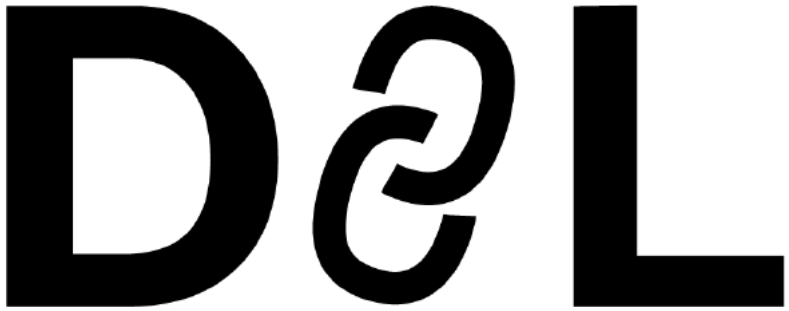

DECLARACIÓN DE PRÁCTICAS Y POLÍTICA DE REGISTRO

Entidad de Registro

Información del documento	
Nombre de documento: **Declaración de Prácticas y Política de Registro de DIGILINK**	
Código de documento: **DL-DPPREG-01**	
Versión: **1.3**	Aprobado por: **Responsable de la Entidad de Registro**
Año: **2024**	Dirigido a: **INDECOPI**

Control de versiones		
Versión	**Fecha**	**Descripción**
1.0	03-01-2022	Elaboración de documento inicial.
1.1	22-03-2022	Se realizaron cambios en el formato.
1.2	17-09-2023	Se realizaron cambios en el formato. Se ha incluido el logo y el código en la cabecera del documento.
1.3	25-01-2024	Cambio de Representante Legal de la empresa.

ÍNDICE

Tabla de contenido

1 INTRODUCCIÓN

DIGILINK S.AC., que en adelante llamaremos "DIGILINK", es una empresa peruana especializada en brindar servicios digitales innovadores de confianza basados en la firma digital desde el año 2021.

Entre sus servicios se encuentran sus funciones como Entidad de Certificación, Entidad de Registro y Autoridad de Sellado de Tiempo, para lo cual DIGILINK se encuentra acreditada ante el INDECOPI para su debido ejercicio.

En calidad de Entidad de Certificación, por medio de su proveedor de servicios GLOBALSIGN, emite certificados digitales a personas naturales y jurídicas.

Como Entidad de Registro, brinda los servicios de verificación de sus clientes, tanto para representantes legales, empleados o agentes automatizados, para la emisión, reemisión o revocación de certificados digitales; así como el registro de las evidencias generadas.

Como entidad de Sellado de Tiempo, DIGILINK asume las responsabilidades de representación de los servicios de sello de tiempo brindados mediante su proveedor GLOBALSIGN, la cual es una infraestructura tercerizada y certificada.

2 OBJETIVO

Este documento tiene como objeto la descripción de las operaciones y prácticas que utiliza DIGILINK para la administración de sus servicios como Entidad de Registro o Verificación – ER, en el marco del cumplimiento de los requerimientos de la "Guía de Acreditación de Entidades de Registros o Verificación (ER)" establecida por el INDECOPI.

3 OBJETO DE LA ACREDITACIÓN

El alcance de la acreditación cubre los sistemas de registro que utiliza DIGILINK en la entrega de sus servicios, y que son proporcionados por la Entidad de Certificación de DIGILINK.

La ER DIGILINK actúa para todos los aspectos de responsabilidad y mediación entre las personas jurídicas y naturales del Estado Peruano y la Entidad de Certificación de DIGILINK.

4 DEFINICIONES Y ABREVIACIONES

Entidad de Certificación – EC	Entidad que presta servicios de emisión, revocación, reemisión, modificación, suspensión de certificados digitales en el marco de la regulación establecida por la IOFE.
Entidad de Registro – ER	Entidad que realiza los procesos de verificación deidentidad de los solicitantes de los servicios de certificación digital y que custodia de forma segura las evidencias de dichos

	procesos.
Declaración de Prácticas de Certificación –DPC o CPS	Documento oficialmente presentado por una Entidad de Certificación a la Autoridad Administrativa Competente, mediante el cual define sus prácticas de certificación.
Política de Certificación – PC o CP	Conjunto de reglas que indican el marco de aplicabilidad de los servicios para una comunidad de usuarios definida y/o clase de aplicación con requisitosde seguridad comunes.
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.

4.1 PKI PARTICIPANTES

4.1.1 ENTIDAD DE CERTIFICACIÓN DIGILINK

DIGILINK, en su papel de Entidad de Certificación, es la persona jurídica privada que presta indistintamente servicios relacionados con las funciones de infraestructura de clave pública (PKI) como el registro de suscriptores, emisión, reemisión, gestión, cancelación u otros servicios inherentes a la certificación digital.

4.1.2 ENTIDAD DE REGISTRO DIGILINK

DIGILINK, brinda los servicios de Entidad de Registro, la cual se encarga de certificar la validez de la información suministrada por el solicitante de un certificado digital, mediante la verificación de su identidad y su registro. Asimismo, la ER puede iniciar o transmitir solicitudes de revocación de certificados y solicitudes de reemisión de certificados.

4.1.3 PROVEEDOR DE SERVICIOS DE CERTIFICACIÓN DIGITAL

Los proveedores de servicios de certificación son terceros que prestan su infraestructura o servicios tecnológicos a la Entidad de Certificación y Registro de DIGILINK, la cual emite certificados digitales de GLOBALSIGN cuando esta entidad así lo requiere y garantizan la continuidad del servicio a los suscriptores y titulares durante todo el tiempo en que se hayan contratado los servicios de certificación digital.

Los servicios de certificación digital que ofrece DIGILINK son provistos en un acuerdo con la Entidad de Certificación de GLOBALSIGN.

4.1.4 TITULAR

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

La figura de Titular será diferente dependiendo de los distintos certificados emitidos por GLOBALSIGN como prestador de servicios de DIGILINK, conforme a lo establecido en el presente documento.

4.1.5 SUSCRIPTOR

Conforme a la IOFE, el Suscriptor es la persona natural responsable del uso de la clave privada, a quien se le vincula de manera exclusiva con un documento electrónico firmado digitalmente utilizando su clave privada.

En el caso que el titular del certificado digital sea una persona natural, sobre ella recaerá la responsabilidad de suscriptor.

En el caso que una persona jurídica sea el titular de un certificado digital, la responsabilidad 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 corresponderán a la persona jurídica. La atribución de responsabilidad del suscriptor, para tales efectos, corresponde a la misma persona jurídica.

