos relacionados con el ciclo de vida del módulo criptográfico, como recepción, uso y desinstalación.

Así mismo la EC registra el tiempo (fecha y hora) en que ocurren los eventos para su inspección y evaluación.

Todos los eventos registrados son almacenados en base de datos seguras y estarán disponibles a solicitud de las autoridades policiales o judiciales.

28.9 Periodo de retención de los registros de auditoría

IDENTITY DEL PERU S.A. almacena la información de los registros de auditoría al menos durante diez (10) años (incluyendo copias). IDENTITY DEL PERU S.A. almacena la información de acuerdo con la Guía de Acreditación de INDECOPI.

28.10 Protección de los registros de auditoría

Los registros de auditoría se protegen mediante control de acceso. Solo el Administrador del Sistema de la EC tiene la posibilidad de acceder a los mismos.

28.11 Procedimientos de backup de los registros de auditoría

Diariamente se genera un respaldo de todos los servicios y sistemas de la EC de IDENTITY DEL PERU S.A..

28.12 Sistema de recogida de información de auditoría (interna o externa)

La información de la auditoría de eventos es recogida internamente y de forma automatizada por el sistema operativo, la red y por el software de gestión de certificados, además de por los datos manualmente generados, que serán almacenados por el personal debidamente autorizado, todo ello compone el sistema de acumulación de registros de auditoría.

28.13 Notificación al sujeto causa del evento

Cuando el sistema de acumulación de registros de auditoría registre un evento, no será necesario enviar una notificación al individuo, organización, dispositivo o aplicación que causó el evento.

29. ANÁLISIS DE VULNERABILIDADES

El análisis de vulnerabilidades queda cubierto por los procesos de auditoría de IDENTITY DEL PERU S.A.. Anualmente se revisan los procesos de gestión de riesgos y vulnerabilidades dentro del marco de revisión de la acreditación de INDECOPI.

IDENTITY DEL PERU S.A. corrige cualquier problema reportado y es registrado por el Gerente Oficial de Seguridad.

30. ARCHIVO DE REGISTROS

30.1 Tipos de eventos archivados

Los siguientes documentos implicados en el ciclo de vida del certificado son almacenados por la EC o por las ERs:

- Todos los datos relativos a los certificados, incluyendo los contratos de suscriptor/titular;
- Los datos relativos a su identificación;
- Solicitudes de emisión y revocación de certificados;
- Estado de acreditación;
- Tipo de documento presentado en la solicitud del certificado;
- Número de identificación único proporcionado por el documento anterior;
- Todos los certificados emitidos o publicados;
- Claves públicas de la EC;
- El registro de auditorías;
- Políticas y Prácticas de Certificación.

IDENTITY DEL PERU S.A. responsable del correcto archivo de todo este material. En cuanto al ciclo de vida de su certificado, la EC debe registrar lo siguiente:

- Generación de claves de la EC;
- Instalación Manual de Claves Criptográficas de EC y su resultado (con la identidad del operador);
- Respaldo de claves de EC;
- Almacenamiento de claves de EC;
- Recuperación de claves de EC;
- Actividades de repositorio de claves de EC;
- Uso de claves de la EC;
- Archivo de claves de EC;
- Retiro de material usado para las claves del servicio;
- Destrucción del certificado de la EC;
- Autorización de la operación con las claves de la EC;
- Identidad de las entidades que manejan cualquier material de las claves (como los componentes de las claves o las claves almacenadas en dispositivos portables o media);
- Datos de acceso a los dispositivos o los medios que alojan las clave;
- Compromiso de una clave privada.

En cuanto al ciclo de vida de los dispositivos criptográficos, la EC debe registrar lo siguiente:

- Dispositivo del equipo e instalación;
- Colocar dentro o remover un dispositivo de almacenamiento;
- Activación y uso del dispositivo;
- Desinstalación del dispositivo;
- Designación de un dispositivo para el servicio y su reparación;
- Retiro del dispositivo.

En cuanto ciclo de vida de las claves del suscriptor, la EC debe registrar lo siguiente:

- Generación de las claves;
- Archivo de las claves (si fuera aplicable);
- Destrucción de las claves;
- Identidad de la entidad que autoriza las operaciones de gestión de las claves;
- Compromiso de las claves.

