Gobierno de Reconciliación y Unidad Nacional

El Pueblo, Presidente!

MHCP

DIRECCIÓN GENERAL DE TECNOLOGÍA

MODELO DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN - DPC Y POLÍTICAS DE CERTIFICADOS - PC DE PROVEEDORES DE SERVICIOS DE CERTIFICACIÓN - PSC

Managua, junio 2023

CONTROL DE REVISIÓN Y ACTUALIZACIÓN (VERSIONES)

Nº	Fecha	Elaborado/ Entrevistado	Revisado	Aprobado	Autorizado
0	Octubre / 2016	Daysi Romero Responsable Departamento de Acreditación y Registro Yuri Dompe Responsable Departamento de Supervisión e Inspección Hans Espinoza Responsable Dirección Acreditación de Firma Electrónica	Hans Espinoza Responsable Dirección Acreditación de Firma Electrónica	Hans Espinoza Responsable Dirección Acreditación de Firma Electrónica	Esperanza Meza Responsable Dirección General de Tecnología
1	Septiembre / 2017	Daysi Romero Responsable Departamento de Acreditación y Registro	Hans Espinoza Responsable Dirección Acreditación de Firma Electrónica Yuri Dompe Responsable Departamento Supervisión e Inspección	Hans Espinoza Responsable Dirección Acreditación de Firma Electrónica	Esperanza Meza Responsable Dirección General de Tecnología
2	Octubre / 2020	Daysi Romero Responsable Departamento de Acreditación y Registro	Hans Espinoza Acuña Responsable Dirección Acreditación de Firma Electrónica Yuri Dompe Responsable Departamento Supervisión e Inspección	Hans Espinoza Responsable Dirección Acreditación de Firma Electrónica	Elba García Responsable Dirección General de Tecnología(a.i)
3	Junio / 2023	Daysi Romero Responsable Departamento de Acreditación y Registro	Hans Espinoza Responsable Dirección Firma Electrónica Yuri Dompe Responsable Departamento de Supervisión e Inspección	Hans Espinoza Responsable Dirección Firma Electrónica	José Díez Responsable Dirección General de Tecnología

MINISTERIO DE HACIENDA Y CRÉDITO PÚBLICO
DGTEC-MHCP
DIRECCIÓN GENERAL

ÍNDICE

I. INTRODUCCIÓN

La Dirección General de Tecnología - DGTEC del Ministerio de Hacienda y Crédito Público - MHCP ha elaborado el presente documento "Modelo de la Declaración de Prácticas de Certificación - DPC y Política de Certificado - PC de Proveedores de Servicios de Certificación – PSC", estructurado en términos generales de acuerdo con la norma técnica IETF RFC 3647, con el propósito de brindar un modelo estándar para guiar a los PSC en elaborar la DCP o PC y que a su vez cumplan con los estándares correspondientes y tengan un alcance internacional. El modelo proporciona una lista completa de temas que potencialmente deben cubrirse en una Declaración de Prácticas de Certificados o una Política de Certificado.

II. JUSTIFICACIÓN DE VERSIÓN

Se generó una nueva versión de este documento, actualizándose los siguientes puntos:

Sección a actualizar	Justificación	Servidor Público/Cargo que solicitó la actualización
Todo el documento.	- Se ajustó la redacción a todo el documento.	Hans Espinoza Responsable Dirección Firma Electrónica.
	- Se realizaron ajustes y actualizaciones en base a revisiones de estándares internacionales, solicitadas.	Hans Espinoza Responsable Dirección Firma Electrónica.
Capitulo IX: Anexos.	- Se agregó el anexo 1: "Estándares Relacionados". - Se ajustó el anexo 2: "Referencia cruzada del contenido de este documento, RFC 3647 y estándares relacionados".	Hans Espinoza Responsable Dirección Firma Electrónica.

III. OBJETIVO

Establecer la estructura de componentes del contenido mínimo para la elaboración y estructuración de la Declaración de Prácticas de Certificación o Políticas de Certificados de los Proveedores de Servicios de Certificación.