4.1.6 SOLICITANTE

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

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

4.1.7 TERCERO QUE CONFÍA

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

4.1.8 ENTIDAD A LA CUAL SE ENCUENTRA VINCULADO EL TITULAR

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

5 SERVICIOS DE CERTIFICACIÓN DIGITAL

DIGILINK brinda los servicios de verificación y registro de usuarios que solicitan la emisión, reemisión, revocación y distribución de los certificados digitales provistos por la Entidad de Certificación de DIGILINK.

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

https://digilink.pe/documentos/

6 RESPONSABILIDADES DE DIGILINK

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

Asimismo, la ER de DIGILINK, representa a la EC para todos los aspectos de ejecución de obligaciones contractuales, responsabilidad y mediación entre las personas jurídicas y naturales del Estado Peruano y la Entidad de Certificación DIGILINK.

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

Las peticiones, quejas o reclamos para la atención de suscriptores y terceros debido a consultas relacionadas con el servicio que dispone la ER, son recibidas directamente por DIGILINK mediante la línea telefónica o correo electrónico. Asimismo, pueden acercarse hacia la oficina de DIGILINK, indicando que presenta una queja, reclamo o petición. Los datos de Contacto se encuentran en esta Declaración de Prácticas y Política de Registro de DIGILINK.

7 USO DEL CERTIFICADO

7.1 TIPOS DE CERTIFICADO

Los tipos de certificado emitidos por DIGILINK, son los siguientes:

CATEGORÍA	TIPO DE CERTIFICADO	DESCRIPCIÓN	REQUISITOS
PERSONA NATURAL	PERSONA NATURAL	Aquellas que tienen la plena capacidad de ejercicio de sus derechos civiles. Las personas naturales asumirán la responsabilidad de titulares y suscriptores de los certificados digitales que adquieren.	- Documento nacional de identidad o Cédula de extranjería - Formulario con datos del

			solicitante - Contrato firmado
PERSONA JURÍDICA	PERSONA JURÍDICA CERTIFICADO DE REPRESENTANTE LEGAL	En el certificado digital del representante legal quedarán registrados todos sus atributos o facultades, los cuales le permitirán utilizar el certificado digital en nombre y representación de la persona jurídica.	- Documento nacional de identidad o Cédula de extranjería - Formulario con datos del solicitante - Vigencia de poder del Representante legal - Ficha RUC - Contrato firmado
	PERSONA JURÍDICA CERTIFICADO DE ATRIBUTOS / EMPLEADO / PERTENENCIA A EMPRESA	Los certificados digitales de los funcionarios o empleados tienen atributos limitados al desenvolvimiento de sus funciones dentro de la persona jurídica.	- Documento nacional de identidad o Cédula de extranjería - Formulario con datos del solicitante - Vigencia de poder del Representante Legal - Ficha RUC - Contrato firmado (firma del Representante y empleado)
	PERSONA JURÍDICA FIRMA DE AGENTES AUTOMATIZADOS	Los certificados digitales solicitados por personas jurídicas para su utilización a través de agentes automatizados. La titularidad de certificados y firmas digitales generadas a partir de dicho	- Documento nacional de identidad o Cédula de extranjería - Formulario con datos del

		certificado digital corresponderá a la persona jurídica.	solicitante - Vigencia de poder del Representante Legal - Ficha RUC
	PROFESIONALES COMO PERSONA JURÍDICA	Aquellas personas que se encuentran colegiadas y habilitadas profesionalmente y desean firmar como profesionales asociados a empresa.	- Documento nacional de identidad o Cédula de extranjería - Formulario con datos del solicitante - Vigencia de poder del Representante Legal - Ficha RUC - Constancia de Habilidad - Contrato firmado

7.2 USOS ADECUADOS DEL CERTIFICADO

Los usos adecuados de los Certificados emitidos son especificados en la Política de Certificación de GLOBALSIGN.

Los Certificados emitidos bajo la CPS de GLOBALSIGN pueden ser utilizados con los siguientes propósitos:

- **Identificación 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 del mismo.

7.3 USOS PROHIBIDOS DEL CERTIFICADO Y EXCLUSIÓN DE RESPONSABILIDAD

Los certificados sólo podrán ser empleados para los usos para los que hayan sido emitidos y especificados en el presente documento y concretamente en la DPC y Políticas de Certificación de GLOBALSIGN.

Se consideran indebidos aquellos usos que no están definidos en la DPC y Políticas de Certificación de GLOBALSIGN o en el presente documento y en consecuencia para efectos legales, DIGILINK y GLOBALSIGN quedan eximidas de toda responsabilidad por el empleo de los certificados en operaciones que estén fuera de los límites y condiciones establecidas para el uso de certificados digitales según tales documentos.

8 PERSONA DE CONTACTO

Datos de la Entidad de Registro:

Nombre: DIGILINK S.A.C

Dirección: Calle Mayorazgo 149, Urb. Chacarilla del Estanque, San Borja

Domicilio: Lima

Teléfono: 933333583 – 998732355

Correo electrónico: informes@digilink.pe

Página Web: https://digilink.pe

9 RESPONSABILIDADES DE LOS TITULARES Y SUSCRIPTORES

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

10 ORGANIZACIÓN QUE ADMINISTRA LOS DOCUMENTOS RPS

DIGILINK administra los documentos de Declaración de Prácticas, y todos los documentos normativos de la ER de DIGILINK.

Para cualquier consulta contactar:

- Nombre: PEDRO SEGUNDO CASTAÑEDA VARGAS
- Cargo: Responsable de la Entidad de Registro de DIGILINK
- Dirección de correo electrónico: pedro.castaneda@digilink.pe

11 PUBLICACIÓN DE LA DECLARACIÓN DE PRÁCTICAS

La Declaración de Prácticas de Registro - RPS de DIGILINK, 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 la siguiente dirección:

https://digilink.pe/documentos/

Todas las actualizaciones o modificaciones relevantes en la documentación de DIGILINK 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 ER de DIGILINK antes de ser publicado, y se controlan las versiones del mismo, a fin de evitar modificaciones y suplantaciones no autorizadas.

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

12 IDENTIFICACIÓN Y AUTENTICACIÓN

DIGILINK mantiene prácticas y procedimientos documentados para autenticar la identidad y otros atributos del Solicitante.

12.1NOMBRES

12.1.1 TIPOS DE NOMBRES

La información relativa a este apartado se encuentra detallada en la DPC de DIGILINK.

12.1.2 NECESIDAD DE QUE LOS NOMBRES TENGAN SIGNIFICADO

La información relativa a este apartado se encuentra detallada en la DPC de DIGILINK.

12.1.3 ANONIMATO Y SEUDOANONIMATO DE LOS TITULARES

La información relativa a este apartado se encuentra detallada en la DPC de DIGILINK.

12.1.4 REGLAS PARA LA INTERPRETACIÓN DE VARIAS FORMAS DE NOMBRE

La información relativa a este apartado se encuentra detallada en la DPC de DIGILINK.

