AC TECNISIGN

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN

OID: 1.3.6.1.4.1.47402.3.7
Versión 1.0
13 de septiembre del 2018

Historial de actualización:

Versión	*Fecha de elaboración*	*Autor*	*Ítem modificado*	*Descripción de la modificación*
v1.0	13/09/2018	Normas y Cumplimiento	No se aplica	Elaboración de AC TECNISIGN

Actualizar controle de versiones

APROBADO POR:

MARCIO NUNES DA SILVA:05174237825

Assinado de forma digital por MARCIO NUNES DA SILVA:05174237825
Dados: 2019.03.16 19:31:10 -03'00'

Índice

1. INTRODUCCIÓN

Este documento es la declaración de prácticas de certificación de AC TECNISIGN (DPC de AC TECNISIGN). Este establece las prácticas que las autoridades de Certificación de VALID («AC») emplean en la prestación de servicios de Certificación que incluyen, pero no se limitan a la emisión, gestión, revocación y renovación de certificados de acuerdo con los requisitos específicos de las Políticas de Certificado de AC TECNISIGN («PC»).

Este documento se destina a:

- Prestadores de servicios de PKI y de Infraestructura Oficial de la Firma Electrónica de AC TECNISIGN que deben operar en términos de sus propias Políticas de Certificado (PC) que cumplan los requisitos establecidos por la DPC.
- Los suscriptores de certificados de AC TECNISIGN que deben entender cómo estos se autentican y cuáles son sus obligaciones como suscriptores de AC TECNISIGN y cómo son protegidos por AC TECNISIGN.
- Partes de confianza que deben entender cuán confiable es un certificado de AC TECNISIGN, o una firma digital que utilice este certificado.

Esta DPC, está en conformidad con el RFC 3647 de la Internet Engineering Task Force (IETF) para la elaboración de la Declaración de Prácticas de Certificación y Política de Certificación.

La DPC de AC TECNISIGN está en conformidad con la versión actual del:
a) CA/Browser Forum - Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates- versión 1.6.2 (disponible en https://cabforum.org/baseline-requirements-documents/).
b) CA/Browser Forum - Guidelines For The Issuance And Management Of Extended Validation Certificates – versión 1.6.8 (disponible en https://cabforum.org/extended-validation/); y
c) CA/Browser Forum - Guidelines For The Issuance And Management Of Extended Validation Code Signing Certificates – versión 1.4 (disponible en https://cabforum.org/ev-code-signing-certificate-guidelines/)

En caso de divergencias entre este documento y estas directrices, prevalece el presente documento.

1.1 Visión general

Esta DPC se aplica a AC TECNISIGN.

Las AC subordinadas de AC TECNISIGN operan sus AC según la DPC y PC de AC TECNISIGN, emitiendo certificados de usuario final.

Autoridades de Registros (AR) son entidades que autentican solicitaciones de certificados de AC TECNISIGN.

AC TECNISIGN y afiliados pueden actuar como AR para los certificados que emiten. VALID y afiliados también celebran relaciones contractuales con empresas que desean administrar sus propias solicitaciones de certificados. Estos clientes corporativos actúan como AR, autenticando pedidos de certificados para sí y para sus indicados. VALID o Afiliados emitirán estas solicitaciones de certificado autenticados.

Dependiendo del tipo de certificado, los Certificados Digitales pueden ser utilizados por los suscriptores para proteger sitios, firmar digitalmente códigos u otros contenidos, firmar digitalmente documentos o e-mails. La persona que en última instancia recibe un documento o comunicación firmada, o accede a un sitio protegido es designada como Parte de Confianza, es decir, que confía en el certificado.

Una parte de confianza debe confiar en un certificado en los términos del contrato de Parte de Confianza enlistada en el sitio de AC TECNISIGN.

1.2 Nombre del documento e identificación

Este documento es la Declaración de Prácticas de Certificación (DPC) de AC TECNISIGN.

1.2.1 CABF identificador de la política

No se aplica.

1.3 Comunidad (participantes en la PKI)

Los servicios de certificado de firma electrónica de AC TECNISIGN están incorporados en una infraestructura de confianza. Básicamente: Autoridad de certificación (AC), Autoridades de Registro (AR), suscriptor, terceros que dependen de certificados y Entidad de Certificación.

1.3.1 Autoridad de certificación

Una Autoridad de certificación (AC) es la organización responsable de la generación, emisión, revocación y gestión de certificados.

Este término se aplica igualmente a las AC Raíces y AC Subordinadas.

Las prácticas y Procedimientos de Certificación empleados por AC TECNISIGN se describen en su Declaración de Prácticas de Certificación (DPC de AC TECNISIGN), la cual se encuentra publicada en la siguiente dirección:

http://ac.tecnisign.net/ac-tecnisign/cps-ac-tecnisignv1.pdf .

1.3.2 Autoridades de registro

Una Autoridad de Registro (AR) es una entidad que realiza la identificación y autenticación de solicitantes de certificado para usuarios finales, inicia o transfiere solicitaciones de revocación de certificados de usuarios finales y aprueba solicitaciones de renovación en nombre de AC TECNISIGN. En el caso de que un tercero actúe como agente de registro, la actividad debe realizarse en total conformidad con el contrato de mandato y con esta Declaración de Prácticas de Certificación. VALID puede actuar como una AR para emisión de certificados.

Las Terceras Partes que establezcan una relación contractual con VALID, podrán operar su propia AR y autorizar la emisión de certificados por AC TECNISIGN. Las AR de terceros deben obedecer todos los requisitos de esta DPC de AC TECNISIGN, y los términos y condiciones de su contrato de servicios corporativos con AC TECNISIGN. Las AR pueden, sin embargo, implementar prácticas más restrictivas con base en sus requisitos internos.

Antes de que AC TECNISIGN autorice a una Tercera Parte a desempeñar una función de AR, TECNISIGN deberá exigir contractualmente que la Tercera Parte:

(1) Cumpla los requisitos de cualificación de la Sección 5.3.1, cuando se aplique a la función de AR;

(2) Guarde la documentación de acuerdo con la Sección 5.5.2;

(3) Cumplir las otras disposiciones de estos Requisitos que se apliquen a la función; y

(4) Cumpla las políticas (DPC y PC) de AC TECNISIGN.

VALID puede designar a una empresa como AR para verificar solicitaciones de certificados de esta propia organización.

1.3.3 Candidato

Las personas que aceptan solicitar un certificado digital, completan el formulario de solicitación y suministran todo el historial exigido por ley y esta DPC para comprobar su identidad de forma confiable.

1.3.4 Suscriptores

Los suscriptores (o suscriptores o titulares) incluyen a todos los usuarios finales (incluidas entidades) de certificados emitidos por AC TECNISIGN. Un suscriptor es la entidad nombrada como usuario final de un certificado. Los suscriptores PUEDEN ser individuos, organizaciones o componentes de infraestructura, como firewalls, enrutadores, servidores de confianza u otros dispositivos usados para proteger comunicaciones dentro de una organización.

En algunos casos, los certificados se emiten directamente a individuos o entidades para uso propio. Sin embargo, en general hay otras situaciones en que la parte que requiere un certificado es distinta del «solicitante» a quien se aplica el certificado. Por ejemplo, una organización puede demandar certificados para sus empleados para permitir que estos representen a la organización en transacciones/negocios electrónicos. En tales situaciones, la entidad que suscribe la emisión de

certificados (es decir, pagada por ellos, ya sea mediante la suscripción de un servicio específico, ya sea como el propio emisor) es diferente de la entidad que es el «solicitante» del certificado (en general, el titular del certificado).

En esta Política de Certificado (PC) de AC TECNISIGN se utilizan dos términos distintos para distinguir entre estos dos roles: «Suscriptor» es la entidad que contrata a VALID para la emisión de credenciales y; «ASUNTO» (Solicitante) es la persona a quien la credencial está vinculada. El Suscriptor asume la responsabilidad final por el uso del certificado, pero el ASUNTO es el individuo que está autenticado cuando el certificado se presenta.

Cuando se utiliza «ASUNTO», es para indicar una distinción del Suscriptor. Cuando se utiliza «Suscriptor», puede referirse solo al Suscriptor como una entidad distinta, pero también se puede utilizar este término para abarcar a los dos. El contexto de uso en la PC invocará el entendimiento correcto.

Las AC técnicamente también son suscriptores de certificados dentro de AC TECNISIGN, ya sea como una AC que emite un certificado autofirmado para sí, ya sea como una AC que emite un Certificado por una AC superior. Las referencias a «entidades finales» y «suscriptores» en la Política de Certificado (PC) de AC TECNISIGN, sin embargo, solo se aplican a usuarios finales.

1.3.5 Partes de Confianza

La Parte de Confianza es una persona física o jurídica que confía de un certificado o firma digital emitida por AC TECNISIGN. La Tercera Parte de Confianza puede o no ser un suscriptor dentro de AC TECNISIGN.

La parte que confía debe ter mecanismos que permitan validar si se trata de un certificado auténtico y si este certificado era válido en el momento en que se produjo la firma del documento.

1.3.6 Entidad de Certificación

La Dirección General de la Propiedad Intelectual (DIGEPIH) que está ubicada en el Instituto de la Propiedad (IP). La Ley de Firma Electrónica aprobada por el Congreso Nacional bajo el decreto número 149-2013 de 30 de julio del 2013.

1.3.7 Prestador de Servicio de Soporte

AC TECNISIGN utiliza los siguientes Prestadores de Servicio de Soporte (PSS) en sus operaciones:

a) VALID CERTIFICADORA DIGITAL LTDA.

b) VALID SOLUÇÕES S.A.

Las PSS son entidades utilizadas por AC TECNISIGN o sus AR vinculadas para desempeñar actividad descrita en esta PC y DPC implementada por AC TECNISIGN se clasifican en tres categorías según el tipo de actividad prestada:

a) facilitación de infraestructura física y lógica;

b) facilitación de recursos humanos especializados; o
c) facilitación de infraestructura física y lógica y de recursos humanos especializados.

1.3.8 Otros participantes

No se aplica.

1.4 Titulares de Certificado

Personas físicas o jurídicas, de derecho público o privado, nacionales o extranjeras, que cumplan los requisitos de esta DPC y de las Políticas de Certificado aplicables, pueden ser Titulares de Certificado. Los certificados pueden ser utilizados por personas físicas, personas jurídicas, en equipos o aplicaciones.

Si el titular del certificado es persona jurídica, será designada persona física como responsable del certificado, que será el titular de la clave privada.

OBLIGATORIAMENTE se designará como responsable del certificado, el representante legal de la persona jurídica o uno de sus representantes legales.

1.4.1 Aplicabilidad

Esta sección enlista las aplicaciones de cada tipo de Certificación en los servicios de Certificación, estableciendo limitaciones y prohibiciones de algunas aplicaciones de certificados.

1.4.1.1 Usos apropiados del certificado

Las Políticas de Certificación correspondientes a cada tipo de servicio de Certificación específica suministrada por AC VALID constituyen los documentos en que determinan los usos y limitaciones de cada certificado empleado, aunque esta sección describe, debido a su relevancia especial, el uso principal de Certificados de AC TECNISIGN.

El principal objetivo de los certificados emitidos por AC TECNISIGN es permitir que el SUSCRIPTOR, firme los documentos. Este certificado permite reemplazar la firma manuscrita por la digital en las relaciones del suscriptor con terceros, del mismo modo se utilizará para ofrecer seguridad en determinadas aplicaciones de almacenamiento certificado.

El uso de dichos certificados ofrece las siguientes Garantías:

- No repudio.

Asegura que el documento proviene del signatario de la persona que lo emite. Este recurso se obtiene por medio de la firma digital realizada por el **Certificado de firma**. El receptor de un mensaje firmado digitalmente será capaz de verificar el certificado o el empleado para dicha firma por medio del servicio de validación de AC TECNISIGN. Esto garantiza que el documento proviene de un signatario específico.

- Integridad

Al utilizar el **Certificado de firma,** es posible verificar si el documento no ha sido modificado por cualquier agente ajeno a la comunicación. Para garantizar la integridad, el cifrado ofrece soluciones basadas en recursos especiales, llamadas funciones de resumen (hash), que se utilizan siempre que se ejecuta una firma digital. El uso de dicho sistema permite verificar si un mensaje firmado no ha sido modificado entre el envío y el recibo.

1.4.1.2 Certificados emitidos para personas físicas

Los certificados emitidos a personas físicas en general se utilizan para firmar y cifrar e-mails y para autenticar aplicaciones (autenticación de cliente).

1.4.1.3 Certificados emitidos para organizaciones

Los certificados de persona jurídica se emiten a las organizaciones tras la autenticación de que la organización existe legalmente y que otros atributos de la organización incluidos en el certificado (excluida la información de suscriptores no verificada) se autentican, y la propiedad de un dominio de internet o e-mail.

1.5 Administración de políticas

1.5.1 Organización que administra este documento

VALID CERTIFICADORA DIGITAL LTDA.
Avenida Paulista, 2064 – 15. Andar
São Paulo/SP - Brasil

1.5.2 Datos de contacto

Normas y Cumplimiento
VALID CERTIFICADORA DIGITAL LTDA.
Avenida Paulista, 2064 – 15. Andar
São Paulo/SP - Brasil
Teléfono: +55 (11) 2575-6800
E-mail: pki.compliance@valid.com

1.5.3 Persona que determina la adecuación de la DPC como política

El Departamento de Gestión de Políticas (Policy Management Department, PMD) de AC TECNISIGN, nombrado como «Normas y Cumplimiento» determina la adecuación y aplicabilidad de esta DPC.

1.5.4 Procedimiento de aprobación de la DPC

La aprobación de esta DPC y las modificaciones siguientes serán realizadas por el Departamento de Gestión de Políticas (PMD). Las modificaciones DEBEN figurar en forma de un documento que contenga una forma modificada de la DPC o un historial de actualización.

Las versiones modificadas estarán disponibles en: http://ac.tecnisign.net/ac-tecnisign .

Las actualizaciones reemplazan cualesquiera disposiciones designadas o conflictivas de esta versión para DPC.

1.6 Definiciones y acrónimos

1.6.1 Definiciones

Véase la tabla de definiciones del apéndice A.

1.6.2 Acrónimos

Véase la tabla de acrónimos del apéndice A.

1.6.3. Referencias

Véase la lista de referencias del apéndice B.

1.6.4. Convenciones

Las palabras clave «DEBE», «NO DEBE», «OBLIGATORIO», «DEBEN», «NO», «DEBEN», «NO DEBEN», «RECOMENDADOS», «PUEDE», y «OPCIONALES» en estos requisitos deben interpretarse de acuerdo con el RFC 2119.

2. Responsabilidades de publicación y repositorio

2.1 Repositorio

AC TECNISIGN es responsable de mantener un repositorio on-line de acceso público, así como información de revocación sobre los Certificados emitidos. El repositorio de AC TECNISIGN está disponible para consulta en: http://ac.tecnisign.net/ac-tecnisign.

2.2 Publicación de la información del certificado

AC TECNISIGN y afiliadas mantienen un repositorio basado en la web que permite que las Terceras Partes efectúen consultas on-line sobre revocación y otra información de estado del Certificado. Cualquier excepción a esto DEBERÁ ser aprobada por el PMD caso a caso y DEBE documentarse en la DPC apropiada. VALID y las afiliadas facilitan a las Partes de confianza información sobre cómo encontrar el repositorio apropiado para verificar el estado del Certificado y, si el OCSP (Protocolo de Estado del Certificado On-line) está disponible, cómo encontrar el respondedor OCSP.

AC TECNISIGN publica los certificados que emite en nombre de sus propias AC y de las AC subordinadas. Tras la revocación del Certificado de un usuario final, VALID publica aviso de tal revocación en el repositorio. Además de eso, VALID emite Listas de Revocación de Certificados (LCR) y, si está disponible, ofrece servicios OCSP (Protocolo de Estado de Certificados On-line) para sus propias AC y AC subordinadas.

VALID publicará una versión actual de los siguientes documentos en sus repositorios:

- Esta DPC de AC TECNISIGN;
- Las PC de AC TECNISIGN;
- Lista de Certificados Revocados (LCR);
- Certificado de AC TECNISIGN;
- Certificación de Titularidad; y
- Contratos de Parte de Confianza.

VALID garantiza que su repositorio esté accesible on-line 24 horas al día, 7 días a la semana (24x7), y que su DPC o PC divulguen las prácticas comerciales de AC TECNISIGN, conforme a lo exigido por el «WebTrust for CAs» y ETSI TS 102 042 y ETSI EN 319 411-1.

2.3 Tiempo o información de la publicación

AC TECNISIGN desarrolla, implementa, aplica y, como mínimo, actualiza anualmente sus políticas (DPC y PC).

Las Actualizaciones de los Contratos de Suscriptores y Contratos de Terceros de Confianza se publican según sea necesario. Los certificados se publican tras su emisión. La información del estado del certificado se publica de acuerdo con lo que determina esta DPC.

2.4 Controles de acceso en repositorios

VALID y afiliados no utilizan intencionalmente medios técnicos para limitar el acceso a sus políticas, información de estado o LCR. AC TECNISIGN y afiliados, sin embargo, pueden exigir que las personas acepten un Contrato de Tercera Parte como condición para acceder a OCSP o LCR. AC TECNISIGN y afiliados deben implementar controles para impedir que personas no autorizadas añadan, excluyan o modifiquen las entradas del repositorio.

3. Identificación y autenticación

La autenticación de la identidad se realiza en la presencia física del solicitante en la Autoridad de Registro (AR). La identificación de solicitantes y titulares de certificados se realiza de acuerdo con las reglas y Procedimientos mencionados en esta sección de la DPC.

3.1 Registros de nombres

Esta sección establece requisitos relacionados con los Procedimientos de identificación y autenticación utilizados durante el registro de suscriptores, que deben efectuarse antes de la emisión y entrega de los certificados.

3.1.2 TIPOS DE NOMBRES

El campo Subject DN (Distinguished Name) contiene toda la información de identificación de la entidad para la cual se emite el certificado, ya sea una entidad legal, persona física o de cualquier otro tipo. Esta información debe identificar de forma exclusiva un certificado emitido por la misma AC para certificados cualificados, es decir: no debe haber dos certificados emitidos por la misma AC cuyo ASUNTO sea idéntico.

3.1.3 SIGNIFICADO DE LOS NOMBRES

Las reglas definidas en la sección anterior garantizan que el Distinguished Name (DN) de los certificados sea suficientemente significativo para vincular la clave pública a una identidad.

3.1.4. Reglas para interpretación de varios tipos de nombre

AC TECNISGN atiende en todos los casos a lo que indica la referencia al estándar X.500 en la ISO/IEC 9594.

3.1.5 Unicidad de nombres

El DN de los certificados debe ser exclusivo. El uso de todos los campos «SUBJECT» garantiza la exclusividad del DN.

3.1.6 Resolución de conflictos relacionados con nombres

AC TECNISIGN no actúa como árbitro o mediador, ni resuelve cualquier disputa respecto a la propiedad de los nombres de personas u organizaciones, nombres de dominio, marcas comerciales o nombres comerciales, etc. De igual manera, este organismo se reserva el derecho de rechazar un pedido de certificado debido a un conflicto de nombre.

3.2 Validación inicial de la identidad

3.2.1. Método para comprobar la posesión de la clave privada

VALID, como proveedor de servicios de AC TECNISIGN, utiliza varios circuitos para emitir certificados en que la clave privada es administrada de manera diferente. La clave privada puede ser generada por el usuario y por la Autoridad de Certificación (AC).

El método para probar la posesión de una clave privada DEBE ser PKCS#10, otra demostración criptográficamente equivalente, u otro método aprobado por VALID. Este requisito no se aplica cuando un par de claves es generado por una AC en nombre de un Suscriptor.

a) Generación de claves por la EC.

i. En Software: Estos se entregan al Suscriptor manualmente o por e-mail por medio de archivos protegidos usando el Estándar PKCS#12. La seguridad del proceso se garantiza porque el código de acceso al archivo PKCS#12, que permite la Instalación de este en las aplicaciones, se entrega por otros medios que no aquel utilizado en la recepción del archivo (e-mail, teléfono).

ii. En Hardware: Las claves son generadas por el Suscriptor y pueden ser entregadas por la EC al Suscriptor, directamente o mediante una entidad de registro en un dispositivo de generación de firma cualificado.

b) Generación de las claves por el Suscriptor.

El Suscriptor cuenta con un mecanismo de generación de claves, ya sea software o hardware. La prueba de la posesión de la clave privada en estos casos es la solicitación recibida por la EC en el formato PKCS # 10

Las Autoridades de Registro (AR) vinculadas a AC TECNISIGN, utilizarán los siguientes requisitos y Procedimientos para la realización de los Procedimientos siguientes:

a) confirmación de la identidad de un individuo: comprobación de que la persona que se presenta como titular del certificado de persona física es realmente aquella cuyos datos constan en la documentación/biometría presentada, si se aplica (recomendable), se prohíbe cualquier tipo de poder para tal fin;

En el caso de persona jurídica, comprobar que la persona física que se presenta como su representante es realmente aquella cuyos datos constan en la documentación presentada, admitida el poder solo si el acto constitutivo prevé expresamente tal posibilidad, para ello, debe estar revestido de la forma pública y con plazo de validez de hasta 90 (noventa) días. El responsable del uso del certificado digital de persona jurídica debe comparecer presencialmente, queda prohibido cualquier tipo de poder para tal fin;

b) confirmación de la identidad de una organización: comprobación de que los documentos presentados se refieren efectivamente a la persona jurídica titular del certificado y de que la persona que se presenta como representante legal de la persona jurídica realmente tiene tal atribución; y

c) emisión del certificado: cotejo de los datos de la solicitación de certificado con los datos que constan en los documentos presentados y liberación de la emisión del certificado en el sistema de AC TECNISIGN.

3.3. Autenticación de la identidad de un individuo

La confirmación de la identidad de un individuo se realiza mediante la presencia física del interesado, con base en documentos personales de identificación legalmente aceptados y por el proceso de identificación biométrica (recomendable).

3.3.1. Documentos para efectos de identificación de un individuo

La identificación y confirmación de la identidad de un individuo se realiza mediante la presencia física del interesado, con base en documentos personales de identificación legalmente aceptados.

Deberá presentarse la siguiente documentación, en su versión original, para fines de identificación de individuo solicitante de certificado:

a) documento nacional de identidad;
b) Pasaporte; y
c) fotografía del rostro del solicitante (recomendable);
d) impresiones digitales del solicitante de un certificado (recomendable).
e) comprobante de residencia o domicilio, emitido como máximo 3 (tres) meses antes de la fecha de la validación presencial (recomendable);
f) Otros documentos admitidos por ley.

Nota 1: Extranjeros pueden presentar el pasaporte o documento de identidad válido.

Nota 2: La emisión de certificados en nombre de los absolutamente incapaces y de los relativamente incapaces observará lo que determina la ley vigente.

3.3.2. Información contenida en el certificado emitido para un individuo

Es Obligatorio el llenado de los siguientes campos del certificado de una persona física con la información que consta en los documentos presentados:

a) nombre completo, sin abreviaciones;

b) número de identificación del documento de identificación;

c) dirección de domicilio.

3.4 Autenticación de la identidad de una organización

Se designará a una persona física como responsable del certificado, la cual será la titular de la clave privada. Preferiblemente, se designará como responsable del certificado el representante legal de la persona jurídica o uno de sus representantes legales.

La confirmación de la identidad de la organización y de las personas físicas se efectúa en los siguientes términos:

a) presencia física del responsable del uso del certificado y firma de la certificación de titularidad del certificado

b) presencia física del (de los) representante(s) legal(es) de la persona jurídica y firma de la certificación de titularidad del certificado.

3.4.1. Documentos para efectos de identificación de una organización

La confirmación de la identidad confirmación de la identidad de una organización se efectúa mediante la presentación de, como mínimo, los siguientes documentos:

a) Acto constitutivo, debidamente registrado en el organismo competente;

b) Documentos de la elección de sus administradores, cuando se aplique; y

c) prueba de inscripción del Registro Tributario Nacional (RTN).

3.4.2 Información contenida en el certificado emitido a una organización

Es Obligatorio el llenado de los siguientes campos del certificado de una organización, con la información que consta en los documentos presentados:

a) Nombre empresarial registrado en el Registro Tributario Nacional (RTN), sin abreviaciones;

b) Número de identificación de la empresa registrado en el RTN;

c) Nombre completo del responsable del certificado, sin abreviaciones; y

d) dirección de la empresa.

3.5 Identificación y autenticación para solicitar una nueva clave

Antes de la expiración del Certificado de Suscriptor existente, es necesario que el suscriptor obtenga un nuevo certificado para seguir utilizando el certificado. AC TECNISIGN no permite la renovación sin la presencia física del solicitante.

3.5.1. Identificación y autenticación para renovación

Los Procedimientos de renovación garantizan que la persona u organización que desea renovar un Certificado de Suscriptor del usuario final sea, de hecho, el suscriptor del certificado anterior. AC TECNISIGN no permite la renovación sin la presencia física del solicitante.

3.5.1.2. Identificación y autenticación para renovación tras la revocación

No se permite la recertificación/renovación tras la revocación.

4. Requisitos operativos del ciclo de vida del certificado

4.1. Solicitación de certificado

4.1.1 Quiénes pueden enviar una solicitación de certificado

A continuación se enlistan las personas que pueden enviar pedidos de certificado:

- Cualquier persona que sea el sujeto del certificado;
- Cualquier representante autorizado de una Organización o entidad; y
- Cualquier representante autorizado de una CA.

4.2 Proceso de solicitud de certificado

En este ítem de la DPC se describen los requisitos y Procedimientos Operativos establecidos por AC TECNISIGN y por las AR vinculadas para las solicitaciones de emisión de certificado. La AR deberá realizar la identificación y autenticación de toda la información de los solicitantes del certificado digital. Estos requisitos y Procedimientos comprenden:

a) la comprobación de atributos de identificación que constan en el certificado, conforme al ítem 3.1;

b) la autenticación, del agente de registro responsable de las solicitaciones de emisión y de revocación de certificados; y

c) la firma, en la certificación de titularidad del certificado por el titular del certificado y por el responsable del uso del certificado, en el caso de persona jurídica.

