

## Resolución Administrativa Interna ATT-DJ-RAI LP 85/2021

La Paz, 28 de octubre de 2021

### VISTOS:

El Informe Técnico ATT-DS-INF TEC LP 153/2021 de 27 de octubre de 2021 (**INFORME TÉCNICO**) emitido por la Unidad de Planificación y Desarrollo Organizacional; Informe Jurídico ATT-DJ-INF JUR LP 1525/2021 de 28 de octubre de 2021, emitido por la Dirección Jurídica (**INFORME JURÍDICO**), la normativa vigente y todo lo que ver convino y se tuvo presente;

### CONSIDERANDO 1.-

Que el Parágrafo II del Artículo 103 de la Constitución Política del Estado, determina que el Estado asumirá como política la implementación de estrategias para incorporar el conocimiento y aplicación de nuevas tecnologías de información y comunicación.

Que la Ley N° 164, de 08 de agosto de 2011, General de Telecomunicaciones, Tecnologías de Información y Comunicación, establece el régimen general de telecomunicaciones y tecnologías de información y comunicación, del servicio postal y el sistema de regulación, en procura del vivir bien garantizando el derecho humano individual y colectivo a la comunicación, con respeto a la pluralidad económica, social, jurídica, política y cultural de la totalidad de las bolivianas y los bolivianos, las naciones y pueblos indígena originario campesinos, y las comunidades interculturales y afrobolivianas del Estado Plurinacional de Bolivia.

Que los numerales 2 y 5 del Artículo 2 de la Ley N° 164, determinan como objetivos de la referida Ley, el asegurar el ejercicio del derecho al acceso universal y equitativo a los servicios de telecomunicaciones, tecnologías de información y comunicación; y promover el uso de las tecnologías de información y comunicación para mejorar las condiciones de vida de las bolivianas y bolivianos. Asimismo, el Artículo 71 de la Ley N° 164 establece como prioridad nacional la promoción del uso de las tecnologías de información y comunicación para procurar el vivir bien de todas las bolivianas y bolivianos.

Que el inciso l) del Artículo 17 del Decreto Supremo N° 0071, de 09 de abril de 2009, dispone entre las competencias de la Autoridad de Fiscalización y Control Social de Telecomunicaciones y Transporte actual Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes – ATT, la implementación de aspectos relativos a la regulación, control, fiscalización y supervisión de los sectores de telecomunicaciones y transporte, en el marco de la Constitución Política del Estado.

Que el inciso f) del Artículo 19 del referido Decreto Supremo, determina entre las atribuciones del Director Ejecutivo de la ATT, ordenar y realizar los actos necesarios para garantizar el cumplimiento de los fines de la Entidad.

Que el Capítulo I del Título IV del Reglamento para el Desarrollo de Tecnologías de Información y Comunicación, aprobado mediante Decreto Supremo N° 1793, de 13 de noviembre de 2013, señala los lineamientos de los Certificados Digitales tales como tipos, función, características, vigencia, y otras características de la Firma Digital. Asimismo, el Capítulo I del Título V del citado Reglamento, determina los Derechos y Obligaciones de los titulares del Certificado Digital.

Que el Artículo 2 del Reglamento para Normar el Uso de la Firma Digital respecto a niveles de seguridad, aprobado con Resolución Ministerial N° 235/18, de 21 de agosto de 2018, establece que la Firma Digital tiene dos niveles de seguridad respecto a los mecanismos que son utilizados para su

  
ANALISTA LEGAL  
AUTORIDAD DE REGULACIÓN Y FISCALIZACIÓN  
DE TELECOMUNICACIONES Y TRANSPORTES



1-LP-14449



creación: Nivel de Seguridad Normal, cuando las claves pública y privada sean generadas mediante software y Nivel de Seguridad Alto, cuando las claves pública y privada sean generadas mediante dispositivos electrónicos criptográficos de seguridad especializados conforme a estándares aprobados por la ATT.

## CONSIDERANDO 2.-

Que en la gestión 2019, se iniciaron acciones de coordinación entre las áreas de Regulación de Tecnologías de Información, Administración y Finanzas, y Planificación y Desarrollo Organizacional a fin de consensuar proyectos de Reglamentos de Uso de la Firma Digital, mismos que se fueron ajustando de acuerdo a sugerencias de diferentes unidades; asimismo, se difundieron las versiones a través de correos electrónicos a las áreas de Tecnología Informática, Administración y Finanzas, Jurídica y Regulación de Tecnologías de Información, a fin de obtener mayores elementos que coadyuven a su emisión.

Que mediante Comunicación Interna ATT-DS-CI LP 16/202, de 8 de enero de 2021, la Unidad de Tecnología Informática remitió a la Unidad de Planificación y Desarrollo Organizacional el Proyecto de Reglamento de Uso de Firma Digital para el Sistema de Gestión y Flujo Documental – SISCOR; asimismo el citado proyecto fue remitido a la Unidad de Auditoría Interna que cursó observaciones a la propuesta, que fueron tomadas en cuenta en el Reglamento. En ese entendido, el 20 de abril de 2021, la Unidad de Planificación y Desarrollo Organizacional convocó a una reunión a efectos de tratar las modificaciones al Reglamento, producto de la misma se realizaron nuevas correcciones quedando la versión final sujeta a aprobación de los involucrados.