12.1.5 SINGULARIDAD DE LOS NOMBRES

La información relativa a este apartado se encuentra detallada en la DPC de DIGILINK.

12.1.6 RECONOCIMIENTO, AUTENTICACIÓN Y PAPEL DE LAS MARCAS RECONOCIDAS

La información relativa a este apartado se encuentra detallada en la DPC de DIGILINK.

13 SOLICITUD DE EMISIÓN DE CERTIFICADOS DIGITALES

13.1 SOLICITUD DE CERTIFICADOS DE PERSONA JURÍDICA

13.1.1 SERVICIOS BRINDADOS

La ER de DIGILINK brinda los siguientes servicios a personas jurídicas:

a) Atención de solicitudes de emisión, revocación y reemisión[1] de certificados de atributos para personas jurídicas de nacionalidad peruana, para ser usados por funcionarios y personal específico, incluso por el Representante legal.

b) Atención de solicitudes de emisión, revocación y reemisión[2] de certificados de atributos para personas jurídicas de nacionalidad extranjera, para ser usados por funcionarios y personal específico, incluso por el Representante legal.

c) Atención de solicitudes de emisión, revocación y reemisión[3] de certificados que serán usados por agentes automatizados de personas jurídicas de

[1] La reemisión dependerá de lo establecido en la DPC o PC de las EC vinculadas

[2] La reemisión dependerá de lo establecido en la DPC o PC de las EC vinculadas

[3] La reemisión dependerá de lo establecido en la DPC o PC de las EC vinculadas

nacionalidad peruana, como, por ejemplo, servidores de firmas de transacciones y servidores de sellado de tiempo.

d) Atención de solicitudes de emisión, revocación y reemisión[4] de certificados que serán usados por agentes automatizados de personas jurídicas de nacionalidad extranjera, como, por ejemplo, servidores de firmas de transacciones y servidores de sellado de tiempo.

e) Atención de solicitudes de emisión, revocación y reemisión[5] de certificados queserán usados para facturación electrónica.

Los certificados brindados por la ER de DIGILINK corresponden a las Entidades de Certificación acreditadas ante el INDECOPI. En este caso, corresponde a DIGILINK y dicha información se encuentra publicada en las siguientes direcciones:

https://digilink.pe/documentos/

13.1.2 AUTORIZADOS PARA REALIZAR LA SOLICITUD

En ambos casos, tanto certificados de atributos como certificados para agentes automatizados, la solicitud debe ser hecha por un representante designado por la persona jurídica, el cual deberá presentar al Operador de Registro de la ER un documento que acredite sus facultades como representante.

13.1.3 MODALIDADES DE ATENCIÓN

Para ambos casos, tanto certificados de atributos como certificados para agentes automatizados, la solicitud puede ser realizada mediante un contrato de suscriptor/titular de los certificados digitales que puede ser celebrado de la siguiente forma:

- De manera remota, siendo validado por el Operador de Registro de DIGILINK, y firmando su contrato electrónicamente.

13.1.4 SOLICITUD DE CERTIFICADOS DE ATRIBUTOS

En el caso de certificados de atributos, la persona jurídica se considera como aspirante a titular del certificado y los empleados vienen a ser los aspirantes a suscriptor.

El solicitante deberá especificar en su solicitud, la lista de suscriptores y el tipo de atributo al que corresponderá cada certificado, diferenciando al representante legal de la persona jurídica de los trabajadores que como parte de su cargo requieren de un certificado digital. Esta lista deberá ser debidamente firmada por el Representante Legal o una persona asignada por él.

Un mismo suscriptor podrá efectuar solicitudes referentes a múltiples titulares, siempre y cuando exista entre las partes una relación de por medio que faculte al suscriptor para proceder de esa manera.

13.1.5 SOLICITUD DE CERTIFICADOS PARA AGENTES AUTOMATIZADOS

[4] La reemisión dependerá de lo establecido en la DPC o PC de las EC vinculadas

[5] La reemisión dependerá de lo establecido en la DPC o PC de las EC vinculadas

En el caso que el certificado esté destinado para ser usado por un agente automatizado, la solicitud debe ser hecha por el representante designado por la persona jurídica dueña del dispositivo. En este caso, la titularidad del certificado 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.

En la solicitud deberá especificarse el propósito del certificado y el nombre del sistemaa emplear.

13.1.6 PERIODO DE VIGENCIA DE LOS CERTIFICADOS

En el caso de los certificados de atributos, el periodo de vigencia de los certificados solicitados no deberá exceder el periodo de tres (3) años de acuerdo con la legislación vigente.

En el caso de certificados para agentes automatizados, el periodo de vigencia puede variar de acuerdo con lo establecido en la Política de Certificación y Declaración de Prácticas de cada Entidad de Certificación a la que la ER de DIGILINK se encuentra vinculada.

13.1.7 RECONOCIMIENTO, AUTENTICACIÓN Y ROL DE LAS MARCAS REGISTRADAS

Los solicitantes de certificados de personas jurídicas no deben incluir nombres en las solicitudes que puedan suponer infracción de derechos de terceros. La ER de DIGILINK tiene el derecho de rechazar una solicitud de certificado a causa de conflicto de nombres, puesto que no se podrá volver a asignar un nombre de titular que ya haya sido asignado a un titular diferente.

Mediante la verificación de la documentación e información presentada por el solicitante contra los Registros Públicos o la embajada correspondiente, la ER de DIGILINK determinará la validez del nombre de la persona jurídica. Sin embargo, no le corresponde a la ER de DIGILINK, determinar si un solicitante de certificados le asiste algún tipo de derecho sobre el nombre que aparece en una solicitud de certificado, asimismo, no le corresponde resolver ninguna disputa concerniente a la propiedad de nombres de personas naturales o jurídicas, nombres de dominio, marcas o nombres comerciales.

13.1.8 IDENTIFICACIÓN Y AUTENTICACIÓN DE SOLICITANTES DE CERTIFICADOS DE PERSONA JURÍDICA

El solicitante deberá acreditar la existencia de la persona jurídica y su vigencia mediante los instrumentos públicos o norma legal respectiva con el documento de vigencia respectivo expedido por los Registros Públicos o mediante la especificación de la norma legal de creación de la persona jurídica correspondiente. La información proporcionada por los solicitantes será validada a través de la consulta a la Superintendencia Nacional de los Registros Públicos.

En el caso de empresas constituidas en el extranjero, se acreditará su existencia y vigencia mediante un certificado de vigencia de la sociedad u otro instrumento equivalente expedido por la autoridad competente en su país de origen.

13.1.9 CONTRATO DEL TITULAR

El Representante Legal de la persona jurídica o una persona asignada por él, debidamente acreditada, deberá firmar un contrato, que en adelante llamaremos "contrato del titular".

A través de dicho contrato, el titular deberá declarar tener conocimiento de los términos y condiciones aplicables a los certificados.

