

RESOLUCIÓN N° 127 -2025-2026-OM-CR

Lima, 2 de julio de 2026

VISTOS:

El Oficio N° 228-2026-DTI-DGA-CR del Departamento de Tecnologías de la Información; el Informe N° 099-2026-AM-OPPM-OM-CR del Área de Modernización; el Memorando N° 1081-2026-OPPM-OM-CR de la Oficina de Planeamiento, Presupuesto y Modernización; y el Informe N° 123-2026-AAJ-OLCC-OM-CR del Área de Asesoría Jurídica de la Oficina Legal y Constitucional del Congreso; y demás antecedentes.

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 que tiene fuerza de ley;

Que, en el marco de la autonomía administrativa que ostenta el Congreso de la República, resulta necesario aprobar, actualizar y/o modificar los instrumentos normativos internos que permitan establecer un orden administrativo en la gestión institucional;

Que, mediante el Informe N° 228-2026-DTI-DGA-CR, el Departamento de Tecnologías de la Información le remite a la Dirección General de Administración la propuesta de actualización de la Directiva N° 13-2023-OM-CR "Gestión de firmas y certificados digitales en el Congreso de la República" aprobada mediante Resolución N° 42-2023-2024-OM-CR de fecha 21 de noviembre de 2023; documento que a su vez fue remitido por el DGA a la Oficina de Planeamiento, Presupuesto y Modernización (OPPM) para su trámite correspondiente;

Que, mediante el Informe N° 099-2026-AM-OPPM-OM-CR el Área de Modernización le remite a la Oficina de Planeamiento, Presupuesto y Modernización, el expediente técnico de la propuesta de formulación de la Directiva N° 57-2026-ASSI-DTI-DGA-CR "Gestión de firmas y certificados digitales en el Congreso de la República" – Primera Versión, en el cual también se justifican las razones para la derogación de la Directiva N° 13-2023-OM-CR "Gestión de firmas y certificados digitales en el Congreso de la República";

Que, mediante el Memorando N° 1081-2026-OPPM-OM-CR, la Oficina de Planeamiento, Presupuesto y Modernización remite a la Oficina Legal y Constitucional del Congreso, la versión final de la propuesta de la Directiva N° 57-2026-ASSI-DTI-DGA-CR "Gestión de firmas y certificados digitales en el Congreso de la República" – Primera Versión, a fin de que se elabore el informe de viabilidad legal correspondiente y la resolución respectiva para su aprobación, previa



Congreso de la República
Oficialía Mayor

verificación de los requisitos exigidos para tal efecto, asimismo, se justifica la razón para la derogación de la Directiva N°13-2023-OM-CR "Gestión de firmas y certificados digitales en el Congreso de la República";

Que, en ese sentido el Área de Asesoría Jurídica de la Oficina Legal y Constitucional del Congreso, a través del informe de vistos, señala que la versión final del proyecto de directiva cumple con los procedimientos y requisitos establecidos en la Directiva N° 10-2024-AM-OPPM-OM-CR sobre "Elaboración de Documentos Normativos del Servicio Parlamentario del Congreso de la República" – Segunda Versión; asimismo, se indica que también se cumple con el debido sustento para la derogación de la Directiva N°13-2023-OM-CR "Gestión de firmas y certificados digitales en el Congreso de la República";

Que, es competencia del Oficial Mayor la aprobación, actualización, o modificación y/o derogación de las directivas;

De conformidad con lo establecido en el artículo 40 del Reglamento del Congreso de la República y con los numerales 7.2.4.4 y 7.2.5.5 de la Directiva N° 10-2024-AM-OPPM-OM-CR – Segunda Versión, con las opiniones favorables de la Oficina de Planeamiento, Presupuesto y Modernización, y del Área de Asesoría Jurídica de la Oficina Legal y Constitucional del Congreso; y

Con cargo a dar cuenta a la Mesa Directiva.

SE RESUELVE:

Artículo Primero. - APROBAR la Directiva N° 57-2026-ASSI-DTI-DGA-CR "Gestión de firmas y certificados digitales en el Congreso de la República" – Primera Versión.

Artículo Segundo. - DEROGAR la Directiva N°13-2023-OM-CR "Gestión de firmas y certificados digitales en el Congreso de la República" aprobada mediante Resolución N° 42-2023-2024-OM-CR de fecha 21 de noviembre de 2023.

Regístrese, comuníquese, cúmplase y archívese.