Que mediante Instructivo Interno ATT-DS-INS INT LP 43/2021, de 01 de octubre de 2021, mismo que considera que la implementación de servicios de Gobierno Electrónico es de vital importancia para la mejora de la eficiencia, eficacia, calidad y transparencia de los servicios públicos; por lo tanto, la integración, desarrollo e implementación de la Firma Digital en la gestión documental institucional es un aspecto importante para la consecución de los objetivos institucionales.

Que el INFORME TÉCNICO concluyó señalando que se elaboró el Reglamento Interno para el Uso de la Firma Digital para el Sistema de Gestión y Flujo Documental – SISCOR en su versión 001. Asimismo, el referido Reglamento está enmarcado en la normativa vigente, incluyendo los aspectos descritos en el Instructivo ATT-DS-INS INT LP 43/2021. Finalmente, el documento adjunto contempla los aspectos relevantes para la implementación de la Firma Digital en la ATT y teniendo en cuenta que el despliegue de la Firma Digital en la gestión documental institucional es el 29 de octubre de 2021, corresponde su aprobación.

Que el INFORME JURÍDICO concluyó señalando que los antecedentes expuestos y la normativa vigente, se concluye que la aprobación del “Reglamento Interno para el Uso de Firma Digital en el Sistema de Gestión y Flujo Documental – SISCOR” en su versión 001, no contraviene ninguna norma legal vigente, por lo que se recomienda, emitir la correspondiente Resolución Administrativa Interna para la aprobación del mismo.

Bajo ese contexto, el Reglamento norma el uso de la Firma Digital para otorgar seguridad y validez a los documentos electrónicos generados, gestionados, asignados, enviados y/o recibidos en el Sistema de Gestión y Flujo Documental – SISCOR; siendo aplicable a todo el personal de la ATT que genera, gestiona y/o deriva documentos y/o actos administrativos firmados digitalmente en el Sistema de Gestión y Flujo Documental – SISCOR, mismo que se enmarca dentro de la normativa vigente,



I-LP-14449





AUTORIDAD DE REGULACIÓN Y FISCALIZACIÓN  
DE TELECOMUNICACIONES Y TRANSPORTES

Resolución Administrativa Interna ATT-DJ-RAI LP 85/2021

estableciendo responsabilidades, plazos y definiciones con la finalidad de contar con un Reglamento que contemple los aspectos relevantes para la implementación de la Firma Digital en la ATT.

**POR TANTO:**

El Director Ejecutivo de la Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes – ATT, Abg. NÉSTOR RÍOS RIVERO, designado mediante Resolución Suprema N° 27479 de 29 de marzo de 2021 emitida por el Presidente del Estado Plurinacional de Bolivia, en ejercicio de sus atribuciones conferidas por ley y demás normas vigentes previamente señaladas;


**RESUELVE:**

**PRIMERO.- APROBAR** el “**REGLAMENTO INTERNO PARA EL USO DE FIRMA DIGITAL EN EL SISTEMA DE GESTIÓN Y FLUJO DOCUMENTAL – SISCOR**”, en su versión 01, de la Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes – ATT, que se encuentra adjunto a la presente Resolución y es parte indivisible e inseparable de la misma.

**SEGUNDO.- INSTRUIR** a la Unidad de Tecnología Informática y a la Unidad de Planificación y Desarrollo Organizacional tomar los recaudos necesarios para dar cumplimiento a la presente Resolución Administrativa Interna, sea mediante el cumplimiento de trámites y la ejecución de actos que demande su plena ejecución, implementación y difusión.

Regístrese y archívese.

  
Abog. Néstor Ríos Rivero  
DIRECTOR EJECUTIVO  
AUTORIDAD DE REGULACIÓN Y FISCALIZACIÓN  
DE TELECOMUNICACIONES Y TRANSPORTES

  
Abog. Roger René Romero Díaz  
DIRECTOR JURÍDICO  
AUTORIDAD DE REGULACIÓN Y FISCALIZACIÓN  
DE TELECOMUNICACIONES Y TRANSPORTES



I-LP-14449

**La Paz:** 13 de Calacoto entre  
av. Los Sauces y av. Costanera  
Nro. 8260.  
Telf: 2-772266 - 2- 615000  
Fax: 2-772299

**Cochabamba:** Av. Ballivian y España  
(El Prado) Nro. 683 primer piso  
Telf: 4-581182 - 4-451184  
4-4581185

**Santa Cruz:** Av. Beni (entre  
4to y 5to anillo) calle 3, edif.  
Gardenia Condominio Club  
Torre Sur. Planta baja of. 2  
Telf: 3-120587 - 3-3120978

