Congreso de la República
Oficialía Mayor

RESOLUCIÓN Nº 42 **-2023-2024-OM-CR**

Lima, 21 de noviembre de 2023

CONSIDERANDO:

Que, el Congreso de la República es un Poder del Estado, representativo de la nación y cuenta con autonomía normativa, económica, administrativa y política, de conformidad con lo dispuesto en el artículo 94 de la Constitución Política del Perú y en el artículo 3 del Reglamento del Congreso de la República que tiene fuerza de ley.

Que, el Área de Modernización de la Oficina de Planeamiento, Presupuesto y Modernización, ha elaborado el proyecto de la Directiva Nº 13-2023-OM-CR denominada "*Gestión de Firmas y Certificados Digitales en el Congreso de la República*".

Que, es necesario formalizar la aprobación de la Directiva Nº 13-2023-OM-CR denominada *"Gestión de Firmas y Certificados Digitales en el Congreso de la República"*, mediante una Resolución de la Oficialía Mayor.

De conformidad con lo establecido en el artículo 40 del Reglamento del Congreso de la República y en la Directiva N° 10-2022-OM-CR "*Lineamientos para la Elaboración y Actualización de Documentos Normativos de Gestión – Directivas – Procedimientos*", aprobada con Resolución N° 067-2021-2022-OM-CR y su Modificación N° 1.

Con cargo a dar cuenta a la Mesa Directiva.

SE RESUELVE:

Artículo Único.- APROBAR la Directiva Nº 13-2023-OM-CR denominada "*Gestión de Firmas y Certificados Digitales en el Congreso de la República*".

Regístrese, comuníquese, cúmplase y archívese.

GIOVANNI FORNO FLOREZ
Oficial Mayor
CONGRESO DE LA REPÚBLICA

DIRECTIVA N° 13-2023-OM-CR

GESTIÓN DE FIRMAS Y CERTIFICADOS DIGITALES EN EL CONGRESO DE LA REPÚBLICA

Firmado digitalmente por: ABENSUR PINASCO Jaime Americo FAU 20161749126 hard
Motivo: Doy V° B°
Fecha: 13/11/2023 16:09:08-0500

Firmado digitalmente por: BRICEÑO DIAZ Gala Tatiana FAU 20161749126 hard
Motivo: Doy V° B°
Fecha: 02/11/2023 14:57:35-0500

Firmado digitalmente por: TORRES SARAVIA Jorge Luis FAU 20161749126 hard
Motivo: Doy V° B°
Fecha: 17/11/2023 14:45:09-0500

Firmado digitalmente por: LUQUE YBACETA Paul Ernesto FAU 20161749126 hard
Motivo: Doy V° B°
Fecha: 06/11/2023 12:27:30-0500

Firmado digitalmente por: GUERRERO ESTRADA Rube Oswaldo FAU 20161749126 hard
Motivo: Soy el autor del documento
Fecha: 06/11/2023 16:48:21-0500

Firmado digitalmente por: RAMOS PAULETT Julian Saul FAU 20161749126 hard
Motivo: Soy el autor del documento
Fecha: 06/11/2023 16:59:24-0500

Firmado digitalmente por: ESPINOZA CRUZ Marisol FAU 20161749126 hard
Motivo: Doy V° B°
Fecha: 09/11/2023 14:37:13-0500

Firmado digitalmente por: SARAVIA BONIFACIO Celia Antonia FAU 20161749126 hard
Motivo: Doy V° B°
Fecha: 31/10/2023 17:14:00-0500

Firmado digitalmente por: ALCANTARA INFANTES William Federico FAU 20161749126 hard
Motivo: Doy V° B°
Fecha: 31/10/2023 17:52:12-0500

DIRECTIVA N° 13-2023-OM-CR

GESTIÓN DE FIRMAS Y CERTIFICADOS DIGITALES EN EL CONGRESO DE LA REPÚBLICA

1. OBJETIVO

Establecer los lineamientos y responsabilidades del procedimiento para otorgar los certificados digitales, así como regular la firma digital en el Congreso de la República.

2. FINALIDAD

Contribuir a la incorporación de la firma digital en los documentos electrónicos relacionados a los procedimientos administrativos y parlamentarios del Congreso de la República, como parte de la estrategia de transformación digital y como medida de ecoeficiencia.

