Resolución Administrativa Regulatoria **ATT-DJ-RAR-TL LP 192/2020**

La Paz, 23 de junio de 2020

VISTOS:

La Resolución Administrativa Regulatoria ATT-DJ-RAR-TL 202/2019 de 16 de abril de 2019 (**R.A.R. 202/2019**); la Resolución Administrativa Regulatoria ATT-DJ-RAR-TL LP 209/2019 de 24 de abril de 2019 (**R.A.R. 845/2018**); el Informe Técnico ATT-DTLTIC-INF TEC LP 136/2020 de 09 de marzo de 2020 (**INF-TEC 136/2020**); el Informe Jurídico ATT-DJ-INF-JUR LP 178/2020 de 23 de junio de 2020 (**INF-JUR 178/2020**); las normas aplicables y todo lo que convino ver y se tuvo presente;

Lic. Juan Carlos Mancilla Peñafiel
ANALISTA LEGAL
AUTORIDAD DE REGULACIÓN Y FISCALIZACIÓN DE TELECOMUNICACIONES Y TRANSPORTES

CONSIDERANDO 1: (Competencias).-

Que las atribuciones, competencias, derechos y obligaciones en materia de telecomunicaciones, tecnologías de la información y comunicación, transportes y del servicio postal, asumidas por la Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes (**ATT**), se encuentran previstas en la Ley N° 164, de 08 de agosto de 2011, General de Telecomunicaciones, Tecnologías de Información y Comunicación (**Ley N° 164**), en relación a lo establecido en el Decreto Supremo N° 0071 de 09 de abril de 2009 (**DS 0071**), quedando sometidas a la ATT, las personas naturales y jurídicas, privadas, comunitarias, públicas, mixtas y cooperativas, con la finalidad de garantizar los intereses y derechos de los usuarios o consumidores, promoviendo de esta manera la economía plural prevista en la Constitución Política del Estado Plurinacional de Bolivia y las leyes en forma efectiva, bajo tuición del Ministerio de Obras Públicas, Servicios y Vivienda.

CONSIDERANDO 2: (Antecedentes).-

Que mediante **R.A.R. 202/2019** se aprobó los Estándares Técnicos y otros Lineamientos para el Funcionamiento de las Entidades Certificadoras, que forman parte del Anexo de dicha Resolución, en cumplimiento de lo establecido por el Decreto Supremo N° 3527 de 11 de abril de 2018.

DIRECTOR EJECUTIVO INTERINO C.A.A.T. A.T.T.

Que mediante **R.A.R. 209/2019** se aprobó el Estándar Técnico para la emisión de Certificados Digitales, así como sus Anexos.

Que mediante Nota ADSIB/NE/1209/2019 la Agencia para el Desarrollo de la Sociedad de la Información – ADSIB en su rol de Entidad Certificadora Autorizada Pública solicitó la habilitación del Servicio HSM en la nube.

Que por Nota ATT-DTLTIC-N LP 4044/2019 de 11 de diciembre de 2019 esta Autoridad solicitó a la ADSIB remitir información complementaria del Servicio propuesto, misma que fue remitida por nota ADSIB/NE/1236/2019

DIRECCIÓN JURÍDICA J.S.M.

Que mediante Nota CD-CTA – N° 0028/2019 Certificaciones Digitales DIGICERT S.R.L. Entidad Certificadora Autorizada Privada solicitó a la Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes – ATT en su calidad de Entidad Certificadora Raíz, la habilitación del Servicio HSM en la nube.

Que por Nota ATT-DTLTIC-N LP 11/2020 de 03 de enero de 2020 esta Autoridad a solicitó Certificaciones Digitales DIGICERT S.R.L. remitir información complementaria referente al Servicio HSM en la nube, misma que fue remitida por nota CD-CTA – N° 0003/2020.

I-LP-9624

Que el **INF-TEC 136/2020** concluyó que a partir de la solicitud formal a la ATT por parte de las Entidades Certificadoras Autorizadas para la habilitación del "Servicio HSM en la nube", la Unidad de Regulación de Tecnologías de la Información, dependiente de la Dirección Técnica Sectorial de Telecomunicaciones y TIC de este Ente Regulador, realizó una propuesta de normativa como instrumento regulatorio con alcance nacional, que permitirá viabilizar la solicitud a través de la Emisión de Certificados Digitales para Firma Digital Remota por parte de las Entidades Certificadoras Autorizadas, el cual consiste en la implementación de infraestructura tecnológica que permita la emisión, administración y custodia de certificados digitales a través de sistemas de control que garanticen los principios del Servicio de Certificación Digital establecidos en el Parágrafo II del artículo 4 del Reglamento para el Desarrollo de Tecnologías de la Información y Comunicación, aprobado por Decreto Supremo N° 1793 de 13 de noviembre de 2013 (**REGLAMENTO TIC**) con el fin de permitir a los signatarios realizar operaciones de firma digital de forma remota, además de verificar que el "ESTÁNDAR TÉCNICO PARA LA EMISION DE CERTIFICADOS DIGITALES PARA FIRMA DIGITAL REMOTA" cumple con las necesidades técnicas de las Entidades Certificadoras Autorizadas para la emisión de los mencionados certificados.

CONSIDERANDO 3: (Marco normativo).-

El Parágrafo II del artículo 20 de la Constitución Política del Estado establece que: *"Es responsabilidad del Estado, en todos sus niveles de gobierno, la provisión de los servicios básicos a través de entidades públicas, mixtas, cooperativas o comunitarias. En los casos de electricidad, gas domiciliario telecomunicaciones se podrá prestar el servicio mediante contratos con la empresa privada. La provisión de servicios debe responder a los criterios de universalidad, responsabilidad, accesibilidad, continuidad, calidad, eficiencia, eficacia, tarifas equitativas y cobertura necesaria; con participación y control social."*

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 (**TIC**).

Que los numerales 2 y 5 del artículo 2 de la Ley N° 164, señala entre sus objetivos, el asegurar el ejercicio del derecho al acceso universal y equitativo a los servicios de telecomunicaciones, tecnologías de información y comunicación; y el 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 misma Ley, declara 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 artículo 81 de la Ley N° 164, dispone que la ATT es la encargada de autorizar, regular, fiscalizar, supervisar y controlar a las entidades certificadoras de acuerdo a lo establecido en la citada Ley y su reglamentación.

Que el artículo 82 de la Ley N° 164, establece que pueden constituirse y operar como entidades certificadoras, las personas jurídicas de derecho público o privado en la prestación de servicios de certificación digital, las que deben cumplir con los requisitos técnicos, económicos y legales establecidos en la presente Ley y su reglamento.

Que el artículo 83 de la Ley N° 164, determina que la Agencia para el Desarrollo de la Sociedad de la Información Bolivia (**ADSIB**), prestará el servicio de certificación para el sector público y la población en general a nivel nacional, conforme a las normas contenidas en la citada Ley, y velará por la autenticidad, integridad y no repudio entre las partes.

I-LP-9624

Que el **REGLAMENTO TIC** tiene por objeto, reglamentar el acceso, uso y desarrollo de las TIC en el marco del Título IV de la Ley N° 164.

Que el artículo 24 del **REGLAMENTO TIC** prescribe que: "*Los certificados digitales deben ser emitidos por la 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 completar la información necesaria para la verificación de la firma digital*".