**Tarija:** Calle Padilla esquina  
Alejandro del Carpio Nro. 878  
Telf: 6-644136 - 6-112611

**Línea Gratuita de Protección  
al Usuario:**  
800-10-6000  
www.att.gob.bo

3 de 3









AUTORIDAD DE REGULACIÓN Y FISCALIZACIÓN  
DE TELECOMUNICACIONES Y TRANSPORTES

## RE029. REGLAMENTO INTERNO PARA EL USO DE FIRMA DIGITAL EN EL SISTEMA DE GESTIÓN Y FLUJO DOCUMENTAL-SISCOR

Versión: 01

Elaborado:	Revisado:	Aprobado:
 <p>Lic. Angélica Quevedo López RESPONSABLE DE GESTIÓN DE CALIDAD AUTORIDAD DE REGULACIÓN Y FISCALIZACIÓN DE TELECOMUNICACIONES Y TRANSPORTES</p>	 <p>Ing. Alberto Encinas JEFE DE TECNOLOGÍA INFORMÁTICA AUTORIDAD DE REGULACIÓN Y FISCALIZACIÓN DE TELECOMUNICACIONES Y TRANSPORTES</p>	 <p>Lic. Alvaro Pedro Cuellar Almendras DIRECTOR ADMINISTRATIVO FINANCIERO AUTORIDAD DE REGULACIÓN Y FISCALIZACIÓN DE TELECOMUNICACIONES Y TRANSPORTES</p>  <p>Lic. Jorge Ariel Arias Vacaflores JEFE DE PLANIFICACIÓN Y DESARROLLO ORGANIZACIONAL AUTORIDAD DE REGULACIÓN Y FISCALIZACIÓN DE TELECOMUNICACIONES Y TRANSPORTES</p>

La última versión de este documento se encuentra en la red informática. Si usted está leyendo una copia impresa, asegúrese que se trata de la versión vigente.



## Contenido

<b>CAPITULO I</b> .....	<b>3</b>
<b>CONSIDERACIONES GENERALES</b> .....	<b>3</b>
ARTÍCULO 1.- (OBJETO).....	3
ARTÍCULO 2.- (ÁMBITO DE APLICACIÓN).....	3
ARTÍCULO 3.- (MARCO LEGAL). ....	3
ARTÍCULO 5.- (MODIFICACIONES Y/O ACTUALIZACIONES AL REGLAMENTO).....	6
<b>CAPITULO II</b> .....	<b>6</b>
<b>FIRMA DIGITAL</b> .....	<b>6</b>
ARTÍCULO 6.- (USO DE LA FIRMA DIGITAL). ....	6
ARTÍCULO 7.- (FINALIDAD DE LA FIRMA DIGITAL).....	6
ARTÍCULO 8.- (BENEFICIOS DE LA FIRMA DIGITAL).....	6
ARTÍCULO 9.- (NATURALEZA DE LOS TRÁMITES).....	6
ARTÍCULO 10. (VALIDEZ JURÍDICA Y PROBATORIA DE DOCUMENTOS FIRMADOS DIGITALMENTE).....	7
ARTÍCULO 11. (CARACTERÍSTICAS DE LA FIRMA DIGITAL). ....	7
ARTÍCULO 12.- (REVOCATORIA DEL CERTIFICADO DIGITAL).....	7
<b>CAPITULO III</b> .....	<b>9</b>
<b>CERTIFICADO DIGITAL</b> .....	<b>9</b>
ARTÍCULO 19.- (ADQUISICIÓN DE DISPOSITIVOS CRIPTOGRÁFICOS). ....	9
ARTÍCULO 20.- (HABILITACIÓN DEL CERTIFICADO DIGITAL).....	9
ARTÍCULO 21.- (CONTENIDO DEL CERTIFICADO DIGITAL). ....	9
ARTÍCULO 22.- (VIGENCIA Y RENOVACIÓN DEL CERTIFICADO DIGITAL).....	10
ARTÍCULO 23.- (EMISIÓN DEL CERTIFICADO DIGITAL – FIRMA DIGITAL).....	10
ARTÍCULO 24.- (OBTENCIÓN DEL CERTIFICADO DIGITAL).....	10
ARTÍCULO 25.- (RESPONSABILIDAD DEL TITULAR DE LA FIRMA DIGITAL). ....	10
ARTÍCULO 26.- (OBLIGACIONES DEL TITULAR DE LA FIRMA DIGITAL).....	10
ARTÍCULO 27.- (DERECHOS DEL TITULAR DE LA FIRMA DIGITAL).....	11
ARTÍCULO 28.- (TARIFAS DEL SERVICIO DE FIRMA DIGITAL).....	11
ARTÍCULO 29.- (REVOCACIÓN Y REACTIVACIÓN DEL CERTIFICADO DIGITAL).....	11
ARTÍCULO 30.- (EXTRAVÍO DE TOKENS).....	11
ARTÍCULO 31.- (CONSERVACIÓN DE LOS DOCUMENTOS ELECTRÓNICOS FIRMADOS DIGITALMENTE).....	12
<b>CAPÍTULO IV</b> .....	<b>12</b>
<b>RESPONSABILIDADES Y OBLIGACIONES DEL FIRMANTE</b> .....	<b>12</b>
ARTÍCULO 32.- (RESPONSABILIDADES).....	12
ARTÍCULO 33.- (OBLIGACIONES).....	12
ARTÍCULO 34.- (RESPONSABILIDADES DEL PARTICIPANTE CON RELACIÓN A SU FIRMA DIGITAL).....	13
ARTÍCULO 35.- (RESPONSABILIDADES DE LAS ÁREAS INVOLUCRADAS).....	13
DISPOSICIÓN FINAL.....	13

Elaborado:		Revisado:		Aprobado:	
------------	--	-----------	--	-----------	--



## CAPITULO I CONSIDERACIONES GENERALES

### Artículo 1.- (Objeto).

El presente Reglamento tiene por objeto normar el uso de la Firma Digital para otorgar seguridad y validez a los documentos electrónicos generados, gestionados, asignados, enviados y/o recibidos en el Sistema de Gestión y Flujo Documental SISCOR.