La EC debe registrar o requerir a la ER el registro de la siguiente información para la solicitud de certificados:

- El método de identificación aplicados y la información usada para el cumplimiento de los requerimientos del suscriptor;
- Registro de la data, números o combinación, única de identificación o documentos de identificación;
- Locación de almacenamiento de las copias de los documentos de identificación y las solicitudes;
- Identidad de la entidad que acepta las solicitudes;
- Método usado para validar documentos de identificación;

- Nombre de la EC que recibe o de la ER que solicita;
- Aceptación del suscriptor del Acuerdo del Suscriptor
- El consentimiento para permitir a la EC o ER guardar registros de datos personales, pasar esta información a terceras partes especificadas, y publicación de certificados.

La EC debe registrar los siguientes eventos sensibles con respectos a la seguridad:

- Lectura o escritura de registros o archivos sensibles de seguridad, incluyendo los registros de auditoría por sí mismos;
- Acciones tomadas contra los datos sensibles de seguridad;
- Cambios de perfiles de seguridad;
- Uso de mecanismos de identificación y autenticación, considerando ambos casos exitosos y no exitosos (incluyendo múltiples intentos fallidos de autenticación);
- Fallos de los sistemas, del hardware y otras anomalías;
- Acciones tomadas por individuos en Roles de Confianza, operadores computacionales, administradores de sistemas, oficiales de seguridad de sistemas;
- Cambios de la afiliación de una entidad;
- Decisiones para saltar procesos y procedimientos de cifrado y autenticación;
- Acceso a los sistemas de la EC y cualquiera de sus componentes.

30.2 Periodo de conservación

Los certificados, los contratos con los suscriptores y cualquier información indicada en el apartado Tipos de eventos archivados, serán conservados durante al menos diez (10) años.

30.3 Protección de archivos

Las medidas de seguridad que se utilizan para garantizar la confidencialidad de los datos proporcionados por los suscriptores y los titulares comprenden la asignación de personal cualificado para su tratamiento y el almacenamiento en cajas de seguridad ignífugas e instalaciones externas. En este mismo sentido, consideramos la protección y confidencialidad de todos los registros cubiertos por el punto 35 de esta Declaración de Practicas de Certificación y otros aspectos de protección de datos e información.

30.4 Procedimientos de backup del archivo de registros

IDENTITY DEL PERU S.A. realiza copias de respaldo anuales de todos sus documentos electrónicos.

30.5 Sistema de archivo de la información de auditoría (interna o externa)

IDENTITY DEL PERU S.A. cuenta con un documento que describe el procedimiento de gestión de registros de auditoría.

30.6 Procedimientos para obtener y verificar información archivada

IDENTITY DEL PERU S.A. dispone de un documento de seguridad donde se describe el proceso para verificar que la información archivada es correcta y accesible.

31. CONTROLES DE LA SEGURIDAD DE LA INFORMACIÓN

IDENTITY DEL PERU S.A. emplea sistemas fiables para ofrecer sus servicios de certificación. IDENTITY DEL PERU S.A. ha realizado controles y auditorías informáticas a fin de establecer una gestión de sus activos informáticos adecuados con el nivel de seguridad requerido en la gestión de sistemas de certificación electrónica.

Respecto a la seguridad de la información se sigue el esquema de certificación sobre sistemas de gestión de la información de acuerdo con las buenas prácticas de la ISO-270001.

Los equipos usados son inicialmente configurados con los perfiles de seguridad adecuados por parte del personal de sistemas de IDENTITY DEL PERU S.A., en los siguientes aspectos:

- Configuración de seguridad del sistema operativo.
- Configuración de seguridad de las aplicaciones.
- Dimensionamiento y planificación de demanda del sistema.
- Configuración de Usuarios y permisos.
- Configuración de eventos de registros de auditoría.
- Plan de copia de respaldo y recuperación.
- Configuración antivirus
- Requerimientos de tráfico de red.