Que el artículo 25 del **REGLAMENTO TIC** modificado por el Decreto Supremo N° 3527 de 11 de abril de 2018 dispone que: "*La ATT, establecerá mediante Resolución Administrativa los tipos, formatos y estructura de certificados digitales que podrán ser emitidos por las Entidades Certificadoras Autorizadas de acuerdo al uso conforme a estándares y recomendaciones internacionales aplicables que promuevan interoperabilidad con otros sistemas*".

Que el artículo 37 del **REGLAMENTO TIC**, determina la estructura jerárquica de la organización de la Infraestructura Nacional de Certificación Digital, estableciendo cuatro (4) niveles: En un primer nivel esta la ATT como ***Entidad Certificadora de Raíz***. En un segundo nivel, se encuentran las ***Entidades Certificadoras***, tanto la pública (ADSIB) como privadas subordinadas a la ATT. En un tercer nivel, se encuentra la ***Agencia de Registro***, como dependiente de una entidad certificadora, encargada de realizar el registro y la identificación de la persona natural o jurídica en forma fehaciente y completa; y, por último, en un cuarto nivel, se ubican los ***Signatarios***, que son todos los usuarios y usuarias finales a quienes se les ha emitido un Certificado Digital por una entidad certificadora.

Que el artículo 38 del **REGLAMENTO TIC** dispone las funciones de la ATT para el cumplimiento de sus atribuciones establecidas en la Ley N° 164, prescribiendo las siguientes: *"c) Definir los requerimientos técnicos que califiquen la idoneidad de las actividades desarrolladas por las entidades de certificación;"* y *"j) Aprobar los reglamentos y procedimientos específicos de las entidades certificadoras para la prestación del servicio de certificación digital, así como sus modificaciones"*.

Que inciso a) del artículo 43 del **REGLAMENTO TIC**, establece como obligación de las Entidades Certificadoras, el cumplir con la normativa vigente y los estándares técnicos emitidos por la **ATT**.

CONSIDERANDO 4: (Análisis y justificación).-

Que el **INF-TEC 136/2020** realizo el análisis correspondiente para la aprobación del ESTÁNDAR TÉCNICO PARA LA EMISION DE CERTIFICADOS DIGITALES PARA FIRMA DIGITAL REMOTA que consiste en la implementación de infraestructura tecnológica que permita la emisión, administración y custodia de certificados digitales a través de sistemas de control que garanticen los principios del Servicio de Certificación Digital establecidos en el parágrafo II del artículo 4 del **REGLAMENTO TIC** con el fin de permitir a los signatarios realizar operaciones de firma digital de forma remota, cuya autorización solamente podrán ser obtenidas y efectuadas por las Entidades Certificadoras Autorizadas pertenecientes a la Infraestructura Nacional de Certificación Digital, debiendo cumplir los estándares aprobados por la Entidad Certificadora Raíz, correspondiendo tanto la Entidad Certificadora Publica autorizada y las Entidades Certificadoras Autorizadas privadas cumplir con los requisitos legales, técnicos y económicos para el efecto, detallando que los dispositivos para la custodia de Certificados Digitales para la firma digital remota, deben ser Módulos de Seguridad de Hardware criptográfico (HSM) que mínimamente cumplan con el estándar FIPS 140-2 Nivel 3 lo propio con la o las copias de seguridad correspondientes, asimismo detalló el procedimiento para su emisión, la auditoría técnica de cumplimiento que se realizara a las Entidades previamente a la autorización para su emisión,

I-LP-9624

el servicio de soporte con el que deberá contar las Entidades Certificadoras Autorizadas como parte de sus servicios, así como la vigencia la cual estará enmarcada en el plazo establecido en el contrato de Entidad Certificadora Autorizada para la provisión de Servicios de Certificación Digital.

Que el **INF-JUR 178/2020** señaló que en virtud a los antecedentes citados y las disposiciones de orden legal mencionadas, se considera y concluye que de acuerdo al análisis y la conclusión plasmada en el **INF-TEC 136/2020** para la solicitud de habilitación del "Servicio HSM en la nube" es necesaria la aprobación del "ESTÁNDAR TÉCNICO PARA LA EMISION DE CERTIFICADOS DIGITALES PARA FIRMA DIGITAL REMOTA" y sus anexos, el cual no contraviene la normativa vigente, por lo tanto, se recomendó emitir la correspondiente Resolución Administrativa Regulatoria.

Que por los antecedentes señalados, así como por lo dispuesto por la normativa vigente es necesario que la ATT como Entidad Certificadora Raíz, apruebe el "ESTÁNDAR TÉCNICO PARA LA EMISION DE CERTIFICADOS DIGITALES PARA FIRMA DIGITAL REMOTA" y sus anexos, teniendo en consideración el análisis realizado y lo concluido en el **INF-TEC 136/2020**, para la emisión de Certificados Digitales para Firma Digital Remota que consiste en la implementación de infraestructura tecnológica que permita la emisión, administración y custodia de certificados digitales a través de sistemas de control que garanticen los principios del Servicio de Certificación Digital establecidos en el parágrafo II del artículo 4 del **REGLAMENTO TIC** con el fin de permitir a los signatarios realizar operaciones de firma digital de forma remota, razón por la cual se emite la presente Resolución Administrativa Regulatoria.

POR TANTO:

El Director Ejecutivo Interino de la ATT, Abog. Carlos Andrés Aliaga Téllez, designado mediante Resolución Ministerial Nº 092 de 29 de mayo de 2020, en uso de sus atribuciones conferidas por ley y demás normas vigentes, a nombre del Estado Plurinacional de Bolivia;

RESUELVE:

PRIMERO.- APROBAR el **"ESTÁNDAR TÉCNICO PARA LA EMISION DE CERTIFICADOS DIGITALES PARA FIRMA DIGITAL REMOTA"** y sus anexos que forman parte indivisible e inseparable de la presente Resolución.

SEGUNDO.- INSTRUIR a la Unidad de Tecnologías de Información y Comunicación de esta Autoridad, publicar la presente Resolución Administrativa Regulatoria en la página web de la ATT, asimismo, conforme a lo dispuesto en el artículo 34 de la Ley N° 2341, de 23 de abril de 2002, de Procedimiento Administrativo, realizar la publicación del presente acto administrativo en un órgano de prensa de circulación nacional.

Regístrese, comuníquese y archívese.

Abog. Carlos Andrés Aliaga Téllez
DIRECTOR EJECUTIVO INTERINO
AUTORIDAD DE REGULACIÓN Y FISCALIZACIÓN
DE TELECOMUNICACIONES Y TRANSPORTE

Abog. Luis Antonio Kosonic Kaune
JEFE DE OPERACIONES LEGALES
DE OTORGAMIENTOS
AUTORIDAD DE REGULACIÓN Y FISCALIZACIÓN
DE TELECOMUNICACIONES Y TRANSPORTES

I-LP-9624

ESTÁNDAR TÉCNICO PARA LA EMISION DE CERTIFICADOS DIGITALES PARA FIRMA DIGITAL REMOTA

ARTÍCULO 1. (OBJETO). -

Establecer las disposiciones generales para la Emisión de Certificados Digitales para Firma Digital Remota, con respecto a la autorización, requisitos y otros aspectos necesarios.

ARTÍCULO 2. (DESCRIPCIÓN DEL SERVICIO). -

La Custodia de Certificados Digitales para la Firma Digital Remota consiste en la implementación de un servicio con los sistemas de control de seguridad correspondientes para la administración y custodia de claves y certificados digitales emitidos por las Entidades Certificadoras Autorizadas, para permitir a los signatarios realizar operaciones de firma digital de forma remota.