### Artículo 2.- (Ámbito de Aplicación).

El presente Reglamento se aplica a todo el personal de la Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes – ATT que genera, otorga visto bueno, revisa, aprueba, y/o deriva documentos y/o actos administrativos firmados digitalmente en el Sistema de Gestión y Flujo Documental SISCOR.

### Artículo 3.- (Marco legal).

- a) Ley N° 1178, de 20 de julio de 1990, de Administración y Control Gubernamentales.
- b) Decreto Supremo N° 23318-A, de 3 de noviembre de 1992, Reglamento de la Responsabilidad por la Función Pública.
- c) Ley N° 164 del 8 de agosto de 2011, Ley General de Telecomunicaciones, Tecnologías de Información y Comunicación.
- d) Decreto Supremo N° 1793 del 13 de noviembre de 2013, Reglamento a la Ley N°164 para el Desarrollo de Tecnologías de Información y Comunicación.
- e) Decreto Supremo N° 3527, del 11 de abril de 2018, que ajusta el Decreto Supremo N° 1793.
- f) Decreto Supremo N° 3525, de 4 de abril de 2018, que establece la política de atención ciudadana, norma el archivo digital, la interoperabilidad y la tramitación digital.
- g) Resolución Ministerial N° 235/18 de 21 de agosto de 2018, emitida por la Presidencia del Estado Plurinacional de Bolivia, que aprueba el Reglamento para normar el uso de la firma digital respecto a niveles de seguridad.
- h) Plan Institucional de Seguridad de la Información de la ATT, aprobado mediante Resolución Administrativa Interna ATT-DJ-RAI LP 126/2019.

### Artículo 4.- (Definiciones).

- a) **Archivo digital:** Es el archivo ordenado con soporte digital, que resguarda la totalidad de los datos, información, documentos y expedientes digitales receptionados, generados y procesados por la entidad pública. Además, debe permitir realizar la búsqueda por referencia y/o tema, fecha, entidad, nombre de la persona que firma, cite y por documento.

Elaborado:		Revisado:		Aprobado:		
------------	---	-----------	---	-----------	---	---



- b) **Autenticación:** Proceso técnico de verificación por el cual se garantiza la identidad del firmante en un mensaje electrónico de datos o documento digital, que contengan firma digital.
- c) **Certificado Digital:** Es un documento digital firmado digitalmente por una entidad certificadora autorizada que vincula unos datos de verificación de firma a un signatario y confirma su identidad. El certificado digital es válido únicamente dentro del periodo de vigencia, indicado en el certificado digital.  
Los certificados digitales deben ser emitidos por una entidad certificadora autorizada, responder a formatos y estándares reconocidos internacionalmente y fijados por la ATT, contener como mínimo los datos que permitan identificar a su titular, a la entidad certificadora que lo emitió, su periodo de vigencia y contemplar la información necesaria para la verificación de la firma digital.
- d) **Clave Pública:** Es una clave alfanumérica creada por medio de algoritmos matemáticos, vinculada a una clave privada e incluida en el Certificado Digital del firmante.
- e) **Clave Privada:** Es una clave alfanumérica creada por medio de algoritmos matemáticos, de responsabilidad exclusiva del firmante y custodiada por éste.
- f) **Criptografía Asimétrica:** Conjunto de técnicas que consisten en el uso de las claves privada y pública para cifrar y descifrar la información, aplicada a los datos para asegurar su confidencialidad, integridad y autenticidad.
- g) **Documento Electrónico:** Mensaje de datos creado, enviado, comunicado, recibido y almacenado por medios electrónicos. Se entiende por electrónico al uso de tecnología que tiene propiedades eléctricas, digitales, magnéticas, inalámbricas, ópticas, electromagnéticas u otras similares.
- h) **Documento Electrónico Firmado Digitalmente:** Documento electrónico al cual se le ha aplicado el método criptográfico asimétrico de generación de Firma Digital.
- i) **Dispositivo Criptográfico basado en Hardware (token):** Dispositivo Criptográfico físico para la generación de Par de Claves, Certificado Digital y firma de documentos que cumpla con el estándar FIPS 140-2 Nivel 2 mínimamente.
- j) **Entidad de Certificación Autorizada (ECA):** Entidad Autorizada que expide Certificados Digitales y presta servicios relacionados con la firma digital.

La ADSIB por mandato de la Ley 164 Art. 83 es la única entidad certificadora autorizada pública, que brinda servicios de certificado digital para Firma Digital al sector público y a la población en general.