La celebración de dicho contrato deberá realizarse antes de la emisión de los certificados.

13.1.10VERIFICACIÓN DE SUSCRIPTORES

Los aspirantes a suscriptores deben ser validados de la siguiente manera:

- De manera remota, siendo validado por el Operador de Registro de DIGILINK, y firmando su contrato electrónicamente.

El proceso de verificación de sus identidades debe cumplir los requerimientos establecidos en el presente documento respecto de la autenticación de personas naturales.

Cuando un individuo solicite la emisión de un certificado que sirva para acreditar el ejercicio de un cargo en concreto, la ER debe requerir a este solicitante las pruebas que evidencien su cargo, incluyendo la facultad de actuar en nombre de la persona jurídica en la que ocupa dicho cargo. Además, debe presentar el original de su propio documento oficial de identidad.

13.2SOLICITUD DE CERTIFICADOS DE PERSONA NATURAL

13.2.1 SERVICIOS BRINDADOS

La ER de DIGILINK brinda los siguientes servicios a personas naturales:

a) Atención de solicitudes de emisión, revocación y reemisión[6] de certificados para personas naturales de nacionalidad peruana.

b) Atención de solicitudes de emisión, revocación y reemisión[7] de certificados de atributos para personas naturales de nacionalidad extranjera.

Los certificados corresponden a la Entidad de Certificación de DIGILINK.

13.2.2 AUTORIZADOS PARA REALIZAR LA SOLICITUD

La solicitud en el caso de personas naturales debe ser hecha por la misma persona que pretende ser titular del certificado

13.2.3 MODALIDADES DE ATENCIÓN

La solicitud puede ser realizada mediante un contrato de suscriptor de los certificados digitales que puede ser celebrado de la siguiente forma:

[6] La reemisión dependerá de lo establecido en la DPC o PC de las EC vinculadas

[7] La reemisión dependerá de lo establecido en la DPC o PC de las EC vinculadas

- De manera presencial o remota, siendo validado por el Operador de Registro de DIGILINK, y firmando su contrato electrónicamente.

13.2.4 SOLICITUD DE CERTIFICADOS DE PERSONA NATURAL

El solicitante deberá realizar su solicitud conforme a las modalidades de atención especificadas en el presente documento, portando el original de un documento oficial de identidad, el mismo que deberá estar en vigor en la fecha de realización del proceso de registro. No se admitirán fotocopias u otro tipo de documento.

13.2.5 CONTRATO DEL SUSCRIPTOR

El solicitante deberá firmar un contrato, que en adelante llamaremos "contrato del suscriptor", el cual contiene las obligaciones que deben cumplir los suscriptores y titulares de conformidad con la legislación de la materia para garantizar el efecto legal de las transacciones realizadas, establecidas por las ER de DIGILINK en coordinación con la EC, así como las consecuencias de no cumplir con el acuerdo.

Este contrato deberá ser firmado de manera electrónica por el solicitante, para luego ser archivado por la ER de DIGILINK.

A través de dicho contrato, el suscriptor deberá declarar tener conocimiento de los términos y condiciones aplicables a los certificados.

La celebración de dicho contrato deberá realizarse antes de la emisión de los certificados.

13.2.6 VERIFICACIÓN DE SUSCRIPTORES

Los aspirantes a suscriptores deben ser validados de la siguiente forma:

- De manera remota, siendo validado por el Operador de Registro de DIGILINK, y firmando su contrato electrónicamente.

13.2.7 PERIODO DE VIGENCIA DE LOS CERTIFICADOS

En el caso de los certificados de personas naturales, el periodo de vigencia de los certificados solicitados no deberá exceder el periodo de tres (3) años de acuerdo a la legislación vigente.

13.2.8 IDENTIFICACIÓN Y AUTENTICACIÓN DE SOLICITANTES DE CERTIFICADOS DE PERSONA NATURAL

La información proporcionada por los solicitantes de nacionalidad peruana será validada por la ER de DIGILINK, a través de un mecanismo de consulta a las bases de datos del RENIEC.

En el caso de personas naturales de nacionalidad extranjera, se acreditará su existencia y vigencia mediante su carnet de extranjería en el portal de Migraciones.

De manera general, no se incluirá en los certificados, información no verificada

del suscriptor o el titular según sea el caso. La IOFE permite una excepción en el caso de la dirección de correo electrónico del suscriptor. En este caso se comprobará que la dirección de correo electrónico que se incluye en el certificado es la que efectivamente desea incluir el solicitante. La ER de DIGILINK no asumirá la responsabilidad de comprobar la existencia de la cuenta de correo electrónico indicada por el solicitante, ni que la dirección sea única, ni su correcto funcionamiento, siendo todo esto responsabilidad del solicitante.

14 PROCESAMIENTO DE LA SOLICITUD

14.1RECHAZO DE LA SOLICITUD DE EMISIÓN DE UN CERTIFICADO

La solicitud será rechazada si el solicitante no está capacitado para participar de la comunidad de usuarios de la IOFE:

a) Tratándose de personas naturales, tener plena capacidad de ejercicio de sus derechos civiles.

b) Tratándose de personas jurídicas, acreditar la existencia de la persona jurídica y su vigencia mediante los instrumentos públicos o norma legal respectiva, debiendo contar con un representante debidamente acreditado para tales efectos.

O si el resultado de la validación realizada por la ER fue negativo, conforme a lo establecido en este documento.

Una EC puede decidir establecer en su CPS u otra documentación relevante, circunstancias adicionales para el rechazo de la solicitud, las cuales serán asumidas por la ER de DIGILINK.

14.2APROBACIÓN DE LA SOLICITUD DE EMISIÓN DE UN CERTIFICADO

En caso de que una solicitud sea aprobada por la ER de DIGILINK realizará lo siguiente:

a) Comunicar a la EC su aprobación para la emisión del certificado mediante un sistema web con control de acceso y la protección de un canal SSL. Este sistema será brindado por cada EC.

b) Se requerirá la firma del contrato del suscriptor.

14.3REGISTRO DE DOCUMENTOS

La ER de DIGILINK registrará y archivará la solicitud, los contratos firmados y los documentos de sustento presentados por el solicitante. Estos documentos serán protegidos contra acceso no autorizado y destrucción conforme a la Política de Seguridad.

14.4MÉTODO PARA PROBAR LA POSESIÓN DE LA CLAVE PRIVADA

La generación del par de claves debe realizarse bajo presencia y responsabilidad no transferible del suscriptor.

Los módulos criptográficos distribuidos por DIGILINK cuentan con la certificación FIPS 140-2.

Sin embargo, solamente el suscriptor deberá conocer las claves de acceso al módulo criptográfico donde se realiza la generación de la clave.