4.2.1 Tiempo de procesamiento de solicitaciones de certificado

Las AC y AR ejecutan el proceso en un plazo razonable a partir del recibo. No hay un tiempo estipulado para completar la tramitación de una solicitud.

Un pedido de certificado permanece activo hasta ser rechazado.

4.3 Emisión de certificado

Solo acepta los certificados digitales cuando la identidad del solicitante se verifica de manera confiable como se indica en la presente Declaración de Prácticas de Certificación. Tras los Procedimientos abordados en el ítem 4.2, AC TECNISIGN realiza la emisión del certificado en su sistema y notifica al titular por e-mail indicando el método de retirada del certificado.

4.4 Aceptación de certificado

El titular del certificado o persona física responsable verifica la información contenida en el certificado y lo acepta si dicha información es íntegra, correcta y verdadera. De lo contrario, el titular del certificado no puede utilizar el certificado y debe solicitar de inmediato su revocación. Al aceptar el certificado, el titular del certificado:

- está de acuerdo con las responsabilidades, obligaciones y deberes mencionados en esta DPC y en la PC correspondiente;
- garantiza que, bajo su conocimiento, ninguna persona sin autorización ha tenido acceso a la clave privada asociada al certificado;
- afirma que toda la información contenida en el certificado, facilitada en la solicitación, es verdadera y se reproduce en el certificado de forma correcta y completa.

La aceptación de todo certificado emitido es declarada implícitamente por el titular en el primer uso del certificado.

4.5 Par de claves y uso del certificado

Para usar la Clave Privada correspondiente a la clave pública en el certificado el suscriptor DEBERÁ aceptar la Certificación de Titularidad y aceptar el certificado. El certificado DEBERÁ usarse legalmente de acuerdo con el Certificación de Titularidad y los términos y condiciones de esta DPC. El uso del certificado DEBE ser consistente con las extensiones del campo KeyUsage incluidas en el certificado.

Los suscriptores DEBERÁN proteger sus claves privadas contra el uso no autorizado y dejarán de usar la clave privada tras la expiración o revocación del certificado. Las partes que no sean del suscriptor NO DEBEN archivar la Clave Privada del suscriptor, salvo a lo que se establece en la Sección 4.12.

4.5.1 Uso de la clave pública y del certificado de la parte de confianza

Las partes de confianza DEBEN aceptar los términos y condiciones del Contrato de Partes de Confianza aplicable como condición para confiar en el certificado.

La confianza en un certificado DEBE ser razonable bajo las circunstancias presentes. Si las circunstancias indican necesidad de Garantías adicionales, la Tercera Parte DEBE obtener tales Garantías para que la confianza se considere razonable.

Antes de cualquier acto de confianza, las Partes de confianza deberán evaluar independientemente:

- la adecuación del uso del Certificado para cada finalidad y determinar si el Certificado se utilizará, de hecho, para el propósito apropiado, que no sea prohibido o limitado por la PC. AC TECNISIGN, AC y AR no son responsables de evaluar la adecuación del uso de un Certificado.
- que el certificado se utiliza de acuerdo con la extensión KeyUsage incluida en el certificado.
- estado del certificado de todas las AC de la cadena de emisión del certificado. Si cualquiera de los Certificados de la Cadena de Certificación ha sido revocado, la Tercera Parte es la única responsable de investigar si la firma digital ha sido realizada por un Certificado de usuario final antes de la revocación de cualquier certificado de la Cadena de Certificación. Cualquier asunción es de riesgo exclusivo de la parte de confianza.

Al asumir que el uso del Certificado es apropiado, las Partes de confianza deberán utilizar el software o hardware apropiado para ejecutar la verificación de firma digital u otras operaciones criptográficas que deseen realizar, con la condición de confiar en los Certificados implicados en cada operación. Tales operaciones incluyen la identificación de la Cadena de Certificación y la verificación de firmas digitales en todos los certificados en la cadena de certificados.

4.6 Recertificación del certificado

La recertificación de certificado es la emisión de un nuevo certificado para el suscriptor sin modificar la clave pública o cualquier otra información en el certificado.

AC TECNISIGN no permite la recertificación de certificados.

4.7 Renovación del certificado

La renovación de certificado es la emisión de un nuevo certificado que utiliza una nueva clave pública. AC TECNISIGN solicita al Candidato que envíe una nueva solicitación de certificado para emitir un nuevo certificado.

4.7.1 Circunstancias para la renovación de certificado

Antes de la expiración del Certificado de Suscriptor existente, es necesario que el Suscriptor renueve el certificado para seguir utilizando el Certificado. También se puede renovar un certificado tras su expiración.

4.8 Modificación del certificado

4.8.1 Circunstancias para la modificación del certificado

La modificación de certificado se refiere al pedido de emisión de un nuevo certificado debido a modificaciones en la información (que no sea la clave pública del suscriptor) en un certificado existente.

La modificación de cualquier información del certificado se considera una nueva emisión de certificado en los términos de la Sección 4.1.

4.9 Suspensión y revocación de certificados

4.9.1 Circunstancias para la revocación

4.9.1.1. Razones para revocar un certificado de suscriptor

Solo bajo las circunstancias enlistadas a continuación el certificado de suscriptor será revocado por AC TECNISIGN (en nombre del Suscriptor) y publicado en una LCR.

Un certificado de usuario final será revocado si:

1. El Suscriptor solicita por escrito que AC TECNISIGN revoque el Certificado;
2. El Suscriptor notifica a AC TECNISIGN que el pedido de certificado original no fue autorizado por él, y que este no concedió autorización retroactiva;

3. AC TECNISIGN, una AR, el Cliente o el Suscriptor obtiene pruebas de que la Clave Privada del Suscriptor correspondiente a la Clave Pública del Certificado fue comprometida o ya no cumple los requisitos de las Secciones 6.1.5 y 6.1.6;
4. AC TECNISIGN, una AR, el Cliente o el Suscriptor obtienen evidencia de que el Certificado fue mal utilizado;
5. AC TECNISIGN, una AR o el Cliente es informado de que un Suscriptor ha violado una o más de sus obligaciones materiales mencionadas en el Contrato de Suscriptor o en los Términos y Condiciones de Uso;
6. AC TECNISIGN, una AR o el Cliente es informado de una modificación material en la información contenida en el Certificado;
7. AC TECNISIGN, una AR o el Cliente es informado de que el Certificado no fue emitido de acuerdo con los requisitos de esta DPC o las PC AC TECNISIGN;
8. AC TECNISIGN determina que cualquier información que figure en el Certificado es imprecisa o engañosa;
9. AC TECNISIGN suspende las operaciones por cualquier motivo y no realiza acuerdos para que otra AC ofrezca el soporte de revocación para el Certificado;
10. El derecho de AC TECNISIGN de emitir Certificados bajo estos Requisitos ha expirado o ha sido revocado o rescindido, a menos que AC TECNISIGN haya realizado acuerdos para seguir manteniendo el Repositorio LCR/OCSP;
11. AC TECNISIGN es informada de un posible compromiso de la Clave Privada de la AC Subordinada usada para emitir el Certificado;
12. La revocación es exigida por la DPC/PC de AC TECNISIGN;
13. El contenido técnico o el formato del Certificado presenta un riesgo inaceptable para los Proveedores de Software de aplicativos o Partes de Confianza;
14. Se terminó el Contrato de Suscriptor con el Suscriptor;
15. La afiliación entre un Cliente Corporativo con un Suscriptor fue rescindida o terminó de otra forma;
16. El Suscriptor no envió el pago cuando era debido;
17. La identidad del Suscriptor no se verificó con éxito de acuerdo con la Sección 3.3.2; o
18. El uso de tal certificado representa riesgos a AC TECNISIGN;
19. Por muerte del suscriptor;
20. Por orden judicial o de Autoridad administrativa competente; y
21. Cualquier otra causa legal prevista en la Declaración de Prácticas de Certificación.

Si el suscriptor o representante/responsable del uso del certificado no solicita la revocación del certificado en el caso de que se presenten las situaciones mencionadas arriba, este será responsable de las pérdidas o daños ocasionados por terceros de buena fe, que confíen en el contenido del certificado.

AC TECNISIGN o AR al considerar si el uso de certificado es perjudicial evalúa, entre otras cosas, lo siguiente:

- La naturaleza y el número de quejas recibidas;
- La identidad del (de los) autor(es);
- La legislación relevante en vigor;
- Las respuestas al supuesto uso perjudicial del Suscriptor

AC TECNISIGN y las certificaciones de titularidad exigen que el usuario final notifique inmediatamente a AC TECNISIGN acerca de la sospecha o compromiso conocido de su clave privada.

AC TECNISIGN o AR PUEDEN revocar un Certificado de administrador si la Autoridad del administrador para actuar como Administrador ha sido suspendida o terminada.

Las Certificaciones de Titularidad exigen que el usuario final notifique inmediatamente a una AR de la sospecha o compromiso conocido de su clave privada.

4.9.1.1.1 Requisitos CABF

AC TECNISIGN revocará un Certificado dentro de las 24 horas.

4.9.1.2. Razones para revocar un certificado de AC subordinada

La AC de emisión debe revocar un certificado de AC subordinada en el plazo de siete (7) días, si ocurre uno o más de los siguientes eventos:

1. La AC subordinada solicita la revocación por escrito;
2. La AC subordinada notifica a la AC Emisora de que la solicitación de certificado original no ha sido autorizada por ella ni ha concedido autorización;
3. La AC de emisión obtiene evidencia de que la clave privada de la AC subordinada correspondiente a la Clave pública del certificado ha sufrido compromiso o ya no cumple los requisitos de las Secciones 6.1.5 y 6.1.6;
4. La AC de emisión obtiene evidencias de que el Certificado ha sido mal utilizado;
5. La AC de emisión es informada de que el Certificado no ha sido emitido de acuerdo con o si la AC subordinada no ha cumplido la PC o la DPC aplicable;
6. La AC emisora determina que cualquier información que figure en el certificado es imprecisa o engañosa;
7. La AC Emisora o la AC Subordinada suspende las operaciones por cualquier motivo y no ha tomado providencias para otra AC para fornecer soporte de revocación para el Certificado;
8. El derecho de la AC emisora o de la AC subordinada de emitir certificados bajo estos requisitos ha expirado o ha sido revocado o suspendido, a menos que la AC de emisión haya tomado providencias para seguir manteniendo el Repositorio LCR/OCSP;
9. La revocación es exigida por la PC o por la DPC de la AC Emisora; o
10. El contenido técnico o el formato del Certificado presenta un riesgo inaceptable para los Proveedores de Software de aplicaciones o Partes de Confianza.

4.9.2 Quiénes pueden solicitar la revocación

El Suscriptor, la RA o la AC de Emisión pueden iniciar la revocación y PUEDEN enviar Informes de Problemas del Certificado, comunicando a la AC de emisión la causa razonable para revocar el certificado.

Los suscriptores individuales pueden solicitar la revocación de sus propios certificados individuales por medio de un representante autorizado de AC TECNISIGN o de una AR.

En el caso de Certificados de la organización, un representante debidamente autorizado de la organización DEBERÁ tener el derecho de solicitar la revocación de Certificados emitidos para la organización.

Un representante debidamente autorizado de AC TECNISIGN, una afiliada o una AR DEBE tener el derecho de solicitar la revocación de un Certificado de Administrador RA.

La entidad que aprobó la solicitud de certificado del suscriptor también DEBERÁ tener el derecho de revocar o solicitar la revocación del certificado del suscriptor.

Solo AC TECNISIGN tiene el derecho de solicitar o iniciar la revocación de los certificados emitidos para sus propias AC.

4.9.2.1 Procedimiento para solicitar la revocación de un certificado de usuario final

Antes de la revocación de un Certificado, VALID verifica si la revocación ha sido solicitada por el Suscriptor del Certificado o por la entidad que aprobó la Aplicación de Certificado. Los procedimientos aceptables para autenticar las solicitudes de revocación de Suscriptor incluyen:

1. Hacer que el Suscriptor de ciertos tipos de certificado presente la Frase de Desafío del Suscriptor (o un equivalente) y revoque el Certificado automáticamente si corresponde a la Frase de Desafío (o equivalente) en el registro;
2. Recibir un mensaje supuestamente del Suscriptor que solicita revocación y que contiene una firma digital verificable con referencia al Certificado por revocar; y
3. Comunicación al Suscriptor que ofrezca Garantías razonables de que la persona u organización que solicita la revocación es, de hecho, el Suscriptor. Dicha comunicación, dependiendo de las circunstancias, puede incluir uno o más de los siguientes datos: teléfono o e-mail. En ambos casos, se necesita una copia de la identificación fotográfica emitida por el gobierno del propietario o controlador del dominio. Además de eso, la confirmación de la solicitación puede efectuarse por medio de contacto telefónico o por otros medios.

Los administradores de AC/AR tienen el derecho de solicitar la revocación de Certificados de Suscriptores en el Subdominio de la AC/AR. AC TECNISIGN y afiliadas DEBERÁN autenticar la identidad de los administradores por medio del control de acceso utilizando SSL y autenticación de cliente antes de permitir que estos ejecuten funciones de revocación.

Las solicitaciones de las AC para revocar un Certificado de AC deben ser autenticadas por sus Entidades Superiores para garantizar que la revocación haya sido, de hecho, solicitada por la AC.

4.9.2.1.1 Requisitos CABF

AC TECNISIGN mantiene una capacidad continua 24x7 para aceptar y responder las solicitudes de revocación y cuestiones relacionadas.

4.9.3 Período de carencia de la solicitación de revocación

Las solicitudes de revocación DEBEN ser enviadas lo más rápidamente posible dentro de un plazo comercialmente razonable.

4.9.4 Plazo en que la AC debe procesar la solicitación de revocación

Las medidas comercialmente razonables para procesar las solicitaciones de revocación se toman sin demora.

AC TECNISIGN da inicio a la investigación de un Relato de Problemas con Certificado en hasta 24 horas tras recibir la solicitud, y decide si la revocación u otra acción apropiada es justificable con base en, como mínimo, los siguientes criterios:

1. La naturaleza del supuesto problema;
2. La cantidad de Relatos de Problemas recibidos respecto a un determinado certificado o suscriptor;
3. La entidad que presentó la queja; y
4. La legislación pertinente.

4.9.5 Requisitos de verificación de revocación para partes de confianza

Los Terceros de Confianza DEBERÁN verificar el estado de los Certificados en los que desean confiar. Partes de confianza PUEDEN verificar el estado del Certificado consultando la LCR más reciente de la AC VALID.

Partes de confianza pueden verificar el estado del Certificado consultando la LCR más reciente de la AC que emitió el Certificado en el que la Parte de Confianza desea confiar. Alternativamente, las Partes de Confianza podrán cumplir este requisito verificando el estado del certificado usando el repositorio con base en la Web aplicable o usando la OCSP (si está disponible). Las AC deben facilitar a las Partes de Confianza información sobre cómo encontrar la LCR apropiada, el repositorio con base en la Web o el respondedor del OCSP (cuando esté disponible) para verificar el estado de revocación.

En el Repositorio de AC TECNISIGN, se publica una «Tabla de referencia de LCR» que permite a las Partes de Confianza localizar la LCR para la AC relevante.

4.9.6 Información de emisión de LCR

Las LCR de AC TECNISIGN deben ser emitidas al menos una vez al año, pero también dentro de las 24 horas siguientes a la revocación un Certificado de AC. Cualquier desvió de esta política general DEBE obtener la aprobación del PMD y ser publicado en la DPC apropiada.

4.9.6.1 Requisitos del estado del certificado de suscriptor

AC TECNISIGN DEBERÁ actualizar y reemitir las LCR al menos una vez cada 7 días, y el valor del campo nextUpdate NO DEBE sobrepasar 10 días del valor del campo thisUpdate.

4.9.6.2 Requisitos del estado del certificado CA subordinado

VALID DEBERÁ actualizar y reemitir las LCR al menos:

a) Una vez cada 12 meses y

b) Dentro de las 24 horas siguientes a la revocación de un Certificado CA Subordinado, y el valor del campo nextUpdate NO DEBE sobrepasar 12 meses del valor del campo thisUpdate.

4.9.7 Publicación máxima para las LCR

Las LCR se publican en el repositorio VALID dentro de un plazo comercialmente razonable tras la generación. Esto, en general se realiza automáticamente dentro de segundos tras la generación.

4.9.8 Período de retención de los LCR

a) Los LCR y certificados de firma digital emitidos por VALID ROOT CA se retienen permanentemente para fines de consulta histórica;
b) Las copias de los documentos de identificación presentados en el momento de la candidatura y la revocación de los certificados y los términos y condiciones de propiedad y responsabilidad deben conservarse durante, como mínimo, 10 (diez) años de la fecha de expiración o revocación del certificado; y
c) la demás información, incluidos los registros de Auditoría, se retienen por, como mínimo, 6 (seis) años.

4.9.9 Disponibilidad de revocación on-line/Verificación de estado

La revocación on-line y otra información de estado del Certificado están disponibles en un repositorio con base en la Web y, cuando está disponible, el OCSP. Los Centros de Procesamiento deben ter un repositorio con base en la Web que permita que Partes de confianza efectúen consultas on-line sobre

la revocación y otra información de estado del Certificado. Un Centro de Procesamiento, como parte de su contrato con un Centro de Servicios, debe hospedar tal repositorio en nombre del Centro de Servicios. Los Centros de Procesamiento facilitan a las Partes de Confianza información sobre cómo encontrar el repositorio apropiado para verificar el estado del Certificado y, si el OCSP está disponible, cómo encontrar el respondedor correcto del OCSP.

Las respuestas del OCSP deben estar de acuerdo con el RFC 6960 o el RFC 5019. Las respuestas del OCSP deben:
1. Estar firmadas por VALID; o
2. Estar firmadas por un Respondedor del OCSP cuyo certificado está firmado por AC TECNISIGN. El certificado de firma OCSP DEBE contener una extensión del tipo id-pkix-ocsp-nocheck, conforme a lo que determina el RFC 6960.

4.9.10 Requisitos para verificación de revocación on-line

Una parte de confianza DEBE verificar el estado de un certificado en el que desea confiar. Si una Parte de Confianza no verificar el estado de un Certificado en el que dicha Parte desea confiar consultando la LCR más reciente, tal Parte de Confianza DEBERÁ verificar el estado del Certificado consultando el repositorio aplicable o solicitando el estado de Certificado por medio del respondedor del OCSP aplicable (en que están disponibles los servicios del OCSP).

VALID soporta un recurso OCSP que utiliza el método GET para Certificados emitidos de acuerdo con estos Requisitos.

Si el respondedor del OCSP recibe una solicitación de estado de un certificado que no haya sido emitido, el respondedor no responderá con un estado «bueno».

VALID monitorea al respondedor para tales solicitaciones como parte de sus Procedimientos de respuesta de seguridad.

4.9.11 Requisitos del CABF para OCSP

4.9.11.1 Estado del certificado para certificados de suscriptor

AC TECNISIGN actualizará la información suministrada por medio de un Protocolo de estado de certificado on-line, como mínimo, cada 4 días. El tiempo máximo de expiración de las respuestas del OCSP de este servicio DEBE ser de 10 días.

4.9.11.2 Estado del certificado para certificados de AC subordinados

AC TECNISIGN actualizará la información suministrada por medio de un Protocolo de Estado de Certificados On-line, como mínimo, (i) cada 4 días y (ii) dentro de 1 hora tras la revocación de un Certificado.

4.9.12 Otras formas disponibles para divulgar la revocación

No se aplica.

4.9.13 Requisitos especiales relativos al compromiso clave

Los involucrados con AC TECNISIGN y las Partes de Confianza Participantes DEBEN ser notificados sobre un compromiso real o supuesto de la clave privada de la AC mediante esfuerzos comercialmente razonables. VALID debe notificar a potenciales Partes de Confianza si descubre, o si tiene razones para sospechar que hubo un compromiso de la clave privada de una de sus propias AC o de una de las AC dentro de su subdominio.

4.9.14 Circunstancias para suspensión

No se aplica.

4.9.15 Quien puede solicitar la suspensión

No se aplica.

4.9.16 Procedimiento para Pedidos de Suspensión

No se aplica.

4.9.17 Periodo límite de suspensión

No se aplica.

4.10 Servicios de estado del certificado

4.10.1 Características operacionales

El estatus de los certificados públicos está disponible por medio del LCR, a través del sitio de AC TECNISIGN (en una URL especificada en la DPC de AC) y por medio de respuesta del OCSP (cuando esté disponible).

Las entradas de revocación en una LCR o Respuesta OCSP NO DEBEN ser removidas hasta la "Fecha de Expiración" del Certificado revocado.

4.10.2 Disponibilidad de Servicio

AC TECNISIGN opera y mantiene su capacidad de LCR y OCSP con recursos suficientes para dar un tiempo de respuesta de diez segundos o menos, en condiciones operacionales normales.

AC TECNISIGN mantiene un repositorio on-line 24x7 para verificar automáticamente el estatus actual de todos los certificados no expirados emitidos por él.

AC TECNISIGN mantiene disponibilidad 24x7 para Respondedor internamente a un Reporte de Problemas de Certificados de alta prioridad y, en su caso, encaminar tal reclamación a las autoridades policiales y/o revocar un Certificado que sea objeto de tal reclamación.

4.10.3 Recursos Operacionales

OCSP es un recurso de servicio de estatus OPCIONAL que no está disponible para todos los productos y DEBE ser específicamente activado para determinados productos.

4.11 Fin de la suscripción

Un suscriptor para terminar una suscripción de un certificado emitido por AC TECNISIGN debe:

- Permitir que su certificado expire sin renovar o recertificar tal certificado;
- Revocar su certificado antes de la expiración del certificado sin substituirlo.

4.12 Custodia y recuperación de las claves

Ningún participante de AC TECNISIGN PUEDE mantener copia de claves privadas de AC, AR o de usuario final.

5. Instalaciones, gestión y controles operativos

Con base en la evaluación de riesgos, AC TECNISIGN desarrolla, implementa y mantiene un plan de seguridad que consiste en procedimientos de seguridad, medidas y productos diseñados para lograr los objetivos establecidos arriba y para gestionar y controlar los riesgos identificados durante la evaluación de riesgo, proporcionales a la sensibilidad de los datos del certificado y procesos de Gestión de los Certificados.

El plan de seguridad necesariamente incluye salvaguardas administrativas, organizacionales, técnicas y físicas apropiadas a la sensibilidad de los datos del certificado y procesos de Gestión de los Certificados.

El plan de seguridad debe también llevar en cuenta la tecnología entonces disponible y los costos de ejecución de las medidas específicas, e implementar un nivel de seguridad razonable y adecuado a los daños que puedan resultar de una violación de la seguridad y de la naturaleza de los datos por proteger.

AC TECNISIGN desarrolla, implementa y mantiene un programa de seguridad amplio proyectado para:

1. Proteger la confidencialidad, integridad y disponibilidad de los datos y procesos de Gestión de los Certificados;
2. Proteger contra amenazas o riesgos a la confidencialidad, integridad y disponibilidad de los datos del certificado y procesos de Gestión de los Certificados;
3. Proteger contra el acceso no autorizado o ilegal, la utilización, divulgación, modificación o destrucción de cualesquier datos del certificado y procesos de Gestión de los Certificados;

4. Proteger contra la pérdida o destrucción accidental o daños a datos del certificado y procesos de Gestión de los Certificados; y
5. Cumplir con todos los otros requisitos de seguridad legales aplicables a AC TECNISIGN.

El Proceso de Gestión de los Certificados incluye:

1. seguridad física y controles ambientales;
2. sistema de controles de integridad, incluyendo gestión de configuración, mantenimiento de la integridad y confiabilidad del código y detección/prevención de malware;
3. seguridad de red y gestión de firewall, incluyendo restricciones por puerto y filtrado de direcciones IP;
4. gestión de usuario, atribuciones separadas por funciones de confianza, concienciación, sensibilización y capacitación; y actividades y plazos límites de inactividad para dar rendición de cuentas individualizadas; y
5. control de Accesos lógicos, registro de las actividades y plazos límite de inactividad para dar rendición de cuentas individualizadas.

El programa de seguridad de AC TECNISIGN incluye una evaluación anual de riesgos para:

1. Identificar amenazas internas y externas previsibles que pueden resultar en acceso no autorizado, divulgación, utilización indebida, modificación o destrucción de cualesquier datos del certificado y procesos de Gestión de los Certificados;
2. Evalúa la probabilidad y potencial daño de esas amenazas, llevando en cuenta la sensibilidad de los datos del certificado y procesos de Gestión de los Certificados; y
3. Evalúa la suficiencia de las políticas, procedimientos, sistemas de información, tecnología y otros que AC TECNISIGN tiene en vigor para combatir estas amenazas.

5.1 Controles Físicos

AC TECNISIGN implementó la política de seguridad física de VALID GLOBAL que soporta los requisitos de seguridad de esta DPC. La conformidad con esas políticas está incluida en los requisitos de auditoría independiente de AC TECNISIGN descritos en la Sección 8.

La Política de Seguridad Física de AC TECNISIGN contiene informaciones sensibles de seguridad y sólo está disponible por medio de acuerdo con VALID GLOBAL. Una visión general de los requisitos son descritos en las subsecciones a continuación.

5.1.1 Construcción y localización de las instalaciones

Las operaciones de AC TECNISIGN son realizadas en un ambiente físicamente protegido que impide, impide y detecta el uso, el acceso o la divulgación no autorizada de informaciones y sistemas confidenciales, sean ellos secretos o públicos.

VALID también mantiene instalaciones de recuperación de desastres para sus operaciones de AC. Las instalaciones de recuperación de desastre de AC TECNISIGN son protegidas por niveles de seguridad física comparables a los de la instalación principal de AC TECNISIGN.

5.1.2 Acceso Físico

Los sistemas de AC TECNISIGN son protegidos por un mínimo de 4 capas de seguridad física, siendo el acceso a los niveles inferiores prerrequisitos para acceso a los niveles superiores.

Privilegios de acceso físico restrictivos controlan progresivamente el acceso a cada capa.