Elaborado:		Revisado:		Aprobado:		
------------	--	-----------	--	-----------	--	--



- k) **Firma digital:** Es la firma electrónica que identifica únicamente a su titular, creada por métodos que se encuentren bajo el absoluto y exclusivo control de su titular, susceptible a verificación; está vinculada a los datos del documento digital de modo tal que cualquier modificación de estos ponga en evidencia su alteración. Cadena de caracteres generados por un método criptográfico asimétrico, que se adjunta o asocia a un documento electrónico para asegurar su autenticidad, integridad y no repudio.
- l) **Firmante o Signatario:** Es el titular de una firma digital que utiliza la misma bajo su exclusivo control y el respaldo de un certificado digital proporcionado por entidades certificadoras autorizadas.
- m) **Expediente Digital:** El expediente digital es el conjunto ordenado de datos, información y documentos digitales, vinculados sobre un determinado asunto, independientemente de la naturaleza de la información que contenga.
- n) **Dispositivo Criptográfico basado en Software (software token):** Dispositivo Criptográfico digital para la generación de Par de Claves, Certificado Digital y firma de documentos que cumpla con el estándar FIPS 140-2 Nivel 1 mínimamente.
- o) **Huella de Identificación ("Hash" o Resumen):** Es el resultado de aplicar algoritmos matemáticos al documento electrónico, para transformarlo en una cadena de caracteres de longitud fija, asociado unívocamente a los datos del documento electrónico original.
- p) **Integridad:** Cualidad, del documento electrónico firmado digitalmente, de estar protegido contra alteraciones accidentales o fraudulentas.
- q) **Nivel de Seguridad:** Alto, cuando se usa un dispositivo de seguridad de hardware (USB) para la firma y almacenamiento del certificado. Normal, cuando se usa un contenedor por software para el almacenamiento del certificado digital y la generación del par de claves.
- r) **Participante:** Es la persona natural autorizada a realizar operaciones, revisiones, validaciones de un documento, acto administrativo o trámite en el Sistema de Gestión y Flujo Documental SISCOR.
- s) **Repudio:** Negativa del firmante o signatario de una operación o comunicación efectuada a reconocer su participación en la misma.
- t) **SISCOR:** Sistema de Gestión y Flujo documental cuya funcionalidad permite la gestión documental y almacenamiento de documentos ya firmados digitalmente.
- u) **Procedimiento de Archivo:** Es el proceso por el cual se resguarda la documentación (física y/o digital) durante el tiempo necesario conforme a normativa. Los responsables del resguardo de la documentación es el personal de archivo.

Elaborado:		Revisado:		Aprobado:		
------------	--	-----------	--	-----------	--	--



- v) **Sistema Informático:** El sistema compuesto de equipos y de personal pertinente que realiza funciones de entrada, proceso, almacenamiento, salida y control con el fin de llevar a cabo una secuencia de operaciones con datos.

**Artículo 5.- (Modificaciones y/o actualizaciones al Reglamento).**

La Unidad de Planificación y Desarrollo Organizacional en coordinación con la Unidad de Tecnología Informática, es responsable de modificar y/o actualizar el presente Reglamento.

**CAPITULO II  
FIRMA DIGITAL**

**Artículo 6.- (Uso de la Firma Digital).**

Los documentos electrónicos habilitados para trámites digitales que son generados en el Sistema de Gestión y Flujo Documental SISCOR, deben ser firmados digitalmente y cumplir con lo establecido en el presente Reglamento. El uso de certificados digitales valida la firma digital.

**Artículo 7.- (Finalidad de la Firma Digital).**

La Firma Digital tiene por finalidad dar seguridad y validez al documento electrónico creado, gestionado y/o enviado por el firmante, garantizando:

- a) Que el documento electrónico fue firmado digitalmente por el firmante (autenticación).
- b) Que el documento electrónico no ha sufrido alteraciones durante su transmisión (integridad).
- c) Que el firmante no pueda desconocer un documento electrónico que ha sido firmado usando su clave privada (no repudio).

**Artículo 8.- (Beneficios de la Firma Digital).**

Los beneficios que tiene la implementación de la Firma Digital son: seguridad, ahorro de tiempo y desplazamientos, no requiere la presencia física, protección al medioambiente reduciendo el uso de papel e impresión de documentos, permite realizar trámites en forma digital, ahorro en mensajería y archivo físico.

**Artículo 9.- (Naturaleza de los trámites).**

- I. De acuerdo a la naturaleza de los trámites, podrán existir trámites mixtos, que involucren la gestión de documentos digitales y documentos físicos como parte de un mismo trámite, en atención a sus procesos específicos.
- II. Asimismo, en aquellos casos que un trámite esté en curso de forma digital y durante el proceso hubiera sucedido la Revocación del Certificado Digital (extravío de token o por

Elaborado:



Revisado:



Aprobado:





sospecha de datos de creación vulnerados) del Servidor Público que le correspondía firmar, firmará de forma manuscrita el documento. El resto del trámite continuará como trámite físico, debiendo ser firmado de forma manuscrita hasta su culminación.

- III. En tanto se consolide la implementación y en la medida que se requiera trabajar en modificaciones normativas para trámites específicos, algunos procesos deberán coexistir entre físicos y digitales; por lo que se imprimirán y firmarán documentos físicamente de acuerdo a requerimientos y necesidades.

#### Artículo 10. (Validez Jurídica y Probatoria de Documentos Firmados Digitalmente).

Los documentos digitales, habilitados en el Sistema de Gestión y Flujo Documental – SISCOR, que sean firmados digitalmente, poseen plena validez jurídica y probatoria conforme lo establecido en el artículo 78 de la Ley N° 164, Ley General de Telecomunicaciones Tecnologías de Información y Comunicación, de 8 de agosto de 2011.