3. ALCANCE

Los lineamientos de la presente directiva son de aplicación directa para los Congresistas, Parlamentarios Andinos y personal de la Organización y Servicio Parlamentario; que cuenten con un certificado digital, para el uso de la firma digital en el marco de sus funciones y competencias.

4. BASE LEGAL

- Reglamento del Congreso de la República.
- Ley Nº 27269, Ley de Firmas y Certificados Digitales.
- Ley N° 27658, Ley Marco de Modernización de la Gestión del Estado y sus modificatorias.
- Ley Nº 27310, Ley que modifica el artículo 11 de la Ley 27269.
- Ley Nº 27419, Ley sobre notificación por correo electrónico.
- Ley Nº 30224, Ley que crea el Sistema Nacional para la Calidad y el Instituto Nacional de calidad y que, en su segunda disposición complementaria modificatoria, Incorpora el artículo 15-A a la Ley 27269.
- Decreto Supremo N° 030-2002-PCM, aprueban el Reglamento de la Ley Marco de Modernización de la Gestión del Estado.
- Decreto Supremo Nº 052-2008-PCM, Reglamento de la Ley de Firmas y Certificados Digitales y modificatorias.
- Decreto Supremo N° 009-2009-MINAM, que establece las medidas de ecoeficiencia para el sector público, así como sus modificatorias.
- Decreto Supremo N° 070-2011-PCM, Decreto Supremo que modifica el Reglamento de la Ley N° 27269, Ley de Firmas y Certificados Digitales, y establece normas aplicables al procedimiento registral en virtud al Decreto Legislativo N° 681 y ampliatorias.
- Decreto Supremo Nº 105-2012-PCM, establecen disposiciones para facilitar la puesta en marcha de la firma digital y modifican al Decreto Supremo Nº 052-2008-PCM, Reglamento de la Ley de Firmas y Certificados Digitales.
- Decreto Supremo Nº 004-2013-PCM, Política Nacional de Modernización de la Gestión Pública.
- Decreto Supremo Nº 026-2016-PCM, que aprueba medidas para el fortalecimiento de la infraestructura oficial de firma electrónica y la implementación progresiva de la firma digital en el Sector Público y Privado.
- Decreto Supremo N° 004-2019-JUS, que aprueba el Texto Único Ordenado de la Ley 27444, Ley del Procedimiento Administrativo General.

- Decreto Supremo N° 029-2021-PCM, Decreto Supremo que aprueba el Reglamento del Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital, y establece disposiciones sobre las condiciones, requisitos y uso de las tecnologías y medios electrónicos en el procedimiento administrativo.
- Decreto Supremo N° 126-2021-PCM, Decreto Supremo que aprueba la Sección Primera del Reglamento de Organización y Funciones de la Presidencia del Consejo de Ministros.
- Resolución de Secretaría de Gobierno y Transformación Digital N° 002-2022-PCM/SGTD, publicada el 24 de setiembre de 2022.
- Reglamento de Organización y Funciones del Servicio Parlamentario.
- Convenio Nº 007-2022-AAJ-OM-CR, para el servicio de sellado de tiempo para la generación de sellos de tiempo al Congreso de la República en su calidad de suscriptor del servicio que puede tener uno o varios usuarios finales.

5. DISPOSICIONES GENERALES

5.1. Del servicio

El Área de Soporte y Servicios Informáticos del Departamento de Tecnologías de la Información, está a cargo de la gestión de los certificados digitales; definiendo en la presente directiva los procedimientos para la solicitud, registro, uso de firmas y cancelación de los certificados.

5.2. De los lineamientos.

a) El congresista, funcionario o servidor público que requiere firmar digitalmente documentos electrónicos, debe hacerlo a través de su certificado digital.

b) No se puede hacer uso de la firma digital institucional en ningún tipo de documento relacionado con trámites de índole personal.

c) Los documentos electrónicos firmados digitalmente, deben contar con un sistema de verificación de acuerdo a lo señalado en la normatividad vigente.

d) En casos excepcionales, cuando no se pueda hacer uso de la firma digital; se procede con firma manuscrita.

5.3. De la firma digital.

La firma digital confirma la identidad del firmante del documento electrónico y garantiza que estos documentos no han sido modificados desde su emisión, es decir, que conservan su integridad; se utiliza para dar veracidad legal a los documentos requeridos para los actos y trámites administrativos o parlamentarios.