5.1.2.1. Actividades operacionales sensibles de AC

Cualquier actividad relacionada con el ciclo de vida del proceso de certificados sucede dentro de niveles físicos más restrictivos. El acceso a cada capa requiere el uso de una credencial de empleado con tarjeta de proximidad. El acceso físico es automáticamente registrado y se graba un vídeo. Se aplican capas adicionales de control de acceso individual, por medio de la utilización de dos factores de autenticación, incluyendo factores biométricos. Personas no autorizadas, incluyendo empleados no autenticados o visitantes, no son permitidos en esas áreas protegidas sin escolta.

El sistema de seguridad física incluye capas adicionales para seguridad de gestión de clave que sirve para proteger tanto el almacenamiento on-line como off-line de los hardwares criptográficos y material de claves de AC TECNISIGN. Las áreas utilizadas para crear y almacenar material criptográfico son provistas de doble control, a través de la utilización de dos factores de autenticación, incluyendo factores biométricos. Hardwares criptográficos de las ACs en modo Online y Offline son protegidas por medio del uso de cofres cerrados, armarios y contenedores.

El acceso a los hardwares criptográficos y material de claves de AC TECNISIGN es limitado de acuerdo con requisitos de segregación de funciones. La abertura y cierre de gabinetes en armarios u otras capas de seguridad se registran para fines de auditoría.

5.1.3 Energía y Aire Acondicionado

Las instalaciones seguras de AC TECNISIGN son equipadas con equipos primarios y de backup de:

- Sistemas de alimentación para asegurar un acceso continuo e ininterrumpido de energía eléctrica; y
- Calefacción / ventilación / sistemas de aire acondicionado para controlar la temperatura y humedad relativa.

5.1.4 Exposición al agua

Las instalaciones seguras de AC TECNISIGN minimizan el impacto de sus sistemas a la exposición al agua.

5.1.5 Prevención y Protección contra Incendios

AC TECNISIGN tomó precauciones razonables para prevenir y extinguir incendios u otras exposiciones perjudiciales a llamas o humos. Las medidas de protección y prevención de incendios de AC TECNISIGN fueron proyectadas para cumplir las reglamentaciones locales de seguridad contra incendios.

5.1.6 Almacenamiento de Medios

Todos los medios conteniendo software de producción y datos, auditoría, archivo o informaciones de backup son almacenadas en instalaciones AC TECNISIGN o en una instalación segura de almacenamiento externo con controles de accesos físicos y lógicos apropiados proyectados para limitar el acceso a personas autorizadas y proteger esos medios contra daños accidentales. (por ejemplo, agua, fuego y electromagnéticos).

5.1.7 Desecho de documentos en papel y dispositivos electrónicos

Documentos sensibles y materiales son triturados antes de ser desechados. El medio usado para colectar o transmitir informaciones confidenciales se hace ilegible antes del descarte. Los dispositivos criptográficos son físicamente destruidos o reducidos a cero de acuerdo con la orientación del fabricante antes del desecho.

Otros residuos son desechados de acuerdo con los requisitos normales de desecho de residuos de AC TECNISIGN.

5.1.8 Instalaciones de seguridad (backup) externas (off-site)

AC TECNISIGN ejecuta backups de rutina de datos críticos del sistema, datos de log de auditoría y otras informaciones confidenciales. Los medios de backup externos son almacenados de manera físicamente segura usando un recurso de almacenamiento de terceros Confiables, y el recurso de recuperación de desastre de AC TECNISIGN.

5.2 Controles procedimentales

5.2.1 Funciones de Confianza

Personas de Confianza incluyen todos los empleados, contratados y consultores que tienen acceso o control sobre autenticación y operaciones criptográficas que pueden afectar materialmente:

- la validación de las informaciones en las Solicitaciones de Certificado;
- la aceptación, rechazo u otro proceso en los pedidos de certificados, solicitaciones de revocación, solicitaciones de renovación, o informaciones de solicitud;
- la emisión o revocación de certificados, incluyendo personas que tienen acceso a particiones restrictas del repositorio de AC TECNISIGN;
- el tratamiento de las informaciones o solicitaciones del Suscriptor.

Se incluyen entre las Personas de Confianza, pero sin limitarse a:

- personal de operaciones criptográficas,
- personal de seguridad,
- personal de la administración del sistema,
- personal de ingeniería, y
- ejecutivos que son designados para gestionar la confiabilidad de la Infraestructura.

AC TECNISIGN considera las categorías de empleados identificadas en esta sección como Personas de Confianza, que dispone de una Posición de Confianza. Personas que necesitan tornarse Personas de Confianza deben concluir con éxito los requisitos de selección establecidos en esta DPC.

5.2.2 Controles de personal

5.2.2.1 Número de personas necesarias por tarea

AC TECNISIGN estableció, mantiene y refuerza los rigorosos procedimientos de control para asegurar la segregación de funciones con base en la responsabilidad del trabajo y para garantizar que más de una Persona de Confianza es necesaria para realizar tareas sensibles.

Políticas y procedimientos de control operan para asegurar la segregación de funciones con base en las responsabilidades del trabajo. Las tareas más sensibles, tales como el acceso y gestión del hardware criptográfico y de material de claves de AC, requieren diversas Personas de Confianza.

Estos procedimientos de control interno son proyectados para asegurar que, al menos, dos (2) Personas de Confianza sean requeridas para tenerse cualquier acceso físico o lógico a los dispositivos. El acceso al hardware criptográfico de AC es rigurosamente requerido por múltiples Personas de Confianza en todo su ciclo de vida, desde la recepción de entrada e inspección hasta la destrucción lógica y/o física. Una vez que un módulo es activado con las teclas de operación, otros controles de acceso son invocados para mantener la segregación de control sobre el acceso físico y lógico para el dispositivo. Personas con acceso físico a los módulos no poseen “Secretos Compartidos” y viceversa.

Otras operaciones manuales requieren la participación de, al menos, dos (2) Personas de Confianza, o una combinación de al menos una Persona de Confianza y un proceso de validación y emisión automatizada. Operaciones manuales para la recuperación de clave puede opcionalmente requerir la validación de dos (2) administradores autorizados.

5.2.3 Identificación y Autenticación para cada perfil

Para todo el personal que necesita tornarse Persona de Confianza, la verificación de la identidad se realiza por medio de la presencia física de esa persona ante Persona de Confianza del área de RR.HH. o de Seguridad y una verificación confiable de su identificación. La identidad es confirmada por medio de procedimientos de verificación de antecedentes descritos en la Sección 5.3.1.

AC TECNISIGN asegura que el personal alcance el estatus de Persona de Confianza antes que las áreas:

- emitan credenciales de Acceso y obtengan acceso a las instalaciones;

- emitan credenciales electrónicas para acceder y ejecutar funciones específicas en AC TECNISIGN, AR u otros sistemas de TI.

5.2.4 Funciones que requieren segregación de tareas

Papeles que requieren separación de tareas incluyen (pero sin limitarse a):

- la validación de informaciones en pedidos de certificado;
- aceptación, rechazo u otro procesamiento de Solicitaciones de Certificado, solicitaciones de revocación, solicitaciones de recuperación de clave o solicitaciones de renovación o informaciones de inscripción;
- la emisión o revocación de Certificados, incluyendo personal con acceso a partes restrictas del repositorio;
- el tratamiento de informaciones o solicitaciones del Suscriptor;
- la generación, emisión o destrucción de un certificado de AC; y
- la carga de una AC para un ambiente de producción.

5.3 Controles de personal

Personas que necesitan tornarse Personas de Confianza deben presentar prueba de antecedentes, cualificaciones y experiencia necesarias para desempeñar las responsabilidades del trabajo competente y satisfactoriamente. Controles de antecedentes son repetidos al menos a cada 5 años para el personal que ocupa cargos de confianza.

5.3.1 Antecedentes, cualificación, experiencia y requisitos de idoneidad

Antes del involucramiento de cualquier persona en el Proceso de Gestión de Certificado, sea como empleado, agente, o un tercero independiente de AC TECNISIGN, esta DEBE verificar la identidad y confiabilidad de tal persona. AC TECNISIGN exige que el personal que busca tornarse Persona de Confianza presente comprobante de la historia, cualificaciones y experiencia necesarias para desempeñar sus responsabilidades de trabajo de manera competente y satisfactoria.

5.3.2 Procedimientos de verificación de antecedentes

Antes del inicio del empleo en un Papel Confiable, AC TECNISIGN realiza verificaciones de antecedentes que incluyen lo siguiente:

- confirmación de empleo anterior;
- verificación de referencia profesional;
- confirmación del grado educacional más alto o más significativo obtenido;
- búsqueda de registros penales; y
- verificación de registros de crédito / financieros.

Los reportes conteniendo informaciones sobre los factores revelados en una verificación de antecedentes son evaluados por los recursos humanos y por el personal de seguridad, que determinan el curso de acción apropiado a la luz del tipo, magnitud y frecuencia de la conducta descubierta por la verificación de antecedentes. Dichas acciones PUEDEN incluir medidas hasta e incluso la cancelación de ofertas de empleo hechas a postulantes para cargos de confianza o el término de personas confiables existentes.

5.3.3 Requisitos de capacitación

AC TECNISIGN ofrece capacitación a sus empleados, así como la capacitación necesaria en el trabajo necesario para que ellos desempeñen sus responsabilidades de trabajo de manera competente y satisfactoria.

AC TECNISIGN mantiene registros de tal capacitación. AC TECNISIGN prevé periódicamente y perfecciona sus programas de capacitación conforme sea necesario.

Los programas de capacitación de AC TECNISIGN son adaptados a las responsabilidades del individuo e incluyen los siguientes temas:

- conceptos básicos de PKI;
- responsabilidades del trabajo;
- políticas y procedimientos de seguridad y operacionales de AC TECNISIGN;
- uso y operaciones de hardware y software implantados;
- reportes y manejo de incidentes y compromisos; y
- procedimientos de recuperación de desastres y continuidad de negocios.

5.3.3.1 Requisitos CABF para capacitación y nivel de habilidad

Además de los requisitos de la Sección 5.3.3, AC TECNISIGN DEBERÁ proporcionar a todo el personal que ejecuta tareas de verificación de informaciones con capacitación de habilidades que comprende:

- políticas y procedimientos de autenticación y evaluación (incluyendo PC y /o DPC),
- amenazas comunes al proceso de verificación de informaciones (incluyendo phishing y otras tácticas de ingeniería social) y
- Requisitos CABFORUM.

AC TECNISIGN DEBERÁ mantener registros de tal capacitación y asegurar que el personal encargado de los deberes del Especialista de Validación mantenga un nivel de habilidad que les permita desempeñar esas tareas satisfactoriamente.

AC TECNISIGN DEBE documentar que cada Especialista en Validación posee las habilidades exigidas por una tarea antes de permitir que el Especialista en Validación realice esa tarea.

AC TECNISIGN DEBERÁ exigir que todos los Especialistas en Validación sean aprobados en un examen dado por AC TECNISIGN sobre los requisitos de verificación de informaciones descritos en los Requisitos de ACBFORUM.

5.3.4 Información y requisitos de reciclaje

AC TECNISIGN da capacitación de actualización y actualizaciones para sus empleados en la extensión y frecuencia necesarias para asegurar que esas personas mantengan el nivel de conocimiento exigido para desempeñar sus responsabilidades de trabajo de manera competente y satisfactoria.

5.3.5 Información y secuencia de rotación de tareas

No se aplica.

5.3.6 Sanciones para acciones no autorizadas

Se toman acciones disciplinarias apropiadas para acciones no autorizadas u otras violaciones de las políticas y procedimientos de AC TECNISIGN. Acciones disciplinarias PUEDEN aun incluir medidas de despido y son proporcionales a la frecuencia y severidad de las acciones no autorizadas.

5.3.7 Requisitos para terceros independientes

En circunstancias limitadas, se pueden usar contratantes independientes o consultores para completar cargos de confianza. Cualquier contratado o consultor que es mantenido en los mismos criterios funcionales y de seguridad que se aplican a empleados de AC TECNISIGN tiene una posición comparable.

El certificado DEBERÁ verificar si el personal de Terceros Contratados involucrados en la emisión de un certificado cumple los requisitos de capacitación y habilidades de la Sección 5.3.3 y los requisitos de retención de documentos y registro de log de la Sección 5.4.1.

Contratados y consultores independientes que no cumplieron o aprobaron los procedimientos de verificación de antecedentes especificados en la Sección 5.3.2 de DPC tienen permiso de acceso a las instalaciones de seguridad de AC TECNISIGN apenas a la medida que son acompañados y supervisados directamente por terceros de confianza en todos los momentos.

5.3.7.1 Obligación de Cumplimiento de Directrices

En todos los casos, AC TECNISIGN DEBE obligar contractualmente a cada afiliada, AR, subcontratado y empresa a cumplir con todos los requisitos aplicables en esta DPC, su PC y ejecutarlos según lo exigido por la propia VALID. AC TECNISIGN DEBERÁ hacer cumplir esas obligaciones e, internamente, auditar cada conformidad de afiliada, AR, subcontratada y empresa con esos requisitos anualmente.

5.3.7.1.2 Atribuciones de Responsabilidad

Según lo especificado en la Sección 9.8.

5.3.8 Documentación suministrada al personal

AC TECNISIGN da a sus empleados la capacitación necesaria y otra documentación necesaria para ejecutar sus responsabilidades de trabajo de manera competente y satisfactoria.

5.4 Procedimientos de auditoría de seguridad

5.4.1 Tipos de Eventos Registrados

AC TECNISIGN y cada Tercero Contratado DEBERÁ registrar detalles de las acciones tomadas para procesar una solicitación de certificado y emitir un Certificado, incluyendo todas las informaciones generadas y la documentación recibida junto a la solicitud de certificado; la hora y la fecha; y el personal involucrado. AC TECNISIGN DEBERÁ disponer esos registros a su Auditor Cualificado como prueba de la conformidad con los requisitos CABFORUM.

AC VALID registra manualmente o automáticamente los siguientes eventos significativos:

Eventos de gestión del ciclo de vida de la clave de AC, incluyendo:

- ✓ Generación, backup, almacenamiento, recuperación, archivo y destrucción de claves;
- ✓ Eventos de gestión del ciclo de vida del dispositivo criptográfico.

Eventos de gestión del ciclo de vida de certificados de CA y del Suscriptor, incluyendo:

- ✓ Solicitaciones de Certificado y revocación;
- ✓ Procesamiento exitoso o fracasado de solicitaciones;
- ✓ Generación y emisión de Certificados y LCRs.

Eventos relacionados a la seguridad, incluyendo:

- ✓ Intentos de acceso al sistema PKI exitosos y fracasados;
- ✓ Acciones de PKI y sistema de seguridad ejecutadas por el personal de AC VALID;
- ✓ Files Archivos o registros confidenciales de seguridad leídos, escritos o excluidos;
- ✓ Modificaciones en el perfil de seguridad;
- ✓ Fallas del sistema, fallas de hardware y otras anomalías;
- ✓ Firewall y actividad del enrutador;
- ✓ Visitor Entrada / salida del visitante de las instalaciones de AC.

Entradas de log incluyen los siguientes elementos:

- ✓ Fecha y hora de la entrada;
- ✓ Serial o número de secuencia de entrada, para lanzamientos contables automáticos;
- ✓ Identidad de la entidad que hace el lanzamiento en el diario;
- ✓ Descripción / tipo de entrada.

5.4.1.1 CABF Tipos de Eventos Requisitos Grabados

Además, AC VALID registra manualmente o automáticamente los siguientes eventos significativos:

- ✓ Todas las actividades de verificación estipuladas en los Requisitos CABFORUM y en esta DPC;
- ✓ Fecha, hora, número de teléfono utilizado, personas habladas y resultados finales de las llamadas telefónicas de verificación;
- ✓ Respuestas OCSP.

5.5 Archivo de registros

5.5.1 Tipos de registros archivados

AC TECNISIGN archiva:

- Todos los datos de auditoría colectados en los términos de la sección 5.4;
- Información de pedidos de certificado;
- Documentación de apoyo al pedido de certificado;
- Informaciones del ciclo de vida del certificado como pedidos de revocación, renovación y aplicación.

5.5.2 Periodo de Retención para Archivo

AC TECNISIGN retiene toda la documentación relacionada a las solicitaciones de certificados y su verificación, certificados y su revocación, por al menos 7 (siete) años después que cualquier certificado, con base en esa documentación, deje de ser válido.

5.5.3 Protección del archivo

AC TECNISIGN protege los archivos para que apenas las Personas de Confianza autorizadas sean capaces de obtener acceso al archivo. El archivo es protegido contra la visualización, modificación, exclusión no autorizada u otra violación por medio del almacenamiento dentro de un Sistema Confiable. Los medios que contienen los datos archivo y las aplicaciones necesarias para procesar los datos archivo, se deben mantener para asegurar que el dato archivo puede ser accedido por el periodo de tiempo establecido en esta DPC.

5.5.4 Procedimientos para copia de seguridad (backup) de archivo

AC TECNISIGN hace el backup incremental diario de los archivos de sus informaciones emitidas del Certificado y realiza backups completos mensualmente. Se deben mantener copias de registros en papel en una instalación segura fuera del local.

5.5.5 Requisitos para sello de tiempo (time-stamping) de registros

Certificados, LCRs y otras bases de revocación deben contener informaciones de hora y fecha.

5.5.6 Sistema de colecta de datos del archivo (interno o externo)

Los sistemas de colecta archivos de AC TECNISIGN son internos, excepto para algunas AR de clientes corporativos. AC TECNISIGN auxilia sus AR de clientes corporativos manteniendo el camino de auditoría. Por lo tanto, los sistemas de colecta de archivos de las AR de clientes corporativos son externos.

5.5.7 Procedimientos para obtener y verificar informaciones del archivo

Apenas el Personal de Confianza autorizado es capaz de obtener acceso a los archivos. La integridad de la información se verifica cuando se restaure.

5.6 Cambio de claves

No se aplica.

5.7 Compromiso y recuperación de desastre

5.7.1 Procedimientos para Tratamiento de Incidentes y Comprometimiento

Backups de las siguientes informaciones de AC se deberán mantener en almacenamiento off-site y hechos disponibles en caso de un comprometimiento o desastre:

- datos de la solicitud de los certificados,
- datos de auditoría, y
- banco de datos de todos los certificados emitidos.

Backups de las claves privadas de AC se deberán generar y mantener de acuerdo con la Sección 6.2.4. AC TECNISIGN mantiene backups de las informaciones precedentes de sus propias ACs.

AC TECNISIGN tiene un Plan de Respuesta a Incidentes y un Plan de Recuperación de Desastres.

AC TECNISIGN documenta los procedimientos de continuidad de negocios y recuperación de desastres proyectados para notificar y proteger razonablemente a los proveedores, suscriptores y partes interesadas de software de aplicativos en caso de un desastre, comprometimiento de seguridad o falla de negocios.

AC TECNISIGN no divulga públicamente sus planes de continuidad de negocios, pero dispone sus planos de continuidad de negocios y planes de seguridad a sus auditores por medio de solicitación.

AC TECNISIGN prueba, revisa y actualiza anualmente esos procedimientos.

El plan de continuidad de negocios incluye:

1. Las condiciones para activar el plan;
2. Procedimientos de emergencia;
3. Procedimientos de fallback;
4. Procedimientos de retomada;
5. Un cronograma de mantenimiento del plan;

6. Requisitos de concienciación y educación;
7. Las responsabilidades de los individuos;
8. Objetivo del tiempo de recuperación (OTR);
9. Pruebas regulares de planes de contingencia;
10. AC TECNISIGN, planifica mantener o restaurar sus operaciones comerciales en tiempo hábil, tras la interrupción o la falla de procesos críticos de negocios;
11. Un requisito para almacenar materiales criptográficos críticos en un local alternativo;
12. Lo que constituye una interrupción del sistema aceptable y un tiempo de recuperación;
13. Con qué frecuencia se toman copias de backup de informaciones comerciales esenciales y software;
14. La distancia de las instalaciones de recuperación al local principal de AC TECNISIGN; y
15. Procedimientos para proteger sus instalaciones conforme sea posible durante el periodo de tiempo tras un desastre y antes de restaurar un ambiente seguro en el local original o remoto.

5.7.2 Recursos de computación, software y / o datos están corrompidos

En el supuesto de corrupción de recursos de computación, software y / o datos, ese caso es relatado para los procedimientos de tratamiento de incidentes de Seguridad de AC TECNISIGN. Dichos procedimientos exigen encaminamiento adecuado, investigación de incidentes y respuesta a incidentes. Si fuere necesario, los procedimientos de comprometimiento de clave AC TECNISIGN o recuperación de desastre serán aprobados.

5.7.3 Procedimientos de comprometimiento de la clave privada de la entidad

Tras la sospecha o compromiso comprobado de las claves privadas de AC TECNISIGN, el equipo de Seguridad de Respuesta a Incidentes de VALID ejecuta los procedimientos de respuesta al comprometimiento de la clave de VALID. Este equipo, que incluye seguridad, personal de criptografía, personal de servicios de producción, y otros representantes de la gestión de VALID, evalúa la situación, desarrolla e implementa el plan de acción con aprobación de la dirección ejecutiva de VALID.

Si la revocación del certificado de AC se exige, los siguientes procedimientos son realizados:

- El estatus de revocación del Certificado es comunicado para las Partes Confiables por medio del Repositorio de AC TECNISIGN de acuerdo con la Sección 4.9.7;
- Se harán esfuerzos comercialmente razonables para dar notificación adicional de la revocación a todos los afectados por la revocación del certificado de AC TECNISIGN; y
- AC generará un nuevo par de claves de acuerdo con la sección 5.6, excepto en el caso que AC esté siendo extinguida de acuerdo con la sección 5.8.

5.7.4 Capacidad de continuidad de negocios tras un desastre

VALID mantiene planes de continuidad de negocios para que, en caso de interrupción de los negocios, se puedan retomar funciones críticas de negocios. VALID mantiene un sitio de contingencia localizado en una instalación geográficamente separada del sitio principal.

El sitio de contingencia está equipado para atender los estándares de seguridad de esta DPC.

En caso de un desastre natural o provocado por el hombre que exija el cese permanente de las operaciones de las instalaciones primarias de VALID, el Equipo de Continuidad de Negocios y el Equipo de Gestión de Incidentes de Operaciones coordinarán con los equipos de gestión funcional cruzada para tomar la decisión de declarar formalmente una situación de desastre y gestionar el incidente. Así que una situación de desastre sea declarada, será iniciada la restauración de la funcionalidad de servicios de producción de VALID en el sitio de contingencia.

AC TECNISIGN desarrolló un Plan de Continuidad de Negocio (PCN) para sus servicios de PKI gestionada, incluyendo el servicio de PKI de AC TECNISIGN. El PCN identifica las condiciones para activar el plan y lo que constituye una interrupción aceptable del sistema y un tiempo de recuperación. El PCN define los procedimientos para que los equipos reconstituyan operaciones de AC TECNISIGN usando datos de backup y copias de backup de las claves de AC TECNISIGN.

Las entidades que operan instalaciones seguras para operaciones de AC y de AR desarrollan, prueban, mantienen y, si fuere necesario, implementan un Plan de Continuidad de Negocio (PCN) proyectado para reducir los efectos de cualquier tipo de desastre natural o causado por el hombre. El PCN debe identificar las condiciones para activar el plan y lo que constituye una interrupción de sistema y un tiempo de recuperación aceptables para la restauración de los servicios de sistemas de información y de las principales funciones de negocios dentro de un objetivo de tiempo de recuperación (Recovery Time Objective RTO) definido.

Además, el PCN deberá incluir:

- ✓ Frecuencia para hacer copias de backup de informaciones y softwares empresariales esenciales,
- ✓ Requisito para almacenar materiales criptográficos críticos (es decir, dispositivo criptográfico seguro y materiales de activación) en un local alternativo;
- ✓ Distancia de separación del sitio de recuperación de desastres para el sitio principal de AC; y
- ✓ Procedimientos para proteger la instalación de Desastres durante el periodo de tiempo después de un desastre y antes de restaurar un ambiente seguro en el local original o remoto.

El PCN debe incluir requisitos administrativos, incluyendo:

- ✓ Cronograma de mantenimiento del plan;
- ✓ Requisitos de concienciación y educación;
- ✓ Responsabilidades de los individuos; y
- ✓ Pruebas regulares de planes de contingencia.

Los sitios de recuperación de desastre tienen las protecciones de seguridad física equivalentes especificadas por AC TECNISIGN.

AC TECNISIGN tiene la capacidad de restaurar o recuperar operaciones esenciales dentro de 48 horas después de un desastre con, por lo menos, soporte para las siguientes funciones:

- ✓ Emisión de certificado;
- ✓ Revocación de certificado;
- ✓ Publicación de informaciones de revocación; y
- ✓ Dando informaciones de recuperación de claves para clientes corporativos.

El banco de datos de recuperación de desastres de AC TECNISIGN SERÁ sincronizado con el banco de datos de producción dentro de los límites de tiempo establecidos en la Guía de Requisitos de Seguridad y Auditoría. El equipamiento de recuperación de desastres de AC TECNISIGN DEBE tener las protecciones físicas de seguridad documentadas en las políticas de seguridad confidenciales de AC TECNISIGN, que incluyen la aplicación de niveles de seguridad física.

5.7.4.1 Requisitos CABF para Capacidad de continuidad de negocios después de un desastre

No se aplica.

5.8 Extinción de AC o AR

Caso sea necesario que AC TECNISIGN cese la operación, AC TECNISIGN hace un esfuerzo comercialmente razonable para notificar Suscriptores, Partes Confiables y otras entidades afectadas de rescisión antes del efectivo término de AC. Donde la cesión de AC sea necesaria, AC TECNISIGN desarrollará un plan de extinción para minimizar la interrupción a Clientes, Suscriptores y Partes Confiables. Tal plan de cierre puede dirigir lo siguiente, conforme sea el caso:

- Notificación a las partes afectadas por la extinción, tales como Suscriptores, Partes Confiables y Clientes, informándolos sobre el estatus de AC;
- Tratar el costo de tal notificación;
- Revocación del Certificado emitido para AC TECNISIGN;
- La conservación de los archivos y registros de AC por el periodo de tiempo requerido en esta PC;
- La continuación de los servicios de suporte a los Suscriptores y al cliente;
- La continuación de los servicios de revocación, como la emisión de LCR;
- La revocación de certificados de usuarios finales no expirados, si fuere necesario;
- Reembolso (si fuere necesario) a los Suscriptores cuyos Certificados válidos fueron revocados por fuerza del plan de extinción, o alternativamente, la emisión de certificados de sustitución por AC sucesora;

- Disposición de la clave privada de AC y los tokens de hardware conteniendo tal clave privada, si fuere aplicable; y
- Procedimientos necesarios para la transición de los servicios de AC para su sucesora.