.....
GIOVANNI PORNO FLOREZ
Oficial Mayor
CONGRESO DE LA REPÚBLICA



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

Directiva – DI	57-2026-ASSI-DTI-DGA-CR
Versión:	PRIMERA VERSIÓN
Páginas:	11
Órgano Responsable:	Departamento de Tecnologías de la información

DESCRIPCIÓN	CARGO O PUESTO	FIRMA
EN SEÑAL DE CONFORMIDAD	DIRECTOR GENERAL DE ADMINISTRACIÓN	 Firmado digitalmente por: BERNAL NEGREIROS Giancarlo FAU 20161749126 soft Motivo: En señal de conformidad Fecha: 01/07/2026 17:01:06-0500
	JEFE DEL DEPARTAMENTO DE TECNOLOGÍAS DE LA INFORMACIÓN	 Firmado digitalmente por: SUEYRAS LOSTAUNAU Luis Alberto FAU 20161749126 hard Motivo: En señal de conformidad Fecha: 10/06/2026 15:50:42-0500
	ÁREA DE SOPORTE Y SERVICIOS INFORMÁTICOS	 Firmado digitalmente por: PAZ CORTES Angel Jeancarlo FAU 20161749126 hard Motivo: En señal de conformidad Fecha: 10/06/2026 15:39:36-0500
VISTO BUENO	JEFE DE LA OFICINA LEGAL Y CONSTITUCIONAL DEL CONGRESO	 Firmado digitalmente por: NODA YAMADA Carlos Ramon FAU 20161749126 soft Motivo: Doy Vº Bº Fecha: 26/06/2026 17:20:06-0500
	JEFE DE LA OFICINA DE PLANEAMIENTO, PRESUPUESTO Y MODERNIZACIÓN	 Firmado digitalmente por: UGARTE HUERTA Nelson Alex FAU 20161749126 soft Motivo: Doy Vº Bº Fecha: 10/06/2026 16:55:32-0500
	JEFE DEL ÁREA DE MODERNIZACIÓN	 Firmado digitalmente por: ZAPATER VELAZCO Silvana FAU 20161749126 soft Motivo: Doy Vº Bº Fecha: 10/06/2026 12:52:09-0500

1. OBJETIVO

Establecer los lineamientos y responsabilidades para el otorgamiento, administración y uso de certificados digitales, así como regular el uso de la firma digital en el Congreso de la República.

2. FINALIDAD

Garantizar, en el marco de la estrategia de transformación digital institucional y como medida de ecoeficiencia, el uso responsable y adecuado de la firma digital en los documentos electrónicos generados en el Congreso de la República.

3. ALCANCE

Los aspectos definidos en la presente directiva son de aplicación para el personal del Departamento de Tecnologías de la Información y para el personal de la Organización Parlamentaria y del Servicio Parlamentario que requieran contar con un certificado digital, para el uso de la firma digital en el ejercicio de sus funciones y competencias.

4. BASE LEGAL

- 4.1. Ley 27269 “Ley de Firmas y Certificados Digitales”.
- 4.2. Ley 27310 Ley que modifica el artículo 11 de la Ley 27269”.
- 4.3. Ley 27419 “Ley sobre notificación por correo electrónico”.
- 4.4. Ley 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.
- 4.5. Decreto Supremo 052-2008-PCM “Reglamento de la Ley de Firmas y Certificados Digitales” y sus modificatorias.
- 4.6. Decreto Supremo 070-2011-PCM, que modifica el Reglamento de la Ley 27269 “Ley de Firmas y Certificados Digitales”, y establece normas aplicables al procedimiento registral en virtud al Decreto Legislativo 681 y ampliatorias.
- 4.7. Decreto Supremo 105-2012-PCM, que establece disposiciones para facilitar la puesta en marcha de la firma digital y modifica el Decreto Supremo 052-2008-PCM Reglamento de la “Ley de Firmas y Certificados Digitales”.
- 4.8. Decreto Supremo 004-2013-PCM “Política Nacional de Modernización de la Gestión Pública”.
- 4.9. Decreto Supremo 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.
- 4.10. Decreto Supremo 029-2021-PCM, que aprueba el Reglamento del Decreto Legislativo 1412 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.

- 4.11. Resolución de Secretaría de Gobierno y Transformación Digital 002-2022-PCM/SGTD, publicada 24 de setiembre de 2022.
- 4.12. Resolución de Secretaría de Gobierno y Transformación Digital 007-2024-PCM/SGTD, publicada 11 de diciembre de 2024 que aprueba la Directiva 002-2024-PCM/SGTD, que regula el uso de la firma digital en las entidades públicas.