La obtención del certificado digital emitido por la Entidad de Certificación para el Estado Peruano ECEP – RENIEC, es mediante el uso del componente de software de firma digital acreditado por INDECOPI. Este certificado habilita al suscriptor para el uso de la firma digital, dándole la misma validez y eficacia jurídica que la de una firma manuscrita.

5.4. De las responsabilidades.

a) Del suscriptor

- Entregar información veraz en la Declaración Jurada para el Suscriptor bajo responsabilidad.

- Generar la clave privada y firmar digitalmente mediante los procedimientos señalados por la Entidad de Certificación para el Estado Peruano ECEP – RENIEC, en una Declaración de Prácticas de Certificación.
- Mantener el control y reserva de la clave privada bajo responsabilidad.
- Descargar e instalar su certificado digital cuando el RENIEC le remite sus accesos a través de su correo electrónico.
- Observar las condiciones establecidas por la Entidad de Certificación para la utilización del certificado digital y la generación de firmas digitales.
- En caso de que la clave privada quede comprometida en su seguridad, el suscriptor debe notificar de inmediato al Representante de la Entidad a través de su correo electrónico institucional, para que proceda a la cancelación del certificado digital.

b) Del representante de la entidad.

El representante de la entidad es designado por el Director General de Administración y presentado ante el RENIEC, en atención a lo indicado en el contrato de prestación de servicios de certificación digital certificado clase III – persona jurídica; es responsable de:

- Administrar la plataforma Integrada de la Entidad de Registro PIER para la gestión de certificados digitales.
- Entregar información veraz durante la solicitud de emisión de certificados digitales y demás procesos de certificación (cancelación, suspensión, reemisión y modificación).
- Actualizar la información provista tanto a la Entidad de Certificación (ECEP – RENIEC) como a la Entidad de registro o verificación (EREP - RENIEC), asumiendo la responsabilidad por la veracidad y exactitud de ésta.
- Solicitar la cancelación de su certificado digital en caso de que la reserva sobre la clave privada se haya visto comprometida, bajo responsabilidad.
- Cumplir permanentemente las condiciones establecidas por la Entidad de Certificación para la utilización del certificado digital.
- Solicitar el servicio de pago en el Banco de la Nación por la emisión de certificados digitales, de acuerdo al TUPA del RENIEC.
- Coordinar con el personal técnico del Área de Soporte y Servicios Informáticos para la instalación del certificado digital.

c) Del jefe del Área de Soporte y Servicios Informáticos.

- Contar con certificados digitales disponibles para la atención de las solicitudes de emisión de nuevos certificados o de reemisión de certificados digitales.
- Mantener un stock de token criptográficos para la atención de instalación de certificados digitales y uso de firma digital.
- Generar y revisar el requerimiento SIGA para solicitar el servicio de contratación de certificados digitales de persona jurídica, según los procedimientos establecidos en el TUPA del RENIEC.

d) Del jefe del Departamento de Tecnologías de la Información.

- Aprobar las solicitudes de certificados digitales, que son gestionadas por el jefe del Área de Soporte y Servicios Informáticos.

- Autorizar la asignación de tokens criptográficos a los suscriptores para el uso de la firma digital de acuerdo a las solicitudes de los Congresistas o funcionarios y servidores debidamente autorizados por sus respectivas jefaturas.

5.5. De la autorización.

El uso de los certificados digitales es para los Congresistas, Parlamentarios Andinos del Perú y funcionarios del Congreso de la República.

El uso de certificados digitales para el personal de la institución es solicitado y sustentado por el Congresista o jefe de los órganos o unidades orgánicas correspondientes.

6. DISPOSICIONES ESPECÍFICAS

6.1. De la designación del representante de la entidad.

El Representante Legal del Congreso de la República, emite un oficio a la Entidad de Registro o Verificación para el Estado Peruano EREP-RENIEC, con la finalidad de comunicar la designación del representante de la entidad o apoderado para que gestione los certificados digitales de los suscriptores del Congreso de la República. El representante de la entidad asume las obligaciones del Art. 15 del Reglamento de la Ley de Firmas y Certificados Digitales, aprobado mediante Decreto Supremo N° 052-2008-PCM. Para el llenado del oficio se utiliza el formato establecido por la EREP-RENIEC.

La Dirección General de Administración pone en conocimiento del representante de la entidad su designación, a fin de que inicie la gestión de los certificados digitales.

El representante de la entidad coordina con la EREP-RENIEC para la emisión de su certificado digital y dar inicio a las gestiones de certificados digitales de los suscriptores del Congreso de la República.