ARTÍCULO 3. (ESTÁNDARES). -

3.1 La RFC 3647 - Política de Certificados de Infraestructura de Clave Pública y Marco de Prácticas de Certificación

3.2 ITU-T X.509 - Estándar de la UIT-T que especifica los formatos para el estándar de certificados de claves públicas y un algoritmo de validación de la ruta de certificación.

ARTÍCULO 4. (NORMATIVA APLICABLE). -

4.1 La Ley N° 164, de 08 de agosto de 2011, Ley General de Telecomunicaciones, Tecnologías de la Información y Comunicación (LEY N° 164).

4.2 Reglamento General a la Ley de Telecomunicaciones, Tecnologías de Información y Comunicación, aprobado mediante Decreto Supremo N° 1793 de 13 de noviembre de 2013.

4.3 Modificación del Reglamento General a la Ley de Telecomunicaciones, Tecnologías de Información y Comunicación, aprobado mediante Decreto Supremo N° 3527 de 11 de abril de 2018.

4.4 Resolución Administrativa Regulatoria ATT-DJ-RAR-TL LP 202/2019 mediante la cual se aprueban los Estándares Técnicos y otros Lineamientos Establecidos para el Funcionamiento de las Entidades Certificadoras.

4.5 Resolución Administrativa Regulatoria ATT-DJ-RAR-TL LP 209/2019 mediante la cual se aprueba el Estándar Técnico para la Emisión de Certificados Digitales

ARTÍCULO 5. (ABREVIATURAS). -

EC: Entidad Certificadora.
ECA: Entidad Certificadora Autorizada como parte de la INCD de Bolivia.
ECR: Entidad Certificadora Raíz.
CP: (CertificatePolicy) Política de Certificación.
CPS: (CertificationPracticeStatement) Declaración de Prácticas de Certificación
ATT: Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes.

I-LP-9624

INCD: Infraestructura Nacional de Certificación Digital.
OID: (ObjectIdentifier) Identificador de Objeto.

ARTÍCULO 6. (DEFINICIONES). -

6.1. Servicio de emisión de Certificados Digitales para Firma Digital Remota: Servicio de emisión, administración y custodia de claves y certificados digitales de signatarios para realizar operaciones de Firma Digital de forma remota.

6.2. Firma digital remota: Es la acción de firmar digitalmente de forma remota utilizando un certificado y par de claves emitidos y custodiados por una Entidad Certificadora Autorizada para prestar el servicio de emisión de Certificados Digitales para Firma Digital Remota

6.3. Certificación Cruzada: Es el proceso por el cual una Entidad Certificadora Autorizada reconoce la validez de un certificado digital emitido por otra Entidad Certificadora Autorizada o Autoridad Certificadora de otro país, previo convenio firmado por ambas, y homologa tal certificado como si fuera de propia emisión, bajo su responsabilidad.

6.4. Log: Se usa el término registro, log o historial de log para referirse a la grabación secuencial en un archivo o en una base de datos de todos los acontecimientos (eventos o acciones) que afectan a un proceso particular (aplicación, actividad de una red informática, etc.).

ARTÍCULO 7. (ALCANCE). -

El presente Estándar Técnico está orientado a establecer las condiciones técnicas, requisitos y otros aspectos necesarios, para la emisión de Certificados Digitales para Firma Digital Remota

Solamente podrán obtener la autorización para la emisión de Certificados Digitales para Firma Digital Remota, las Entidades Certificadoras Autorizadas pertenecientes a la Infraestructura Nacional de Certificación Digital.

ARTÍCULO 8. (CERTIFICADOS DIGITALES). –

La emisión, administración y custodia de los Certificados Digitales para Firma Digital Remota, solamente podrán ser efectuadas por las Entidades Certificadoras Autorizadas pertenecientes a la Infraestructura Nacional de Certificación Digital.

La emisión, administración y custodia de los Certificados Digitales para Firma Digital Remota, deberán cumplir los estándares aprobados por la Entidad Certificadora Raíz.

ARTÍCULO 9. (REQUISITOS PARA PRESTAR EL SERVICIO). -

I. REQUISITOS LEGALES

Se considera como requisito legal los presentados para la Autorización de Prestación de Servicios de Certificación Digital, sin embargo, en cuanto se requiera la ECR podrá solicitar alguna documentación que vea conveniente.

I-LP-9624

II. REQUISITOS TÉCNICOS

Deberá Presentar la Políticas de Certificación (CP) actualizadas para la emisión de Certificados Digitales para Firma Digital Remota, considerando mínimamente:

1.- Un Plan de Cese de Actividades.

2.-. Se debe asegurar la protección de datos personales de los signatarios garantizando mínimamente las consideraciones del artículo 56 del Reglamento para el Desarrollo de las TIC (Decreto Supremo N° 1793):

a) Declaración de Prácticas de Certificación (CPS) (De acuerdo al contenido mínimo del Anexo 4) actualizadas para la emisión de Certificados Digitales para Firma Digital Remota.
b) Infraestructura tecnológica: describir detalladamente la plataforma tecnológica incluyendo diagramas y un detalle pormenorizado de hardware, software, dispositivos de comunicación y seguridad con los que cuenta, sus características y funcionalidad.
c) Planes y procedimientos para recuperación ante desastres (Certificación ISO 22301 o el contenido mínimo del Anexo 5).
d) Políticas y procedimientos de seguridad y evaluación de riesgos (Certificación ISO 27001 o el contenido mínimo de los Anexos 6 y 7).
e) Procedimiento y condiciones que deberán cumplir las ECAs para la emisión de Certificados Digitales para Firma Digital Remota para la conservación de los documentos físicos y digitalizados, asegurando el almacenamiento de los mismos en cumplimiento a los estándares de seguridad de los servidores ubicados en el territorio y bajo la legislación del Estado Plurinacional de Bolivia (Certificación ISO 30300 o el contenido mínimo del Anexo 8).
f) Para la emisión de Certificados Digitales para Firma Digital Remota, la Entidad Certificadora Autorizada debe implementar un ambiente de control para mantener confidencialidad, disponibilidad e integridad de la información, estableciendo medidas preventivas y reactivas a través del uso de tecnología, políticas, prácticas, procesos y procedimientos para el propósito.
g) Sin perjuicio de lo establecido en el inciso e); la Entidad Certificadora Autorizada podrá hacer uso de infraestructura alojada en el exterior como servicio; garantizando de la misma forma que lo hace con su infraestructura, los requisitos de confidencialidad, disponibilidad, integridad y seguridad previstos en este estándar, en la Resolución Administrativa Regulatoria ATT-DJ-RAR-TL LP 202/2019, así como en recomendaciones y estándares internacionales (ISO 27000, ETSI 319 401 y ETSI 319 411-2).
   Para tal caso, la ECA deberá presentar:
   1) El contrato o convenio con el proveedor de la infraestructura como servicio, así como los términos bajo los cuales dicho acuerdo se suscribe y los alcances del mismo.
   2) Declaración de la ECA sobre la responsabilidad ante cualquier incidente de seguridad a la infraestructura contratada, garantizando el cumplimiento de los requisitos para la custodia en la infraestructura contratada.

h) La Entidad Certificadora Autorizada – ECA deberá contar con un sistema de información permanente y actualizada de acceso libre vía web para la Firma Digital Remota con la siguiente información:
   1) Procedimientos de certificación digital.
   2) Procedimientos de Firma Digital Remota.
   3) Condiciones de validación, renovación, baja, suspensión y revocación y usos del certificado digital.
   4) Certificados Digitales suspendidos y revocados con los siguientes datos:

I-LP-9624

i. Numero único de serie.
ii. Fecha de emisión.
iii. Vigencia y restricciones aplicables.