IV. BASE LEGAL

- Ley No.729 "Ley de Firma Electrónica", publicada en la Gaceta Diario Oficial No. 165 del 30 de agosto del 2010.
  Arto.15. Entidad Rectora de Acreditación de Firma Electrónica.

- Decreto Presidencial No. 57-2011 "Reglamento de Ley 729 – Ley de Firma Electrónica", publicado en la Gaceta Diario Oficial No. 211 del 8 de noviembre del 2011.
  Arto. 12. inciso 3.
  Arto. 14.
  Arto. 17. La Entidad Rectora definirá el contenido de la Declaración de Prácticas de Certificación.
  Arto. 20. inciso 2.
  Arto. 22. inciso 2, inciso 3, inciso 6.
  Arto. 37.

V. GLOSARIO DE TÉRMINOS Y SIGLAS

Los siguientes términos se encuentran definidos en la Ley No.729 Ley de Firma Electrónica:

Certificado: Certificación electrónica que vincula unos datos de verificación de firma a una persona y confirma la identidad de esta.

Firma Electrónica: Son datos electrónicos integrados en un mensaje de datos o lógicamente asociados a otros datos electrónicos que puedan ser utilizados para identificar al titular en relación con el mensaje de datos e indicar que el titular aprueba la información contenida en el mensaje de datos.

Firma Electrónica Certificada: Es la que permite identificar al titular y ha sido creada por medios que este mantiene bajo su exclusivo control de manera que vinculada al mismo y a los datos a los que se refiere permite que sea detectable cualquier modificación ulterior a estos.

Proveedor de Servicios de Certificación: Entidades que otorgan, registran, mantienen y publican los Certificados de Firma Electrónica, para lo cual generan, reconocen y revocan claves en forma expedita y segura, siendo personas jurídicas que pueden prestar otros servicios relacionados con la firma electrónica.

Titular: Es la persona que posee los datos de creación de firma y que actúa en nombre propio o de la persona que representa.

Los siguientes términos se encuentran definidos en el Decreto No. 57-2011 reglamento de la Ley No. 729 Ley de firma electrónica:

Autoridad de Certificación: Son aquellas a las cuales uno o más usuarios han confiado la creación y asignación de certificados de firma electrónica certificada.

Autoridad de Registro: Entidad delegada por el certificador registrado para la verificación de la identidad de los solicitantes y otras funciones dentro del proceso de expedición y manejo de certificados de firma electrónica certificada. Representa el punto de contacto entre el usuario y el certificador registrado.

Declaración de Prácticas de Certificación: Manifestación del Proveedor de Servicios de Certificación sobre las políticas y procedimientos que aplica para la prestación de sus servicios.

Los siguientes términos se encuentran definidos en la Recomendación Estándar Internacional ISO/IEC 27099:

Autenticación: Suministro de garantía de que la identidad alegada de una entidad es correcta.

Autoridad de Política: Parte u organismo con la autoridad final y la responsabilidad de especificar las políticas de certificación.

Parte que Confía: Destinatario de un certificado que actúa basándose en ese certificado, firmas digitales[1] verificadas usando ese certificado, o ambos.

Política de Certificado: Conjunto de reglas con nombre que indica la aplicabilidad de un certificado a una comunidad particular o clase de aplicación con requisitos de seguridad comunes.

Suscriptor: Entidad que se suscribe con una autoridad de certificación en nombre de uno o más sujetos.

[1] Firma electrónica basada en certificado.

Los siguientes términos se encuentran definidos en la Recomendación RFC 3647:

Datos de activación: Valores de datos, distintos de las claves, que se requieren para operar módulos criptográficos y que deben protegerse (por ejemplo, un PIN, una contraseña o una clave compartida manualmente colocada).

Identificación: El proceso de establecer la identidad de un individuo o una organización. En el contexto de una infraestructura de clave pública, la identificación se refiere a dos procesos:

- Establecer que un nombre propio de una persona u organización corresponde a una identidad en el mundo real de un individuo u organización.
- Establecer que un individuo u organización que solicite o que buscan el acceso a algo bajo ese nombre es, de hecho, el individuo nombrado u la organización que especifica.