#### Artículo 11. (Características de la Firma Digital).

La Firma Digital, para ser usada en el Sistema de Gestión y Flujo Documental SISCOR, debe poseer las siguientes características mínimas:

- Los datos de creación de la firma digital, deben estar bajo control exclusivo del firmante.
- Debe identificar al firmante.
- Debe ser única para cada documento electrónico firmado digitalmente.
- Debe ser susceptible de verificación, usando la clave pública del firmante.
- Debe estar ligada al documento electrónico, de manera que, si éste es modificado, la Firma Digital del documento modificado se invalida.

#### Artículo 12.- (Revocatoria del Certificado Digital).

- La revocatoria del Certificado Digital implica su inhabilitación por la Entidad de Certificación, invalidando su uso para nuevos documentos electrónicos firmados digitalmente, aspecto que será notificado oportunamente por la Unidad de Recursos Humanos a la ECA y a la Unidad de Tecnología Informática.
- Los participantes de la gestión documental deberán obligarse a revocar el Certificado Digital en cualquiera de los casos siguientes:
  - Cuando la confidencialidad de la clave privada ha sido puesta en duda o corre peligro de que se le dé un uso indebido.
  - Cuando la clave privada ha sido eliminada, destruida o es inaccesible.
  - Cuando el participante deja sin efecto los poderes conferidos al firmante.
  - Por orden judicial o de autoridad administrativa competente.

Elaborado:		Revisado:		Aprobado:		
------------	--	-----------	--	-----------	--	--



### Artículo 13.- (Prohibiciones).

Queda terminantemente prohibido por el titular de la Firma Digital:

- a) Usar la Firma Digital para beneficio particular o privado.
- b) Transferir el token (dispositivo criptográfico) a otro servidor público para firmar por él.
- c) Prestar el token (dispositivo criptográfico). Temporal o permanentemente a otra institución o particular.
- d) Dañar o alterar las características físicas o técnicas del token.
- e) Utilizar el token para fines ajenos a los estrictamente institucionales.
- f) Usar firma digital en documentos que no sean generados por la ATT.

### Artículo 14.- (Previsiones y aspectos no contemplados en el presente Reglamento).

Los aspectos no previstos en el presente reglamento serán resueltos en el marco de la normativa legal vigente.

### Artículo 15.- (Presunción de autoría y responsabilidad).

Para efectos legales y administrativos, todos los documentos asociados a una Firma Digital en SISCOR se presumirán vigentes al momento de su emisión, íntegro, auténtico y de la autoría y responsabilidad del servidor público que lo emite, revisa y/o aprueba o participa del flujo del mismo; siempre y cuando se ajusten a los procedimientos y controles dispuestos por este Reglamento.

### Artículo 16.- (Impresión y/o reproducción de documentos firmados digitalmente).

- I. Los documentos firmados digitalmente podrán imprimirse de acuerdo a la naturaleza del trámite o destino; por lo tanto, las impresiones o reproducción de documentos digitales firmados digitalmente en SISCOR, tienen validez probatoria y se encuentran permitidos.
- II. Excepcionalmente, ante la imposibilidad de suscribir un documento de forma digital, el mismo podrá ser suscrito firmado de forma manuscrita, teniendo el mismo valor. Los documentos que se suscriban de manera manuscrita, concluirán su ciclo de aprobación en la misma forma.

### Artículo 17.- (Casos excepcionales).

Los documentos firmados digitalmente pueden ser sujetos de modificación o anulación a través del Sistema de Gestión y Flujo Documental – SISCOR.

- I. **Modificación.-** Si un documento fuera sujeto de modificación, esta acción deberá ser realizada por el emisor original, con la aprobación de su inmediato superior, detallando en la glosa el motivo que sustente la modificación.

Elaborado:		Revisado:		Aprobado:		
------------	--	-----------	--	-----------	--	--



- II. **Anulación.-** Si un documento fuera objeto de anulación, juntamente con su número correlativo pasará a estado de “Anulado”, acción que debe ser realizada por el emisor original con la aprobación de su inmediato superior, detallando en la glosa el motivo que sustente la anulación.

### CAPITULO III CERTIFICADO DIGITAL

#### Artículo 18.- (Tipo de Certificado Digital).

De conformidad a lo establecido en la Resolución Ministerial N° 235/18, cuando la entidad pública es emisora del documento, se deberá utilizar Firma Digital con nivel de seguridad alto (dispositivo criptográfico), en este sentido su uso es absolutamente necesario.

#### Artículo 19.- (Adquisición de Dispositivos Criptográficos).

- I. La inclusión de Firma Digital en la gestión documental Institucional, demanda que todos los servidores públicos que trabajan en la entidad y generan, participan, revisan, aprueban, y/o dan conformidad de un acto administrativo puedan firmar digitalmente el mismo tal como lo harían en un documento físico.
- II. En ese sentido, todos los servidores públicos de la Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes – ATT, deberán adquirir por cuenta propia el dispositivo criptográfico (token) por única vez; el cual pasará a ser de su propiedad en adelante.
- III. El dispositivo criptográfico (token) se utilizará como requisito único e indispensable para poder habilitarse en el SISCOR e interactuar en los procesos de gestión documental.

#### Artículo 20.- (Habilitación del Certificado Digital).

La Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes, proporcionará mediante la Entidad Certificadora Autorizada (ECA), el Certificado Digital asociado al firmante.