14.5TIEMPO PARA EL PROCESAMIENTO DE LA SOLICITUD DE UN CERTIFICADO

Una vez validada la información proporcionada por el suscriptor, si el resultado de la validación es positivo, la ER de DIGILINK enviará a la respectiva EC la autorización de la emisión del certificado de manera inmediata.

El máximo tiempo de respuesta para la emisión del certificado será de cinco (05) días, luego de haber sido aprobada la validación de identidad y del pago respectivo.

14.6EMISIÓN DEL CERTIFICADO

La emisión del certificado será realizada mediante el correo electrónico del suscriptor, registrado en su solicitud.

15 SOLICITUD DE REEMISIÓN DE CERTIFICADOS DIGITALES

La reemisión de un certificado es un proceso programado cada vez que un nuevo par de claves debe ser emitido debido a que la fecha de su expiración es cercana y su periodo de vigencia es menor a un plazo máximo de un año. En los casos que el certificado del titular hubiera expirado o hubiera sido revocado, deberá seguirse el proceso de solicitud para la emisión de un nuevo certificado descrito en el presente documento.

Sólo se podrá realizar una única reemisión de certificado.

El proceso de reemisión es opcional para las EC, por ello la habilitación del proceso dependerá de si dicha habilitación se encuentra establecida en la CPS de la EC que emitió el certificado.

Los procedimientos, requisitos de solicitud y responsabilidades en el uso de los certificados, pueden tener variación de acuerdo con lo establecido en la Política de Certificación y Declaración de Prácticas de cada Entidad de Certificación a la que la ER de DIGILINK se encuentra vinculada, para cada tipo de certificado, tales documentos de la EC son publicados en las siguientes direcciones web:

https://digilink.pe/documentos/

Sin embargo, conforme a lo establecido en la normatividad peruana, la ER de DIGILINK realizará como mínimo, los siguientes procedimientos de verificación para la validación de la identidad de una persona jurídica o natural:

15.1SOLICITUD DE RE-EMISIÓN CERTIFICADOS DE PERSONA JURÍDICA

15.1.1 SERVICIOS BRINDADOS

La ER de DIGILINK brinda los siguientes servicios a personas jurídicas:

a) Atención de solicitudes de reemisión[8] de certificados de atributos para personas jurídicas de nacionalidad peruana, para ser usados por funcionarios y personal específico, incluso por el Representante legal.

b) Atención de solicitudes de reemisión de certificados de atributos para personas jurídicas de nacionalidad extranjera, para ser usados por funcionarios y personal específico, incluso por el Representante legal.

c) Atención de solicitudes de reemisión de certificados que serán usados por agentes automatizados de personas jurídicas de nacionalidad peruana, como, por ejemplo, servidores de firmas de transacciones y servidores de sellado de tiempo.

d) Atención de solicitudes de reemisión de certificados que serán usados por agentes automatizados de personas jurídicas de nacionalidad extranjera, como, por ejemplo, servidores de firmas de transacciones y servidores de sellado de tiempo.

e) Atención de solicitudes de reemisión[9] de certificados para facturación electrónica.

Los certificados corresponden a la Entidad de Certificación y de Registro de DIGILINK.

15.1.2 AUTORIZADOS PARA REALIZAR LA SOLICITUD

Sólo los titulares de certificados pueden solicitar la reemisión de certificados, por lo que, en ambos casos, tanto certificados de atributos como certificados para agentes automatizados, la solicitud debe ser hecha por un representante designado por la persona jurídica, el cual deberá presentar al Operador de Registro de la ER, un documento que acredite sus facultades como representante.

Si como parte de la solicitud inicial el representante ya ha sido validado y registrado por la ER de DIGILINK, bastará con presentar su solicitud firmada electrónicamente. El solicitante deberá presentar su documento oficial de identidad.

15.1.3 MODALIDADES DE ATENCIÓN

Para ambos casos, tanto certificados de atributos como certificados para agentes automatizados, la solicitud puede ser realizada mediante la siguiente forma:

- De manera remota, siendo validado por el Operador de Registro de DIGILINK, y firmando su contrato electrónicamente.

15.1.4 SOLICITUD DE RE-EMISIÓN DE CERTIFICADOS DE ATRIBUTOS

El solicitante deberá especificar en su solicitud, la lista de suscriptores y el tipo de atributo al que corresponderá cada certificado, diferenciando al

[8] La reemisión dependerá de lo establecido en la DPC o PC de las EC vinculadas

[9] La reemisión dependerá de lo establecido en la DPC o PC de las EC vinculadas

representante legal de la persona jurídica de los trabajadores que como parte de su cargo requieren de un certificado digital. Esta lista deberá ser debidamente firmada por el Representante Legal o una personaasignada por él.

15.1.5 SOLICITUD DE RE-EMISIÓN DE CERTIFICADOS PARA AGENTES AUTOMATIZADOS

En el caso que el certificado esté destinado para ser usado por un agente automatizado, la solicitud debe ser hecha por el representante designado por la persona jurídica dueña del dispositivo.

En la solicitud deberá especificarse el propósito del certificado y el nombre del sistema a emplear.

15.1.6 IDENTIFICACIÓN Y AUTENTICACIÓN DE SOLICITANTES DE RE-EMISIÓN DE CERTIFICADOS DE PERSONA JURÍDICA

La ER de DIGILINK comprobará que la información del titular y del suscriptor contenida en la solicitud continúa siendo válida, respecto de la existencia de la persona jurídica en los Registros Públicos y de los suscriptores en la base de datos del RENIEC.

Si cualquier información del titular o del suscriptor hubiere cambiado, se registrará adecuadamente la nueva información. En este caso el titular o su representante deben presentar documentos que respalden dichas modificaciones.

En el caso de empresas constituidas en el extranjero, el solicitante deberá acreditar la continuidad de su existencia y vigencia mediante un certificado de vigencia de la sociedad u otro instrumento equivalente expedido por la autoridad competente en su país de origen.

En el caso de suscriptores extranjeros, estos tendrán que presentar al Operador de Registro, su documento oficial de identidad o carnet de extranjería.

15.2SOLICITUD DE RE-EMISIÓN DE CERTIFICADOS DE PERSONA NATURAL

15.2.1 SERVICIOS BRINDADOS

La ER de DIGILINK brinda los siguientes servicios a personas naturales:

a) Atención de solicitudes de reemisión[10] de certificados para personas naturales de nacionalidad peruana.

b) Atención de solicitudes de reemisión[11] de certificados de atributos para personas naturales de nacionalidad extranjera.

Los certificados corresponden a la Entidad de Certificación de DIGILINK.

15.2.2 AUTORIZADOS PARA REALIZAR LA SOLICITUD

La solicitud en el caso de personas naturales debe ser hecha por la misma

[10] La reemisión dependerá de lo establecido en la DPC o PC de las EC vinculadas

[11] La reemisión dependerá de lo establecido en la DPC o PC de las EC vinculadas

persona que pretende ser titular del certificado.