31.1 Requisitos técnicos de seguridad específicos

Cada servidor de IDENTITY DEL PERU S.A. incluye las siguientes funcionalidades:

- Control de acceso a los servicios de EC y gestión de privilegios;
- Imposición de separación de tareas para la gestión de privilegios;
- Identificación y autenticación de roles asociados a identidades;
- Archivo del historial del Firmante y la EC y datos de auditoría;
- Auditoría de eventos relativos a la seguridad;
- Auto-diagnóstico de seguridad relacionado con los servicios de la EC;
- Mecanismos de recuperación de claves y del sistema de EC Las funcionalidades expuestas son realizadas mediante una combinación de sistema operativo, software de PKI, protección física y procedimientos.

31.2 Evaluación de la seguridad informática

La seguridad de los equipos viene reflejada por un análisis de riesgos iniciales de tal forma que las medidas de seguridad implantadas son respuesta a la probabilidad e impacto producido cuando un grupo de amenazas definidas puedan aprovechar brechas de seguridad.

31.3 Controles de desarrollo de sistemas

IDENTITY DEL PERU S.A. cuenta con un procedimiento de control de cambios en las versiones de sistemas operativos y aplicaciones que impliquen una mejora en sus funciones de seguridad o que corrijan cualquier vulnerabilidad detectada. Como respuesta a los análisis de intrusión y vulnerabilidades se realizan las adaptaciones de los sistemas y aplicaciones que pueden tener problemas de seguridad y a las alertas de seguridad recibidas desde los servicios de seguridad gestionadas contratados con terceros, se realizan ejecutan los RFC (Request for Changes) correspondientes para la incorporación de los parches de seguridad o la actualización de las versiones con problemas.

En el RFC se incorporan y se documentan las medidas tomadas para la aceptación, ejecución o la denegación de dicho cambio. En los casos que la ejecución de la actualización o corrección de un problema incorpore una situación de vulnerabilidad o un riesgo importante se incorpora en el análisis de riesgos y se ejecutan controles alternativos hasta que el nivel de riesgo sea asumible.

31.4 Controles de gestión de seguridad

IDENTITY DEL PERU S.A. desarrolla las actividades precisas para la formación y concienciación de los empleados en materia de seguridad. Los materiales empleados para la formación y los documentos descriptivos de los procesos son actualizados después de su aprobación por un grupo para la gestión de la seguridad. Para realizar esta función dispone de un plan de formación anual.

IDENTITY DEL PERU S.A. exige mediante contrato, las medidas de seguridad equivalentes a cualquier proveedor externo implicado en las labores de certificación.

32. CONTROLES DE SEGURIDAD DE LA RED

IDENTITY DEL PERU S.A. protege el acceso físico a los dispositivos de gestión de red y dispone de una arquitectura que ordena el tráfico generado basándose en sus características de seguridad creando secciones de red claramente definidas. Esta división se realiza mediante el uso de cortafuegos.

La información que se transfiere por redes no seguras se realiza de forma cifrada mediante uso de protocolos SSL.

33. AUDITORÍA Y OTROS CONTROLES

IDENTITY DEL PERU S.A. se somete a auditorías periódicas como se describe en los apartados siguientes.

33.1 Frecuencia o circunstancias de las auditorías y controles

IDENTITY DEL PERU S.A. lleva a cabo auditorías internas y externas. La auditoría interna se llevará a cabo una vez al año. Así mismo, las evaluaciones técnicas del INDECOPI se llevarán a cabo una vez al año y/o cada vez que el INDECOPI lo requiera.

33.2 Identidad/calificación del auditor

INDECOPI se encarga de enviar un listado de auditores siendo decisión de la EC de IDENTITY DEL PERU S.A. la selección del auditor de dicha lista.

33.3 Relación entre el auditor y la entidad auditada

Los auditores son profesionales independientes de la EC de IDENTITY DEL PERU S.A. y no tienen ninguna relación laboral al momento de realizar una auditoría a la EC.