#### Artículo 21.- (Contenido del Certificado Digital).

El Certificado Digital deberá contener, por lo menos, la siguiente información:

- a) Datos que identifiquen al firmante: Nombres y Apellidos, número de Cédula de Identidad, Nombre del Cargo que ocupa.
- b) Clave pública del firmante.
- c) Fecha y hora de emisión y expiración del Certificado Digital.
- d) Cualquier limitación de uso y responsabilidad a la que esté sometido el Certificado Digital.
- e) Algoritmo y huella de identificación del Certificado Digital.
- f) Número de serie del Certificado Digital.

Elaborado:		Revisado:		Aprobado:		
------------	--	-----------	--	-----------	--	--



#### Artículo 22.- (Vigencia y Renovación del Certificado Digital).

- I. La vigencia del certificado digital será establecida por la Entidad Certificadora Autorizada (ECA);
- II. Antes del vencimiento, el certificado digital podrá ser renovado por un periodo similar previa solicitud ante la ECA.
- III. El Certificado Digital será renovado anualmente y mientras el servidor público preste servicios laborales en la ATT.
- IV. El proceso de renovación deberá realizarse y gestionarse por la Unidad de Recursos Humanos antes del vencimiento.

La Unidad de Recursos Humanos tendrá como insumo la información reportada por el propietario del Certificado Digital con al menos cinco (5) días hábiles previos a la fecha de vencimiento.

#### Artículo 23.- (Emisión del Certificado Digital – Firma Digital).

Los certificados y firmas Digitales utilizados en el Sistema de Gestión y Flujo Documental – SISCOR son emitidos por la Entidad Certificadora Autorizada, bajo sus reglamentos y procedimientos establecidos.

#### Artículo 24.- (Obtención del Certificado Digital).

La Unidad de Recursos Humanos, gestionará la obtención del Certificado de la Firma Digital ante la Entidad Certificadora Autorizada para los servidores públicos dependientes de la Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes – ATT.

#### Artículo 25.- (Responsabilidad del Titular de la Firma Digital).

El titular de la Firma Digital, es responsable por las acciones, actos y omisiones realizados durante el periodo de vigencia de la firma digital y los resultados emergentes de los mismos sujetos a la Ley N° 1178 y al régimen de responsabilidad por la función pública.

#### Artículo 26.- (Obligaciones del Titular de la Firma Digital).

El titular de la Firma Digital, tiene las siguientes obligaciones:

- a) Proporcionar información fidedigna y susceptible a verificación por parte de la Entidad Certificadora Autorizada (ECA), para fines de obtención de la Firma Digital.
- b) Efectuar la actualización de sus datos personales en la ECA una vez al año.
- c) Notificar oportunamente a través de correo electrónico a las Unidades de Tecnología Informática y Recursos Humanos cuando los datos de creación de su Firma Digital hayan sido conocidos por terceros no autorizados y que podría ser indebidamente utilizada, debiendo, solicitar la revocación de su Firma Digital.
- d) Realizar seguimiento a reactivación de la Firma Digital, que será gestionada personalmente ante la ECA.

Elaborado:		Revisado:		Aprobado:		
------------	--	-----------	--	-----------	--	--



- e) Proporcionar a la Unidad de Recursos Humanos la fecha de vencimiento del Certificado Digital, con anticipación de cinco (5) días hábiles, a fin de que se gestione la renovación.

**Artículo 27.- (Derechos del Titular de la Firma Digital).**

El titular de la Firma Digital, tiene por derechos los establecidos en el artículo 54 del Reglamento a la Ley 164 para el Desarrollo de Tecnologías de Información y Comunicación aprobado mediante Decreto Supremo N°1793.

**Artículo 28.- (Tarifas del Servicio de Firma Digital).**

La ATT, asumirá el costo de la tarifa establecida por la ECA para la prestación del servicio de Firma Digital de los titulares propietarios del dispositivo criptográfico (token), para el uso de firma digital.

**Artículo 29.- (Revocación y Reactivación del Certificado Digital).**

- I. **Revocación.-** La Unidad de Recursos Humanos reportará a la Unidad de Tecnología Informática cuando se produzca una situación de Revocación del Certificado Digital.

La Unidad de Recursos Humanos, una vez conocido el hecho, gestionará ante la ECA de manera inmediata la revocación del Certificado Digital.

La Revocación del Certificado Digital puede producirse por la desvinculación laboral de algún servidor público o cuando el titular reporte que los datos de creación de su firma hayan sido conocidos por terceros no autorizados y que podría ser indebidamente utilizada, razones por las que solicite la revocación de su Firma Digital.

- II. **Reactivación.-** La Reactivación del Certificado Digital se dará luego de una revocación del mismo cuando el titular hubiera reportado a la Unidad de Recursos Humanos que los datos de creación de su firma hayan sido conocidos por terceros no autorizados.

Las gestiones de Reactivación del Certificado Digital serán realizadas por el titular de la Firma Digital ante la ECA.

**Artículo 30.- (Extravío de Tokens).**

- I. En caso de extravío del Token, el Servidor Público deberá notificar el hecho mediante correo electrónico a la Unidad de Recursos Humanos con la finalidad que gestione de inmediato la revocación del Certificado Digital ante la ECA.
- II. La gestión de reposición es responsabilidad del Servidor Público realizando el depósito bancario o transferencia bancaria del monto correspondiente a la reposición de manera inmediata.