5.9 Seguridad de datos

Tanto las ACs y otras Autoridades Firmantes son obligadas a cumplir las obligaciones previstas en esta Sección.

5.9.1 Objetivos

VALID desarrolla, implementa y mantiene un programa de seguridad amplio proyectado para:

1. Proteger la confidencialidad, integridad y disponibilidad de los Datos del Certificado y Procesos de Gestión de los Certificados;
2. Proteger contra amenazas o riesgos para la confidencialidad, integridad y disponibilidad de los Datos del Certificado y Procesos de Gestión de los Certificados;
3. Protéjase contra el acceso no autorizado o ilegal, la utilización, divulgación, modificación o destrucción de cualesquier Datos del Certificado y Procesos de Gestión de los Certificados;
4. Proteger contra la pérdida o destrucción accidental o daños a Datos del Certificado y Procesos de Gestión de los Certificados; y
5. Cumplir con todos los otros requisitos legales de seguridad aplicables a AC.

5.9.2 Evaluación de Riesgo

VALID realiza una Evaluación de Riesgo anual que:

1. Identifica amenazas internas y externas previsibles que pueden resultar en acceso no autorizado, divulgación, uso indebido, modificación o destrucción de cualesquier datos de certificado o Procesos de Gestión de Certificado;

2. Evalúa la probabilidad y posibles daños de esas amenazas, llevando en cuenta la sensibilidad de los Procesos de Datos de Certificado y Gestión de Certificados; y

3. Evalúa la suficiencia de las políticas, procedimientos, sistemas de información, tecnología y otros arreglos que AC tiene en vigor para combatir dichas amenazas.

5.9.3 Plan de Seguridad

Con base en los resultados de la Evaluación de Riesgo anual, VALID desarrolla, implementa y mantiene un Plan de Seguridad que consiste en procedimientos, medidas y productos de seguridad proyectados para alcanzar los objetivos establecidos y para gestionar y controlar los riesgos identificados durante la Evaluación de Riesgo, con la sensibilidad de los Procesos de Datos de Certificado y Gestión de Certificados.

El Plan de Seguridad incluye salvaguardas administrativas, organizacionales, técnicas y físicas apropiadas a la sensibilidad de los Procesos de Datos de Certificado y Gestión de Certificados. El Plan de Seguridad lleva en cuenta la tecnología disponible a la época y el costo de implementar las

medidas específicas e implementa un nivel razonable de seguridad apropiado a los daños que pueden resultar de una violación de seguridad y de la naturaleza de los datos que se protegerán.

6. Controles Técnicos de Seguridad

6.1 Generación de par de claves e instalación

6.1.1 Generación de par de claves

La generación de pares de claves se DEBE ejecutar usando Sistemas Confiables y procesos que proporcionen la fuerza criptográfica necesaria de las claves generadas y eviten la pérdida, divulgación, modificación o uso no autorizado de claves privadas. Este requisito se aplica a Suscriptores de usuarios finales, clientes corporativos que usan, ACs que generan previamente pares de claves en tokens de hardware de Suscriptor de usuario final.

VALID recomienda que la generación de pares de claves del servidor de Administración Automatizada se ejecute usando un módulo criptográfico certificado FIPS 140-1 nivel 2 u otro estándar similar usado en Brasil.

La generación de pares de claves del Suscriptor generalmente se realiza por el Suscriptor. El Suscriptor generalmente usa un módulo criptográfico certificado FIPS 140-1 nivel 1 provisto con su software de navegador para generación de claves. Para Certificados del servidor, el Suscriptor generalmente usa el utilitario de generación de claves provisto con el software del servidor de web.

6.1.1.1. CABF CA Requisitos de generación de par de claves

Para pares de claves de la AC raíz creados que (i) se usan como pares de claves de la AC raíz o (ii) par de claves generados para una AC subordinada que no sea la operadora de la AC raíz o una afiliada de la AC raíz:

1. preparar y seguir un script de generación de clave;

2.tener un auditor cualificado para testimoniar el proceso de generación del par de claves de la AC raíz o grabar un vídeo de todo el proceso de generación del par de claves de la AC raíz; y

3.mandar un Auditor Cualificado emitir un reporte opinando que la AC siguió su ceremonia-clave durante el proceso de generación de clave y certificado y los controles usados para asegurar la integridad y la confidencialidad del par de claves.

Para otros pares de claves de la AC que son para el operador de la AC raíz o una afiliada de la CA raíz, AC TECNISIGN debe:

1. preparar y seguir un script de generación de claves; y

2.tener un auditor cualificado para testimoniar el proceso de generación del par de claves de la AC raíz o grabar un vídeo de todo el proceso de generación del par de claves de la AC raíz.

En todos los casos, AC TECNISIGN:

1.genera las claves en un ambiente físicamente seguro, según lo descrito en las PCs y su DPC;

2.genera claves de AC TECNISIGN usando personal en funciones de confianza bajo los principios de control de varias personas y dividir el conocimiento;

3.genera claves de AC TECNISIGN dentro de módulos criptográficos que cumplen los requisitos técnicos y de negocios aplicables, según lo divulgado en esta DPC y sus PCs.

4.registra sus actividades de generación de claves AC; y

5.mantiene controles efectivos para dar garantía razonable de que la Clave Privada ha sido generada y protegida en conformidad con los procedimientos descritos en esta DPC y sus PCs.

6.1.2 Entrega del par de claves para el Suscritor

Las claves privadas de los Suscriptores generalmente son generadas por el usuario final y, por lo tanto, la entrega de la clave privada para un Suscriptor no se aplica.

Si AC TECNISIGN o cualquiera de sus ARs se entera de que una Clave Privada del

Suscriptor fue comunicada a una persona no autorizada o una organización no afiliada al Suscriptor, AC TECNISIGN revocará todos los certificados que incluyan la Clave Pública correspondiente a la Clave Privada comunicada.

Si AC TECNISIGN o cualquiera de sus ARs generó la Clave Privada en nombre del Suscriptor, AC TECNISIGN debe cifrar la Clave Privada para transporte para el Suscriptor.

6.1.3 Entrega de clave pública al emisor del certificado

Cuando una clave pública es transferida para AC emisora para ser ingresada en un certificado, se debe entregar por medio de un mecanismo que asegura que la clave pública no haya sido alterada durante el tránsito y que el solicitante del Certificado posea la clave privada correspondiente a la clave pública transferida. El mecanismo aceptable dentro de AC TECNISIGN para entrega de clave pública es un paquete de solicitación de suscripción del Certificado PKCS#10 o un método equivalente, asegurando que:

- La clave pública no fue alterada durante el tránsito; y
- El Solicitante del Certificado posee la clave privada correspondiente a la clave pública transferida.

AC TECNISIGN al ejecutar Ceremonias de Generación de Claves transfiere la clave pública del módulo criptográfico en que se creó para el módulo criptográfico de la AC superior (el mismo módulo criptográfico, si fuere un CCA), agrupándola en una solicitación PKCS#10.

6.1.4 Entrega de la Clave Pública de la CA para Partes Confiadas

AC TECNISIGN proporciona la cadena de certificación completa (incluyendo AC TECNISIGN y cualesquier ACs de la cadena) al Suscriptor del usuario final por medio de la emisión del Certificado. El download de los certificados también se PUEDE hacer en: http://ac.tecnisign.net/ac-tecnisign/ac-tecnisignv1.p7b .

VALID hará un esfuerzo razonable para que las claves públicas de AC TECNISIGN se incluyan en los Certificados Raíz que ya están embutidos en muchos aplicativos de software populares, tornando desnecesarios mecanismos especiales de distribución de raíces. Además, en muchos casos, una Parte Confiada usando el protocolo S/MIME recibirá automáticamente, además del Certificado del Suscriptor, los Certificados (y, por lo tanto, las claves públicas) de todas las ACs subordinadas a AC TECNISIGN.

6.1.5 Tamaño de las claves

Los pares de claves DEBEN tener extensión suficiente para impedir que otros determinen la clave privada del par de claves usando el análisis criptográfico o el periodo de utilización esperada de esos pares de claves.

El Estándar de AC TECNISIGN es:

. para AC emitida después del 18/08/2011:

- tamaños de clave para usuarios finales: RSA de 2048 bits

- algoritmo de suscripción digital hash: SHA-2

El tamaño de clave generado sigue las mejores prácticas descriptas por WebTrust y CA/Browser Forum Baseline Requirements y una revisión anual es realizada en extensiones de clave para determinar el periodo de uso de clave apropiado con recomendaciones seguidas.

Tras la expiración del certificado AC, la clave privada es destruida correctamente al final del periodo de archivo.

6.1.5.1 Requisitos CABF para tamaños de clave

Certificados de AC raíz	Periodo de validez con inicio a partir del 31 de diciembre de 2010	Periodo de validez con inicio a partir del 31 de diciembre de 2010
Algoritmo Digest	MD5 (NO RECOMENDADO), SHA-1, SHA-256, SHA-384 o SHA-51	SHA-1*, SHA-256, SHA-384 or SHA-512
Módulo DSA mínimo y tamaño del divisor (bits) ***	2048**	2048
Curva ECC	NIST P-256, P-384, or P-521	

Módulo DSA mínimo y tamaño del divisor (bits) ***	L= 2048, N= 224 or L= 2048, N= 256

Certificado de AC subordinada	Periodo de validez con inicio a partir del 31 de diciembre de 2010	Periodo de validez con inicio a partir del 31 de diciembre de 2010
Algoritmo Digest	SHA-1, SHA-256, SHA-384 o SHA-512	SHA-1*, SHA-256, SHA-384 or SHA-512
Módulo DSA mínimo y tamaño del divisor (bits) ***	1024	2048
Curva ECC	NIST P-256, P-384, or P-521	
Módulo DSA mínimo y tamaño del divisor (bits) ***	L= 2048, N= 224 or L= 2048, N= 256	

Certificado de suscriptores	Final del periodo de validez en o antes del 31 de diciembre de 2013	Periodo de validez que termina después del 31 de diciembre 2013
Digest algorithm	SHA-1*, SHA-256, SHA-384 or SHA-512	SHA-1*, SHA-256, SHA-384 or SHA-512
Minimum RSA modulus size (bits)	1024	2048
ECC curve	NIST P-256, P-384, or P-521	
Minimum DSA modulus and divisor size (bits) ***	L= 2048, N= 224 or L= 2048, N= 256	

* SHA-1 PODE ser usado con claves RSA de acuerdo con los criterios definidos en la Sección 7.1.3.

** Un Certificado de AC Raíz emitido antes del 31 de diciembre de 2010 con un tamaño de clave RSA menor que 2048 bits aún PUEDE servir como un ancla de confianza para Certificados de suscriptor emitidos de acuerdo con estos Requisitos.

*** L y N (las extensiones de bit del módulo p y del divisor q, respectivamente) son descritos en la Suscripción Digital Estándar, FIPS 186-4 (http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf).

6.1.6 Generación de parámetros de clave pública y verificación de calidad

Los participantes de AC TECNISIGN deben generar los parámetros-clave necesarios de acuerdo con un estándar equivalente aprobado por PMD.

Los mismos estándares se deben usar para verificar la calidad de los parámetros clave generados.

RSA: AC TECNISIGN debe confirmar que el valor del exponente público es un número impar igual a 3 o más. Además, el exponente público debe estar en el intervalo entre 216 + 1 y 2256-1. El módulo también debe tener las siguientes características: un número impar, no la potencia de un primo, y no tiene factores menores que 752. [Fuente: Sección 5.3.3, NIST SP 800-89].

DSA: Aunque el FIPS 800-57 diga que los parámetros de dominio PUEDEN ser dispuestos en algún sitio accesible, los certificados DSA compatibles deben incluir todos los parámetros del dominio. Eso es para asegurar la máxima interoperabilidad entre el software de la tercera parte confiable. AC TECNISIGN debe confirmar que el valor de la clave pública tiene la representación y el rango correctos exclusivos en el campo y que la clave posee el orden correcto en el subgrupo. [Fuente: Sección 5.3.1, NIST SP 800-89].

ECC: AC TECNISIGN debe confirmar la validez de todas las claves usando la Rutina de Validación de Clave Pública Completa ECC o la Rutina de Validación de Clave Pública Parcial ECC. [Fuente: Secciones 5.6.2.3.2 y 5.6.2.3.3, respectivamente, del NIST SP 56A: Revisión2].

6.1.7 Propósitos de uso de la clave (conforme el campo “key usage” en la X.509 v3)

No se aplica.

Las Claves privadas correspondientes a Certificados Raíz NO Se DEBEN usar para suscribir Certificados, excepto en los siguientes casos:

1. Certificados auto suscriptos para representar la propia AC Raíz;
2. Certificados para ACs Subordinados y Certificados Cruzados;
3. Certificados para fines de Infraestructura (certificados de papeles administrativos, certificados internos de dispositivos operacionales de la AC); y
4. Certificados para verificación de respuesta OCSP.

6.1.8 Controles de Protección de Clave Privada y Módulo Criptográfico

Los suscriptores son obligados por contrato a tomar las precauciones necesarias para evitar la pérdida, divulgación, modificación o uso no autorizado de claves privadas.

6.1.9 Estándares y Controles del Módulo Criptográfico

Las claves privadas dentro de AC TECNISIGN deben ser protegidas usando un Sistema Confiable y los detentores de claves privadas deben tomar las precauciones necesarias para evitar la pérdida, divulgación, modificación o uso no autorizado de esas Claves Privadas de acuerdo con esta PC, obligaciones contractuales y requisitos documentados en las Políticas de seguridad confidenciales de AC TECNISIGN. Suscriptores de usuarios finales tienen la opción de proteger sus claves privadas en una tarjeta inteligente u otro token de hardware. Los clientes de AC TECNISIGN y AR deben proteger segmentos de clave privada en esos servidores usando un Sistema Confiable.

AC TECNISIGN recomienda que los clientes de AR ejecuten todas las operaciones criptográficas de la AR la Administración Automatizada en un módulo criptográfico certificado nivel FIPS 140-2 nivel 3 u otro estándar similar usado en Brasil.

VALID recomienda que los certificados SSL ejecuten operaciones criptográficas en un módulo criptográfico con clasificación de al menos 140-2 nivel 3, módulo criptográfico certificado u otro estándar similar usado en Brasil.

6.1.10 Control múltiple de personas (n de m) para clave privada

VALID implementó mecanismos técnicos y de procedimientos que exigen la participación de varios individuos confiables para ejecutar operaciones criptográficas de CA confidenciales. VALID usa el "Secretos Compartidos (Secret Share)" para dividir los datos de activación necesarios para usar una clave privada de la CA en partes separadas llamadas "Secretos Compartidos" que sólo se mantienen por individuos capacitados y confiables llamados "Shareholders". Un número límite de "Secretos Compartidos (Secret Share)" (m) del número total de Comparticiones Secretas creadas y distribuidas para un determinado módulo criptográfico de hardware (n) es NECESARIO para activar una clave privada de la AC almacenada en el módulo.

El número límite de comparticiones necesarias para suscribir un certificado de AC es 8 (ocho). Se debe notar que el número de comparticiones distribuidas para tokens de recuperación de desastres PUEDE ser menor que el número distribuido para tokens operacionales, mientras el número límite de comparticiones permanece el mismo. Los Secret Share son protegidos de acuerdo con esta DPC.

6.1.11 Custodia de Clave Privada

Las claves privadas de la AC no son custodiadas.

6.1.12 Backup de Clave Privada

AC TECNISIGN crea copias de backup de claves privadas de la AC para fines de recuperación de rutina y recuperación de desastres. Esas claves son almacenadas de manera cifrada en los módulos criptográficos de hardware y en los dispositivos de almacenamiento de claves asociados. Los módulos criptográficos usados para almacenamiento de claves privadas de la AC cumplen los requisitos de esta DPC. Las claves privadas de AC son copiadas para los módulos criptográficos de hardware de backup, de acuerdo con esta DPC.

Los módulos criptográficos utilizados para almacenamiento de las claves privadas de la AC en el local están sujetos a los requisitos de esta DPC. Módulos conteniendo copias de recuperación de desastre de claves privadas de AC están sujetos a los requisitos de esta DPC.

Las claves privadas cuyo backup se hace deben protegerse contra modificación o divulgación no autorizada por medios físicos o criptográficos. Las copias de seguridad son protegidas con un nivel de protección física y criptográfica igual o superior al de los módulos criptográficos en el sitio de AC TECNISIGN, como en un sitio de recuperación de desastre o en otra instalación externa segura, como un cofre bancario.

AC TECNISIGN recomienda que los Clientes Corporativos que tengan tokens de administración Automatizados que no estén sujetos al servicio hagan backup de sus claves privadas y los protejan contra modificación no autorizada o divulgación por medios físicos o criptográficos.

AC TECNISIGN no mantiene copia de seguridad de las claves privadas de certificado de suscripción digital emitido por ella.

6.1.13 Archivo de Clave Privada

Tras la expiración del certificado de AC TECNISIGN, el par de claves asociado al certificado seguramente se mantendrá por un periodo de al menos 5 años utilizando módulo criptográfico que cumplen los requisitos de esta DPC. Estos pares de claves de AC no se deben usar para cualesquier eventos de suscripción tas la fecha de vencimiento del correspondiente certificado.

ACs subordinadas a AC TECNISIGN ejecutan los mismos controles establecidos para AC TECNISIGN.

AC TECNISIGN no archiva copias de claves privadas del Suscriptor.

6.1.14 Transferencia de clave privada en módulo criptográfico

AC TECNISIGN genera el par de claves de AC en los módulos criptográficos de hardware en los cuales se usarán las claves. Además, VALID hace copias de los pares de claves de AC para fines de recuperación de rutina y recuperación de desastres. Donde los pares de claves de AC son copiados para otro módulo criptográfico de hardware, esos pares de claves son transportados entre los módulos en el formato cifrado.

Si AC de Emisión generó la Clave Privada en nombre da AC Subordinada, entonces AC Emisora debe cifrar la clave privada para transporte para AC subordinada. Si AC de emisión supiere que una clave privada de AC subordinada se comunicó a una persona no autorizada o a una organización que no sea afiliada a AC subordinada, AC Emisora revocará todos los certificados que incluyan la clave correspondiente a la clave privada comunicada.
La entrada de una clave privada en un módulo criptográfico debe usar mecanismos para evitar pérdida, robo, modificación, divulgación no autorizada o uso no autorizado de tal clave privada.

Los participantes de AC TECNISIGN que pre generan claves privadas y las transfieren para un token de hardware, por ejemplo, transfieren las claves privadas generadas de los Suscriptores para una tarjeta inteligente, transfieren con seguridad esas claves privadas para el token en la medida necesaria para evitar pérdida, robo, modificación, divulgación no autorizada o uso no autorizado de esas claves privadas.

6.1.15 Almacenamiento de Clave Privada en el Módulo Criptográfico

La entrada de una clave privada en un módulo criptográfico debe usar mecanismos para evitar pérdida, robo, modificación, divulgación no autorizada o uso no autorizado de tal clave privada.

6.1.16 Método de activación de Clave Privada

AC TECNISIGN protege los datos de activación de sus claves privadas contra pérdida, robo, modificación, divulgación no autorizada o uso no autorizado.

El Estándar de AC TECNISIGN para Suscriptores la protección de Clave Privada es:
. Use una contraseña de acuerdo con la Sección 6.4.1 o seguridad de fuerza equivalente para autenticar el Suscriptor antes de la activación de la clave privada, que incluye, por ejemplo, una contraseña para operar la clave privada o una contraseña de login o protección de pantalla del Windows; y
. Tomar medidas comercialmente razonables para la protección física de la estación de trabajo del Suscriptor para impedir el uso de la estación de trabajo y su clave privada asociada sin la autorización del Suscriptor.

Cuando desactivadas, las claves privadas se mantienen apenas de modo cifrado.

6.1.17 Método de Desactivación de la Clave Privada

Suscriptores de usuarios finales DEBEN proteger sus claves privadas. Esas obligaciones se extienden a la protección de la clave privada después de suceder una operación de clave privada. La clave privada se puede desactivar después de cada operación, después del logoff del sistema o después de la remoción de una tarjeta inteligente de la lectora de tarjeta inteligente, dependiendo del mecanismo de autenticación usado por el usuario.

Las claves privadas del Suscriptor se pueden desactivar después de cada operación, después del logoff del sistema o después de la remoción de una tarjeta inteligente de la lectora de tarjeta inteligente, dependiendo del mecanismo de autenticación usado por el usuario. En todos los casos, los usuarios finales tienen la obligación de proteger adecuadamente sus claves privadas de acuerdo con su DPC.

6.1.18 Método de destrucción de clave privada

Caso sea necesario, todas las claves privadas se deben destruir de una manera que asegure razonablemente que no sobren residuales de la clave que puedan llevar a la reconstrucción de la clave.

AC TECNISIGN utiliza la función de reducción a cero de sus módulos criptográficos de hardware y otros medios apropiados para asegurar la destrucción completa de las claves privadas de AC. Cuando realizadas, se registran las actividades de destrucción de la clave de AC.

6.1.19 Clasificación del Módulo Criptográfico

Vea la Sección 6.1.9.

6.2 Otros aspectos de la gestión de par de claves

6.2.1 Archivo de Clave Pública

AC TECNISIGN y Certificados de Suscriptor de usuario final almacenan sus propias claves públicas en backup y se archivan como parte de los procedimientos de backup de rutina de VALID.

6.2.2 Períodos Operacionales del Certificado y Períodos de Uso del Par de Claves

El Periodo Operacional para los Certificados se DEBE definir de acuerdo con los plazos establecidos en la Tabla a continuación. Los Certificados de Suscriptor de usuario final que son renovaciones de certificados de suscriptor existentes PUEDEN tener un periodo de validez más largo (hasta 3 meses).

El periodo de uso para pares de claves del Suscriptor es igual al Periodo Operacional de sus Certificados, excepto por el hecho de que las claves privadas PUEDEN continuar siendo usadas después del Periodo Operacional para descriptografía y verificación de suscripción. El Periodo Operacional de un Certificado termina con su expiración o revocación. Una AC no debe emitir certificados si sus Períodos Operacionales se extienden más allá del periodo de uso del par de claves de AC. Por lo tanto, el periodo de uso del par de claves de AC es necesariamente menor que el periodo operacional del Certificado de AC. Específicamente, el periodo de uso es el Periodo Operacional del Certificado de AC menos el Periodo Operacional de los Certificados que CA emite. Al final del periodo de uso para un par de claves de Suscriptor o AC, el Suscriptor o AC DEBERÁ, a partir de ahí, interrumpir todo el uso del par de claves, excepto a medida que un AC necesite suscribir informaciones de revocación hasta el final del Periodo Operacional del último Certificado emitido.

Certificado emitido por Periodo de validez	***Periodo de validez***
AC RAÍZ auto suscrita (4096 bit RSA)	Hasta 20 años
Ac RAÍZ para AC on-line	Hasta 15 años
AC intermediaria off-line para CA on-line	Hasta 15 años
AC on-line para suscriptor individual del usuario	Normalmente, hasta 3 años, pero en las condiciones descritas abajo, hasta 6 años en las condiciones descritas abajo, sin opción de renovación o nuevo registro. Después de 6 años, se REQUIEREN nuevas inscripciones.
AC on-line para suscriptor organizacional de entidad final	Normalmente, hasta 6 años, en las condiciones descritas abajo, sin opción de renovación o nueva digitación. Después de 6 años, se REQUIEREN nuevas inscripciones.
Certificados de suscriptor emitidos de acuerdo con CABF Requirements	No se aplica.

Excepto según lo observado en esta sección, los postulantes de AC TECNISIGN DEBEN interrumpir todo uso de sus pares de claves tras el término de sus períodos de uso.

Cualquier excepción a este procedimiento requiere aprobación del PMD y DEBE documentarse en la DPC pertinente.

Los certificados emitidos por AC TECNISIGN para los usuarios finales PUEDEN tener Períodos Operacionales (validez) superiores a 1 (un) año, hasta 5 (cinco) años, si se cumplen los siguientes requisitos:

- ✓ Protección de los pares de claves del Suscriptor con relación a su ambiente operacional para Certificados de la Organización, operación con la protección mejorada de un data center y para Certificados Individuales, los pares de claves de los Suscriptores residen en un token de hardware, como una tarjeta inteligente;
- ✓ Los suscriptores son NECESARIOS para someterse a procedimientos de nueva autenticación al menos a cada 3 años en los términos de la Sección 3 de DPC;
- ✓ Si un Suscriptor no consigue concluir los procedimientos de nueva autenticación de acuerdo con la Sección 3 de DPC con éxito, o fuere incapaz de probar la tenencia de tal clave privada cuando sea NECESARIO por lo expuesto arriba, AC revocará automáticamente el Certificado del Suscriptor.

Cualquier excepción a este procedimiento requiere la aprobación del PMD y DEBE documentarse en la DPC y PC pertinente.

6.2.2.1 CABF Requisitos del Periodo de Validez

Los Certificados de Suscriptor emitidos después del 1º de marzo de 2018 DEBEN tener un Periodo de Validez no superior a 1825 días.

Los Certificados de Suscriptor emitidos después de 1º de julio de 2016, pero antes del 1º de marzo de 2018, NECESITAN tener un Periodo de Validez superior a 39 meses.

6.3 Datos de activación

6.3.1 Generación e Instalación de Datos de Activación

Los participantes de AC TECNISIGN, que generan e instalan datos de activación para sus claves privadas deben usar métodos que protejan los datos de activación a la medida necesaria para evitar pérdida, robo, modificación, divulgación no autorizada o uso no autorizado de esas claves privadas.

A medida que se usan las contraseñas como datos de activación, los Suscriptores deben generar contraseñas que no pueden ser fácilmente adivinadas o quebradas por ataques.