15.2.3 MODALIDADES DE ATENCIÓN

La solicitud puede ser realizada mediante las siguientes formas:

- De manera remota, siendo validado por el Operador de Registro de DIGILINK, y firmando su contrato electrónicamente.

15.2.4 SOLICITUD DE CERTIFICADOS DE PERSONA NATURAL

El solicitante deberá realizar su solicitud en cualquiera de las modalidades de atención especificadas en el presente documento.

15.2.5 IDENTIFICACIÓN Y AUTENTICACIÓN DE SOLICITANTES DE CERTIFICADOS DE PERSONA NATURAL

La información proporcionada por los solicitantes de nacionalidad peruana será validada por la ER de DIGILINK a través de un mecanismo de consulta a las bases de datos del RENIEC.

En el caso de personas naturales de nacionalidad extranjera, se acreditará su existencia y vigencia mediante su carnet de extranjería.

De manera general, no se incluirá en los certificados, información no verificada del suscriptor o el titular según sea el caso. La IOFE permite una excepción en el caso de la dirección de correo electrónico del suscriptor. En este caso se comprobará que la dirección de correo electrónico que se incluye en el certificado es la que efectivamente desea incluir el solicitante. La ER de DIGILINK no asumirá la responsabilidad de comprobar la existencia de la cuenta de correo electrónico indicada por el solicitante, ni que la dirección sea única, ni su correcto funcionamiento, siendo todo esto responsabilidad del solicitante.

Si cualquier información del titular o del suscriptor hubiere cambiado, se registrará adecuadamente la nueva información. En este caso el titular o su representante deben presentar documentos que respalden dichas modificaciones.

16 PROCESAMIENTO DE LA SOLICITUD DE REEMISIÓN

16.1RECHAZO DE LA SOLICITUD DE EMISIÓN DE UN CERTIFICADO

La solicitud será rechazada si el solicitante no está capacitado para participar de la comunidad de usuarios de la IOFE:

a) Tratándose de personas naturales, tener plena capacidad de ejercicio de sus derechos civiles.

b) Tratándose de personas jurídicas, acreditar la existencia de la persona jurídica y su vigencia mediante los instrumentos públicos o norma legal respectiva, debiendo contar con un representante debidamente acreditado para tales efectos.

O si el resultado de la validación realizada por la ER fue negativo, conforme a lo establecido en este documento.

Una EC puede decidir establecer en su CPS u otra documentación relevante, circunstancias adicionales para el rechazo de la solicitud, las cuales serán asumidas por la ER de DIGILINK.

16.2APROBACIÓN DE LA SOLICITUD DE EMISIÓN DE UN CERTIFICADO

En caso de que una solicitud sea aprobada por la ER de DIGILINK realizará lo siguiente:

a) Se requerirá la firma del contrato del suscriptor.

b) Comunicar a la EC su aprobación para la reemisión del certificado mediante un sistema web con control de acceso y la protección de un canal SSL. Este sistema será brindado por cada EC.

16.3REGISTRO DE DOCUMENTOS

La ER de DIGILINK registrará y archivará la solicitud, los contratos firmados y los documentos de sustento presentados por el solicitante. Estos documentos serán protegidos contra acceso no autorizado y destrucción conforme a la Política de Seguridad.

16.4MÉTODO PARA PROBAR LA POSESIÓN DE LA CLAVE PRIVADA

La generación del par de claves debe realizarse bajo presencia y responsabilidad no transferible del suscriptor, en un módulo criptográfico con la certificación FIPS 140-2. Sin embargo, solamente el suscriptor deberá conocer las claves de acceso al módulo criptográfico donde se realiza la generación de la clave.

16.5TIEMPO PARA EL PROCESAMIENTO DE LA SOLICITUD DE UN CERTIFICADO

Una vez validada la identidad del solicitante, si el resultado de la validación es positivo, la ER de DIGILINK enviará a la respectiva EC la autorización de la emisión del certificado de manera inmediata.

El máximo tiempo de respuesta para la reemisión del certificado será de cinco (05) días, luego de haber sido aprobada la validación de identidad y del pago respectivo.

16.6REEMISIÓN DEL CERTIFICADO

La reemisión del certificado será realizada mediante el correo electrónico del suscriptor, registrado en su solicitud.

17 SOLICITUD DE REVOCACIÓN DE CERTIFICADOS

17.1CIRCUNSTANCIAS PARA REALIZAR LA SOLICITUD

El titular y el suscriptor del certificado están obligados, bajo responsabilidad, a solicitarla revocación al tomar conocimiento de la ocurrencia de, al menos, alguna de las siguientes circunstancias:

- Por exposición, puesta en peligro o uso indebido de la clave privada.
- Por deterioro, alteración o cualquier otro hecho u acto que afecte la clave privada.

- Revocación de las facultades de representación y/o poderes de los representantes legales o apoderados de la persona jurídica
- Cuando la información contenida en el certificado ya no resulte correcta.
- Cuando el suscriptor deja de ser miembro de la comunidad de interés o se sustrae de aquellos intereses relativos a la EC.
- 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.
- Por decisión de la legislación respectiva.

Para mayor detalle sobre la revocación de certificados digitales, revisar la DPC de DIGILINK.

17.2SOLICITUD DE REVOCACIÓN DE CERTIFICADOS

17.2.1 SERVICIOS BRINDADOS

La ER de DIGILINK brinda los siguientes servicios:

a) Atención de solicitudes de revocación de certificados para personas naturales de nacionalidad peruana.

b) Atención de solicitudes de revocación de certificados de atributos para personas naturales de nacionalidad extranjera.

c) Atención de solicitudes de revocación de certificados de atributos para personas jurídicas de nacionalidad peruana, para ser usados por funcionarios y personal específico, incluso por el Representante legal.

d) Atención de solicitudes de revocación de certificados de atributos para personas jurídicas de nacionalidad extranjera, para ser usados por funcionarios y personal específico, incluso por el Representante legal.

e) Atención de solicitudes de revocación de certificados que serán usados por agentes automatizados de personas jurídicas de nacionalidad peruana, como, por ejemplo, servidores de firmas de transacciones y servidores de sellado de tiempo.

f) Atención de solicitudes de revocación de certificados que serán usados por agentes automatizados de personas jurídicas de nacionalidad extranjera, como, por ejemplo, servidores de firmas de transacciones y servidores de sellado de tiempo.

g) Atención de solicitudes de revocación de certificados para facturación electrónica.

Los certificados corresponden a la Entidad de Certificación de DIGILINK.