5) Procedimientos de reclamos.
6) Plan tarifario de los servicios a prestar.
7) Domicilio legal, teléfonos y correo electrónico de contacto.
8) Modelo de Contrato tipo con suscriptores o signatarios (Anexo 1).
9) Términos y condiciones del Servicio actualizados (Anexo 2).

3.- Dispositivos para la Emisión de Certificados Digitales para Firma Digital Remota:

1.- Los dispositivos para la emisión, administración y custodia de Certificados Digitales para Firma Digital Remota, deben ser Módulos de Seguridad de Hardware criptográfico (HSM) que mínimamente cumplan con el estándar FIPS 140-2 Nivel 3, lo propio con la o las copias de seguridad correspondientes, garantizando lo siguiente:

a) La confidencialidad de la información utilizada para la generación de par de claves y emisión de certificados digitales para firma digital remota;
b) La información utilizada para la generación de par de claves y emisión de certificados digitales solo puedan aparecer una vez en la práctica;
c) La información utilizada para la generación de par de claves y emisión de certificados digitales pueda ser protegida por el firmante legítimo de forma fiable frente a su utilización por otros.

2. Los dispositivos para la custodia de claves y firma digital remota garantizarán la integridad de la información que debe firmarse y no impedirán que dicha información se muestre al signatario antes de firmar.
3. La generación o la gestión de la información para la generación de par de claves y emisión de certificados digitales en nombre del signatario solo podrán ser realizados por una Entidad Certificadora Autorizada – ECA.
4. Sin perjuicio del inciso c) del parágrafo 1., los prestadores de Servicios de Custodia de Certificados Digitales que gestionen la información para la generación de par de claves y emisión de certificados digitales en nombre del signatario podrán duplicar los datos de creación de firma únicamente con el objetivo de efectuar una copia de seguridad con el propósito de recuperación ante desastres siempre que se cumpla el siguiente requisito:

   El nivel de seguridad para la información duplicada (copia de respaldo) debe ser al menos el mismo que se tiene para la información original.

III. REQUISITOS ECONÓMICOS

Los requisitos económicos para la prestación del Servicio de Custodia de Certificados Digitales para la Firma Digital Remota, son los siguientes:

a) Plan de negocio proyectado para un período de cinco (5) años, vinculados a la autorización solicitada que contenga además el programa de inversiones generales a efectuar.

b) Presentación de su estructura tarifaría a la ATT para su aprobación y registro de acuerdo al artículo 42 del Reglamento para el Desarrollo de las Tecnologías de Información y Comunicación aprobado por el Decreto Supremo Nº 1793.

I-LP-9624

ARTICULO 10 (VIGENCIA)

La vigencia estará enmarcada en el plazo establecido en el contrato de Entidad Certificadora Autorizada para la provisión de Servicios de Certificación Digital.

ARTÍCULO 11 (PROCEDIMIENTO PARA LA AUTORIZACIÓN DEL SERVICIO)

Las Entidades Certificadoras Autorizadas interesadas en la Emisión de Certificados Digitales para Firma Digital Remota, deben presentar su solicitud de autorización ante el Director Ejecutivo de la ATT.

Posterior a la Auditoria de cumplimiento y a través del Dictamen que especifica claramente que la ECA puede realizar la Emisión de Certificados Digitales para Firma Digital Remota, ésta podrá proveer el servicio correspondiente a los signatarios.

ARTÍCULO 12 (AUDITORIA TÉCNICA DE CUMPLIMIENTO).-

En cumplimiento a los artículos precedentes, se realizará una Auditoria Técnica de Cumplimiento, previa Emisión de Certificados Digitales para Firma Digital Remota, el solicitante podrá aportar elementos de juicio o indicios destinados a demostrar que el servicio que se prestará cumple con los requisitos y condiciones establecidos en el presente estándar.

Este proceso debe realizarse conjuntamente entre el personal de la ATT y el personal técnico del solicitante, esta labor se realizará en base a un cronograma propuesto por el solicitante.

Una vez realizada la Auditoria Técnica de Cumplimiento y aprobados los requisitos y condiciones establecidos en el presente estándar a través del dictamen de Auditoria, los solicitantes deberán coordinar con la ATT el inicio de la prestación del Servicio.

ARTÍCULO 13 (SERVICIO DE SOPORTE).-

Las Entidades Certificadoras Autorizadas – ECA, como parte de sus servicios, deben implementar los mecanismos necesarios para proporcionar el servicio de soporte técnico que corresponda a cada uno de los servicios que presta.

Las Entidades Certificadoras Autorizadas – ECA deberán publicar los medios por los cuales brindará el servicio de soporte técnico.

Capítulo II
OTROS ASPECTOS

ARTÍCULO 14 (INTERRUPCIONES DEL SERVICIO)

I. Una Entidad Certificadora Autorizada - ECA, no podrá interrumpir la operación de su servicio, o de parte del mismo, ni podrá suspender la prestación de dichos servicios por más de treinta (30) minutos continuos, sin la autorización previa y por escrito de la ATT y después de haber informado a los usuarios que resultaren afectados a través de comunicación directa o un medio de comunicación masiva, por lo menos con cinco (5) días de anticipación.

I-LP-9624

II. En casos de emergencia, eventos de fuerza mayor o caso fortuito que justifiquen la actuación de la Entidad Certificadora Autorizada - ECA, ésta deberá reportar a la ATT en el menor plazo posible, que en ningún caso podrá exceder los tres (3) días hábiles de ocurrido el hecho.

III. Las interrupciones programadas de duración menor o igual a treinta (30) minutos no requieren autorización de la ATT.

ARTÍCULO 15 (CERTIFICADOS EMITIDOS POR ENTIDADES EXTRANJERAS)

En el marco del artículo 80 de la Ley N° 164, que establece que los certificados digitales emitidos por entidades certificadoras extranjeras tienen la misma validez y eficacia jurídica reconocida, siempre y cuando tales certificados sean reconocidos por una entidad certificadora autorizada nacional que garantice, en la misma forma que lo hace con sus propios certificados, el cumplimiento de los requisitos, el procedimiento, así como la validez y vigencia del certificado, la Entidad Certificadora Autorizada que reconozca los certificados digitales emitidos por Entidades Certificadoras extranjeras, deberá presentar:

1) Copia del instrumento correspondiente que evidencie la constitución formal de la empresa, así como la autorización por parte de la entidad o autoridad competente en el lugar de origen para la prestación de Servicios de Certificación Digital.
2) El acuerdo(s) entre ambas Entidades Certificadoras, donde se declare la validez de la certificación cruzada, así como los términos bajo los cuales dicho acuerdo se suscribe y los alcances del mismo.
3) Declaración de la ECA sobre el reconocimiento de los Certificados de la Entidad Certificadora extranjera, donde garantice la validez de los certificados emitidos por la Entidad Certificadora extranjera en la misma forma que lo hace con sus propios certificados, el cumplimiento de los requisitos, el procedimiento, así como la validez y vigencia del certificado.