Los datos de activación (secret share) usados para proteger los tokens conteniendo claves privadas de AC TECNISIGN son generados de acuerdo con los requisitos de esta DPC. La creación y distribución de comparticiones secretas se registran.

Las directrices de selección, de contraseña del VALID exigen que las contraseñas:

- ✓ se generen por el usuario;
- ✓ tengan al menos quince caracteres;
- ✓ tengan al menos un carácter alfabético y un carácter numérico;
- ✓ tengan al menos una letra minúscula;
- ✓ no contengan muchas incidencias del mismo carácter;
- ✓ no sea el mismo que el nombre del perfil del operador; y
- ✓ no contenga una substring larga del nombre del perfil del usuario.

VALID también recomienda el uso de dos mecanismos de autenticación de factor (por ejemplo, token y contraseña, biométrico y token, o biométrico y contraseña) para activación de clave privada.

6.3.2 Protección de Datos de Activación

Los participantes de AC TECNISIGN deben proteger los datos de activación de sus claves privadas usando métodos que protegen contra pérdida, robo, modificación, divulgación no autorizada o uso no autorizado de esas claves privadas.

Suscriptores de usuarios finales deben proteger los datos de activación de sus claves privadas, si hubiere, a la medida necesaria para evitar la pérdida, robo, modificación, divulgación no autorizada o uso no autorizado de esas claves privadas.

VALID recomienda enfáticamente que todos los Suscriptores almacenen sus claves privadas de modo cifrado y protejan sus claves privadas por medio del uso de una contraseña fuerte y/o fuerte. Se incentiva el uso de dos mecanismos de autenticación de factor (por ejemplo, token y contraseña, biométrico y token, o biométrico y contraseña).

6.3.2.1 Otros aspectos de los datos de activación

6.3.2.1.1 Transmisión de Datos de activación

Cuando los datos de activación de las claves privadas son transmitidos, AC TECNISIGN debe proteger la transmisión usando métodos que protegen contra la pérdida, robo, modificación, divulgación o uso no autorizado de esas claves privadas.

6.3.2.1.2 Destrucción de datos de activación

Los datos de activación de las claves privadas de AC se deben destruir usando métodos que protejan contra pérdida, robo, modificación, divulgación no autorizada o uso no autorizado de las claves privadas protegidas por esos datos de activación. Tras los períodos de retención determinados en la Sección 5.5.2, AC TECNISIGN debe desactivar los datos de activación por sustitución y/o destrucción física.

6.4 Controles de seguridad informática

Las funciones de AC y AR suceden en los Sistemas Confiables, de acuerdo con los estándares documentados en las políticas de seguridad confidenciales de AC TECNISIGN.

6.4.1 Requisitos Técnicos Específicos de Seguridad Computacional

La red de producción de VALID es lógicamente separada de otros componentes. Esa separación impide el acceso a la red, excepto por medio de procesos de aplicativos definidos. VALID usa firewalls para proteger la red de producción contra invasiones internas y externas y limitar la naturaleza y el origen de las actividades de red que PUEDEN acceder a los sistemas de producción.

VALID requiere el uso de contraseñas con extensión mínima de caracteres y una combinación de caracteres alfanuméricos y especiales. VALID requiere que las contraseñas sean modificadas periódicamente.

El Acceso directo a las bases de datos que soportan la operación de VALID es limitado a Personas de Confianza del equipo de Operaciones de Producción y que tengan un motivo para dicho acceso. VALID aplica la autenticación multifactor para todas las cuentas capaces de causar directamente la emisión de certificados.

Los servidores de gateway deben incluir la siguiente funcionalidad: control de acceso a servicios de CC, identificación y autenticación para inicio de servicios de AC, reutilización de objeto para memoria de acceso aleatorio de AC, uso de criptografía para comunicación de sesión y seguridad de banco de datos, archivo de AC y usuario final, historia de suscriptor y datos de auditoría, auditoría de eventos relacionados a la seguridad, auto prueba de servicios de AC relacionados a la seguridad y camino Confiable para identificación de funciones de PKI e identidades asociadas.

Las ARs deben asegurar que los sistemas que mantienen el software de AR y los archivos de datos son Sistemas Confiables, protegidos contra acceso no autorizado.

Las ARs separan lógicamente el acceso a esos sistemas y a esas informaciones de otros componentes. Esa separación impide el acceso, excepto por medio de procesos definidos. Las ARs deben usar firewalls para proteger la red contra intrusiones internas y externas y limitar la naturaleza y fuente de las actividades que PUEDEN acceder esos sistemas e informaciones. Las ARs requieren el uso de contraseñas con una extensión mínima de caracteres y una combinación de caracteres alfanuméricos y especiales, y debe exigir que las contraseñas sean modificadas periódicamente y conforme sea necesario. El Acceso directo a las bases de datos que soportan la operación de AR es limitado a Personas de Confianza del equipo de Operaciones de Producción y que tengan un motivo para ese acceso.

6.4.1.1 Requisitos CABF para Sistema de Seguridad

AC TECNISIGN debe aplicar la autenticación multifactor para todas las cuentas capaces de causar directamente la emisión de certificados.

6.4.2 Controles técnicos del ciclo de vida

6.4.1 Controles de Desarrollo de Sistema

Las aplicaciones son desarrolladas e implementadas por VALID de acuerdo con los estándares de desarrollo de sistemas y gestión de cambios de VALID. VALID también proporciona software para sus clientes corporativos para la ejecución de RA y ciertas funciones de CA. Ese software es desarrollado de acuerdo con los estándares de desarrollo del sistema VALID.

El software desarrollado por VALID, cuando cargado por primera vez, da un método para verificar si el software en el sistema ha sido originado por VALID, no ha sido modificado antes de la instalación y es la versión que se pretende usar.

6.4.3 Controles de gestión de seguridad

VALID posee mecanismos y/o políticas en vigor para controlar y monitorear la configuración de sus sistemas de AC. VALID analiza periódicamente la integridad de sus sistemas de AC.

6.4.4 Controles de seguridad del ciclo de vida

No se aplica.

6.5 Controles de seguridad de red

Las funciones de AC y RA son realizadas usando redes protegidas de acuerdo con los estándares documentados en las políticas de seguridad confidenciales de AC TECNISIGN (en el caso de VALID y afiliadas) para impedir el acceso no autorizado, adulteración y ataques de negación de servicio. Las comunicaciones de informaciones confidenciales deben ser protegidas usando criptografía punto a punto para confidencialidad y suscripciones digitales para no repudio y autenticación.

6.6 Sello de tiempo

Certificados, LCR y otras entradas del banco de datos de revocación DEBEN contener informaciones de hora y fecha.

7. PERFILES DE CERTIFICADO, LCR Y OCSP

7.1 Perfil del certificado

Según lo descrito en la Política de Certificado de AC TECNISIGN.

7.1.1 Número(s) de la versión

Según lo descrito en la Política de Certificado de AC TECNISIGN.

7.1.2 Extensiones de certificado

Según lo descrito en la Política de Certificado de AC TECNISIGN.

7.1.2.1 Subject Alternative Name

Según lo descrito en la Política de Certificado de AC TECNISIGN.

7.1.2.2. Aplicación del RFC 5280

Para fines aclaratorios, un Pre Certificado, según lo descrito en la RFC 6962 - Certificate Transparency, no se considerará un "certificado" sujeto a los requisitos descritos en la RFC 5280 - Infraestructura de Claves Públicas - Internet X.509 y Lista de Certificados Revocados (LCR) por estas Políticas.

7.1.3 Identificadores de los algoritmos

Según lo descrito en la Política de Certificado de AC TECNISIGN.

7.1.3.1 Requisitos CABF para identificadores de algoritmos

Según lo descrito en la Política de Certificado de AC TECNISIGN.

7.1.4 Formatos de nombres

Los Certificados de AC TECNISIGN son completados con el Issuer Name y el Subject Distinguished Name requeridos previstos en la sección 7 de la Política de Certificado - PC.

Además, los certificados de suscriptor de usuario final generalmente incluyen un campo Organizational Unit adicional que contiene un aviso declarando que los términos de uso del Cert*ificado son establecidos en una URL, la URL debe* ser un indicador del Contrato de Parte Confiable aplicable. Se deberán permitir excepciones al requisito anterior cuando limitaciones de espacio, formateo o interoperabilidad dentro de los Certificados hagan imposible la utilización de la organización en conjunto con el aplicativo para el cual los Certificados se destinan o si una indicación del Contrato de Parte Confiable aplicable sea incluida en la extensión de la política del certificado.

7.1.4.1 Información del emisor (Issuer)

Según lo descrito en la Política de Certificado de AC TECNISIGN.

7.1.4.2. Información del emitente (Subject): certificados de usuario final

Según lo descrito en la Política de Certificado de AC TECNISIGN.

7.1.4.2.1. Requisitos CABF para Subject Alternative Name Extension

Según lo descrito en la Política de Certificado de AC TECNISIGN.

7.1.4.2.1.1. Dirección IP reservada o nombre interno

Según lo descrito en la Política de Certificado de AC TECNISIGN.

7.1.4.2.2. Requisitos CABF para el campo Subject Distinguished Name Fields

Según lo descrito en la Política de Certificado de AC TECNISIGN.

7.1.4.3. Subject Information: para Certificados de AC Raíz y AC Subordinadas

Según lo descrito en la Política de Certificado de AC TECNISIGN.

7.1.4.3.1. Subject Distinguished Name Fields

Según lo descrito en la Política de Certificado de AC TECNISIGN.

7.1.5 Requisitos CABF restricciones de nombre

Según lo descrito en la Política de Certificado de AC TECNISIGN.

7.1.6 Identificador del objeto de la política de certificados

Según lo descrito en la Política de Certificado de AC TECNISIGN.

7.1.6.1. identificadores CP Reservados (Reserved CP Identifiers)

Según lo descrito en la Política de Certificado de AC TECNISIGN.

7.1.6.2. Certificados de AC Raíz

Según lo descrito en la Política de Certificado de AC TECNISIGN.

7.1.6.3. Certificados de AC Subordinadas

Según lo descrito en la Política de Certificado de AC TECNISIGN.

7.1.6.4. Certificados de usuario final

Según lo descrito en la Política de Certificado de AC TECNISIGN.

7.1.6.5 Requisitos CABF para PC Object Identifier

7.1.6.5.1 Requisitos CABF para PC Object Identifier para EV

Según lo descrito en la Política de Certificado de AC TECNISIGN.

7.1.7 Uso de la extensión de restricciones de políticas

Según lo descrito en la Política de Certificado de AC TECNISIGN.

7.1.8 Sintaxis y semántica de los calificadores de política

Según lo descrito en la Política de Certificado de AC TECNISIGN.

7.1.9 Semántica de procesamiento para extensiones críticas

Según lo descrito en la Política de Certificado de AC TECNISIGN.

7.2 PERFIL DE LA LCR

Según lo descrito en la Política de Certificado de AC TECNISIGN.

7.2.1 Versión

Según lo descrito en la Política de Certificado de AC TECNISIGN.

7.2.2 Extensiones de LCR y sus entradas

Según lo descrito en la Política de Certificado de AC TECNISIGN.

7.3 Perfil OCSP

Según lo descrito en la Política de Certificado de AC TECNISIGN.

7.3.1 Número(s) de la versión

Según lo descrito en la Política de Certificado de AC TECNISIGN.

7.3.2 Extensiones OCSP

Según lo descrito en la Política de Certificado de AC TECNISIGN.

8. Auditoría de cumplimiento y otras evaluaciones

Tras el inicio de las operaciones, VALID y Afiliadas pasan por una auditoría de conformidad periódica ("Auditoría de Conformidad") para asegurar la conformidad con los Estándares de AC TECNISIGN.

Se realiza un examen anual de **WebTrust for Certification Authorities v2.1** o posterior (o equivalente) para operaciones del datacenter y operaciones de gestión de claves de VALID que dan soporte a los servicios públicos de AC.

Además de esas auditorías de conformidad, VALID y las afiliadas DEBEN realizar otras revisiones e investigaciones para asegurar la confiabilidad de AC TECNISIGN, que incluyen, pero sin limitarse a:

- Una "Revisión de Seguridad y Prácticas" de un Afiliado antes que se permita iniciar las operaciones;
- La "Revisión de Seguridad y Prácticas" consiste en una revisión de las instalaciones seguras, documentos de seguridad, DPC, acuerdos relacionados a AC TECNISIGN, política de privacidad y planes de validación de un afiliado para asegurar que el afiliado cumpla los estándares de AC TECNISIGN;

- VALID tiene el derecho, a su único y exclusivo criterio, de realizar en cualquier momento una "Auditoría / Fiscalización" sobre sí misma, una afiliada en el caso que VALID crea que la entidad auditada no cumplió los estándares de AC TECNISIGN, haya sufrido un incidente o comprometimiento, o haya actuado o fallado en actuar, de tal manera que la falla de la entidad auditada, el incidente o compromiso, o el acto o falla configure amenaza real o potencial a la seguridad o integridad de AC TECNISIGN;
- VALID tiene el derecho de realizar "Revisiones Suplementarias de Gestión de Riesgo" sobre sí propio, un afiliado después de las constataciones incompletas o excepcionales en una Auditoría de Conformidad o como parte del proceso general de gestión de riesgos en el curso normal de los negocios.

VALID tiene el derecho de delegar la realización de esas auditorías, revisiones e investigaciones a la Entidad Superior de la entidad que se está auditando, revisando o investigando, o a una empresa de auditoría subcontratada. Las entidades que están sujetas a una auditoría, revisión o investigación deben proporcionar total cooperación a VALID y al equipo que realiza la auditoría, revisión o investigación.

AC TECNISIGN debe siempre:

1. Emitir Certificados y operar su PKI de acuerdo con todas las leyes aplicables a sus negocios y a los Certificados que emite en todas las jurisdicciones en que opera;
2. Cumplir con estos requisitos;
3. Cumplir los requisitos de auditoría establecidos en esta sección; y
4. Ser licenciado como una AC en cada jurisdicción donde opera, si el licenciamiento fuere necesario por la ley de esa jurisdicción para la emisión de certificados.

Requisitos CABF para auditorías

No se aplica.

Requisitos CABF para auditorías para EV

No se aplica.

8.1 Frecuencia y Circunstancias de evaluación

Auditorías de Conformidad son conducidas al menos anualmente, a expensas de la entidad auditada. Las auditorías se deben realizar sobre secuencias ininterrumpidas de periodos de auditoría con cada periodo no superior a un año de duración.

Certificados que se pueden usar para emitir nuevos certificados deben estar:
. Técnicamente de acuerdo con la sección 7.1.5 de PC y auditado solamente de acuerdo con la sección 8.7, o
. Técnicamente sin restricciones y totalmente auditado, de acuerdo con todos los requisitos restantes de esta sección.

Un certificado es considerado capaz de ser usado para emitir nuevos certificados si contiene una extensión X.509v3 basicConstraints, con el conjunto de valores Boolean de AC TECNISIGN definido como VERDADERO y, por lo tanto, por definición, ser un Certificado AC Raíz o un Certificado AC Subordinada.

(1) Si AC TECNISIGN tuviere un Reporte de auditoría válido indicando la conformidad con uno de los esquemas de auditoría listados en la Sección 8.1, entonces ninguna evaluación de pre operacional es necesaria.
(2) Si AC TECNISIGN no tuviere un Reporte de auditoría indicando la conformidad con uno de los esquemas de auditoría listados en la Sección 8.1, entonces, antes de emitir Certificados Públicamente Confiables, AC TECNISIGN deberá presentar una evaluación "point-in-time" ejecutada con éxito de acuerdo con las normas aplicables conforme uno de los esquemas de auditoría relacionados en la Sección 8.1. La evaluación "point-in-time" se debe concluir no antes de 12 meses de la emisión de Certificados Públicamente Confiables y debe seguirse por una auditoría completa mediante ese esquema dentro de 90 días de la emisión del primer Certificado Públicamente Confiable.

8.2 Identidad / Cualificaciones del Evaluador

La auditoría de AC TECNISIGN se debe realizar por un Auditor Cualificado.

Un Auditor Cualificado significa una persona física o una persona jurídica o un grupo de personas físicas o jurídicas que poseen colectivamente las siguientes cualificaciones y habilidades:

1. Independencia con relación al objeto de la auditoría;
2. La capacidad de realizar una auditoría que aborde los criterios especificados en uno de los esquemas de auditoría Elegible (ver Sección 8.1);
3. Emplea personas con dominio en el examen de la tecnología de Infraestructura de Claves Públicas, informaciones, herramientas y técnicas de seguridad, tecnología de la información y auditoría de seguridad y capacidad de certificar como tercero;
4. (Para auditorías realizadas de acuerdo con cualquier de las normas del ETSI) ser acreditadas de acuerdo con la ISO 17065, aplicando los requisitos especificados en la ETSI EN 319 403;
5. (Para auditorías realizadas de acuerdo con el estándar WebTrust) licenciadas por el WebTrust;
6. Vinculado por ley, reglamentación gubernamental o código de ética profesional; y
7. Excepto en el caso que una Agencia Interna de auditoría del Gobierno, mantenga seguro de Responsabilidad Profesional / Errores y Omisiones con cobertura de al menos un millón de dólares.

8.3 Relación de asesor con la entidad evaluada

Las auditorías de conformidad de las operaciones de VALID son realizadas por una empresa de contabilidad pública independiente de VALID.

8.4 Tópicos abordados por la evaluación

AC TECNISIGN debe ser sometida a una auditoría de acuerdo con uno de los siguientes esquemas:

1. WebTrust para Autoridades de Certificación v2.1;
2. Un sistema nacional que audite la conformidad con el ETSI TS 102 042 / ETSI EN 319 411-1; o
3. Si una AC del gobierno es obligada por su Política de Certificados a usar un esquema de auditoría interna diferente, puede usar tal esquema, desde que la auditoría (a) englobe todos los requisitos de uno de los esquemas arriba o (b) consista en criterios comparables que estén disponibles para revisión pública.

Cual sea el esquema escogido, debe incorporar procedimientos periódicos de monitoreo y/o rendición de cuentas para asegurar que sus auditorías sigan siendo conducidas de acuerdo con los requisitos del esquema.

La auditoría debe ser conducida por un Auditor Cualificado.

Para Terceros que no sean ARs, AC TECNISIGN debe recibir un reporte de auditoría, emitido de acuerdo con las normas de auditoría que fundamentan los esquemas de auditoría aceptados encontrados en la Sección 8.1, que da una opinión si el desempeño del Tercero está en conformidad con las políticas de la parte o políticas de VALID. Si la opinión es que el Tercero no está en conformidad, AC TECNISIGN no debe permitir que el Tercero siga desempeñando funciones delegadas.

El periodo de auditoría para el Tercero no debe exceder de un año (idealmente alineado con la auditoría de AC TECNISIGN). Sin embargo, si AC TECNISIGN o el Tercero estuviere en operación, control o supervisión de una Entidad Gubernamental y el esquema de auditoría fuere concluido a lo largo de varios años, la auditoría anual debe cubrir al menos los controles principales que son REQUERIDOS para ser auditados anualmente por tal esquema, incrementado de la parte de todos los controles no esenciales que pueden realizarse con menos frecuencia, pero en ningún caso cualquier control no esencial se puede auditar con menos frecuencia que una vez a cada tres años.

8.4.1 Auditoría de ARs

SE RECOMIENDA que las ARs que autorizan la emisión de certificados SSL se sometan a una auditoría anual en conformidad con sus obligaciones bajo VALID. Mediante solicitación de VALID, las ARs deben pasar por una auditoría observando cualesquier excepciones o irregularidades a las políticas de AC TECNISIGN y las medidas tomadas para remediar las irregularidades.

8.4.2 Auditoría de VALID y de un Afiliado

VALID y cada afiliada PUEDEN ser auditadas de acuerdo con las directrices provistas por el American Institute of Certificate Public Accounts para los Reportes de Service Organizations Control (SOC) sobre los riesgos asociados a las Organizaciones de Servicios. Sus Auditorías de Conformidad son WebTrust para Autoridades de Certificación o un estándar de auditoría equivalente aprobado por

VALID, que incluye Reporte de Políticas y Procedimientos en Operación y Prueba de Eficacia Operacional.

8.5 Acciones tomadas como resultado de la deficiencia

Después de recibir un reporte de auditoría de Conformidad, la Entidad Superior de la entidad auditada debe entrar en contacto con la parte auditada para discutir cualesquier excepciones o deficiencias presentadas por la Auditoría de Conformidad. VALID tiene el derecho de discutir dichas excepciones o deficiencias con la parte auditada. La entidad auditada y la Entidad Superior deben, de buena fe, usar esfuerzos comercialmente razonables para llegar a un acuerdo sobre un plan de acción correctiva para corregir los problemas que causan las excepciones o deficiencias e implementar el plan.

En caso de falla de la entidad auditada en desarrollar dicho plan de acción correctivo o implementarlo, o si el reporte revela excepciones o deficiencias que VALID y la Entidad Superior de la entidad auditada crean razonablemente representar una amenaza inmediata a la seguridad o integridad de VALID, entonces:

(a) VALID y/o la Entidad Superior deben determinar si una revocación y un relato de comprometimiento son necesarios;

(b) VALID y/o la Entidad Superior tienen el derecho de suspender los servicios de una entidad auditada; y

(c) Si fuere necesario, VALID y/o la Entidad Superior pueden terminar su contrato con la entidad auditada basándose en esa DPC.

8.6 Comunicación de los Resultados

El Reporte de auditoría DEBERÁ declarar explícitamente que engloba los sistemas y procesos relevantes usados en la emisión de todos los Certificados que posean uno o más de los OIDs relacionados en la Sección 7.1.6.1 de la PC.

Después de cualquier Auditoría de Conformidad, la entidad auditada debe proporcionar a VALID el reporte anual y certificados con base en su auditoría o auto auditoría en hasta 14 días tras la conclusión de la auditoría y en un máximo de 45 días después de la fecha del inicio de las operaciones.

AC TECNISIGN dispone su Reporte de auditoría anual en el plazo máximo de tres (3) meses tras el final del periodo de auditoría. En caso de un retraso superior a tres meses, VALID debe presentar una carta explicativa firmada por el Auditor Cualificado.

8.7. Auto Auditorías

8.7.1. Requisitos CABF de Auto Auditorías

Durante el periodo en que AC emite certificados, AC TECNISIGN debe monitorear la adherencia a esta DPC, su PC y controlar rigurosamente su calidad de servicio, realizando auto auditorías al menos trimestralmente, contra una muestra seleccionada aleatoriamente de por lo menos un certificado o al menos el 3% de los certificados emitidos por ella durante el periodo que comienza inmediatamente después de la muestra anterior a la auto auditoría que haya sido realizada. Excepto para Terceros que pasan por una auditoría anual que cumpla los criterios especificados en la Sección 8.1, AC TECNISIGN debe controlar rigurosamente la calidad de servicio de los certificados emitidos conteniendo informaciones verificadas por un Tercero o por ter un Especialista en Validación empleado por AC TECNISIGN. Auditorías trimestrales contra una muestra seleccionada aleatoriamente de por lo menos un certificado o el 3% de los certificados verificados por el Tercero en el periodo que se inicia inmediatamente después que la última muestra haya sido retirada. AC TECNISIGN debe rever las prácticas y procedimientos de cada Tercero para asegurar que el Tercero esté en conformidad con las DPC y PC relevante.
AC TECNISIGN DEBERÁ auditar internamente la conformidad de cada Tercero con estos requisitos anualmente.

Durante el periodo en que una AC subordinada emite certificados, AC que firmó el certificado de AC subordinada debe monitorear la adhesión a PC de su AC y la DPC de la AC subordinada. AC debe asegurar que los requisitos de la PC se están aplicando al menos trimestralmente, contra una muestra seleccionada aleatoriamente de por lo menos un certificado o por lo menos el 3% de los Certificados emitidos por AC Subordinada, durante el periodo que comienza inmediatamente después que la muestra de auditoría anterior haya sido tomada.

8.7.2. Requisitos CABF de la Auto Auditorías para certificados EV y Suscripción de Código EV

No se aplica.

9. Otros asuntos comerciales y legales

9.1 Tarifas

9.1.1 Emisión de Certificado o Tasas de Renovación

AC TECNISIGN tiene derecho de cobrar los usuarios finales por la emisión, gestión y renovación de Certificados.

9.1.2 Tarifas de Acceso al Certificado

VALID no cobra tarifas como condición para disponer las LCRs en un repositorio o en otras formas para las Partes Confiables.

9.1.3 Tarifas para Revocación o para Estatus de Certificado

VALID no cobra tarifas como condición para disponer las LCRs exigidas por la DPC en un repositorio o en otras formas disponibles para las Partes Confiables. Sin embargo, VALID tiene el derecho de cobrar una tarifa para proveer LCRs personalizadas, u otros servicios de informaciones de valor agregado de revocación y de estatus de certificados. VALID no permite el acceso a informaciones de revocación, informaciones de estatus de certificado o timbre de fecha/hora en sus repositorios por terceros que provean productos o servicios que utilicen esas informaciones de estatus del Certificado sin el consentimiento por escrito previo de VALID.

9.1.4 Tasas por otros servicios

AC TECNISIGN no cobra una tasa por el acceso a esta DPC. Cualquier uso hecho para otros fines que no sea la simple visualización del documento, como reproducción, redistribución, modificación o creación de trabajos derivados, DEBERÁ estar sujeto a un contrato de licencia con la entidad tenedora de los derechos de autor del documento. Las ACs emisoras pueden cobrar por otros servicios adicionales, como el servicio de timestamping.

9.1.5 Política de Devolución

En el subdominio de AC TECNISIGN, la siguiente política de devolución reproducida en www.tecnisign.com/cancelacion , está en vigor:

VALID se adhiere y está en conformidad con prácticas y políticas rigurosas en la realización de operaciones de certificación y emisión de certificados. Sin embargo, si por algún motivo un suscriptor no estuviere completamente satisfecho con el certificado emitido para él, el suscriptor puede solicitar que AC TECNISIGN revoque el certificado dentro de treinta (30) días de la emisión y de al suscriptor una devolución. Tras el periodo inicial de 30 (treinta) días, un suscriptor puede solicitar que AC TECNISIGN revoque el certificado y de una devolución si AC TECNISIGN viola una garantía u otra obligación material conforme esta PC relacionada al certificado del suscriptor. Después que VALID revoque el certificado del suscriptor, VALID abonará inmediatamente al suscriptor.