33.4 Aspectos cubiertos por los controles

En líneas generales, las auditorías verifican:

- Que la EC tiene un sistema que garantiza la calidad del servicio prestado;
- Que la EC cumple con los requerimientos de las Políticas de Certificación que gobiernan la emisión de los distintos certificados digitales;
- Que la CPS/DPC, se ajusta a lo establecido en las Políticas, con lo acordado por la AAC y con lo establecido en la normativa vigente;
- Que la EC gestione de forma adecuada la seguridad de sus sistemas de información.

33.5 Auditoría de los registros

Los registros de las auditorías serán revisados como parte de la auditoría anual por la Autoridad Administrativa Competente (AAC) de la IOFE-INDECOPI y sus auditores o el personal que se designe para esta auditoría.

33.6 Auditoría de archivos

Los archivos serán revisados y auditados como parte de la auditoría anual por la Autoridad Administrativa Competente (AAC) de la IOFE-INDECOPI y sus auditores o el personal que se designe para esta auditoría.

33.7 Auditoría de los procedimientos y controles

Los procedimientos y controles serán revisados y auditados como parte de la auditoría anual por la Autoridad Administrativa Competente (AAC) de la IOFE-INDECOPI y sus auditores o el personal que se designe para esta auditoría.

33.8 Tratamientos de los informes de auditoría

Una vez recibido el informe de la auditoría llevada a cabo, IDENTITY DEL PERU S.A. tomará las acciones correspondientes. IDENTITY DEL PERU S.A. ha desarrollado un documento Plan de auditorías que detalla este tipo de evaluación.

34. CONFIDENCIALIDAD DE LA INFORMACIÓN

34.1 Tipo de información de carácter confidencial

Se considerará confidencial o privada toda la información que no esté catalogada expresamente como pública. No se difunde información declarada como confidencial sin el consentimiento expreso por escrito de la entidad, persona u organización que la haya otorgado el carácter confidencial a dicha información, a no ser que exista una imposición legal.

IDENTITY DEL PERU S.A., dispone de una adecuada política de tratamiento de información y de los modelos de acuerdo de confidencialidad que deberán firmar todas las personas que tengan acceso a información confidencial.

Asimismo, cumple en todo caso con la normativa vigente en cada momento en materia de protección de datos personales. En este sentido, este documento sirve, de conformidad con la Ley de Protección de Datos Personales – Ley N°29733, la Norma Marco de Privacidad y la Guía de Acreditación para Entidades de Certificación Digital y Entidades Conexas, en los ámbitos legales, regulatorios y contractuales.

34.2 Información privada

LA EC de IDENTITY DEL PERÚ S.A mantendrá en reserva todo material e información reservado que corresponda a la información de seguridad de su infraestructura e información, y otra información de carácter personal y confidencial de los suscriptores y de los terceros que confían, incluyendo términos contractuales, planes de negocio y propiedad intelectual, además de:

- Información que puede permitir a partes no autorizadas establecer la existencia o naturaleza de las relaciones entre los suscriptores, titulares y los terceros que confían;
- Información que pueda permitir a partes no autorizadas la construcción de un perfil de las actividades de los suscriptores, titulares o terceros que confían.

34.3 Información no privada

Toda información que no vulnere los derechos de los suscriptores, titulares, y terceros que confían. Toda información que haya sido autorizada y permitida por sus autores y titulares.

34.4 Tipo de información considerada no confidencial

Se considera como información no confidencial o pública:

- La contenida en la presente DPC y en las Políticas;
- La información contenida en los certificados.
- La información publicada y publicitada por medios oficiales públicos de la EC.

35. PREPARACIÓN ANTES DEL TÉRMINO Y CESE DE UNA EC

35.1 Cese de la EC de IDENTITY DEL PERÚ S.A.

Antes del cese de su actividad como EC, IDENTITY DEL PERU S.A. realizará las siguientes actuaciones:

- Proveerá de los fondos necesarios, mediante carta fianza, para continuar la finalización de las actividades de revocación;
- Informará a los suscriptores, titulares y terceros que confían del cese con por lo menos treinta (30) días calendario de anticipación;

- Transferirá sus obligaciones relativas al mantenimiento de la información de registro y de los registros de auditoría durante el periodo de tiempo indicado en la DPC.
- Las claves privadas de la EC serán destruidas o deshabilitadas para su uso;
- IDENTITY DEL PERU S.A. mantendrá los certificados activos y el sistema de verificación y revocación hasta la extinción de todos los certificados emitidos;
- Todas estas actividades estarán recogidas en detalle en el Plan de continuidad de IDENTITY DEL PERU S.A..