17.2.2 AUTORIZADOS PARA REALIZAR LA SOLICITUD

De acuerdo con lo estipulado por la Ley, el tipo de personas que pueden solicitar la revocación de un certificado son:

- El titular del certificado
- El suscriptor del certificado.
- La EC o ER que emitió el certificado.
- Un juez que de acuerdo a la Ley decida revocar el certificado.
- Un tercero que tenga pruebas fehacientes del uso indebido del certificado, el compromiso de clave u otro motivo de revocación mencionado en la Ley, los reglamentos de acreditación y el presente documento.

En el caso de personas jurídicas, los titulares de certificados pueden solicitar la revocación de certificados, por lo que, en ambos casos, tanto certificados de atributos como certificados para agentes automatizados, la solicitud debe ser hecha por un representante designado por la persona jurídica, el cual deberá presentar al Operador de Registro de la ER, un documento que acredite sus facultades como representante.

Si como parte de la solicitud inicial el representante ya ha sido validado y registrado por la ER de DIGILINK, bastará con presentar su solicitud firmada de manera manuscrita o con firma digital al Operador de Registro. En el caso de que la solicitud sea firmada de manera manuscrita, el solicitante deberá presentar su documento oficial de identidad.

17.2.3 IDENTIFICACIÓN Y AUTENTICACIÓN DE LOS SOLICITANTES

En los casos de que la solicitud sea presencial:

- Los suscriptores deben presentar en la ER como mínimo su documento oficial de identidad.
- El representante asignado por la persona jurídica debe presentar documentos que acrediten dicha representación y la voluntad de dicha persona jurídica.
- Los terceros (diferentes de la EC, el suscriptor y el titular) deberán presentar en la ER pruebas fehacientes del uso indebido del certificado de acuerdo con la ley vigente, junto a la orden judicial respectiva.

17.2.4 MODALIDADES DE ATENCIÓN

La solicitud puede ser realizada por los titulares y suscriptores mediante las siguientes formas:

- De manera remota, mediante un correo electrónico enviado desde la cuenta del representante asignado por la persona jurídica o por el suscriptor. Dicha cuenta debe ser la registrada inicialmente en el proceso de solicitud.

- De manera remota en una comunicación directa con la EC, mediante un canal brindado al suscriptor en el momento de la solicitud de emisión de los certificados.

Para todos los demás actores, diferentes a los suscriptores y titulares, la solicitud deberá ser de manera remota con la ER de DIGILINK.

La EC no requerirá realizar la solicitud a la ER en los casos que el suscriptor haya infringido las obligaciones descritas en su contrato o en caso sea necesario por revocación del certificado de la EC. Una EC puede revocar los certificados que ha emitido, siempre y cuando los motivos de revocación estén claramente especificados en su CPS y se encuentren de acuerdo con la legislación vigente.

17.2.5 SOLICITUD DE REVOCACIÓN DE CERTIFICADOS DE ATRIBUTOS

El solicitante deberá especificar en su solicitud, la lista de suscriptores y el tipo de atributo al que corresponderá cada certificado, diferenciando al representante legal de la persona jurídica de los trabajadores que como parte de su cargo requieren de un certificado digital. Esta lista deberá ser debidamente firmada por el Representante Legal o una persona asignada por él.

17.2.6 SOLICITUD DE REVOCACIÓN DE CERTIFICADOS PARA AGENTES AUTOMATIZADOS

En el caso que el certificado esté destinado para ser usado por un agente automatizado, la solicitud debe ser hecha por el representante designado por la persona jurídica dueña del dispositivo.

17.2.7 SOLICITUD DE REVOCACIÓN DE CERTIFICADOS DE PERSONA NATURAL

El solicitante deberá realizar su solicitud en cualquiera de las modalidades de atención especificadas en el presente documento.

18 PROCESAMIENTO DE LA SOLICITUD DE REVOCACIÓN

18.1 RECHAZO DE LA SOLICITUD DE REVOCACIÓN EMISIÓN DE UN CERTIFICADO

La solicitud de revocación de certificado será rechazada en caso no se cumpla con alguna de las modalidades de solicitud o que el solicitante no se encuentre debidamente autorizado conforme a lo descrito en el presente documento.

Adicionalmente, la solicitud será rechazada si el solicitante no está capacitado para participar de la comunidad de usuarios de la IOFE:

a) Tratándose de personas naturales, tener plena capacidad de ejercicio de sus derechos civiles.

b) Tratándose de personas jurídicas, acreditar la existencia de la persona jurídica y su vigencia mediante los instrumentos públicos o norma legal respectiva, debiendo contar con un representante debidamente acreditado para tales efectos.

O si el resultado de la validación realizada por la ER fue negativo, conforme a lo establecido en este documento.

Una EC puede decidir establecer en su CPS u otra documentación relevante, circunstancias adicionales para el rechazo de la solicitud, las cuales serán asumidas por la ER de DIGILINK.

18.2APROBACIÓN DE LA SOLICITUD DE REVOCACIÓN DE UN CERTIFICADO

En caso de que una solicitud sea aprobada por la ER de DIGILINK, se realizará lo siguiente:

a) Comunicar a la EC su aprobación para la revocación del certificado mediante un sistema web con control de acceso y la protección de un canal SSL. Este sistema será brindado por cada EC.

b) Una copia de dicha solicitud firmada será enviada a la EC o almacenada en la ER de DIGILINK conforme a los acuerdos celebrados con la EC.

18.3REGISTRO DE DOCUMENTOS

La ER de DIGILINK registrará y archivará la solicitud y los documentos de sustento presentados por el solicitante dejando constancia de la persona que efectúa la solicitud, la relación que tiene ésta con el titular, las razones de la solicitud, las acciones tomadas para la verificación de la veracidad de la solicitud, fecha y hora de la revocación y de la notificación de la misma a la EC, sus suscriptores y los terceros que confían.

Estos documentos serán protegidos contra acceso no autorizado y destrucción conforme a la Política de Seguridad.

En caso de que no se acepte la revocación, se dejará constancia de los hechos que motivaron dicha denegatoria.

18.4TIEMPO PARA EL PROCESAMIENTO DE LA SOLICITUD DE REVOCACIÓN

Una vez validada la información proporcionada por el suscriptor, si el resultado de la validación es positivo, la ER de DIGILINK enviará a la respectiva Área de GlobalSign encargada de la autorización de la revocación del certificado. Una vez comunicado a la EC, este tiempo no debe ser mayor a 2 horas para la actualización de la base de datos de las consultas OCSP y de 24 horas para la actualización de la lista CRL.

18.5REVOCACIÓN DEL CERTIFICADO

La revocación del certificado será comunicada al suscriptor y titular mediante el correo electrónico del suscriptor, registrado en su solicitud.

19 GESTIÓN DE LA SEGURIDAD

Las medidas de seguridad adoptadas para proteger los activos críticos que sostienen los servicios de registro son señaladas en la Política de Seguridad de la ER de DIGILINK.

20 GESTIÓN DE OPERACIONES

20.1MÓDULO CRIPTOGRÁFICO

La generación de claves de los suscriptores es realizada en módulos criptográficos certificados con FIPS 140-2.