Para solicitar una devolución, contacte la atención al cliente en: www.tecnisign.com/cancelacion . Esta política de devolución no es un recurso exclusivo y no limita otros recursos que están disponibles para los suscriptores.

9.2 Responsabilidad Financiera

9.2.1 Cobertura de Seguro

VALID, afiliadas y ARs (en su caso) deben mantener un nivel comercialmente razonable de cobertura de seguro para errores y omisiones, sea por medio de un programa de seguro de errores y omisiones con una aseguradora o una retención auto asegurada. Este requisito de seguro no se aplica a entidades gubernamentales.

9.2.2 Otros Activos

VALID, Afiliadas y ARs deben tener recursos financieros suficientes para mantener sus operaciones y cumplir sus obligaciones, y ellos deben ser razonablemente capaces de asumir los riesgos de responsabilidad para los Suscriptores y Terceros de Confianza.

9.2.3 Cobertura de la garantía extendida

Algunos participantes de AC TECNISIGN ofrecen programas de garantía extendida que ofrecen a los suscriptores del certificado SSL protección contra pérdidas o daños debidos a un defecto en la emisión del certificado por el participante o a otras consecuencias causadas por la negligencia o violación de sus obligaciones contractuales, desde que el suscriptor del certificado o certificado cumplió sus obligaciones conforme el contrato de servicio aplicable. Los participantes de AC TECNISIGN que ofrecen programas de garantía extendida son NECESARIOS para incluir informaciones de programa en esta DPC.

9.2.4 Seguros para Certificados EV y Suscripción de Código EV

No se aplica.

9.3 Confidencialidad de las informaciones de negocio

9.3.1 Ámbito de Informaciones Confidenciales

Los siguientes registros de suscriptores deben, de acuerdo con la Sección 9.3.2, mantenerse confidenciales y privados (“Informaciones Confidenciales / Privadas”):

- Registros de solicitud de AC, aprobados o reprobados;
- Registros de solicitud de certificado;
- Registros transaccionales (registros completos y el camino de auditoría de las transacciones);
- Registros de camino de auditoría creados o retenidos por VALID;
- Reportes de auditoría creados por VALID (a medida que dichos reportes se mantengan) o por sus respectivos auditores (internos o públicos);
- Planificación de contingencia y planes de recuperación de desastres; y
- Medidas de seguridad que controlan las operaciones de hardware y software de VALID y la administración de servicios de certificados y servicios de solicitud.

9.3.2 Informaciones fuera del ámbito de Informaciones Confidenciales

Certificados, revocación de certificados y otras informaciones de estatus, repositorios de la e informaciones contenidas en ellos no son considerados Informaciones Confidenciales / Privadas.

Informaciones no expresamente consideradas Informaciones confidenciales / confidenciales de acuerdo con la Sección 9.3.1 deben ser consideradas confidenciales o privadas.

Esta sección está sujeta a las leyes de privacidad aplicables.

9.3.3 Responsabilidad de Proteger Informaciones Confidenciales

Los participantes de AC TECNISIGN que reciben informaciones privadas deben protegerlas de verse comprometidas y divulgadas a terceros.

9.4 privacidad de las informaciones personales

9.4.1 Plan de Privacidad

VALID y afiliadas deben implementar una política de privacidad de acuerdo con los requisitos internos de VALID. Tales políticas de privacidad DEBEN estar en concordancia con las leyes de privacidad locales aplicables. VALID y afiliadas no deben divulgar o vender los nombres de los usuarios de certificado u otras informaciones de identificación sobre ellos, sujetándose a la sección 9.3.2 y al derecho de una AC de transferir tales informaciones a una AC sucesora en los términos de la sección 5.8.

VALID implementó una Política de Privacidad, localizada en http://www.validcertificadora.com.br/politicadeprivacidade, en conformidad con esta sección.

9.4.2 Informaciones consideradas Confidenciales

Cualquier información sobre Abonados que no esté públicamente disponible a través del contenido del certificado emitido, directorio de certificados y LCRs online es tratada como privada.

9.4.3 Informaciones no consideradas Confidenciales

Sujetándose a las leyes locales, todas las informaciones tornadas públicas en un certificado no son consideradas privadas.

9.4.4 Responsabilidad de Proteger información confidencial

Los participantes de AC TECNISIGN que recibieren informaciones privadas deben protegerlas de verse comprometidas y ser divulgadas a terceros y deben cumplir con todas las leyes de privacidad locales en su jurisdicción.

9.4.5 Notificación y Consentimiento para utilización de informaciones Confidenciales

Salvo indicación en contrario en esta DPC, en la Política de Privacidad aplicable o por contrato, las informaciones privadas no serán usadas sin el consentimiento de la parte a quien esas informaciones se aplican.

Esta sección está sujeta a las leyes de privacidad aplicables.

9.4.6 Divulgación a pedido de proceso judicial o administrativo

VALID debe divulgar Informaciones Confidenciales / Privadas si, de buena fe, VALID crea que:

- la divulgación es necesaria en respuesta a intimaciones y órdenes de allanamiento;
- la divulgación es necesaria en respuesta a procesos judiciales, administrativos u otros procesos legales durante el proceso de descubrimiento en una acción civil o administrativa, como intimaciones, interrogatorios, solicitaciones de admisión y solicitaciones de producción de documentos.

Esta sección está sujeta a las leyes de privacidad aplicables.

9.4.7 Otras Circunstancias de Divulgación de Informaciones

Las políticas de privacidad DEBERÁN contener disposiciones relativas a la divulgación de Informaciones Confidenciales / Privadas a la persona que la divulgare a VALID o al afiliado.

Esta sección está sujeta a las leyes de privacidad aplicables.

9.5 Derechos de Propiedad Intelectual

La asignación de Derechos de Propiedad Intelectual entre los Participantes de Subdominio de VALID que no sean Abonados y Terceros de Confianza es regida por los acuerdos aplicables entre esos Participantes de Subdominio de VALID.

Las subsecciones subsiguientes a la sección 9.5 se aplican a los Derechos de Propiedad Intelectual en relación a los Abonados y Terceros de Confianza.

9.5.1 Derechos de Propiedad en informaciones de Certificados y revocación

Las ACs retienen todos los Derechos de Propiedad Intelectual sobre los Certificados e informaciones de revocación que ellas emiten. VALID concede permiso para reproducir y distribuir certificados en una base no exclusiva y libre de royalties, siempre y cuando sean reproducidos integralmente y que el uso de certificados esté sujeto al Contrato de Parte Confiable referido en el Certificado.

VALID concede permiso para usar las informaciones de revocación para ejecutar las funciones de la Parte Confiable, sujetas al Contrato de Uso de LCR aplicable, al Contrato de Parte Confiable o a cualquier otro contrato aplicable.

9.5.2 Derechos de Propiedad de la DPC

AC TECNISIGN y los participantes reconocen que VALID retiene todos los Derechos de Propiedad Intelectual en esta DPC.

9.5.3 Derechos de Propiedad para nombres

Un Solicitante de Certificado retiene todos los derechos que posee (si los hubiere) en cualquier marca registrada, marca de servicio o nombre comercial contenido en cualquier Solicitación de Certificado y *distinguished name* dentro de cualquier Certificado emitido para tal Solicitante de Certificado.

9.5.4 Derechos de Propiedad para Claves y Materiales afines

Los pares de claves correspondientes a los certificados de las ACs y de los usuarios finales son propiedad de las ACs y usuarios finales que son los respectivos Objetos de estos Certificados, independientemente del medio físico donde ellos son almacenados y protegidos, y tales personas poseen todos los derechos de propiedad intelectual referentes a estos pares de claves.
Sin limitar lo anteriormente expuesto, las claves públicas y certificados de AC Raíz son de propiedad de VALID. VALID licencia fabricantes de software y hardware para reproducir tales certificados de AC Raíz para colocar copias en dispositivos de hardware o software confiables.

Por último, *Secret Shares* de la clave privada de una AC son de propiedad de la AC, y la AC retiene todos los derechos de propiedad intelectual de tales *Secret Shares*, aunque no puedan obtener la posesión física de esas *Secret Shares* de AC TECNISIGN.

9.6 Representaciones y Garantías

9.6.1 Representaciones y Garantías de la AC

AC TECNISIGN garantiza que:

- No existe adulteración material conocida sobre los datos del Certificado u oriunda de las entidades que aprobaron la Solicitación de Certificado o emitieron el Certificado;
- No existen errores en la información en el certificado que fueron introducidas por las entidades que aprobaron la Solicitación de Certificado o emitieron el certificado como resultado de una falla en ejercer el debido cuidado en la Gestión de la Solicitación de Certificado o creación del certificado,
- Sus Certificados cumplen con todos los requisitos materiales de esta DPC y PCs aplicables; y
- Los servicios de revocación y el uso del repositorio atienden a todos los requisitos de esta DPC y PCs aplicables en todos los aspectos relevantes.

9.6.1.1 CABF Garantías y Obligaciones

Al emitir un certificado, AC TECNISIGN da las garantías enumeradas aquí para los siguientes Beneficiarios:

1. El Suscriptor que es parte en el Contrato de Abonado o en los Términos de Uso del Certificado;
2. Todos los Proveedores de Software de aplicación con quien la AC Raíz firmó un contrato para inclusión de su Certificado de AC Raíz en software distribuido por tal proveedor de Software de aplicativo; y
3. Todas las partes confiadas que razonablemente confían en un certificado válido.

AC TECNISIGN garantiza a los beneficiarios de certificados que, durante el período en que el certificado es válido, AC TECNISIGN cumplió estos Requisitos en su PC y en la DPC, para emisión y gestión del Certificado.

Las Garantías de Certificado incluyen específicamente y no taxativamente lo siguiente:

1. Derecho de Usar Nombre de Dominio o Dirección de IP: que, en el momento de la emisión, AC TECNISIGN
(i)implementó un procedimiento para verificar si el Requirente tenía el derecho de usar, o tenía el control del(os) Nombre(s) de Dominio y direcciones de IP enumeradas en el campo *Asunto* del Certificado y extensión s*ubjectAltNam*e (o, solamente en el caso de Nombres de Dominio, fue delegado tal derecho o control por alguien que tenía tal derecho de usar o controlar); (ii) siguió el procedimiento al emitir el Certificado; y (iii) describió con precisión el procedimiento en sus DPC y/o PC;

2. Autorización para el Certificado: que, en el momento de la emisión, AC TECNISIGN (i) implementó un procedimiento para verificar si el *Asunto* autorizó la emisión del Certificado y que el Requirente Representante está autorizado a solicitar el certificado en nombre del objeto del certificado; (ii) siguió el procedimiento al emitir el certificado; y (iii) describió con precisión el procedimiento en sus DPC y/o PC;

3. Precisión de la Información: que, en el momento de la emisión, AC TECNISIGN (i) implementó un procedimiento para verificar la exactitud de todas las informaciones contenidas en el Certificado (con excepción del campo *organizationalUnitName*); (ii) siguió el procedimiento al emitir el Certificado; y (iii) describió con precisión el procedimiento en sus DPC y/o PC;

4. Ninguna información engañosa: que, en el momento de la emisión, AC TECNISIGN (i) implementó un procedimiento para reducir la probabilidad de que las informaciones contenidas en el campo *organizationalUnitName* fuesen engañosas; (ii) siguió el procedimiento al emitir el certificado; y (iii) describió con precisión el procedimiento en sus DPC y/o PC;

5. Identidad del Requirente: que, si el certificado contuviere informaciones sobre la identidad del requirente, AC TECNISIGN (i) implementó un procedimiento para verificar la identidad del Requirente de acuerdo con la sección 3.2 de la PC; (ii) siguió el procedimiento al emitir el Certificado; y (iii) describió con precisión el procedimiento en sus DPC y/o PC;

6. Declaración de Titularidad: si AC TECNISIGN y el Suscriptor no fueren afiliados, el Abonado y AC TECNISIGN serán parte de un Contrato de abonado jurídicamente válido y aplicable que atienda a estos requisitos, o si AC TECNISIGN y el Abonado fueren la misma entidad o fueren afiliados, el representante del Requirente reconoció los Términos de Uso;

7. Status: AC TECNISIGN mantiene un Repositorio 24x7 públicamente accesible con informaciones actuales sobre el status (válido o revocado) de todos los certificados no expirados; y

8. Revocación: AC TECNISIGN revocará el certificado por cualquiera de las razones especificadas en sus DPC y/o PCs;

La AC Raíz será responsable por la performance y garantías de la AC Subordinada, en conformidad con esta DPC, y para todas las responsabilidades y obligaciones de indemnización de la AC Subordinada con esta DPC. Si la AC raíz fuese la AC subordinada que emite los contratos de abonados de certificados, puede incluir representaciones y garantías adicionales.

9.6.1.2 Garantías para Certificado EV

No se aplica.

9.6.1.3 Garantías para Certificado Code Signing EV

No se aplica.

9.6.2 Representaciones y Garantías de la AR

AC TECNISIGN y sus ARs garantizan que:

- No existen declaraciones falsas en el Certificado conocidas u originarias de las entidades que aprueban la Solicitación de Certificado o emiten el Certificado;
- No existen errores en las informaciones contenidas en el Certificado que fueron introducidas por las entidades que aprueban la Solicitación de Certificado como resultado de una falla en ejercer un cuidado razonable en la gestión de la Solicitación de Certificado;
- Sus Certificados atienden a todos los requisitos materiales de esta DPC y de la PC aplicable y
- Los servicios de revocación (cuando aplicable) y el uso de un repositorio atienden a todos los requisitos materiales de esta DPC y a la PC aplicable en todos los aspectos relevantes.

Contratos de suscriptor pueden incluir representaciones y garantías adicionales.

9.6.3 Representaciones y Garantías del Suscriptor

Los abonados garantizan que:

- Cada firma digital creada usando la clave privada correspondiente a la clave pública listada en el Certificado, y la firma digital del Suscriptor y el Certificado fue aceptado y se encuentra operacional (no expirado o revocado) en el momento en que la firma digital es creada;
- La clave privada está protegida y ninguna persona no autorizada tuvo acceso a la clave privada del Suscriptor;
- Todas las representaciones hechas por el Suscriptor en la Solicitación de Certificado enviada por el Abonado son verdaderas;

- Todas las informaciones proporcionadas por el Suscriptor y contenidas en el Certificado son verdaderas;
- El certificado está siendo usado exclusivamente para fines autorizados y legales, de acuerdo con todos los requisitos materiales de esta PC y del DPC aplicable; y
- El Suscriptor es un usuario final y no una AC, y no está usando la clave privada correspondiente a cualquier clave pública enlistada en el Certificado para fines de firmar digitalmente cualquier Certificado (o cualquier otro formato de clave pública certificada) o LCR, como una AC.

Contratos de suscriptor pueden incluir representaciones y garantías adicionales.

9.6.3.1 Requisitos CABF para Acuerdo de suscriptor

AC TECNISIGN exige, como parte del Contrato de Subscripción o Términos de Uso, que el Solicitante declare los compromisos y garantías en esta sección para el beneficio de AC TECNISIGN y de los Beneficiarios de la Certificación.

Antes de la emisión de un Certificado, AC TECNISIGN obtiene, para el beneficio expreso de AC TECNISIGN y de los Beneficiarios de la Certificación:

1. El acuerdo del Requirente al Contrato de suscriptor con AC TECNISIGN; o
2. El reconocimiento del Requirente de los Términos de Uso.

AC TECNISIGN implementa un proceso para garantizar que cada Contrato de suscriptor o Términos de Uso sea legalmente aplicable contra el Solicitante. En ambos casos, el Contrato debe ser aplicado al Certificado a ser emitido de acuerdo con el pedido de certificado.

AC TECNISIGN puede usar un contrato electrónico o "click-through", siempre y cuando VALID haya determinado que tales acuerdos son legalmente ejecutables. Un Contrato separado puede ser usado para cada solicitación de certificado, o un único Contrato puede ser usado para cubrir varias solicitaciones futuras de certificado y los Certificados resultantes, siempre y cuando cada Certificado emitido por AC TECNISIGN al Solicitante sea claramente cubierto por el Acuerdo o Términos de uso del Suscriptor.

El Contrato de Subscripción o los Términos de Utilización deben contener disposiciones que impongan al propio Requirente (o hecha por el Solicitante en nombre de su principal o agente bajo un subcontratado o lista de servicio de hospedaje) las siguientes obligaciones y garantías:

1. **Precisión de la Información:** la obligación y garantía de proporcionar informaciones precisas y completas en todo momento, tanto en la solicitación del certificado como conforme solicitado por AC TECNISIGN en conexión con la emisión del (os) Certificado(s) a ser proporcionados(s) por AC TECNISIGN;
2. **Protección de Clave Privada:** la obligación y garantía por parte del Requirente de tomar todas las medidas razonables para asegurar el control, mantener confidencial y proteger adecuadamente la Clave Particular que corresponde a la Clave Pública a ser incluida en el Certificado solicitado(s) (y cualquier dato o dispositivo de activación asociado, por ejemplo, contraseña o token);

3. **Aceptación del Certificado:** la obligación y garantía de que el Suscriptor revisará y verificará el contenido del Certificado en cuanto a su precisión;

4. **Uso del certificado:**

i. EV Certificates: No se aplica.
ii. EV Code Signing Certificate: No se aplica.

5. Reporte y Revocación: la obligación y garantía de solicitar rápidamente la revocación del Certificado, y dejar de usarlo y su Clave Privada asociada, en el caso de:

a. tener evidencias de que el certificado fue usado para firmar el código sospechoso - para Certificado de firma de Código EV;
b. cualquier información en el Certificado es, o se torna, incorrecta o imprecisa; o
c. existe cualquier abuso o compromiso real o sospechoso de los datos de activación principales o de la clave privada del Suscriptor asociada a la Clave Pública incluida en el Certificado;

6. **Término del Uso del Certificado:** la obligación y garantía de cesar inmediatamente todo uso de la Clave Privada correspondiente a la Clave Pública incluida en el Certificado en la revocación de ese Certificado por razones de Compromiso de Clave;

7. **Responsividad:** la obligación de responder a las instrucciones de AC TECNISIGN relativas al Compromiso de Claves o al uso indebido del Certificado dentro de un período de tiempo especificado;

8. **Confirmación y Aceptación:** reconocimiento y aceptación de que AC TECNISIGN tiene el derecho de revocar el certificado inmediatamente si el Requirente violare los términos del Contrato de Subscripción o Términos de Uso o si AC TECNISIGN descubriere que el Certificado está siendo usado para permitir actividades tales como ataques de phishing, fraude o la distribución de malware.

En el caso de certificado de firma de código EV: No se aplica.

9.6.4 Representaciones y Garantías de las Partes Confiables

No se aplica.

9.6.5 Representaciones y Garantías de Otros Participantes

No se aplica.

9.7 Exención de garantías

En la medida de lo permitido por la ley aplicable, los Contratos de abonados y Terceros de Confianza deben negar las posibles garantías de VALID, incluyendo cualquier garantía comercial o adecuación a una finalidad específica que esté fuera del contexto de la DPC de AC TECNISIGN.

9.8 Limitaciones de responsabilidad

En la medida que VALID emitió y gestionó el(os) certificado(s) en cuestión en conformidad con su Política de Certificados y su Declaración de Prácticas de Certificación, VALID no tiene responsabilidad con el Suscriptor, cualquier Parte Confiable o cualquier otro tercero por cualquier daño o perjuicio sufrido como resultado del uso o confianza en tales certificados. Las limitaciones de responsabilidad deben incluir una exclusión de daños indirectos, especiales, incidentales y consecuenciales. Ellos también deben respetar los límites de responsabilidad de cien dólares estadounidenses (USD 100,00) que acotan los daños de VALID y del afiliado.
La responsabilidad (y/o limitación de los mismos) de los Abonados debe ser según establecido en los Contratos de firma aplicables.

La responsabilidad (y/o limitación de la misma) de las ARs y la AC aplicable será establecida en el(os) contrato(s) entre ellas.

La responsabilidad (y/o limitación de la misma) de las Partes Confiadas será según establecido en los Contratos de Parte Confiable aplicables.

Para tareas delegadas, AC TECNISIGN y cualquier Tercero pueden asignar responsabilidad entre sí contractualmente en la medida que determinan, pero AC TECNISIGN permanece totalmente responsable por el desempeño de todas las partes de acuerdo con esta DPC y/o PC, como si las tareas no hubieren sido delegadas.

Si AC TECNISIGN hubiere emitido y gestionado el Certificado en conformidad con su DPC y PC, AC TECNISIGN se exime de la responsabilidad ante los Beneficiarios de la Certificación o cualquier otro tercero por cualquier pérdida sufrida como resultado del uso o confianza en tal Certificado especificadas en la DPC y PC de AC TECNISIGN.

Si AC TECNISIGN no emitió o gestionó el Certificado en conformidad con su PC y DPC, AC TECNISIGN procura limitar la responsabilidad del Suscriptor y a las Partes Confiadas, independientemente de la causa de la acción o de la teoría legal planteada, por todo y cualquier reclamo, pérdida o daño sufrido como resultado del uso o confianza en tal Certificado por cualquier medio apropiado que desee.
Si AC TECNISIGN elige limitar su responsabilidad por Certificados que no sean emitidos o gestionados en conformidad con su PC y DPC, AC TECNISIGN incluirá las limitaciones de responsabilidad en su DPC y PC de AC TECNISIGN.

9.8.1 Requisitos CABF de Limitaciones de responsabilidad

Para tareas delegadas, AC TECNISIGN y otros Terceros pueden asignar la responsabilidad por el desempeño contractual, pero la AC debe ser considerada como teniendo todas las obligaciones de acuerdo con estos requisitos, como si no hubieren sido ejecutadas como habiendo sido delegadas.

Si AC TECNISIGN gestionó el certificado en conformidad con los requisitos del CABF, DPC y PC, AC TECNISIGN se exime de responsabilidad ante los Beneficiarios de la Certificación o cualquier otro tercero por cualquier pérdida sufrida como resultado del uso o confianza en tales certificados más allá de aquellos especificados en la DPC y PC de AC TECNISIGN. Si AC TECNISIGN no hubiere emitido o gestionado el certificado en conformidad con los requisitos de la CABF y su PC y/o DPC, AC

TECNISIGN PODRÁ limitar su responsabilidad del Suscriptor y a las Partes Confiadas, independientemente de la causa de la acción o de la teoría jurídica planteada, por todo y cualquier reclamo, pérdida o daño sufrido como resultado del uso o confianza en tal certificado por cualquier medio apropiado que AC TECNISIGN desear. Si AC TECNISIGN optare por limitar su responsabilidad por certificados que no sean emitidos o gestionados en conformidad con los requisitos CABF, DPC y PC, la AC debe incluir las limitaciones de responsabilidad en la DPC y PC de AC TECNISIGN.

9.8.2 Limitaciones de Responsabilidad para EV

No se aplica.

9.9 Indemnizaciones

9.9.1 Indemnización por abonados

En la medida de lo permitido por la ley aplicable, los Abonados son llamados a indemnizar a VALID por:

- Falsedad o distorsión de hecho por el Suscriptor en la Solicitación del Certificado del Abonado;
- Falla del Suscriptor en divulgar un hecho relevante sobre la Solicitación del Certificado, si la declaración falsa u omisión hubiere sido hecha con negligencia o con la intención de engañar a cualquier parte;
- Falla del Suscriptor en proteger la clave privada del Abonado, en usar un Sistema Confiable o en tomar las precauciones necesarias para evitar el compromiso, la pérdida, la divulgación, la modificación o el uso no autorizado de la clave privada del Abonado; o
- Uso de un nombre por el Suscriptor (incluyendo, no taxativamente, un nombre común, nombre de dominio o dirección de e-mail) que infringe los Derechos de Propiedad Intelectual de un tercero.

El Contrato de Subscripción aplicable puede incluir obligaciones adicionales de indemnización.

Sin perjuicio de cualquier limitación a su responsabilidad para con los Abonados y Partes Confiadas, AC TECNISIGN entiende y reconoce que los Proveedores de Software de aplicación que poseen un contrato de distribución de Certificado Raíz en vigor con la AC Raíz no asumen ninguna obligación o responsabilidad potencial de AC TECNISIGN bajo estos requisitos o que, de otro modo, podría existir debido a la emisión o mantenimiento de Certificados o a la confianza depositada por Partes Confiadas u otros. Así, AC TECNISIGN defiende, indemniza y exime a cada Proveedor de Software de aplicación de todo y cualquier reclamo, daño y pérdida sufrida por tal Proveedor de Software de aplicativo relacionado a un certificado emitido por AC TECNISIGN, independientemente de la causa de la acción o de la teoría legal planteada. Eso no se aplica, sin embargo, a cualquier reivindicación, daño o pérdida sufrida por tal Proveedor de Software de aplicativo relacionado a un Certificado emitido por AC TECNISIGN cuando tal reclamo, daño o pérdida fue causado directamente por el software del Proveedor de Software de aplicativo exhibido como no confiable un certificado que aún sea válido o sea exhibido como confiable: (1) el certificado que haya expirado o (2) el certificado que fue revocado

(pero solo en los casos en que el status de revocación estuviere disponible en el momento online de AC TECNISIGN online y el software del aplicativo no hubiere verificado ese status o ignorado una indicación de status revocado).

9.9.2 Indemnización de las Partes Confiables

En la medida de lo permitido por la ley aplicable, los Contratos de Terceros de Confianza deben exigir que las Partes Confiadas indemnicen a VALID por:

- Falla del Terceros de Confianza para ejecutar las obligaciones de un Tercero de Confianza;
- La confianza de la Parte Confiable en un Certificado que no es razonable bajo las circunstancias; o
- La falla de la Parte Confiable en verificar el status de tal Certificado para determinar si el Certificado expiró o fue revocado.

El Contrato de Parte Confiable aplicable puede incluir obligaciones adicionales de indemnización.