Los documentos que se acompañen deberán encontrarse en idioma español. Si las fuentes originales provinieran de otro idioma, éstas deberán ser traducidas de manera oficial.

ARTÍCULO 16 (IDENTIFICACIÓN DE LOS CERTIFICADOS DIGITALES PARA FIRMA DIGITAL REMOTA)

Con el propósito de identificar los Certificados Digitales emitidos para Firma Digital Remota, se define la siguiente estructura de OIDs, complementando la establecida a través de Resolución Administrativa Regulatoria ATT-DJ-RAR-TL LP 209/2019:

OID	Descripción
2.16.68.0.0.0.1.14.1.2.0.X.2.2.0.0	CERTIFICADO DIGITAL DE PERSONA JURIDICA PARA FIRMA DIGITAL SIMPLE GENERADO PARA FIRMA DIGITAL REMOTA
2.16.68.0.0.0.1.14.1.2.0.X.2.2.0.1	CERTIFICADO DIGITAL DE PERSONA JURIDICA PARA FIRMA DIGITAL AUTOMATICA PARA FIRMA DIGITAL REMOTA *
2.16.68.0.0.0.1.14.1.2.0.X.2.2.1.0	CERTIFICADO DIGITAL DE PERSONA NATURAL PARA FIRMA DIGITAL SIMPLE GENERADO PARA FIRMA DIGITAL REMOTA
2.16.68.0.0.0.1.14.1.2.0.X.2.2.1.1	CERTIFICADO DIGITAL DE PERSONA NATURAL PARA FIRMA DIGITAL AUTOMÁTICA PARA FIRMA DIGITAL REMOTA *

I-LP-9624

*: Siempre y cuando se garantice la seguridad de los certificados, la integridad de la transacción y la comunicación.

ARTICULO 23 (INCUMPLIMIENTO). -

El incumplimiento a cualquier disposición del presente reglamento implica una infracción de acuerdo a los alcances del Reglamento de Sanciones vigente.

ARTICULO 24 (MODIFICACIONES AL ESTÁNDAR TÉCNICO). -

El presente estándar está sujeto a modificaciones de acuerdo al artículo 38 inciso j) del Reglamento para el Desarrollo de las TIC aprobado por el Decreto Supremo Nº 1793.

I-LP-9624

ANEXO 1: MODELO DE CONTRATO TIPO DE LAS ENTIDADES CERTIFICADORAS AUTORIZADAS – ECA PARA LA FIRMA DIGITAL REMOTA CON LOS SIGNATARIOS.

MODELO DE CONTRATO DE ADHESIÓN PARA CUSTODIA DE CERTIFICADOS DIGITALES PARA FIRMA DIGITAL REMOTA

Conste por el tenor del presente Documento Privado, que los suscribientes acuerdan celebrar un Contrato para la CUSTODIA DE CERTIFICADOS DIGITALES PARA LA FIRMA DIGITAL REMOTA, que con el reconocimiento o validación de las firmas surtirá los mismos efectos de documento público, sujeto a las siguientes cláusulas:

PRIMERA (PARTES CONTRATANTES).- Intervienen en la suscripción del presente Contrato:

1.1.-Entidad Certificadora Autorizada ……, representada(o) legalmente por……por el Sr.(a)……..en virtud al Documento Legal Aplicable: ……..... N°……/……de fecha de……del……otorgado mediante Notaría de Fe Pública N° ……..que para efectos de éste Contrato se denominará……..

(LLENAR EN CASO DE PERSONA NATURAL)

1.2.-El/la Señor/ra/ita……., C.I.N°……. , que en lo sucesivo se denominará SIGNATARIO(A), cuyos datos personales se detallan en el Anexo de Solicitud de Provisión de Servicios, mismo que forma parte integrante e inseparable del presente Contrato para todos los efectos legales.

(LLENAR EN CASO DE PERSONA JURIDICA)

1.3.-La Empresa……., legalmente representada(o) por el Sr.(a)……., en virtud al Poder Especial……../ de fecha…….de……del……., otorgado ante la Notaría de Fe Pública N°……a cargo del Dr.(a) ……con C.I……con MatriculaN°……con NIT N°……con Domicilio legal……que en lo sucesivo se denominará……., cuyos datos se detallan en el Anexo de Solicitud de Provisión de Servicios mismo que forma parte integrante e inseparable del presente Contrato para todos los efectos legales.

SEGUNDA (ANTECEDENTES).- Descripción del (los) servicio(s) a prestar, usos del certificado y limitaciones.

TERCERA (OBJETO DEL CONTRATO)- Describir el objeto del Contrato del servicio y la no transferibilidad de las claves y el certificado digital.

CUARTA (TÉRMINOS Y CONDICIONES).-Establecer que el servicio a contratar se someterá a sus términos y condiciones, señalando que deben formar parte integrante, indivisible, e inseparable del presente Contrato para todos los efectos legales (debiendo realizar un breve resumen).

QUINTA (PLAZO DEL CONTRATO, VIGENCIA Y PRORROGA).- Establecer plazo, vigencia y prórroga o renovación del Contrato de acuerdo a la normativa establecida por el ente regulador.

I-LP-9624

SEXTA (PLAZOS PARA LA ENTREGA, HABILITACIÓN, SUSPENSIÓN, REVOCACIÓN Y VIGENCIA DEL SERVICIO).- Establecer y describir los plazos, costos y requisitos señalados en los términos y condiciones del servicio a contratar.

SÉPTIMA (TITULARIDAD).- Describir la titularidad del uso del servicio a contratar.

OCTAVA (ESTRUCTURA TARIFARIA).- Establecer estructura tarifaria según lo señalado en los términos y condiciones del servicio a contratar.

NOVENA (FACTURACIÓN Y COBRANZA).- Establece los plazos señalados en los términos y condiciones.

DÉCIMA (DERECHOS Y OBLIGACIONES).- Describir derechos y obligaciones según señala en los términos y condiciones.

(DE LA USUARIA O USUARIO)

(DE LA ECA)

DÉCIMA SEGUNDA (EXENCIONES DE RESPONSABILIDAD).- Descripción para la ECA, en consideración a los marcos legales aplicables, sobre el servicio, la responsabilidad civil y penal u otro que se considere pertinente. Causales y condiciones bajo las cuales deba efectuarse la Revocatoria.

DÉCIMA TERCERA (ATENCIÓN DE RECLAMOS).- Describir los procedimientos y sus plazos de acuerdo a la normativa regulatoria aplicable.

DÉCIMA CUARTA (SERVICIOS DE INFORMACIÓN Y ASISTENCIA).- Establecer y detallar los horarios, días de atención, teléfono(s) y dirección del mismo.

DÉCIMA QUINTA (DECLARACIÓN EXPRESA).- Relativo a la voluntad de las partes y considerando que no media presión para la firma del presente Contrato.

DÉCIMA SEXTA (INVIOLABILIDAD Y PROTECCIÓN DE LA INFORMACIÓN DE LA USUARIA O USUARIO).- Establecer la manera de proteger la información proporcionada por la usuaria o usuario a la ECA.

DÉCIMA SÉPTIMA (RESOLUCIÓN Y RESCISIÓN DEL CONTRATO).-Describe y establece las formas y atribuciones de la disolución del Contrato.