5. RESPONSABILIDADES

- 5.1. El Departamento de Tecnologías de la Información (en adelante, DTI) es responsable de aprobar el requerimiento de adquisición de los certificados digitales y token criptográficos.
- 5.2. El Área de Soporte y Servicios Informáticos (en adelante, ASSI) es responsable de gestionar el stock y coordinar la obtención de los certificados digitales y tokens criptográficos para congresistas, parlamentarios andinos, servidores del Servicio Parlamentario y personal de confianza de la Organización Parlamentaria, además de instalar los certificados digitales en los equipos de los usuarios.
- 5.3. El representante de la entidad ante el RENIEC es responsable de gestionar la solicitud, anulación y cancelación de certificados digitales, registrar los pagos, administrar la Plataforma Integrada de la Entidad de Registro (PIER) para la gestión de certificados digitales, comunicar el stock disponible de certificados digitales al ASSI. Así como coordinar con el personal técnico para la instalación del certificado digital.
- 5.4. El suscriptor es responsable de brindar información veraz, así como del uso, custodia y reserva de la clave privada y del token criptográfico asignado. En caso de que la clave privada quede comprometida en su seguridad, debe comunicarlo de inmediato al representante de la entidad a través de su correo electrónico para que proceda a la cancelación del certificado.

6. DISPOSICIONES GENERALES

6.1. Del certificado digital

La obtención del certificado digital emitido por la Entidad de Certificación para el Estado Peruano ECEP–RENIEC se realiza 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.

6.2. De la firma digital

- 6.2.1 La firma digital confirma la identidad del firmante del documento electrónico y garantiza que este documento no ha sido modificado desde su emisión, es decir, que conserva su integridad; se utiliza para dar veracidad legal a los documentos requeridos para los actos y trámites administrativos o parlamentarios.

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

6.2.3 La validación de la firma digital debe realizarse a través de las plataformas oficiales reconocidas por el Estado Peruano que permiten verificar su autenticidad, integridad y vigencia.

Se utiliza el siguiente validador de la Plataforma Nacional de Firma Digital – Firma Perú: <http://apps.firmaperu.gob.pe/web/validador.xhtml>.

6.3. De la autorización

6.3.1 El congresista, Parlamentario Andino, servidores del Servicio Parlamentario y personal de confianza de la Organización Parlamentaria que requieran contar con un certificado digital, deben solicitarlo al jefe del DTI a través de su correo institucional.

6.3.2 Para el caso de los servidores del Servicio Parlamentario y/o del personal de confianza de la Organización Parlamentaria, el certificado digital es solicitado por el congresista, parlamentario andino y/o jefe del órgano inmediato superior.

7. DISPOSICIONES ESPECÍFICAS

7.1. De la designación del representante de la entidad

7.1.1 El representante de la entidad que administra la plataforma PIER para la gestión de certificados digitales 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.

7.1.2 La Dirección General de Administración remite 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 de la plataforma PIER para que gestione los certificados digitales de los suscriptores del Congreso de la República.

7.1.3 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.

7.1.4 El representante de la entidad coordina con la EREP-RENIEC para la emisión del certificado inicial correspondiente, con lo que se inician las gestiones para las solicitudes de certificados digitales de los suscriptores del Congreso de la República, así como está encargado de:

- Administrar la Plataforma Integrada de la Entidad de Registro (PIER) para la gestión de certificados digitales.

- Registrar información veraz durante la solicitud de emisión de certificados digitales, anulación y cancelación de certificados digitales.
- 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 la misma.
- Cumplir permanentemente las condiciones establecidas por la Entidad de Certificación para la utilización del certificado digital.
- Verificar el stock disponible e informar al ASSI de la ampliación de stock para la atención de solicitudes de certificados digitales.
- Coordinar con el personal técnico del ASSI la instalación del certificado digital.

7.2. De la designación del representante alternativo

- 7.2.1 La designación de un representante alternativo por parte del representante de la entidad permite que, en caso de presentarse alguna contingencia, el alternativo pueda realizar la gestión de certificados digitales de la entidad.
- 7.2.2 El representante de la entidad es quien registra al representante alternativo en la plataforma PIER, indicando el periodo de tiempo y el motivo por el cual va a desempeñar el rol asignado; dicho trabajador ya debe contar con un certificado digital vigente. Asimismo, el representante de la entidad adjunta el documento de sustento que avala la selección del suscriptor para cumplir el rol de representante alternativo, generando una solicitud la cual debe ser firmada por el representante de la entidad.
- 7.2.3 Adicionalmente, el representante legal de RENIEC 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 alternativo estará apto para desempeñarse en la gestión de certificados digitales.