6.2. De la solicitud del certificado digital.

Para solicitar un certificado digital, el aspirante a suscriptor llena verazmente el formulario: "Declaración Jurada de identificación no presencial para solicitar certificado digital - Persona Jurídica" establecido por el RENIEC para tal fin. El formulario puede ubicarlo en la sección Formatos de la INTRANET del Congreso de la República.

Una vez llenada la declaración jurada de identificación no presencial para solicitar certificado digital, el aspirante la remite desde su correo institucional al correo institucional del representante de la entidad solicitando la firma digital. Debe sustentar los motivos de su solicitud y para el caso de servidores, debe añadirse la autorización expresa de su respectiva jefatura.

6.3. Del proceso del registro.

a) El representante de la entidad recibe el formato de la Declaración Jurada y revisa que estén todos los datos, foto y firma de acuerdo al instructivo de llenado del formato. En caso hubiera algún error de forma, devuelve el correo al aspirante a suscriptor para su corrección.

b) Luego de revisar el formato y declararlo conforme, el representante de la entidad realiza la gestión de un nuevo certificado digital de persona jurídica a través de la Plataforma Integrada de la Entidad de Registro PIER.

En caso el RENIEC detecte datos incorrectos o incompletos, deniega la solicitud y automáticamente envía un correo al aspirante a suscriptor (solicitante) para que realice las correcciones de los datos.

c) Para efectuar el registro se debe verificar si se cuenta con certificados disponibles y generar la solicitud de los aspirantes registrados. Culminado el registro, la plataforma PIER remite automáticamente un correo informativo al aspirante a suscriptor.

d) La Entidad de Registro o Verificación para el Estado Peruano EREP-RENIEC, procede de acuerdo a los procedimientos establecidos por el RENIEC.

e) Recibido el correo de aprobación por parte del RENIEC, el aspirante a suscriptor puede ponerse en contacto con la Mesa de Ayuda del Área de Soporte y Servicios Informáticos del Congreso y solicitar apoyo técnico durante la instalación del certificado, incluyendo el programa REFIRMA, JAVA u otro software que se requiera para el funcionamiento de la firma digital.

f) Una vez instalado el certificado digital, el aspirante a suscriptor pasa a ser un suscriptor que cuenta con certificado digital y puede hacer uso de la firma digital.

6.4. Del uso de la firma digital.

Los suscriptores hacen uso de la firma digital para firmar documentos electrónicos asignados de acuerdo a sus funciones, utilizando el software REFIRMA o un documento electrónico generado por los sistemas informáticos del Congreso de la República.

Los suscriptores son responsables del contenido del documento electrónico en el que firmen digitalmente utilizando el software REFIRMA, o los sistemas informáticos del Congreso de la República.

El uso de la firma digital en una primera hoja de un conjunto de documentos no exime a los suscriptores de cumplir con lo indicado en la documentación adjunta o sustento de ser el caso, que sean establecidos para la atención del documento o del procedimiento administrativo.

El documento electrónico firmado digitalmente es presentado en un archivo PDF y almacenado con las firmas digitales correspondientes para futuras referencias.

Cuando por razones técnicas no se pueda hacer uso de la firma digital mediante los sistemas informáticos del Congreso de la República o REFIRMA, los suscriptores deben reemplazarla por la firma digital utilizando su DNI electrónico. De no poder firmar digitalmente en ninguno de los casos anteriores o cuando no se pueda hacer uso de la firma digital; se procede con firma manuscrita con el fin de no paralizar las labores diarias en el cumplimiento de sus funciones.

6.5. De la cancelación del certificado digital.

El certificado se cancela en forma automática, luego de que se ha aprobado un certificado digital y la EREP-RENIEC ha enviado un correo al aspirante a suscriptor, han pasado más de treinta (30) días y el aspirante a suscriptor no ha descargado su certificado digital.

La cancelación manual es efectuada por el representante de la entidad cuando el suscriptor ha dejado de ser miembro de la Entidad o en los casos señalados en la normatividad que al respecto defina RENIEC; también procede ante la solicitud expresa de cancelación de su certificado digital o el de un servidor público a su cargo.