Elaborado:		Revisado:		Aprobado:		
------------	--	-----------	--	-----------	--	--



- III. Una vez realizada la gestión de reposición, el Servidor Público coordinará con la ECA la entrega del Dispositivo Criptográfico (Token).
- IV. Habiendo repuesto el Dispositivo Criptográfico (Token), el Servidor Público comunicará vía correo electrónico a la Unidad de Recursos Humanos.
- V. Las gestiones de reactivación del Certificado Digital y consiguiente rehabilitación de la Firma Digital estarán a cargo del Servidor Público.

**Artículo 31.- (Conservación de los Documentos Electrónicos Firmados Digitalmente).**

Los documentos electrónicos firmados digitalmente en el Sistema de Gestión y Flujo Documental - SISCOR, deberán ser conservados, así como el registro de aplicación y validación de la Firma Digital y archivos anexos, de acuerdo a normativa vigente.

**CAPÍTULO IV  
RESPONSABILIDADES Y OBLIGACIONES DEL FIRMANTE  
EN EL SISTEMA DE GESTIÓN Y FLUJO DOCUMENTAL - SISCOR**

**Artículo 32.- (Responsabilidades).**

- a) Cada servidor público (participante de la elaboración de un documento y/o trámite) deberá acreditar en el Sistema de Gestión y Flujo Documental - SISCOR, su firma digital, cada vez que necesite firmar los documentos que son de su autoría, participación o registrar su visto bueno de acuerdo con los procedimientos que correspondan.
- b) Cada firmante deberá contar con su respectiva Firma Digital, emitida de acuerdo a los procedimientos y estándares definidos.
- c) El Sistema de Gestión y Flujo Documental – SISCOR, no guardará ni almacenará la clave privada del Titular ni los datos relacionados a su firma digital, siendo esta de entera autonomía del mismo.

**Artículo 33.- (Obligaciones).**

El Firmante de documentos o actos administrativos creados en el Sistema de Gestión y Flujo Documental - SISCOR, deberá:

- a) Firmar digitalmente el documento electrónico de acuerdo a los lineamientos establecidos.
- b) Mantener el control exclusivo y la debida confidencialidad de la clave privada bajo su responsabilidad.
- c) Cuando el usuario (firmante) del Sistema de Gestión y Flujo Documental SISCOR genere sus documentos electrónicos firmados digitalmente, deberá asegurar que los datos y el mecanismo de firma estén resguardados de manera segura y confidencial a fin de evitar su uso no autorizado.

Elaborado:		Revisado:		Aprobado:		
------------	--	-----------	--	-----------	--	--



**Artículo 34.- (Responsabilidades del Participante con Relación a su Firma Digital).**

- I. Cada participante es responsable de los actos de su firma en virtud de su participación en la elaboración, revisión y/o participación en un documento o trámite.
- II. Los documentos y/o actos administrativos entre los firmantes, aprobadores y revisores en el Sistema de Gestión y Flujo Documental SISCOR deberán considerar al menos las responsabilidades siguientes:
  - a) Por el contenido de los documentos firmados digitalmente con la clave privada del firmante y por los efectos que estos generen.
  - b) Por la información proporcionada para la generación de la firma Digital y por el contenido de éste.
  - c) Por el uso no autorizado de la clave privada.

**Artículo 35.- (Responsabilidades de las áreas involucradas).**

**a) Unidad de Tecnología Informática es responsable de:**

- 1) La actualización del Sistema de Gestión Documental Digital para la inclusión de procesos que permitan el uso de Firma Digital según normativa vigente y en plazos programados.
- 2) Realizar capacitaciones sobre el uso del Sistema de Gestión y Flujo Documental SISCOR al personal de la ATT.
- 3) Administrar el Sistema de Gestión y Flujo Documental SISCOR.

**b) Unidad de Recursos Humanos es responsable de:**

- 1) Instruir a los servidores públicos que se incorporan a la ATT, adquirir por cuenta propia el dispositivo criptográfico (token), dispositivo que se utilizará como requisito único e indispensable para poder habilitarse en el SISCOR e interactuar en los procesos de gestión documental.
- 2) Gestionar ante la ECA la revocación de los Certificados Digitales del personal que se desvincule de la Institución.
- 3) Gestionar ante la ECA la revocación de los Certificados Digitales del personal que hubiera reportado que los datos de su Firma Digital hayan sido conocidos por terceros no autorizados y que podría ser indebidamente utilizada.
- 4) Realizar gestiones necesarias ante la Entidad Certificadora Autorizada (ECA) para proporcionar el Certificado Digital asociado al firmante.

Elaborado:		Revisado:		Aprobado:		
------------	---	-----------	---	-----------	---	---



### DISPOSICIÓN FINAL

**ÚNICA.** - En tanto la normativa no sea modificada o se emita una nueva, toda notificación a ser realizada dentro de los procedimientos administrativos llevados a cabo en el marco del Reglamento de la Ley de Procedimiento Administrativo para el SIRESE, aprobado por Decreto Supremo N° 27172 de 15 de septiembre de 2003, seguirán siendo realizados en el marco de la normativa vigente.

Elaborado:		Revisado:		Aprobado:		
------------	--	-----------	--	-----------	--	--