7.3. Del procedimiento de obtención del certificado digital

- 7.3.1 Para solicitar un certificado digital, el aspirante a suscriptor remite desde su correo institucional al correo institucional del representante de la entidad la solicitud de un certificado digital. Debe sustentar los motivos de su solicitud y, en el caso de servidores, debe añadirse la autorización expresa de su respectiva jefatura.
- 7.3.2 El representante de la entidad recibe el correo de solicitud de obtención de certificado digital y revisa que estén todos los datos y la autorización. En caso de que falte la autorización, remite correo al aspirante a suscriptor para su corrección.

- 7.3.3 De encontrarse todo conforme, el representante de la entidad realiza la gestión de obtención de certificado digital a través de la Plataforma Integrada de la Entidad de Registro PIER.
- 7.3.4 Culminado el registro, la plataforma PIER remite automáticamente un correo al aspirante a suscriptor para que inicie el proceso de validación facial de la identificación del suscriptor.
- 7.3.5 El aspirante a suscriptor procede a la validación de su identificación de acuerdo con los procedimientos establecidos por el RENIEC. Al ser validado correctamente, la plataforma PIER remite automáticamente un correo al aspirante aprobando la validación y dando las indicaciones para la instalación del certificado digital.
- 7.3.6 Recibido el correo de aprobación por parte del RENIEC, el aspirante a suscriptor procede a la instalación del certificado digital. En caso de que tenga inconvenientes, puede ponerse en contacto con la Mesa de Ayuda del ASSI, a fin de que esta realice la instalación del certificado digital.
- 7.3.7 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.

7.4. Del uso de la firma digital

- 7.4.1 Los suscriptores hacen uso de la firma digital para refrendar los documentos electrónicos asignados en cumplimiento de sus funciones; utilizan el software REFIRMA o un documento electrónico generado por los sistemas informáticos del Congreso de la República.
- 7.4.2 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.
- 7.4.3 La firma digital aplicada a una hoja de un expediente o documento electrónico no exime a los suscriptores de cumplir con las disposiciones establecidas en toda la documentación adjunta o de sustento, las cuales son exigibles para la atención del trámite o procedimiento administrativo.
- 7.4.4 El documento electrónico firmado digitalmente es presentado en un archivo PDF y almacenado con las firmas digitales correspondientes para futuras referencias.
- 7.4.5 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.
- 7.4.6 Para firmar un documento, el suscriptor debe indicar el motivo de la firma que puede ser:

- Soy el autor del documento.
- En señal de conformidad.
- Doy V.º B.º.
- Por encargo.
- Doy fe.

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

- 7.5.1 Todo suscriptor que utilice la firma digital en documentos institucionales debe incorporar obligatoriamente la imagen institucional del Congreso de la República, conforme a lo establecido en el “Manual de Uso de la Identidad Visual del Congreso de la República”. Queda prohibido el uso de imágenes distintas, bajo responsabilidad administrativa.
- 7.5.2 El personal técnico del ASSI es responsable de verificar que el software REFIRMA cuente con la imagen institucional autorizada para la firma digital al momento de su instalación en los equipos de los suscriptores. Asimismo, el Área de Ingeniería de Software debe asegurar que los sistemas informáticos institucionales que empleen firma digital incorporen dicha imagen institucional.

7.6. De la anulación automática del certificado digital

El certificado digital se anula de forma automática cuando, habiéndose aprobado su emisión, no haya sido instalado en el equipo del suscriptor dentro del plazo de treinta (30) días calendario.

7.7. De la cancelación del certificado digital

La cancelación del certificado digital es efectuada por el representante de la entidad en los siguientes casos:

- Por sece del suscriptor.
- La información contenida en el certificado no es correcta.
- Deterioro o alteración o pérdida que afecta el PIN de acceso a la clave privada.
- Exposición o uso indebido del PIN de acceso a la clave privada.
- Solicitud expresa por el suscriptor o por su funcionario superior.

En cualquier otro caso, debe ser autorizado por el jefe del ASSI.

7.8. De la renovación del certificado digital

- 7.8.1 La renovación del certificado digital es tramitada por el suscriptor como si fuera un nuevo certificado digital a fin de que continúe firmando digitalmente sus documentos oficiales. En el caso de los servidores, no requiere nueva autorización, debido a que es una continuidad de sus funciones asignadas.
- 7.8.2 El suscriptor es responsable de solicitarlo treinta (30) días antes de la caducidad del certificado digital vigente. Los certificados digitales tienen vigencia de un (01) año calendario.