6.6. De la reemisión del certificado digital.

La reemisión del certificado digital permite brindar un nuevo certificado digital sin necesidad que se adjunte la declaración jurada del suscriptor, es tramitada antes de que caduque el certificado digital que fuese brindado a través de una declaración jurada. El procedimiento a seguir es el siguiente:

a) El suscriptor solicita autorización al representante de la entidad de la reemisión del certificado digital 30 días antes de que caduque su certificado digital vigente. Los certificados digitales de persona jurídica tienen vigencia de un año calendario.

b) El representante de la entidad selecciona los certificados digitales que están por caducar dentro de los 30 días calendario y autoriza al suscriptor a obtener un nuevo certificado digital a través de la plataforma PIER. Le debe llegar un correo al suscriptor con las indicaciones a seguir.

c) El suscriptor sigue las indicaciones del correo y atiende su propia solicitud ingresando a la plataforma PIER en la opción "Reemisión del Certificado Digital".

d) Una vez firmada y presentada la solicitud por el suscriptor, debe ir a la opción Usuario DC Delivery de la plataforma PIER para instalar su certificado digital.

e) En caso de presentarse dificultades, el suscriptor puede solicitar el apoyo técnico a la Mesa de Ayuda del Área de Soporte y Servicios Informáticos para los puntos 3) y 4).

6.7. De la designación del representante alterno.

La designación de un representante alterno por parte del representante de la entidad permite que, en caso de presentarse alguna contingencia, el alterno pueda realizar la gestión de certificados digitales de la entidad.

El representante de la entidad registra al representante alterno, quien debe tener un certificado digital vigente indicando el periodo de tiempo y el motivo por el cual desempeñará el rol asignado. Asimismo, el representante de la entidad adjunta el documento de sustento el cual avala la selección del suscriptor para cumplir el rol asignado, generando una solicitud la cual debe ser firmada por el representante de la entidad.

Adicionalmente, el representante legal ingresa a la plataforma PIER para aprobar la solicitud generada por el representante de la entidad. Cuando la solicitud ha sido aprobada por el representante legal, el suscriptor seleccionado para cumplir el rol de representante alterno estará apto para desempeñarse en la gestión de certificados digitales.

6.8. Del pago por certificados digitales.

Es competencia del jefe del Área de Soporte y Servicios Informáticos realizar las gestiones administrativas para solicitar la contratación de servicios de certificados digitales antes de quedarse sin certificados disponibles para ser asignados a los suscriptores. Los certificados digitales de persona jurídica tienen una vigencia de un año calendario y un costo que está estipulado en el TUPA del RENIEC.

Una vez, que se ha realizado la contratación de servicios de certificados digitales con el pago a través del Banco de la Nación, es necesario que el representante de la entidad realice el registro del comprobante de pago en la plataforma PIER a fin de contar con certificados digitales disponibles para la asignación del suscriptor.

En el comprobante de pago debe estar el RUC del Congreso de la República.

6.9. De la gestión de los equipos criptográficos para el suscriptor.

a) De la asignación del token criptográfico.

El congresista o funcionario solicita la asignación de token criptográfico remitiendo el pedido con documento al jefe del Departamento de Tecnologías de la Información.

El jefe del Departamento de Tecnologías de la Información deriva el pedido al jefe del Área de Soporte y Servicios Informáticos para su evaluación de acuerdo a la disponibilidad de stock.

El token criptográfico se entrega a través del Acta de Entrega/Devolución (Anexo 1).

El token criptográfico que haya sido perdido, destruido, deteriorado o averiado durante el periodo en que fue asignado a un suscriptor, es restituido por éste con otro token criptográfico con características iguales, similares o mejores en valor comercial actual y homologado por el RENIEC. Para todos estos casos, el suscriptor debe realizar la denuncia policial respectiva y remitirla al jefe del Área de Soporte y Servicios Informáticos para realizar la cancelación correspondiente.

b) De la devolución del token criptográfico.

En el caso de cese de funciones o labores, el suscriptor debe devolver el token criptográfico, como parte de la entrega de cargo, al Área de Soporte y Servicios Informáticos mediante Acta de Entrega/Devolución (Anexo 1).

6.10. Del uso de la imagen institucional en la firma digital.

Todo suscriptor de la institución que haga uso de la firma digital en los documentos institucionales debe hacerlo con la imagen institucional del Congreso de la República de acuerdo a lo indicado en el "*Manual de uso de la Identidad Visual del Congreso de la República*". Se encuentra prohibido utilizar otras imágenes en la firma digital, bajo responsabilidad.