9.9.3 Indemnización para Proveedores de Software

Sin perjuicio de cualquier limitación en su responsabilidad para con los Abonados y Terceros de Confianza, la AC entiende y reconoce que los Proveedores de Software Aplicativo que poseen un contrato de distribución del Certificado Raíz en vigor con la AC Raíz no asumen ninguna obligación o potencial responsabilidad de la AC bajo estos o que, de otra forma, pueda existir debido a la emisión o mantenimiento de Certificados o a la confianza depositada por Partes Confiadas u otros.

Así, la AC debe defender, indemnizar y eximir a cada Proveedor de Software de la aplicación de cualquier y toda reivindicación, daño y pérdida sufrida por tal Proveedor de Software de aplicativo relacionado a un Certificado emitido por la AC, independientemente de la causa de la acción o teoría legal planteada. Esto no se aplica, sin embargo, a cualquier reivindicación, daño o pérdida sufrida por tal Proveedor de Software de aplicativo relacionado a un Certificado emitido por la AC donde tal reclamo, daño o pérdida fue causado directamente por el software del Proveedor de Software de aplicativo exhibido como no confiable. Un certificado que aún es válido o exhibido como confiable: (1) un certificado que expiró o (2) un certificado que fue revocado (pero solo en los casos en que el status de revocación estuviere disponible en el momento en la AC online y el software del aplicativo falló al verificar ese status o ignoró una indicación de status revocado).

9.10 Validez y Término de la DPC

9.10.1 Alteración de la DPC

La DPC se torna efectiva después de la publicación en el Repositorio de AC TECNISIGN. Las alteraciones de esta DPC entran en vigor después de la publicación en el Repositorio de VALID.

9.10.2 Validez de la DPC

Esta DPC es alterada periódicamente y permanecerá en vigor hasta que sea substituida por una nueva versión.

9.10.3 Efecto después del Término de la PC

Aún después del término de esta DPC, los participantes de AC TECNISIGN son vinculados a estos términos para todos los certificados emitidos por el resto del período de validez de tales certificados.

9.11 Avisos individuales y comunicaciones con participantes

Salvo disposición en contrario por acuerdo entre las partes, los participantes del Subdominio de VALID deben usar métodos comercialmente razonables para comunicarse entre sí, teniendo en cuenta la importancia y el asunto de la comunicación.

9.12 Alteraciones

9.12.1 Proceso de alteración

Las alteraciones de esta DPC pueden ser efectuadas por la Autoridad de Gestión de Políticas de AC TECNISIGN. Las alteraciones deben ser presentadas en la forma de un documento que contenga una versión corregida de la DPC o de una actualización. Actualizaciones substituyen cualquier disposición designada o en conflicto de la versión referenciada de la DPC. El PMD debe determinar si las alteraciones en la DPC exigen una alteración en los object identifiers (OID) de las políticas de Certificado correspondientes a cada tipo de Certificado.

9.12.2 Mecanismo de Notificación y Periodicidad

VALID y la PMD se reservan el derecho de alterar la DPC sin notificación de alteraciones que no sean relevantes, incluyendo, no taxativamente, correcciones de errores tipográficos, alteraciones en URLs y alteraciones en las informaciones de contacto. La decisión del PMD de designar alteraciones como materiales o no materiales queda a criterio exclusivo del PMD.

El PMD deberá enviar a los Afiliados notificación de alteraciones materiales de la PC propuesta por el PMD. La nota debe indicar el texto de las alteraciones propuestas y el período para comentarios. Los Afiliados deben publicar o proporcionar un link para las alteraciones propuestas en sus propios repositorios dentro de un plazo razonable después del recibimiento del aviso de tales alteraciones.

El PMD solicita alteraciones propuestas de la DPC de otros participantes de AC TECNISIGN. Si el PMD considera a tal enmienda deseable y propone la implementación de la enmienda, el PMD debe notificar tal enmienda de acuerdo con esta sección.

Sin perjuicio de cualquier disposición de la PC en contrario, si el PMD cree que alteraciones materiales a la DPC son necesarias inmediatamente para interrumpir o impedir una violación de la seguridad de AC TECNISIGN o de cualquier parte de ella, VALID y el PMD tienen el derecho de realizar tales alteraciones por publicación en el Repositorio VALID. Tales alteraciones entrarán en vigor inmediatamente después de la publicación. Dentro de un plazo razonable después de la publicación, VALID debe notificar a los Afiliados sobre tales alteraciones.

9.12.2.1 Período para comentario

Excepto cuando indicado de otra forma, el plazo para cuestionar sobre alteraciones de la PC debe ser de 15 días, a partir de la fecha en que las variables fueren publicadas en el Repositorio de VALID. Cualquiera de los participantes de AC TECNISIGN tiene el derecho de enviar comentarios del PMD hasta el final del período de comentarios.

9.12.2.2 Mecanismo para lidiar con Comentarios

El PMD DEBE considerar cualquier comentario sobre las enmiendas propuestas. El PMD DEBE:

(a) permitir que las alteraciones propuestas entren en vigor sin alteración;

(b) enmendar las enmiendas propuestas y republicarlas como una nueva enmienda cuando REQUERIDO; o

(c) c) retirar las alteraciones propuestas.

La PMD tiene el derecho de retirar las alteraciones propuestas, notificando a los afiliados y proporcionando un aviso en la sección Actualizaciones y Avisos de Prácticas del Repositorio VALID. A menos que las enmiendas propuestas sean enmendadas o retiradas, ellas entrarán en vigor al término del período para comentarios.

9.12.3 Circunstancias en las cuales OID deben ser alterados

Si el PMD determina que una alteración es necesaria en el identificador de objeto correspondiente a una política de Certificado, la alteración DEBERÁ contener nuevos identificadores de objeto para las políticas de Certificado correspondientes a cada tipo de Certificado. De lo contrario, las alteraciones NO DEBEN exigir una alteración en el identificador de objeto de la política de certificados.

9.13 Provisiones para Resolución de Litigios

9.13.1 Disputas entre VALID, AR, Afiliados y Clientes

Las disputas entre uno o más involucrados DEBEN ser resueltas de acuerdo con las disposiciones de los acuerdos aplicables entre las partes.

9.13.2 Disputas con Abonados, usuarios finales o Partes Confiables

En la medida de lo permitido por la ley aplicable, los Términos de titularidad y Contratos de Parte Confiable deben contener una cláusula de resolución de disputas. Las disputas que involucran a VALID requieren un período inicial de negociación de 60 (sesenta) días, seguido por litigio en el tribunal de la ciudad sede de AC TECNISIGN.

9.14 Ley Aplicable

Sujeto a cualquier límite que conste en la legislación aplicable, las leyes de Brasil DEBERÁN regir la aplicabilidad, la construcción, la interpretación y la validez de esta PC, independientemente de contrato u otra elección de disposiciones legales. Esta elección de ley es hecha para asegurar procedimientos e interpretación uniformes para todos los Participantes de AC TECNISIGN, no importando donde ellos estén localizados.
Esta disposición de la ley aplicable se aplica solo a esta DPC. Acuerdos que incorporen la DPC por referencia pueden tener sus propias disposiciones de derecho administrativo, siempre que esta sección regule la aplicabilidad, la construcción, la interpretación y la validez de los términos de la DPC por separado e independiente de las demás disposiciones de tales acuerdos, sujeto a cualquier limitación apareciendo en la ley aplicable.

Esta DPC está sujeta a las leyes, reglas, reglamentos, resoluciones, decretos y órdenes nacionales, estaduales, locales y extranjeras aplicables, incluyendo, no taxativamente restricciones a la exportación o importación de software, hardware o informaciones técnicas.

Si un tribunal u órgano gubernamental con jurisdicción sobre las actividades cubiertas por las PCs y su DPC determina que el cumplimiento de cualquier requisito obligatorio es ilegal, tal requisito será considerado reformado en la medida mínima necesaria para tornar el requisito válido y legal. Esto se aplica solamente a operaciones o emisiones de certificados que están sujetas a las leyes de esa jurisdicción. Las partes involucradas deben notificar a CA/Browser Forum sobre los hechos, circunstancias y leyes involucradas, para que CA/Browser Forum pueda revisar sus directrices adecuadamente.

9.15 Conformidad con la ley aplicable

Esta DPC está sujeta a las leyes, reglas, reglamentos, resoluciones, decretos y órdenes nacionales, estaduales, locales y extranjeras aplicables, incluyendo, no taxativamente las restricciones sobre la exportación o importación de software, hardware o informaciones técnicas.

9.15.1 Conformidad con CABFORUM

No se aplica.

9.16 Disposiciones Diversas

9.16.1 Acuerdo Integral

No se aplica.

9.16.2 Atribución

No se aplica.

9.16.3 Desvinculación

En el caso de un conflicto entre estos requisitos y una ley, reglamento u orden gubernamental (en adelante denominada "Ley") de cualquier jurisdicción en la cual AC TECNISIGN opera o emite certificados, AC TECNISIGN puede modificar cualquier requisito en conflicto en la medida mínima necesaria para tornar el requisito válido y legal en la jurisdicción. Esto se aplica solamente a operaciones o emisiones de certificados sujetos a esa ley. En este caso, AC TECNISIGN debe inmediatamente (y antes de emitir un certificado bajo el requisito modificado) incluir en esta sección una referencia detallada a la Ley que exige una modificación de estos Requisitos bajo esta sección, y la modificación específica de estos Requisitos implementada por AC TECNISIGN.

9.16.3.1 CABF Requisitos de Desvinculación

AC TECNISIGN DEBE también (antes de emitir un certificado bajo el requisito modificado) notificar a CA/Browser Forum sobre las informaciones relevantes recién adicionadas a esta DPC, enviando un mensaje a **questions@cabforum.org** y recibiendo la confirmación de que él fue publicado en el Public Mailing List y es indexado en el Archivo de Mensajes Públicos disponible en**:** **https://cabforum.org/pipermail/public/** (u otras direcciones de e-mail y links que el Fórum puede designar), para que CA/Browser Forum pueda considerar posibles revisiones a estos requisitos en conformidad.

Cualquier modificación a la práctica de AC TECNISIGN habilitada en esta sección DEBE ser descontinuada si y cuando la Ley no se aplique más, o estos requisitos fueren modificados para posibilitar el cumplimiento de ambos y de la Ley simultáneamente. Una alteración apropiada en la práctica, la modificación en la DPC y de las PCs y un aviso en el CA/Browser Forum, conforme descrito arriba, DEBEN ser hechos en el plazo de 90 días.

9.16.4 Aplicación (Honorarios y Renuncia de Derechos de abogado)

No se aplica.

9.16.5 Fuerza Mayor

En la medida de lo permitido por la ley aplicable, los Términos de titularidad y Contratos de Parte Confiable deben incluir una cláusula de fuerza mayor que proteja a VALID y el Afiliado aplicable.

No se aplica.

Apéndice A: Tabla de siglas y acrónimos

Certificación en español	Certificación en ingles	Definición
Participante de la AC	AC Participant	Un individuo u organización que tiene uno o más de los siguientes roles en la infraestructura de AC: AC TECNISIGN, Afiliado, Cliente, Suscriptor o Parte Confiable
PKI AC	AC PKI	consiste en sistemas que colaboran para suministrar e implementar AC
Repositorio de la AC	AC Repository	base de datos de certificados y otra información relevante de la AC a la que se accede on-line
Estándares de la AC	AC Standards	Estándares legales y requisitos técnicos utilizadas por la AC para la emisión, administración, revocación, renovación y uso de Certificados
Administrador	Administrator	Una persona de confianza dentro de la organización de una AC o AR que ejecuta funciones de validación de la AR o AC
Certificado de administrador	Administrator Certificate	Un certificado emitido a un administrador que solo puede utilizarse para ejecutar funciones de AC o AR
Afiliado	Affiliate	Una tercera parte confiable (corporación, asociación, joint venture u otra entidad controladora, controlada o bajo control común con otra entidad) que entró en un acuerdo con AC TECNISIGN para ser una distribuidora de servicios o AR dentro de un territorio específico
AICPA	AICPA	Instituto Americano de Contadores Públicos Certificados
ANSI	ANSI	El American National Standards Institute
Solicitante	Applicant	La persona física o jurídica que solicita un certificado o su renovación. Una vez que se emite el certificado, el solicitante es referido como «Suscriptor». Para Certificados emitidos para dispositivos, el solicitante es la entidad que controla u opera el dispositivo nombrada en el certificado

Representante del Solicitante	Applicant Representative	Una persona física que representa al solicitante y que tiene Autoridad expresa para representar al solicitante: (i) que solicita el certificado en nombre del solicitante, o (ii) que firma y envía el Contrato de Suscriptor en nombre del Solicitante, o (iii) que reconoce y acepta los Termos de Uso del Certificado en nombre del Solicitante
Carta de certificación	Attestation Letter	Una carta que certifica determinada información en el proceso de solicitud del certificado
Período de Auditoría	Audit Period	el período comprendido entre el primer día (inicio) y el último día de operaciones (final) cubierto por el análisis. (lo que es diferente del período de tiempo en que los auditores están realizando la auditoría).
Informe de Auditoría	Audit Report	Un informe de un auditor cualificado afirmando opinión del auditor cualificado sobre si los procesos y controles de una entidad en conformidad con las disposiciones obligatorias de esas exigencias
Autorización de *Domain Name*	Authorization *Domain Name*	Autorización para uso del *Domain Name* usado en la emisión de certificado para un determinado

		FQDN.
Puerta autorizada	Authorized Port	Una de las puertas siguientes: 80 (http), 443 (http), 25 (SMTP), 22 (SSH).
Radical del *Domain Name*	Base *Domain Name*	La porción inicial del FQDN. Es el primero nudo a la izquierda de *Domain Name* (por ejemplo, "example.co.uk" o "example.com").
BIPM	BIPM	Bureau Internacional de Pesos y Medidas
BIS	BIS	(US Government) Bureau de Industria y Seguridad
Entidad de negocios	Business Entity	Cualquier entidad que no es una organización privada, entidad gubernamental o entidad no comercial como aquí definido. Ejemplos incluyen, pero no taxativamente, asociaciones generales, asociaciones no incorporadas, en nombre individual, etc.

AC	CA	Autoridad de Certificación
CAA	CAA	Certification Authority Authorization
ccTLD	ccTLD	Country Code Top-Level Domain
CEO	CEO	Chief Executive Officer
Certificado	Certificate	Un documento electrónico que usa criptografía para ligar una clave pública a una identidad. Contiene, al menos, el nombre de la AC emisora, identificación del Suscriptor, la clave pública del abonado, Período de validez del Certificado, un número de serie de certificado y es digitalmente firmado por la AC.
Solicitante de certificado	Certificate Applicant	Un individuo u organización que solicita la emisión de un certificado por una AC
Solicitación de certificado	Certificate Application	Un pedido de un Requirente a una autoridad de certificación para la emisión de un certificado
Aprobador del certificado	Certificate Approver	la persona física del requirente o un agente autorizado que ten autoridad expresa para representar el requirente: (i) actuar como un solicitador del certificado y autorizar otros empleados o terceros para actuar como un solicitador del certificado, y (ii) aprobar pedidos de certificado EV presentado por otros Requirentes de certificado.
Cadena de Certificados	Certificate Chain	Una lista ordenada de Certificados conteniendo al menos: (i) Certificado de usuario final, (ii) Certificado de la AC emisora. Si la AC emisora no es autofirmada, deberá contener el certificado de la AC que la emitió
Datos del certificado	Certificate Data	pedidos de certificados y datos relacionadas con el mismo (si obtenido a partir del Requirente o de otra forma) de posesión o control de la AC
Proceso de Gestión de los Certificados	Certificate Management Process	Procesos, prácticas y procedimientos relacionados con el uso de claves, software y hardware, por el cual AC verifica datos de certificados, emite certificados, mantiene un repositorio y revoca certificados
Política de Certificado (PC)	Certificate Policy (CP)	Un conjunto de reglas que indica la aplicabilidad de un certificado nombrado para una determinada comunidad y/o

		implementación de PKI con los requisitos de seguridad.

Relato de Problemas con Certificado	Certificate Problem Report	Queja de sospecha de compromiso de la clave, utilización indebida de certificados, u otros tipos de fraude, compromiso, mal uso, o por conducta inadecuada relacionadas con los certificados
Requirente del certificado	Certificate Requester	Una persona física que actúa como el requirente, un agente autorizado que tiene autoridad expresa para representar al requirente, o una tercera parte (como un ISP o empresa de hospedaje) que completa y envía una solicitación de Certificado EV en nombre del requirente.
Lista de Certificados Revocados (LCR)	Certificate Revocation List (CRL)	Una lista emitida periódicamente firmado digitalmente por una AC, con la identificación de los Certificados que fueron revocados antes de la fecha de validez, de acuerdo con la sección 3.4. La lista generalmente indica el nombre del emisor de la LCR, la fecha de emisión, la fecha de la próxima edición del LCR, números de serie de los certificados revocados, fecha de revocación y las razones específicas para la revocación
Solicitud de Firma de Certificado (CSR)	Certificate Signing Request (CSR)	Un mensaje conteniendo un pedido para emisión de un certificado
Autoridad de Certificación (AC)	Certification Authority (CA)	Una organización que es responsable por la creación, emisión, revocación y gestión de certificados. El término se aplica igualmente a las ACs Raíz y ACs subordinadas.
Autoridad de Certificación Autorizada (CAA)	Certification Authority Authorization (CAA)	Como descrito en RFC 6844 (http: tools.ietf.org/html/rfc6844): “Autoridad Certificadora Autorizada (CAA) Lista para cada DomainName la Autoridad de Certificación (AC) autorizada para emitir certificados para ese dominio. La publicación de la CAA permite que una AC pública implemente controles adicionales para reducir el riesgo de emisión indebida de certificados”

Declaración de Prácticas de certificación (DPC)	Certification Practice Statement (CPS)	Uno de los varios documentos que forman el cuadro de gobernanza en que los certificados son creados, emitidos, gerenciados y usados. AC TECNISIGN o una Afiliado emplea los requisitos de su DPC para aprobar o rechazar pedidos de certificado, emitir, gerenciar y revocar certificados.
AC TECNISIGN	AC TECNISIGN	Significa, en relación a cada sección de esta DPC, AC TECNISIGN Certificadora Digital SA
AC TECNISIGN AC ASOCIADA	AC TECNISIGN AC PARCERIA	La infraestructura de clave pública basada en certificado regido por AC TECNISIGN
Director Financiero	CFO	Director Financiero
Frase de desafío	Challenge Phrase	Una frase secreta elegida por el Solicitante durante la inscripción para un certificado. Cuando emitido un certificado, el Solicitante se torna un Suscriptor y una AC o AR puede usar la Frase de identificación para autenticar el Abonado cuando el abonado intenta revocar o renovar el Certificado del Abonado
CICA	CICA	Canadian Institute of Chartered Accountants
CIO	CIO	Chief Information Officer

CISO	CISO	Jefe de Información Security Officer
Auditoría de conformidad	Compliance Audit	Una auditoría periódica en una AC o AR, para determinar su conformidad con las normas que le son aplicables
Compromiso	Compromise	Una violación (o sospecha de violación) de una política de seguridad, en que una divulgación no autorizada o pérdida de control sobre informaciones confidenciales, puede haber ocurrido. Con relación a las claves privadas, un Compromiso es una pérdida, robo, divulgación, modificación, utilización no autorizada, u otro compromiso de la seguridad de la clave privada
Información Privada/Confidencial	Confidential/Private Information	Informaciones que deben ser mantenidas confidenciales y privadas conforme la sección 2.8.1
Pedido de confirmación	Confirmation Request	Una verificación utilizando otro medio de comunicación que el primariamente

		utilizado solicitando la confirmación del determinado hecho.
Persona confirmadora	Confirming Person	Un individuo dentro de la organización de un candidato de determinado hecho
Suscriptor del contrato	Contract Signer	Una persona física que es el requirente o un agente autorizado que tiene autoridad expresa para representar al requirente, y que tiene autoridad en nombre del requirente para firmar contratos de abonados.
Control	Control	"Control" (y sus significados correlativos, "controlado por" y "bajo el control") significa posesión, directa o indirectamente, del poder de: (1) orientar la gestión, personal, finanzas, o planes de tal entidad; (2) controlar la elección de una mayoría de la administración; o (3) votar esa parte de las acciones votantes necesarios para "control" bajo la ley de la jurisdicción de la entidad de incorporación o registro, pero en ningún caso menor de 10%.
COO	COO	Director de operaciones
País	Country	un miembro de las Naciones Unidas o una región geográfica reconocida como un estado soberano por al menos dos países miembros de la ONU.
PC	CP	Política de Certificación
CPA	CPA	Chartered Accountant Professional
DPC	CPS	Declaración de Prácticas de Certificación
LCR	CRL	Lista de Certificados Revocados
Contrato de Utilización de LCR	CRL Usage Agreement	Un acuerdo que establece los términos y condiciones bajo las cuales una LCR puede ser usada
Certificación cruzada	Cross Certificate	Un certificado que es usado para establecer una relación de confianza entre dos CAs Raíz
CSO	CSO	Director de seguridad
CSPRNG	CSPRNG	Un generador de números aleatorios utilizado en el sistema criptográfico.
Cliente	Customer	Una organización o persona física que es Cliente de AC TECNISIGN AC ASOCIADA

DBA	DBA	Nombre conocido de una empresa (“doing business as”
Tercero Delegado	Delegated Third Party	La persona física o jurídica que no es la AC, y cuyas actividades no están dentro del alcance de las auditorías de AC o AR, pero es autorizado por la AC para auxiliar en el proceso de gestión de certificados a través de la realización o cumplimiento de uno o más de los requisitos aquí encontrados.
Cuenta de depósitos	Demand Deposit Account	La cuenta de depósito mantenida en un banco u otra institución financiera, los fondos depositados en que son pagables en efectivo.
DNS	DNS	Domain Name System
Autorización del dominio	Domain Authorization	Correspondencia u otra documentación suministrada por persona/órgano comprobando la autoridad de un candidato para solicitar un certificado para un nombre de dominio específico
Documento de Autorización de dominio	Domain Authorization Document	Documentación proporcionada titular de Domain Name o la persona o entidad enlistada en el WHOIS como el Domain Name Requerent (incluyendo cualquier servicio de registro confidencial y anónimo, o proxy) que compruebe la autoridad de un candidato para solicitar un certificado para un nombre de dominio específico
Contacto del dominio	Domain Contact	El Titular, contacto técnico o contrato administrativo (o el equivalente bajo el ccTLD) del Domain Name como enlistado en la ficha WHOIS de la Base de Datos o en un registro de DNS SOA.
Nombre de dominio	Domain Name	El nombre atribuido a un nudo en el Domain Name System (DNS).
Propietario del Nombre de dominio	Domain Name Registrant	A veces referido como el “dueño” de un nombre de dominio, pero más propiamente la persona (s) o entidad (es) registrada como teniendo el derecho de controlar como un nombre de dominio es usado; la persona física o jurídica que estar enlistado como el “Requirente” por WHOIS u otro administrador de Domain Name nacional.