DÉCIMA OCTAVA (INTEGRIDAD DEL CONTRATO).- Establece una breve descripción de los documentos que forman parte del presente Contrato, como formularios, documentos requeridos por la ECA, los términos y condiciones del servicio ofrecido, entre otros, los mimos que deberán ser entregados al momento de la suscripción del contrato.

DÉCIMA NOVENA (CLÁUSULA DE INTERPRETACIÓN).-En caso de duda sobre la interpretación del presente Contrato, se aplicará lo más favorable al usuario o usuaria.

VIGÉSIMA (ACEPTACIÓN).- Describir la conformidad del(a) usuaria o usuario y la aceptación por parte del proveedor de servicio, debiendo entregarse copia del presente Contrato al usuario o usuaria en el momento de la suscripción del contrato.

I-LP-9624

ANEXO 2: CONTENIDO MÍNIMO DE LOS TÉRMINOS Y CONDICIONES DE LAS ECA.

TÉRMINOS Y CONDICIONES PARA LA CUSTODIA DE CERTIFICADOS DIGITALES PARA FIRMA DIGITAL REMOTA

1. DESCRIPCIÓN DEL SERVICIO Y ASPECTOS ASOCIADOS: Detallar de manera exhaustiva la descripción de los objetos y servicios a brindar.

2. MODALIDADES DE LA PRESTACIÓN DEL SERVICIO: Describir por nombre de modalidad los servicios involucrados en el contrato.

3. REQUISITOS TÉCNICOS NECESARIOS PARA ACCEDER AL SERVICIO: Establecer cuáles son los requisitos mínimos necesarios para acceder al servicio. Asimismo, debe informar a los usuarios de las variables técnicas que pueden afectar la prestación del servicio y las limitaciones de éste.

4. HABILITACIÓN Y PLAZO PARA LA PROVISIÓN DEL SERVICIO: Establecer los plazos para la habilitación del servicio.

5. TARIFAS: En este caso los proveedores de servicios deberán establecer las tarifas considerando criterios sustentados y orientados en costos a la Custodia de Certificados Digitales para la Firma digital remota, previa presentación y aprobación por parte de la ATT según lo establecido por el artículo 42 del Reglamento para el Desarrollo de las TIC aprobado mediante D.S. 1793 y publicadas en medios de comunicación escrita en su página web.

6. DERECHOS Y OBLIGACIONES DE LOS USUARIOS DEL SERVICIO: Para la elaboración de este punto la ECA deberá listar y regirse a lo establecido en el artículo 54 y artículo 55 de la Ley N° 164, y los artículos 52, 53, 54 y 55 del D.S. 1793, modificado mediante Decreto Supremo N° 3527 de 11 de abril de 2018.

7. DERECHOS Y OBLIGACIONES DEL PROVEEDOR DE SERVICIOS: Para la elaboración de este punto el proveedor de servicios deberá listar y regirse a lo establecido en el artículo 54, 55, 58 y 59 de la Ley N° 164 y los artículos 43 al 46 y 56 del D.S. 1793, modificado mediante Decreto Supremo 3527 de 11 de abril de 2018.

8. ATENCIÓN DE CONSULTAS, RECLAMACIONES Y EMERGENCIAS O SERVICIOS DE INFORMACIÓN Y ASISTENCIA: Para la elaboración de este punto el proveedor de servicios debe regirse a lo establecido en el Reglamento de la Ley de Procedimiento Administrativo para el Sistema de Regulación Sectorial aprobado por D.S. 27172. El contratante tiene derecho a recibir por parte de la ECA, a través de la Oficina de Atención del Consumidor ODECO, la debida atención y procesamiento de sus reclamaciones por cualquier deficiencia en la prestación de servicio.

9. MEDIDAS PARA SALVAGUARDAR LA INVIOLABILIDAD DE LAS TELECOMUNICACIONES Y PROTECCIÓN DE LA INFORMACIÓN: Para la elaboración de

I-LP-9624

este punto el proveedor de servicios debe regirse a lo establecido por el artículo 56 de la Ley N° 164 que establece la inviolabilidad y secreto de las comunicaciones.

10. CAMBIO O MODIFICACIONES EN LA LEY O REGLAMENTOS DE TELECOMUNICACIONES: Los términos y condiciones deben estar enmarcados en la Ley de Telecomunicaciones y sus Reglamentos vigentes. Cualquier modificación futura a estas disposiciones legales será de aplicación inmediata en lo concerniente a los términos y condiciones.

I-LP-9624

ANEXO 3: CONTENIDO MÍNIMO DE LAS POLÍTICAS DE CERTIFICACIÓN DE LOS CERTIFICADOS DIGITALES PARA FIRMA DIGITAL REMOTA

POLÍTICAS DE CERTIFICACIÓN

I-LP-9624

ANEXO 4: CONTENIDO MÍNIMO DEL DOCUMENTO DE DECLARACIÓN DE PRÁCTICAS DE LOS CERTIFICADOS DIGITALES PARA FIRMA DIGITAL REMOTA

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN

1. Introducción.
    1.1. Identificación y nombre del documento
2. Definiciones y abreviaturas
    2.1. Abreviaturas
    2.2. Definiciones
3. Conceptos generales
    3.1. Custodia de Certificados Digitales para la Firma Digital Remota
    3.2. Alcance del servicio
    3.3. Comunidad de usuarios y ámbito de aplicación
        3.3.1. Suscriptores
        3.3.2. Terceros aceptantes
        3.3.3. Ámbito de aplicación
4. Política del servicio
5. Obligaciones y limitación de responsabilidades
6. Declaración de Prácticas del servicio
    6.1. Gestión de los módulos criptográficos HSM
    6.2. Gestión del ciclo de vida de los slots
    6.3. Del par de claves
        6.3.1. Generación y protección del par de claves
        6.3.2. Distribución de la clave pública
        6.3.3. Destrucción de la clave privada
    6.4. CSR y Certificados Digitales
        6.4.1. Creación del CSR
        6.4.2. Importar el Certificado Digital
    6.5. Uso de los Certificados Digitales almacenados
7. Suscripción al servicio
    7.1. Suscripción Pre Pago
    7.2. Suscripción Post Pago
8. Disponibilidad del servicio
9. Operación y gestión por parte de la ECA
    9.1. Gestión de la seguridad
    9.2. Control de riesgos e inventario de activos
    9.3. Seguridad del personal
    9.4. Seguridad física
    9.5. Gestión de las operaciones

I-LP-9624

ANEXO 5: CONTENIDO MÍNIMO DE LOS PLANES Y PROCEDIMIENTOS PARA RECUPERACIÓN ANTE DESASTRES DE LAS ENTIDADES CERTIFICADORAS AUTORIZADAS – ECA PARA LA CUSTODIA DE CERTIFICADOS DIGITALES PARA FIRMA DIGITAL REMOTA

PLANES Y PROCEDIMIENTOS PARA RECUPERACIÓN ANTE DESASTRES

Principios:

La Entidad Certificadora Autorizada debe mantener controles que permitan una seguridad razonable de continuidad de las operaciones en caso de un desastre. Estos controles incluyen, como mínimo:

a) El desarrollo y prueba de un plan de continuidad de negocio que incluye un proceso de recuperación de desastres para los componentes críticos del sistema;
b) el almacenamiento de materiales criptográficos necesarios (es decir, dispositivos de activación y de materiales criptográficos seguros) estén en una ubicación alternativa;
c) el almacenamiento de copias de seguridad de los sistemas, los datos y la información de configuración están en una ubicación alternativa, y
d) existe la disponibilidad de un sitio alternativo, equipamiento y conectividad para permitir la recuperación.