El personal técnico del Área de Soporte y Servicios Informáticos debe verificar que el software REFIRMA cuente con la imagen institucional autorizada para la firma digital al momento de instalarla en el equipo de cómputo del suscriptor. Asimismo, el Área de Ingeniería de Software debe asegurarse que los sistemas informáticos del Congreso de la República que hagan uso de la firma digital cuentan con la imagen institucional del Congreso de la República.

7. ANEXOS

- **ANEXO N° 1:** Acta de Entrega/Devolución
- **ANEXO N° 2:** Glosario

ANEXO N° 1

ACTA DE ENTREGA/ DEVOLUCIÓN DE TOKEN CRIPTOGÁFICO

Tipo de Trámite: Entrega ☐ Devolución ☐

I Información General

Órgano o Unidad Orgánica:			
Apellidos y Nombres del Solicitante			
DNI:		Fecha:	____/_____/_____

II Del Equipo

Características	Información
Nombre del Dispositivo:	_____
Marca:	_____
Homologado por:	RENIEC

III De la Conformidad

Por medio del presente documento confirmo la recepción __ / devolución __ de un token criptográfico destinado para la firma de documentos electrónicos utilizando el software REFIRMA, el mismo que se encuentra asociado al certificado digital de persona jurídica obtenido a mi nombrepor intermedio del Congreso de la República.

Firma del Solicitante	Firma del Especialista del Área de Soporte Técnico y Servicios Informáticos

ANEXO N° 2

GLOSARIO

a) Aspirante a suscriptor: Es la persona que se encuentra inscrito en una Lista de Aspirante a Suscriptor para la emisión de su certificado digital.

b) Certificado Digital: Es un archivo electrónico emitido por una entidad de certificación que permite generar la firma digital en los documentos electrónicos.

c) Clave privada: Es un sistema de criptografía asimétrica usada por el destinatario de un mensaje de datos para verificar la firma digital puesta en dicho mensaje y que puede ser conocida por cualquier persona.

d) Declaración jurada para el Suscriptor: Es la declaración jurada de identificación no presencial para solicitar el certificado digital – persona jurídica en el marco de los D.S N° 008-2020-SA y D.S N° 044-2020-PCM que declara estado de emergencia nacional. Con este documento se inicia el trámite del certificado digital – persona jurídica para uso institucional.

e) ECEP – RENIEC: Entidad de Certificación para el Estado Peruano, la cual se encarga de proporcionar, emitir o cancelar los certificados digitales para personas naturales y jurídicas, así como, para funcionarios, empleados y servidores públicos, para el ejercicio de sus funciones y la realización de actos de administración interna e interinstitucional y para las personas expresamente autorizadas por la entidad pública correspondiente.

f) EREP - RENIEC: Entidad de Registro o Verificación para el Estado Peruano, la cual se encarga del levantamiento de datos, comprobación de la información del solicitante, identificación y autenticación de los Titulares y Suscriptores, aceptación y autorización de las solicitudes de emisión y cancelación de certificados digitales.

g) Equipo Criptográfico: Es un dispositivo, tal como una tarjeta inteligente (smartcard o token criptográfico), que permite almacenar de manera segura el certificado digital del suscriptor.

h) PDF: Es un formato de almacenamiento de documentos digitales independiente de plataformas de software o hardware.

i) PIER: Plataforma Integrada de la Entidad de Registro. Plataforma Integrada de la Entidad de Registro del RENIEC, que permite gestionar las solicitudes de emisión y cancelación de certificados digitales de persona jurídica y de agente automatizado de las entidades públicas del Estado Peruano.

j) Proceso: Es un conjunto de actividades o eventos (coordinados u organizados) que se realizan o suceden (alternativa o simultáneamente) bajo ciertas circunstancias con un fin determinado.

k) Representante de la Entidad: Persona natural que cuenta con facultades para representar al Congreso de la República en los trámites de certificado digital ante la EREP – RENIEC. Dentro de la plataforma PIER gestiona listas de autorización para los suscriptores, designa un representante alterno y también cancela los certificados digitales de sus suscriptores.

l) Suscriptor: Es un congresista, parlamentario andino, funcionario o servidor nombrado o contratado del Congreso de la República que tiene asignado un certificado digital de persona jurídica para uso de la firma digital en un documento electrónico, expediente electrónico o sistema informático. En casos autorizados por el titular de la entidad puede tener un token criptográfico asignado.

8. ÍNDICE

Página