Registro de Dominio	Domain Name Registrar	La persona o entidad que registra nombres de dominio bajo los auspicios o por acuerdo con: (i) la Corporación de Internet para Atribución de Nombres y Números (ICANN), (ii) una autoridad / registradora nacional de Domain Name, o (iii) una Red de Información (incluyendo sus filiales, constructores, delegados, sucesores o cesionarios)
Namespace de dominio	Domain Namespace	El conjunto de todos los nombres de dominio posibles que están subordinados a un único nudo en la Domain Name System.
Fecha final	Entry Date	La fecha que define el fin del período de validez de un certificado.
EV	EV	extended Validation
EV Autoridad	EV Authority	Una fuente que no sea el Aprobador del Certificado, donde la verificación ocurre y que es expresamente autorizada para tomar las medidas descritas en estas directrices en relación a las solicitaciones de certificado EV
Certificado EV	EV Certificate	Un certificado digital que contiene informaciones previstas en las directrices “EV” y que han sido validados de acuerdo con las directrices

Beneficiarios de Certificado EV	EV Certificate Beneficiaries	Personas a quien la AC y su AC Raíz establece Garantías específicas para certificados EV
Reemisión de Certificado EV	EV Certificate Reissuance	El proceso por el cual un candidato que tiene un certificado EV válido (no expirado y no revocado) realiza un pedido a la AC que emitió el certificado EV original, para que un nuevo certificado EV sea emitido para el mismo nombre de organización y Domain Name antes del vencimiento del Certificado EV existente, pero con la validez final coincidente con la del Certificado EV actual
Renovación de Certificados EV	EV Certificate Renewal	El proceso por el cual un candidato que tiene un certificado EV válido (no expirado y no revocado) realiza un pedido a la AC que emitió el certificado EV original, para que un nuevo certificado EV sea emitido para el mismo nombre de organización y Domain Name antes del vencimiento del Certificado EV existente, pero con la validez final no coincidente con la del

		Certificado EV actual
Pedido de Certificado EV	EV Certificate Request	Un pedido de un candidato a la AC solicitando que sea emitido un certificado EV al Requirente, a través de pedido válidamente autorizado por el requirente y firmado por el Representante del requirente.
Garantías de Certificado EV	EV Certificate Warranties	En conjunto con la autoridad de certificación que emite un certificado EV, la AC y su raíz AC, garantizan, durante el período cuando el Certificado EV es válido, que la AC sigue los requisitos, las directrices y políticas EV de la AC para verificar la precisión de las informaciones contenidas en el Certificado EV y emitirlo
Certificado de Firma de Código EV	EV Code Signing Certificate	Un certificado que contiene informaciones especificadas para Firma de Código y fue validado de acuerdo con las orientaciones de "EV for Codesign"
Emisor de certificado de Firma de Código EV	EV Code Signing Certificate Issuer	La AC que emitió un Certificado de firma de Código EV para un suscriptor o una autoridad de firma
Objeto de certificado de Firma de Código EV	EV Code Signing Object	Un certificado de firma de código EV emitido por una AC
EV OID	EV OID	Un número de identificación, en la forma de un "identificador de objeto", que está incluido en el campo *CertificatePolicies* de un certificado que: (i) indica qué declaración de política AC respetó para ese certificado, y (ii) sea el identificador de política de EV CA / Browser Forum o un identificador de política que, por preacuerdo con una o más aplicaciones, marca el certificado como siendo un certificado EV.
Políticas EV	EV Policies	Prácticas, políticas y procedimientos para

		Certificados EV auditables, con una DPC y/o PC, que son desarrollados, implementados y ejecutados por la AC y su AC raíz
Procesos EV	EV Processes	Las claves, software, procesos y procedimientos por los cuales la AC verifica los datos bajo las directrices EV del CA / Browser Forum, emite Certificados, mantiene un repositorio y revoca

		certificados EV
Firma EV	EV Signature	Un archivo de datos electrónicos cifrado, que está anexado o lógicamente asociado a otros datos electrónicos, y que (i) identifica y está únicamente ligado al signatario de los datos electrónicos, (ii) es creado con medios que el signatario puede mantener bajo su control exclusivo y (iii) estar ligado de una forma, de modo que haga cualquier alteración subsiguiente que venga a ser hecha para los datos electrónicos detectables.
Validación Extendida	Extended Validation	Procedimientos de validación definidos por las directrices para Certificados Extended Validation publicados por un fórum constituido por las principales autoridades de certificación y proveedores de navegadores
FIPS	FIPS	Federal Information Processing Standard del Gobierno de los Estados Unidos de Norteamérica
FQDN	FQDN	Nombre de dominio totalmente cualificado
Nombre de dominio totalmente cualificado	Fully-Qualified Domain Name	Un nombre de dominio que incluye los rótulos de todos los nudos superiores en el DNS
gTLD	gTLD	Generic TopLevel Domain
Solicitación de certificado de Alto Riesgo	High Risk Certificate Request	Un pedido para que AC identifique como necesitando examen complementario en función de criterios internos y bancos de datos mantenidos por la AC, que puede incluir nombres con mayor riesgo de phishing u otro uso fraudulento, nombres contenidos en los pedidos de certificado anteriormente rechazados o revocados, la lista de Navegación Segura del Google, o

		nombres que AC identifica usando sus propios criterios de mitigación de riesgos
IANA	IANA	Internet Assigned Numbers Authority
EU ENLATO	ICANN	Internet Corporation for Assigned Names and Numbers
IFAC	IFAC	International Federation of Accountants
IM	IM	Mensaje instantáneo
Confirmación independiente del Requirente	Independent Confirmation From Applicant	La confirmación de un hecho en particular recibido por la AC en conformidad con las Informadas por el requirente.
Individual	Individual	Una persona física
Derecho de propiedad intelectual	Intellectual Property Rights	Derechos bajo uno o más de los siguientes: derechos de autor, patentes, secretos comerciales, marcas registradas y cualquier otro derecho de propiedad intelectual
Autoridad de Certificación intermedia	Intermediate Certification Authority	La Autoridad de Certificación cuyo Certificado está localizado dentro de una Cadena de Certificados entre el Certificado de la AC raíz y el Certificado de autoridad de certificación que emitió el certificado del Suscriptor
Nombre interno	Internal Name	La cadena de caracteres (no una dirección de IP) en los campos Common Name o Subject Alternative Name de un Certificado que no puede ser verificado dentro del DNS público en el momento de la emisión del certificado, pues no consta en dominios registrados en el banco de datos IANA.
Nombre del servidor interno	Internal Server Name	La Name Server (que puede o no incluir un nombre de dominio no registrado) que no puede ser

		resuelto usando el DNS público
Organización Internacional	International Organization	Una organización fundada por un documento constitutivo, por ejemplo, una carta, tratado, convención o documento semejante,

		firmado por, como mínimo, dos estados soberanos
ISO	ISO	International Organization for Standardization
ISP	ISP	Proveedor de internet (Internet Service Provider)
AC emitente	Issuing CA	En relación a un Certificado particular, la AC que emitió el certificado. Esta podría ser una AC raíz o una AC subordinada
compromiso de clave	Key Compromise	La clave privada se considera que está comprometida si su valor ha sido divulgado a una persona no autorizada, una persona no autorizada tuvo acceso a ella, o existe una posibilidad técnica por la cual una persona no autorizada puede descubrir su valor. La clave privada es también considerada comprometida si los métodos han sido creados permitiendo fácilmente calcularlo con base en la clave pública (como una clave débil Debian, ver http://wiki.debian.org/SSLkeys) o si hubiere evidencia clara de que el método específico usado para generar la clave privada fue fallido.
Ceremonia de Generación de Clave	Key Generation Ceremony	Un procedimiento donde es generado un par de claves de la AR de la AC o, su clave privada es transferida a un módulo criptográfico, su clave privada es backupeada, y/o su clave pública recibe un certificado.
Script de Generación de Clave	Key Generation Script	Un procedimiento documentado para la generación de un par de claves
Administrador del Gestión de Llaves	Key Manager Administrator	Un administrador que ejecuta las principales funciones de generación y recuperación en una infraestructura de claves públicas (PKI)
Par de Claves	Key Pair	La clave privada y su clave pública asociada
Entidad legal	Legal Entity	Una asociación, corporación, asociación, propiedad, confianza, entidad gubernamental u otra entidad con personalidad jurídica en un país

Existencia Legal	Legal Existence	Una organización privada, entidad gubernamental o entidad empresarial tiene existencia legal si ha sido válidamente constituida y no rescindida, disuelta o abandonada
Practicante legal	Legal Practitioner	Una persona que es un abogado como descrito en estas directrices y competente para emitir un parecer sobre las alegaciones del requirente
LSVA	LSVA	evaluación de vulnerabilidad de seguridad lógica
Autenticación manual	Manual Authentication	Un procedimiento donde las Solicitaciones de Certificado son evaluadas y aprobadas manualmente, una por una por un Administrador usando una interfaz web
NIST	NIST	Instituto Nacional de Estándares y Tecnología - National Institute of Standards and Technology (Gobierno de los EUA)
No repudio	Non-repudiation	Un atributo de una comunicación que la protege contra una parte que deslealmente negare su origen,

		negando que fue sometido, o negando su entrega. Nota: la excepción de los certificados ICPBRASIL, solo una sentencia en un tribunal o comisión de arbitraje pueden definitivamente garantizar el no repudio. Por ejemplo, una firma digital puede servir de prueba en una disputa de no repudio por un tribunal, pero no constituye por si sola prueba de no repudio
Informaciones del Suscriptor no verificadas	Non-verified Subscriber Information	Las informaciones sometidas por un Solicitante de Certificado a una AC o AR, e incluidas en un Certificado, que no hayan sido confirmadas por la AC o AR
Notario	Notary	Una persona legalmente constituida para autenticar la ejecución de una firma en un documento.
Identificador de Objeto	Object Identifier	Un identificador alfanumérico o numérico único registrado bajo el Órgano Internacional de Estandarización aplicable a un objeto específico o clase de objeto

OCSP	OCSP	Online Certificate Status Protocol – Protocolo online de estado del certificado
OCSP Responder	OCSP Responder	Un servidor online operado bajo la autoridad de la AC que responde por pedidos de estado de certificado.
AC offline	Offline CA	ACs Raíz y otras ACs intermedias que son mantenidos fuera del aire por razones de seguridad, a fin de protegerlos de posibles ataques de invasores por medio de la red. Esas ACs no emiten certificados de usuario final.
OID	OID	Object Identifier
AC online	Online CA	ACs que emiten certificados de usuario final son mantenidas online, de modo que brinden servicios de forma continua
Protocolo online de estado del certificado	Online Certificate Status Protocol	Un protocolo de verificación online de Certificados para proporcionar informaciones de status Certificado en tiempo real a las Partes Confiables
Período operacional	Operational Period	El período que se inicia con la fecha y hora en que un certificado es emitido (o a una fecha y hora indicada en el certificado) y termina con la fecha y la hora en que el certificado expira, si no ha sido anteriormente revocado
Controladora	Parent Company	Una empresa que controla a una empresa subsidiaria
PIN	PIN	Número de identificación personal
PKCS	PKCS	Public-Key Cryptography Standard
PKCS # 10	PKCS #10	Public-Key Cryptography Standard # 10, desarrollado por RSA Security Inc., que define una estructura para una Solicitación de Firma de Certificado
PKCS # 12	PKCS #12	Public-Key Cryptography Standard # 12, desarrollado por RSA Security Inc., que define un medio seguro para la transferencia de claves privadas
PKI	PKI	Public Key Infrastructure – Infraestructura de Claves Públicas

Lugar de negocios	Place of Business	La localización de cualquier instalación (como una fábrica, tienda, almacén, etc.) donde el negocio del candidato es conducido

PMD	PMD	Departamento de Gestión de Políticas
Departamento de Gestión de Políticas (PMD)	Policy Management Authority (PMD)	El área dentro AC TECNISIGN responsable por la construcción y aprobación de las políticas de AC
Clave privada	Private Key	La clave de un par de claves que es mantenida en secreto por el titular del par de claves, y que es usado para crear firmas digitales y/o para descriptografiar registros electrónicos o archivos que fueron criptografiados con la clave pública correspondiente
Organización privada	Private Organization	La entidad no gubernamental legal cuya existencia fue creada por un registro (o un acto) en una Agencia reguladora o el equivalente en el territorio
Clave pública	Public Key	La clave de un par de claves que pueden ser divulgadas públicamente por el titular de la clave privada correspondiente y que es utilizado por una parte Confiable para verificar firmas digitales creadas con la correspondiente clave privada del titular y/o para criptografiar mensajes para que ellos puedan ser descifrados solo con clave privada correspondiente del titular
Infraestructura de Claves Publicas	Public Key Infrastructure	La arquitectura, organización, técnicas, prácticas, procedimientos, hardware, software, personas, reglas, políticas y obligaciones que colectivamente soportan la implementación y operación de un sistema criptográfico de clave pública
Certificado públicamente confiable	Publicly-Trusted Certificate	Un certificado que es confiable en virtud del hecho que el certificado de la AC raíz correspondiente es distribuido como un ancla de confianza en aplicaciones ampliamente disponibles
QGIS	QGIS	Fuente de Información Cualificada del Gobierno - Qualified Government Information Source
QIIS	QIIS	Fuente de Información Independiente Cualificada - Qualified Independent Information Source
QTIS	QTIS	Fuente de Información Tributaria Cualificada del Gobierno - Qualified Government Tax Information

		Source
Auditor cualificado	Qualified Auditor	La persona física o jurídica que cumple con los requisitos de la sección 8.2 Identidad / Cualificaciones del Asesor
Fuente de Información Cualificado del Gobierno	Qualified Government Information Source	Un banco de datos mantenido por una entidad gubernamental (por ejemplo, archivos SEC) que cumple con los requisitos de la sección 11.11.6.
Fuente de Información Tributaria Cualificada del Gobierno	Qualified Government Tax Information Source	Un banco de datos mantenido por una entidad gubernamental que contiene específicamente informaciones fiscales relativas a organizaciones privadas, entidades empresarias, o individuos
Fuente de Información Independiente Cualificada	Qualified Independent Information Source	banco de datos proyectado con la finalidad de proporcionar con precisión las informaciones para las cuales es consultado, y que es generalmente reconocida como una fuente confiable de tales informaciones.
AR	RA	Autoridad de registro

Valor aleatorio	Random Value	Un valor especificado por la AC para el Requirente, que exhibe por lo menos 112 bits de entropía.
Nombre Registrado del Dominio	Registered Domain Name	Un nombre de dominio que fue registrado en un órgano de registro de dominio.
fuente confiable de datos	Reliable Data Source	un documento de identificación o fuente de datos usado para verificar Informaciones de Identidad que es generalmente reconocida entre las empresas comerciales y gobiernos como de confianza, y que fue creado por un tercero para otros fines que no son para que el requirente obtenga un certificado.
Domicilio oficial	Registered Office	El domicilio oficial de una empresa, como registrado en el órgano competente, adónde los documentos oficiales son enviados y donde avisos legales son recibidos.
Agencia de registro	Registration Agency	La Agencia Gubernamental que registra informaciones de negocios en relación a la formación de negocios de una entidad o autorización para realizar negocios bajo una licencia, carta u otra certificación

Autoridad de registro	Registration Authority	una entidad legal que es responsable por la identificación y autenticación de datos del certificado, pero no es una AC y, por tanto, no firma ni emite certificados. Una AR puede auxiliar en el proceso de solicitud de certificados o proceso de revocación o ambos.
Número de registro	Registration Number	El número único atribuido a una organización privada por el órgano competente
Institución financiera regulada	Regulated Financial Institution	una institución financiera que es regulada, supervisada, y examinada por órgano gubernamental, nacional, estadual o municipal, autoridades centrales o locales.
Método confiable de Comunicación	Reliable Method of Communication	Un método de comunicación, tal como un domicilio postal, número de teléfono o dirección de e-mail, que fue verificado utilizando una fuente alternativa al Requirente.
Parte Confiable	Relying Party	Cualquier persona física o jurídica que se basa en un certificado válido. Un proveedor de software aplicativo no es considerado una Parte Confiable pues el software distribuido por tales Proveedores solo exhibe informaciones relativas a un certificado.
Acuerdo de Parte Confiable	Relying Party Agreement	Un contrato usado para establecer los términos y condiciones en que un individuo u organización actúa como Tercero confiada en relación a los certificados.
Repositorio	Repository	Un banco de datos online que contiene documentos públicamente divulgados de la AC (tales como las políticas de certificación y declaraciones de Prácticas de Certificación) e informaciones de estado del Certificado, sea en la forma de una LCR o una respuesta OCSP
solicitación de token	Request Token	Un valor derivado en un método especificado por la AC que demuestra el control por el pedido de certificado. La solicitación de token debe incorporar la clave usada en el pedido de certificado. La solicitación de token puede incluir un timestamp

		para indicar cuando él fue creado. La solicitación de token puede incluir otras informaciones para garantizar su singularidad. La solicitación de token que incluye un timestamp permanecerá válido por no más de 30 días a partir del momento de la creación. La solicitación de token que incluye un timestamp debe ser tratada como inválida si su hora se encuentra en el futuro. La solicitación de token que no incluya un timestamp es válida para una única utilización y AC no deberá reutilizarlo para una validación posterior. La vinculación debe utilizar un algoritmo de firma digital o un algoritmo de hash criptográfico por lo menos tan fuerte como aquella a ser usada en la firma del pedido de certificado.
contenido requerido de la página de internet	Required Website Content	un valor aleatorio o una solicitación de token, en conjunto con informaciones adicionales que identifica el Suscriptor, conforme especificado por la AC.
Dirección de IP Reservada	Reserved IP Address	Una dirección de IPv4 o IPv6 que la IANA ha marcado como reservado: http://www.iana.org/assignments/ipv4-addressspace/ipv4-address-space.xml http://www.iana.org/assignments/ipv6-addressspace/ipv6-address-space.xml
Certificado minorista	Retail Certificate	Un certificado emitido por AC TECNISIGN, a individuos u organizaciones que solicitan uno por uno a AC TECNISIGN en su página de internet.
RFC	RFC	Pedido de comentarios - Request for comment
AC raíz	Root CA	Autoridad Certificadora Raíz
Certificado raíz	Root Certificate	El certificado autofirmado emitido por la AC raíz para identificarse y facilitar la verificación de los certificados emitidos por sus ACs subordinadas
Autoridad Certificadora Raíz	Root Certification Authority	La AC, que actúa como una AC raíz y emite certificados de ACs subordinadas a ella
Script de Generación de Clave Raíz	Root Key Generation Script	Un procedimiento documentado para la generación de un par de claves de AC raíz

RSA	RSA	Un sistema de criptografía de clave pública inventado por Rivest, Shamir y Adelman
S/MIME	S/MIME	Seguro MIME (extensiones multipropósito de correo de Internet - multipurpose Internet mail extensions)
SAR	SAR	Requisitos de Auditoría de Seguridad
SEC	SEC	Comisión de Valores Mobiliarios - Securities and Exchange Commission (Gobierno de los EUA)
Secreto Compartido	Secret Share	Una porción de una clave privada de la AC o una porción de los datos de activación necesarios para operar una clave privada de AC en régimen de secreto compartido
Secreto compartido	Secret Sharing	La práctica de separar la clave privada de la AC o los datos de activación para operar una clave privada de AC, a fin de reforzar el control de varias personas sobre las operaciones de clave privada de la AC bajo sección 6.2.2
Secure Sockets Layer	Secure Sockets Layer	El método estándar de la industria para proteger
		comunicaciones Web, desarrollada por Netscape Communications Corporation. El protocolo de seguridad SSL proporciona criptografía de datos, autenticación de servidor, integridad de mensaje y autenticación cliente opcional para una conexión TCP/IP
Revisión de Prácticas de Seguridad	Security and Practices Review	La revisión de un Afiliado, realizada por AC TECNISIGN antes que la filial sea autorizada para operar
SOC	SOC	Servicio de Control de Organización Estandarizado - Service Organization Control standard
Estado soberano	Sovereign State	Un estado o país que administra su propio gobierno, y no es dependiente, o sujeto a otro poder.
SSL	SSL	Secure Sockets Layer

Sujeto	Subject	La persona natural, dispositivo, sistema, unidad o entidad jurídica identificada en un Certificado como sujeto y titular de una clave privada correspondiente a una clave pública. El sujeto (asunto) es tanto el suscriptor cuanto un dispositivo bajo el control y operación del Abonado. El término "Asunto" puede, en el caso de un Certificado corporativo, consultar el equipamiento o dispositivo que contiene una clave privada. Un Titular es atribuido a un nombre exclusivo, que es vinculado a una clave pública contenida en el Certificado del Titular
Información de la Identidad del Asunto	Subject Identity Information	Informaciones que identifican el asunto del certificado. Las Informaciones de la Identidad del Asunto incluyen un nombre de dominio enlistado en la extensión subjectAltName o en el campo commonName
AC subordinada	Subordinate CA	Una autoridad de certificación cuyo certificado es firmado por la AC raíz, u otra AC subordinada
Assinante	Subscriber	en el caso de un certificado individual, una persona que es el asunto del y para el cual fue emitido un certificado. En el caso de un Certificado corporativo, una organización que posee el equipamiento o dispositivo que es el asunto del y para el cual fue emitido el Certificado. Un suscriptor es capaz, y está autorizado a usar la clave privada que corresponde a la clave pública enlistada en el Certificado
Contrato de suscriptor	Subscriber Agreement	Un acuerdo entre AC TECNISIGN AC ASOCIADA o la AR y el Requirente / Suscriptor que especifica los derechos y responsabilidades de las partes.
Empresa subsidiaria	Subsidiary Company	Una empresa que es controlada por una empresa madre.
Entidad Superior	Superior Entity	Una entidad por sobre otra entidad dentro de una PKI
Entidad Gubernamental Superior	Superior Government Entity	Con base en la estructura de gobierno en una subdivisión política, la entidad o entidades que tienen la capacidad de administrar,

		dirigir y controlar las actividades del Gobierno.
Revisión suplementaria de Gestión de Riesgo	Supplemental Risk Management Review	Una revisión de una entidad por AC TECNISIGN después del descubrimiento de datos incompletos o excepcionales en una Auditoría de Conformidad de la entidad o como parte del proceso general de

		gestión de riesgo
código sospechoso	Suspect code	Código que contiene funcionalidad maliciosa o vulnerabilidades serias, incluyendo spyware, malware y otro código que se instala sin el consentimiento del usuario y/o resiste su propia remoción, y código que puede ser explotado de formas no destinadas por sus designers para comprometer la confiabilidad de las plataformas en que él ejecuta.
Certificado de AC subordinado técnicamente limitado	Technically Constrained Subordinate CA Certificate	Un certificado de AC subordinado que usa una combinación de configuraciones de uso extendido de clave y configuraciones de restricción de nombre para limitar el ámbito en que la AC subordinada puede emitir Certificados de AC o usuario final adicionales.
Términos de uso	Terms of Use	Disposiciones relativas a la guarda y aceptación de uso de un certificado emitido en conformidad con esos requisitos cuando el requirente / Suscriptor es una filial de la AC o es la AC.
Certificado del test	Test Certificate	Un certificado con un período máximo de validez de 30 días, y que: (i) incluye una extensión crítica como especificado en la OID (2.23.140.2.1), o (ii) es emitida bajo una AC donde no existe cadena de certificado para un certificado de AC raíz sujeta a estos requisitos.
timestamp Authority	Timestamp Authority	Una organización que atribuye fecha y hora a datos, afirmando así que los datos existían en el tiempo especificado
TLD	TLD	Top-Level Domain
TLS	TLS	Transport Layer Security

Traductor	Translator	Un individuo o entidad empresarial que posee el conocimiento y la experiencia necesaria para traducir con precisión las palabras de un documento escrito en una lengua a la lengua nativa de la AC.
Persona de Confianza	Trusted Person	Un empleado, contratado o consultor de un área de AC TECNISIGN AC ASOCIADA responsable por la gestión de la infraestructura de la entidad, sus productos, sus servicios, sus instalaciones, y/o sus prácticas de acuerdo con lo dispuesto en la sección 5.2.1
Posición de Confianza	Trusted Position	Las posiciones dentro de un área de AC TECNISIGN AC ASOCIADA que debe ser poseída por una persona de confianza.
Sistema confiable	Trustworthy System	Hardware de computadora, software y procedimientos que son razonablemente seguros contra invasiones y abuso; proporcionando un nivel razonable de disponibilidad, confiabilidad y operación correcta; son adecuados para ejecutar las funciones pretendidas; y hacen cumplir la política de seguridad aplicables.
TTL	TTL	Tiempo de Vida – Time to Live
Nombre de Dominio no registrado	Unregistered Domain Name	Un nombre de dominio que no es un nombre de dominio registrado.
UTC (k)	UTC(k)	Tiempo Universal Coordinado - National realization of Coordinated Universal Time
certificado válido	Valid Certificate	Un certificado que pasó por el procedimiento de
		validación especificado en la RFC 5280
Especialistas de validación	Validation Specialists	Alguien que ejerce las funciones de validación de informaciones especificados por estos requisitos
Período de validez	Validity Period	El período de tiempo medido a partir de la fecha en que el certificado es emitido hasta la fecha de expiración
Parecer Legal Verificado	Verified Legal Opinion	Un documento que reúne los requisitos especificados en la sección 11.11.1 de estas directrices

Método de comunicación Verificada	Verified Method of Communication	El uso de un número de teléfono, un número de fax, una dirección de e-mail o dirección postal de entrega confirmada por la AC, de acuerdo con la sección 11.5 como una forma confiable de comunicarse con el Requirente.
Carta Profesional Verificada	Verified Professional Letter	Carta de Profesional Verificada
VOID	VOID	Voice Over Internet Protocol
Programa EV WebTrust	WebTrust EV Program	Los procedimientos de auditoría adicionales especificados para ACs que emiten certificados EV por la AICPA / CICA para ser usados en conjunto con su Programa WebTrust para Autoridades de Certificación
Programa WebTrust para ACs	WebTrust Program for CAs	La versión actual del Programa AICPA / CICA WebTrust para Autoridades Certificadoras
Seal WebTrust de confiabilidad	WebTrust Seal of Assurance	Una declaración de conformidad resultante del Programa WebTrust para ACs
Certificado Wildcard	Wildcard Certificate	Un certificado conteniendo un asterisco (*) en la posición más a la izquierda del campo Subject contenido en el certificado SSL
Nombre de Dominio Wildcard	Wildcard Domain Name	Un nombre de dominio que consiste en un único carácter asterisco seguido por un único carácter punto (“*”.) seguido por un nombre de dominio totalmente cualificado

Tabla. Siglas y definiciones

Apéndice B: Referencias

- CA/Browser Forum - Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates- version 1.6.7 (available at https://cabforum.org/baseline-requirementsdocuments/)
- CA/Browser Forum - Guidelines For The Issuance And Management Of Extended Validation Certificates – version 1.6.8 (available at https://cabforum.org/extended-validation/)
- ETSI EN 319 403, Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers.
- ETSI EN 319 411-1, Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements.
- ETSI TS 102 042, Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates.
- FIPS 140-2, Federal Information Processing Standards Publication - Security Requirements For Cryptographic Modules, Information Technology Laboratory, National Institute of Standards and Technology, May 25, 2001.
- ISO 21188:2006, Public key infrastructure for financial services -- Practices and policy framework.
  Network and Certificate System Security Requirements, v.1.0, 1/1/2013.
- NIST SP 800-89, Recommendation for Obtaining Assurances for Digital Signature Applications, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-89.pdf .
- RFC2119, Request for Comments: 2119, Key words for use in RFCs to Indicate Requirement Levels, Bradner, March 1997.
- RFC2527, Request for Comments: 2527, Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework, Chokhani, et al, March 1999.
- RFC3647, Request for Comments: 3647, Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework, Chokhani, et al, November 2003.
- RFC4366, Request for Comments: 4366, Transport Layer Security (TLS) Extensions, Blake-Wilson, et al, April 2006.
- RFC5019, Request for Comments: 5019, The Lightweight Online Certificate Status Protocol (OCSP) Profile for High-Volume Environments, A. Deacon, et al, September 2007.
- RFC5280, Request for Comments: 5280, Internet X.509 Public Key Infrastructure: Certificate and Certificate Revocation List (CRL) Profile, Cooper et al, May 2008.
- RFC6844, Request for Comments: 6844, DNS Certification Authority Authorization (CAA) Resource Record, Hallam-Baker, Stradling, January 2013.
- RFC6960, Request for Comments: 6960, X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP. Santesson, Myers, Ankney, Malpani, Galperin, Adams, June 2013.

- WebTrust for Certification Authorities , SSL Baseline with Network Security, Version 2.1, available at http://www.webtrust.org/principles-and-criteria/docs/item85228.pdf
- X.509, Recommendation ITU-T X.509 (10/2012) | ISO/IEC 9594-8:2014 (E), Information technology – Open Systems Interconnection – The Diretory: Public-key and attribute certificate frameworks.
- Ley Sobre Firmas Electrónicas Decreto N°,149-2013 publicado en el Diario Oficial LA GACETA el 11 de diciembre del 2013
- ACUERDO EJECUTIVO № 41-2014, emitido el 12 de diciembre del 2014 (Oficio SECM №155-2015) y publicado en el Diario Oficial LA GACETA el 21 de mayo del 2015