35.2 Cese de la ER de IDENTITY DEL PERÚ S.A.

Antes de su finalización, la ER de IDENTITY DEL PERU S.A. informará al INDECOPI, a los suscriptores, titulares y terceros que confían sobre el cese de sus operaciones con por lo menos treinta (30) días calendario de anticipación.

36. DATOS DE ACTIVACIÓN

36.1 Generación e instalación de los datos de activación

Los datos de activación de las EC se generan y se almacenan en smartcards o tokens criptográficos únicamente en posesión de personal autorizado.

36.2 Protección de los datos de activación

Solo el personal autorizado conoce los PINs y contraseñas para acceder a los datos de activación.

36.3 Otros aspectos de los datos de activación

No estipulados.

37. OTROS ASUNTOS LEGALES Y COMERCIALES

37.1 Tarifas de emisión de certificados y renovación

Los precios de los servicios de certificación o cualesquiera de los servicios relacionados estarán disponibles en la página web de IDENTITY DEL PERU S.A..

37.2 Tarifas de acceso a los certificados

El acceso a los certificados emitidos es gratuito, no obstante, la EC se reserva el derecho de imponer alguna tarifa para los casos de descarga masiva de CRLs o cualquier otra circunstancia que a juicio de la EC deba ser gravada.

37.3 Tarifas de acceso a la información relativa al estado de los certificados o los certificados revocados

La EC proveerá de un acceso a la información relativa al estado de los certificados libre y gratuita.

37.4 Tarifas por el acceso al contenido de estas políticas de certificación

El acceso al contenido de la presente Política de Certificación será gratuito en su formato digital.

37.5 Política de reintegros

La EC dispondrá de una política de reintegros que se encuentra descrita en los contratos con los suscriptores y a través de la página web: https://soluti.pe/legal/devolucion-dinero

38. DERECHOS DE PROPIEDAD INTELECTUAL

La EC de IDENTITY DEL PERU S.A. es titular de los derechos de propiedad intelectual, que puedan derivarse del sistema de certificación que regula esta DPC y sus políticas. Se prohíbe, por tanto, cualquier acto de reproducción, distribución, comunicación pública y transformación de cualquiera de los elementos que son titularidad exclusiva de la EC sin la autorización expresa por su parte.

No obstante, no necesitará autorización de la EC para la reproducción del Certificado cuando la misma sea necesaria para su utilización por parte del Tercero que confía legítimo y con arreglo a la finalidad del Certificado, de acuerdo con los términos de esta DPC y sus Políticas.

39. RESOLUCIÓN DE DISPUTAS

Para la resolución de disputas el titular/suscriptor podrá escribir desde el correo electrónico que brindó a la ER con los argumentos de la disputa en mención al correo electrónico o dirección física y postal declarada en el punto “Formas de Contacto”, para su revisión y del ser del ámbito será atendido brindando respuesta al titular/suscriptor.

De llegar a alguna disputa o incumplimiento entre las partes, los costos incluido el honorario de abogados será asumido por cada parte.

40. CONFORMIDAD CON LA LEY APLICABLE

IDENTITY DEL PERU S.A. es afecta y cumple con las obligaciones establecidas por la IOFE-INDECOPI, a los requerimientos de la Guía de Acreditación para Entidades de Certificación Digital EC, al Reglamento de la Ley de Certificados Digitales, y a la Ley de Firmas y Certificados Digitales – Ley 27269, para el reconocimiento legal de los servicios que brinda la EC de IDENTITY DEL PERU S.A. bajo las directrices definidas en el presente documento.

41. BIBLIOGRAFÍA

- Guía de Acreditación para Entidades de Certificación Digital EC, INDECOPI
- Ley de Firmas y Certificados Digitales – Ley 27269
- Decreto Supremo 052-2008
- Decreto Supremo 070-2011
- Decreto Supremo 105-2012