La Entidad Certificadora Autorizada mantiene controles para proporcionar una seguridad razonable de que las posibles interrupciones a los suscriptores y a las partes que confían se reduzcan al mínimo, como resultado de la interrupción o la degradación de los servicios.

Controles:

1. La Entidad Certificadora Autorizada, tiene una gestión de procesos para desarrollar y mantener sus planes de continuidad del negocio. La Entidad Certificadora Autorizada tiene una estrategia de planificación para la continuidad del negocio basado en una evaluación adecuada del riesgo.

2. La Entidad Certificadora Autorizada, tiene un plan de continuidad del negocio para mantener o restablecer las operaciones de manera oportuna después de la interrupción o el fracaso de los procesos críticos. El plan de continuidad del negocio se refiere a lo siguiente:
   a) Las condiciones para la activación de los planes;
   b) los procedimientos de emergencia;
   c) procedimientos alternativos;
   d) los procedimientos de reanudación;
   e) un programa de mantenimiento para el plan;
   f) los requisitos de educación y sensibilización;
   g) las responsabilidades de los individuos;
   h) el objetivo de tiempo de recuperación (RTO), y;
   i) las inspecciones periódicas de los planes de contingencia.

3. Los planes de continuidad del negocio incluyen los procesos de recuperación de desastres para todos los componentes críticos de un sistema, incluyendo el hardware, el software y las claves, en el caso de fallo de uno o más de estos componentes. En concreto:

I-LP-9624

a) Los dispositivos criptográficos utilizados para el almacenamiento de las claves privadas de los suscriptores se almacenan de forma segura en un lugar fuera del sitio para la recuperación en el caso de un desastre en instalaciones primarias, y;
b) las acciones clave secretas necesarias o componentes clave, necesarios para utilizar y gestionar los dispositivos criptográficos de recuperación de desastres, se almacenan de forma segura en una ubicación fuera del sitio.

4. Se toman regularmente copias de seguridad de la información empresarial esencial. Los requisitos de seguridad de estas copias son consistentes con los controles de la información respaldada.
5. La Entidad Certificadora Autorizada, identifica y organiza un sitio alternativo donde las operaciones básicas se pueden restaurar en caso de un desastre en el sitio principal. Los equipos de repliegue y los medios de copia de seguridad están situados a una distancia segura para evitar daños por desastre en el sitio principal.
6. Los planes de continuidad del negocio incluyen los procedimientos para asegurar su facilidad en la medida de lo posible durante el período de tiempo después de un desastre y antes de restaurar un entorno seguro ya sea en el original o en un sitio remoto.
7. Los planes de continuidad del negocio hacen frente a los procedimientos de recuperación aplicados si los recursos de computación, software o los datos están dañados o son sospechosos de estar dañados.
8. Los planes de continuidad del negocio son probados con regularidad para asegurarse de que están al día y son efectivos.
9. Los planes de continuidad de negocios definen un tiempo de interrupción del sistema aceptable, el tiempo de recuperación, y el tiempo medio entre fallos, como se describe en el CP o CPS.
10. Los planes de continuidad de negocios son mantenidos por las revisiones periódicas y las actualizaciones para asegurar su eficacia constante.
11. La Entidad Certificadora Autorizada mantiene procedimientos para la terminación, la notificación de los afectados, y para transferir los registros archivados correspondientes a un custodio, como se describe en el CP o CPS.

I-LP-9624

ANEXO 6: CONTENIDO MÍNIMO PARA LOS PLANES Y PROCEDIMIENTOS DE SEGURIDAD Y EVALUACIÓN DE RIESGOS DE LAS ENTIDADES CERTIFICADORAS AUTORIZADAS PARA LA CUSTODIA DE CERTIFICADOS DIGITALES PARA LA FIRMA DIGITAL REMOTA

CONSIDERACIONES DE SEGURIDAD DE LAS ENTIDADES CERTIFICADORAS AUTORIZADAS RELACIONADAS A LA CUSTODIA DE CERTIFICADOS DIGITALES PARA LA FIRMA DIGITAL REMOTA

Controles:

1. Un documento de política de seguridad de la información, que incluya los controles de seguridad física, el control de acceso del personal, los controles técnicos y de procedimiento, todo esto debe estar aprobado por las instancias correspondientes, debidamente publicada y comunicada a todos los empleados.
2. La política de seguridad de la información incluye lo siguiente:
   a) Una definición de la seguridad de la información, sus objetivos generales y ámbito de aplicación, la importancia de la seguridad como un mecanismo que permite el intercambio de información;
   b) Una declaración de intenciones de gestión, el apoyo a los objetivos y principios de la seguridad de la información;
   c) Una explicación de las políticas de seguridad, los principios, las normas y los requisitos a cumplir de particular importancia para la organización;
   d) Una definición de las responsabilidades generales y específicas para la gestión de seguridad de la información, incluidos los incidentes de seguridad de información, y
   e) Las referencias a la documentación, que apoya la política.
3. Un proceso de revisión definido para el mantenimiento de la política de seguridad de la información, incluyendo las responsabilidades y las fechas de revisión.

Infraestructura de la Seguridad de la Información

1. La alta dirección o un comité de seguridad de la información de gestión de alto nivel tienen la responsabilidad de asegurarse de que haya una clara dirección y gestión de apoyo para gestionar los riesgos de manera efectiva.
2. Un grupo de administración o un comité de seguridad debe existir para coordinar la aplicación de controles de seguridad de la información y la gestión del riesgo.
3. Las responsabilidades para la protección de los activos individuales, y para llevar a cabo procesos específicos de seguridad están claramente definidos.
4. Se tiene una administración de procesos de autorización para facilitar nuevos procesos de información y es seguido.

Seguridad de Acceso de Terceros

1. Existen procedimientos y se aplican para controlar el acceso físico y lógico a las instalaciones de los proveedores de servicios y los sistemas por parte de terceros.
2. Si existe necesidad del proveedor de servicios para permitir el acceso de terceros a las instalaciones y los sistemas de este, se realiza una evaluación de riesgos para determinar las implicaciones de seguridad y los requisitos de control específicos.
3. Los preparativos en cuanto al acceso de terceros a las instalaciones y los sistemas de los

I-LP-9624

proveedores de servicios se basan en un contrato formal que contenga los requisitos de seguridad necesarios.

Subcontratación

1. Si los proveedores de servicios externalizan la gestión y control de todos o algunos de sus sistemas de información, redes o entornos de escritorio, los requisitos de seguridad de los proveedores de servicios se abordan en un contrato acordado entre las partes.
2. Si los proveedores de servicios eligen delegar una parte de las funciones de estos a otra parte, los proveedores de servicios mantienen la responsabilidad en la realización de las funciones externalizadas y la definición y mantenimiento de un estado de la CPS.

I-LP-9624

ANEXO 7: CONTENIDO MÍNIMO PARA LA ADMINISTRACIÓN DE OPERACIONES DE LAS ENTIDADES CERTIFICADORAS AUTORIZADAS PARA LA CUSTODIA DE CERTIFICADOS DIGITALES PARA LA FIRMA DIGITAL REMOTA.