7.9. Del pago por certificados digitales

- 7.9.1 Es competencia del jefe del ASSI gestionar oportunamente la contratación del servicio de certificados digitales, a fin de garantizar su disponibilidad. Estos certificados tienen una vigencia de un (01) año calendario y su costo se encuentra establecido en el TUPA del RENIEC.
- 7.9.2 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.

7.10. De la gestión del token criptográfico para el suscriptor

7.10.1 Asignación del token criptográfico

- 7.10.1.1 El congresista, parlamentario andino o funcionario solicita la asignación de token criptográfico remitiendo el pedido al jefe del ASSI, quien evalúa de acuerdo con la disponibilidad de stock.
- 7.10.1.2 El jefe del ASSI es responsable de mantener el stock necesario de tokens criptográficos y gestionar su reposición de manera oportuna.
- 7.10.1.3 La entrega del token criptográfico se formaliza mediante la suscripción del “Acta de Entrega/Devolución” (Anexo 01).
- 7.10.1.4 En caso de pérdida, deterioro, destrucción o avería del token criptográfico durante su uso, el suscriptor debe reemplazarlo por uno de características iguales, similares o superiores, homologado por RENIEC. Asimismo, debe presentar la denuncia policial correspondiente y comunicar el hecho al ASSI para la gestión de la cancelación del certificado digital.

7.10.2 Devolución del token criptográfico

En caso de cese de funciones o labores, el suscriptor debe devolver el token criptográfico, como parte del proceso de entrega de cargo, al ASSI mediante el “Acta de Entrega/Devolución” (Anexo 01).

8. ANEXOS

N° DE ANEXO	DETALLE
ANEXO 01	Acta de Entrega/Devolución de Token Criptográfico.
ANEXO 02	Glosario de Términos

ANEXO 01



Departamento de Tecnologías de la Información
Área de Soporte y Servicios Informáticos

ACTA DE ENTREGA/DEVOLUCIÓN DE TOKEN CRIPTOGRÁFICO

Tipo de Trámite: Entrega ☐ Devolución ☐

I. Información General

Órgano/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 nombre por intermedio del Congreso de la República.

Firma del Solicitante

Firma del Especialista del Área de
Soporte y Servicios Informáticos

ANEXO 02

GLOSARIO DE TÉRMINOS

- **Aspirante a suscriptor:** Es la persona que se encuentra inscrita en una Lista de Aspirante a Suscriptor para la emisión de su certificado digital.
- **Certificado Digital:** Es un archivo electrónico emitido por una entidad de certificación que permite generar la firma digital en los documentos electrónicos.
- **Clave privada:** Es un sistema de criptografía asimétrica usado 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.
- **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. 008-2020-SA y D.S. 044-2020-PCM que declara estado de emergencia nacional. Con este documento se inicia el trámite del certificado digital – persona jurídica para uso institucional.
- **ECEP – RENIEC:** Entidad de Certificación para el Estado Peruano; 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.
- **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.
- **PIER: Plataforma Integrada de la Entidad de Registro:** Plataforma de 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.
- **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.
- **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.
- **Token Criptográfico:** Es un dispositivo, tal como una tarjeta inteligente (smartcard o token criptográfico), que permite almacenar de manera segura el certificado digital del suscriptor.

9. ÍNDICE

	Página
1. OBJETIVO	2
2. FINALIDAD	2
3. ALCANCE	2
4. BASE LEGAL	2
5. RESPONSABILIDADES	3
6. DISPOSICIONES GENERALES	3
6.1. Del certificado digital	3
6.2. De la firma digital	3
6.3. De la autorización	4
7. DISPOSICIONES ESPECÍFICAS	4
7.1. De la designación del representante de la entidad	4
7.2. De la designación del representante alterno	5
7.3. Del procedimiento de obtención del certificado digital	5
7.4. Del uso de la firma digital	6
7.5. Del uso de la imagen institucional en la firma digital	7
7.6. De la anulación automática del certificado digital	7
7.7. De la cancelación del certificado digital	7
7.8. De la renovación del certificado digital	7
7.9. Del pago por certificados digitales	8
7.10. De la gestión del token criptográfico para el suscriptor	8
7.10.1 Asignación del token criptográfico	8
7.10.2 Devolución del token criptográfico	8
8. ANEXOS	8
9. ÍNDICE	11