Asimismo, los módulos criptográficos usados por los Operadores de Registro cumplen los requerimientos o son equivalentes a los requerimientos de FIPS 140-2 nivel de seguridad 2 como mínimo.

20.2RESTRICCIONES DE LA GENERACIÓN DE CLAVES

Las claves pueden ser generadas solamente por los propios suscriptores.

20.3ENTREGA DE LA CLAVE PÚBLICA

Cuando un suscriptor genera su propio par de claves o par de claves del titular, las claves públicas correspondientes deben ser entregadas al emisor del certificado de manera tal que se asegure la autenticidad de dicho suscriptor.

En los casos en que las ER's acepten las claves públicas en representación de los emisores de los certificados, éstas deberán ser entregadas a dicho emisor de manera tal que se asegure el mantenimiento de la asociación que debe existir entre el titular y la clave.

20.4DEPÓSITO DE CLAVE PRIVADA

La ER de DIGILINK no genera copias de las claves privadas de los suscriptores ni de los Operadores de Registro en ninguna modalidad.

20.5DATOS DE ACTIVACIÓN

Los datos de activación del módulo criptográfico serán administrados por los suscriptores. En caso de obtener módulos criptográficos de DIGILINK, se brindará la información correspondiente para realizar la asignación de los de activación por canales seguros.

21 CONTROLES DE SEGURIDAD COMPUTACIONAL

Los sistemas de registro utilizados por DIGILINK, son provistos y administrados por ECs acreditadas por el INDECOPI. La ER sólo accede a estos sistemas vía web con acceso vía certificados digitales de los Operadores de Registro o mediante un canal seguro.

22 AUDITORÍAS

22.1FRECUENCIAS DE AUDITORÍAS

Las auditorías internas se llevarán a cabo al menos una vez al año en la ER de DIGILINK.

Las evaluaciones técnicas del INDECOPI se llevarán a cabo una vez al año y cada vez que el INDECOPI lo requiera. En dichas evaluaciones, se revisarán los registros y archivos generados por la ER.

22.2CALIFICACIONES DE LOS AUDITORES

La selección de los auditores depende del INDECOPI.

22.3RELACIÓN DEL AUDITOR CON LA ER

Los auditores o asesores deben ser independientes de la ER de DIGILINK.

23 MATERIAS DE NEGOCIO Y LEGALES

23.1TARIFAS

Las tarifas por los servicios de registro y certificación digital serán definidas directamente con sus clientes, a través de Propuestas comerciales enviadas a los solicitantes.

23.2POLÍTICAS DE REEMBOLSO

Las políticas de reembolso por los servicios de registro serán definidas en la DPC de la EC.

23.3COBERTURA DE SEGURO

DIGILINK proporciona a sus clientes servicios de registro amparados por la cobertura del Seguro de Responsabilidad Civil de la Entidad de Certificación que protege las actividades de la Entidad de Registro DIGILINK, conforme a lo requerido por el INDECOPI.

23.4PROVISIONES Y GARANTÍAS

Las garantías por los servicios de registro y certificación digital serán definidas en los contratos de titulares, en relación con errores u omisiones en la identificación del suscriptor, procesamiento de las solicitudes de certificado o de revocación y protección de datos personales provistos.

23.5EXCEPCIONES DE GARANTÍAS

La ER de DIGILINK no se responsabiliza en casos de compromiso de la clave en manos del

suscriptor, o cualquier solicitud no realizada según los procedimientos definidos en el presente documento.

23.6OBLIGACIONES DE LOS SUSCRIPTORES Y TITULARES

Las obligaciones de los suscriptores y titulares se definen en la DPC de la EC y en sus respectivos contratos.

En particular los suscriptores y titulares tienen la responsabilidad de solicitar la revocación de sus certificados en casos de compromiso de su clave privada.

23.7OBLIGACIONES DE LOS TERCEROS QUE CONFÍAN

Las obligaciones del tercero que confía son verificar el estado de confiabilidad de los certificados dentro de los términos establecidos en el marco de la IOFE.

23.8INDEMNIZACIÓN

Los casos de indemnización son definidos en los contratos de los titulares y suscriptores.

23.9NOTIFICACIONES

Los medios de notificación serán definidos en los contratos de titulares y suscriptores.

23.10 ENMENDADURAS Y CAMBIOS

Las enmendaduras y cambios serán comunicados al INDECOPI y luego de su aprobación serán publicadas en el repositorio y notificadas a los titulares y suscriptores, conforme a los medios especificados en sus contratos.

23.11 RESOLUCIÓN DE DISPUTAS

El procedimiento de resolución de disputas será definido en los contratos de los titulares.

23.12 CONFORMIDAD CON LA LEY APLICABLE

La ER de DIGILINK se compromete a cumplir la ley aplicable a las operaciones de registro: las Guías de Acreditación de Entidades de Registro o Verificación del INDECOPI, la Ley de Firmas y Certificados Digitales y su Reglamento.

23.13 SUBROGACIÓN

La ER de DIGILINK no delega sus responsabilidades respecto de las operaciones de registro sobre terceros no autorizados por la IOFE. Todos los casos de responsabilidad de otros participantes como las EC son especificados en este documento.

23.14 FUERZA MAYOR

Las cláusulas de fuerza mayor serán definidas en los contratos de los titulares.

23.15 DERECHOS DE PROPIEDAD INTELECTUAL

La ER de DIGILINK, tiene derechos de propiedad intelectual sobre todos sus documentos normativos, planes, herramientas de software de firma digital y material comercial, y no podrán ser modificados o atribuidos a otra entidad de manera no autorizada.

24 FINALIZACIÓN DE LA ER DE DIGILINK

Antes de su finalización, la ER de DIGILINK informará a los suscriptores, titulares y terceros que confían sobre el cese de sus operaciones con por lo menos treinta (30) días calendario de anticipación. Mientras que, al INDECOPI, se le informará con por lo menos sesenta (60) días calendario de anticipación.

Todas las solicitudes y contratos de suscriptores y titulares serán transferidos al INDECOPI o a otro Prestador de Servicios de Certificación designado por éste.

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

Se advertirá a todos los suscriptores, titulares y terceros que confían, respecto a los cambios y todo tipo de condición asociada a la continuidad del uso de los certificados emitidos por una ER que finaliza o transfiere sus operaciones, mediante un comunicado publicado en la siguiente dirección:

https://digilink.pe

25 BIBLIOGRAFÍA

(1) Guía de Acreditación de Entidades de Registro o Verificación, INDECOPI
(2) Ley de Firmas y Certificados Digitales – Ley 27269
(3) Ley de Protección de Datos Personales – Ley 29733
(4) Decreto Supremo 052-2008
(5) Decreto Supremo 070-2011