CONSIDERACIONES PARA LA ADMINISTRACIÓN DE OPERACIONES DE LAS ENTIDADES CERTIFICADORAS AUTORIZADAS PARA LA CUSTODIA DE CERTIFICADOS DIGITALES PARA LA FIRMA DIGITAL REMOTA

Principios:
El proveedor de servicios mantiene controles para proporcionar una seguridad razonable de que:

a) Se garantiza el funcionamiento correcto y seguro de las instalaciones de procesamiento de información del proveedor de servicios;
b) El riesgo de fallo de los sistemas del proveedor de servicios se reduce al mínimo;
c) La integridad de los sistemas del proveedor de servicios y la información está protegido contra virus y software malicioso;
d) El daño de los incidentes de seguridad y fallos de funcionamiento se reduce al mínimo mediante el uso de las notificaciones de incidentes y procedimientos de respuesta, y;
e) los medios están bien manejados para protegerlos de daños, robo y acceso no autorizado.

Controles:
Procedimientos operacionales y responsabilidades

1. Los procedimientos operativos del proveedor de servicios están documentados y mantenidos para cada área funcional.
2. La gestión formal de las responsabilidades y procedimientos existen para controlar los cambios de equipamiento del proveedor de servicios, de software y procedimientos operativos.
3. Los deberes y áreas de responsabilidad están segregadas en orden para reducir oportunidades no autorizadas de modificaciones o mal uso de la información y los servicios.
4. Los ambientes de pruebas de desarrollo y los ambientes operacionales están separadas.
5. Se prioriza el uso externo de los ambientes de gestión de servicios, riesgos y controles de confianza identificados, además del contratante, e incorporado en el contrato.

Planificación y Aceptación del Sistema

1. Las demandas de capacidad son monitoreadas y se realizan proyecciones de las necesidades futuras de capacidad, para asegurar que la capacidad de procesamiento y almacenamiento adecuados estén disponibles.
2. Los criterios de aceptación para los nuevos sistemas de información, actualizaciones y nuevas versiones se establecen y se realizan pruebas adecuadas del sistema antes de la aceptación.
3. Protección contra virus y software malicioso
4. Se implementan controles de detección y prevención para proteger los sistemas contra virus y software malicioso. Existen programas de sensibilización de los empleados.

Reporte de Incidentes y Respuesta

1. Existe un procedimiento formal de notificación de incidentes de seguridad que establece las acciones a tomar en la recepción de un informe de incidente. Esto incluye una definición y documentación de las responsabilidades asignadas y procedimientos de escalamiento. Las incidencias se reportan a la ECR como una cuestión de urgencia.
2. Los usuarios están obligados a observar y reportar las deficiencias observadas o sospechadas de

I-LP-9624

seguridad en los sistemas del proveedor de servicios, o amenazas a los sistemas o servicios a medida que se detecten.

3. Existen procedimientos y son seguidos para informar de fallos de hardware y software.
4. Existen procedimientos y se siguen para evaluar que la acción correctiva se toma para los incidentes reportados.
5. Existe un proceso formal de gestión de problemas que permite a los tipos, volúmenes y los impactos de incidentes y fallos de funcionamiento ser documentados, cuantificados y controlados.

Manejo del Papel y la Seguridad

1. Los procedimientos para la gestión de los medios informáticos extraíbles requieren lo siguiente:
   a) Si ya no es necesario, el contenido de cualquier medio reutilizable que se va a eliminar o remover de la organización, se borra o se destruye el medio informático;
   b) Se requiere autorización para todos los medios que hayan sido removidos de la organización y se mantiene un registro para mantener una pista de auditoría, y
   c) Todos los medios informáticos extraíbles, se guardan en un ambiente seguro, de acuerdo con las especificaciones de los fabricantes.
2. Los equipos que contienen medios de almacenamiento (por ejemplo, discos duros, fijos) se los revisa para determinar si contienen datos sensibles antes de su eliminación o reutilización. Los dispositivos de almacenamiento que contienen información sensible debe estar físicamente destruidos o sobrescritos de forma segura antes de su eliminación o reutilización.
3. Existen procedimientos para el manejo y almacenamiento de la información y se cumplen con el fin de proteger dicha información contra su divulgación o uso no autorizado.
4. La documentación del sistema está protegida del acceso no autorizado.

I-LP-9624

ANEXO 8: CONTENIDOS MÍNIMOS DE LOS PROCEDIMIENTOS Y LAS CONDICIONES QUE DEBERÁN CUMPLIR LAS ENTIDADES CERTIFICADORAS AUTORIZADAS PARA LA CONSERVACIÓN DE LOS DOCUMENTOS FÍSICOS Y DIGITALIZADOS.

PROCEDIMIENTOS Y CONDICIONES PARALA CONSERVACIÓN DE DOCUMENTOS DE LAS ENTIDADES CERTIFICADORAS AUTORIZADAS PARA LA CUSTODIA DE CERTIFICADOS DIGITALES PARA LA FIRMA DIGITAL REMOTA

1. **Para la conservación y mantenimiento de archivos físicos, digitales o mixtos mínimamente se establece:**
   a) Una vez terminado el proceso de registro de la solicitud (emisión, renovación, revocación o remisión) de los certificados, se debe almacenar la información generada y el almacenamiento de las claves y el certificado en forma segura.
   b) Si la información es física, se procederá a la foliación de la documentación generada durante el proceso
   c) Si la información es digital, se almacena con identificadores que permitan acceder fácilmente a la información.
   d) Si la documentación es entregada en formato físico después de foliada, deberá ser escaneada, con el fin de contar con un archivo digital ordenado por número de certificado en carpetas distribuidas por años.
   e) El archivo físico debe ser mantenido ordenado en carpetas que deben contar con rótulos impresos en el lomo donde se especifique el número y tipo de certificado
   f) Se mantendrá un archivo físico, ordenados en medios de almacenamiento de la información rotulados con escritura clara a computadora en la que especificará el número y tipo de certificado
   g) Después de terminada cada auditoría externa realizada por la ATT, se procederá a empastar la documentación física.
   h) La documentación debe estar archivada hasta 5 años después de la revocación del certificado o el cambio de claves del signatario.
   i) En caso de contar con un archivo digital se debe respaldar la información por gestión al cierre de cada una, esta copia se debe encontrar disponible para las auditorías de la ATT.

2. **Para la conservación y mantenimiento de archivos físicos, digitales o mixtos se establecen las siguientes directrices:**
   a) Toda la documentación generada en los registros de signatarios deberá conservarse de manera ordenada y cronológica, separando mes, año y tipo de documento.
   b) La documentación digital y los archivos digitales deben conservarse de manera ordenada y cronológica, separando mes, año y tipo de documento.
3. **Destrucción de los documentos**
   a) La Política de Certificación especifica el medio a través del cual se realiza la destrucción de claves y del certificado del signatario.
   b) La CP o CPS especifican los requisitos para la destrucción de todas las copias y fragmentos de las claves públicas y privadas y el certificado del signatario al final del ciclo de vida del par de claves.
   c) La CP especifica los requisitos para el uso y manejo de hardware criptográfico y los procesos de autenticación de abonado (y las acciones posteriores) en el que el hardware criptográfico está en otras ubicaciones físicas (es decir, un HSM conectado a un ordenador central o servidor remoto).
   d) La destrucción de la documentación física, digital o mixta de la Entidad Certificadora Autorizada debe ser coordinada por la ATT.

I-LP-9624