Participante: Una persona u organización que desempeña un rol dentro de una Infraestructura de Clave Pública como suscriptor, parte que confía, Autoridad de Certificación y Autoridad de Registro.

Validación: El proceso de identificación de los solicitantes de certificados. "Validación" es parte de la "identificación" y se refiere a la identificación en el contexto del establecimiento de la identidad de los solicitantes de certificados.

Las siguientes siglas/acrónimos son definidos o complementados en esta normativa:

AC: Autoridad de Certificación.

AP: Autoridad de Política.

AR: Autoridad de Registro.

DGTEC: Dirección General de Tecnología.

DPC: Declaración de Prácticas de Certificación.

IEC: Comisión Electrónica Internacional - International Electrotechnical Commission.

IETF: Grupo de Trabajo de Ingeniería de Internet - Internet Engineering Task Force.

INCP: Infraestructura Nicaragüense de Clave Pública.

ISO: Organización Internacional de Normalización - International Standardization Organization.

LAV: Listas de Autorización y Validación.

LCR: Lista de Certificados Revocados.

OID: Identificador de Objeto - Object Identifier.

PC: Política de Certificado.

PECL: Protocolo de Estado del Certificado en Línea.

PSC: Proveedor de Servicio de Certificación.

RFC: Solicitud de Comentarios -Request For Comment.

SEI - CMM: Modelo de Madurez de Capacidad del Instituto de Ingeniería de Software - Software Engineering Institute´s Capability Maturity Model.

SGSI: Sistema de Gestión de Seguridad de la Información.

TSDM: Metodología de Desarrollo de Software Confiable – Trusted Software Development Methodology.

UIT: Unión Internacional de Telecomunicaciones.

URL: Localizador de Recursos Uniforme - Uniform Resource Locator.

Formas verbales

Las formas verbales que se muestran a continuación, son usadas para indicar requisitos, recomendaciones, permitidos y excepcionalidades que deben seguirse para poder cumplir con lo establecido en este documento.

Excepcionalidades: Puede, Posible, No puede.

Requisito: Debe, Requerido, No debe.

Recomendación: Debería, Recomendado, No debería.

Permitido: Podría, Permitido, Opcional, No es necesario. Adicionalmente texto escrito entre corchetes “[ ]” se considerara opcional.

VI. CONSIDERACIONES GENERALES

Declaración de Prácticas de Certificación - DPC y Política de Certificados - PC

La PC establece un conjunto de reglas que describe la aplicabilidad de un certificado dentro de una comunidad específica o clase de aplicación, es un conjunto de reglas con respecto al nivel de confianza que cumplen Personas Usuarias de certificados asociados para un propósito particular. También especifica los criterios acordados y cumplidos por una autoridad de certificación antes de que los certificados utilizados por dicha autoridad de certificación puedan ser aceptados por una parte que confía.

La DPC proporciona una descripción detallada de los procedimientos y controles implementados por la AC para emitir, administrar, revocar, renovar o cambiar las claves de los certificados con el propósito de cumplir con los requisitos de la PC, mientras que una PC es más general.

El propósito de la DPC es definir claramente los procedimientos y prácticas de las AC para gestionar los riesgos asociados con las PC.

La AC es la entidad responsable de realizar los seis componentes de servicios: a) registro, b) fabricante del certificado, c) difusión, d) gestión de revocación, e) servicio de estado de revocación y f) suministro del dispositivo sujeto (opcional), así como también la AC es responsable de definir los controles para lograr

que los componentes de servicios cumplan con los requisitos establecidos en la PC, estos están documentados en la DPC.

El propósito de la PC es establecer qué deben hacer las personas participantes. Por el contrario, la DPC establece cómo una AC[2] y otras Personas Participantes en un dominio determinado implementan procedimientos y controles para cumplir con los requisitos establecidos en la PC. El propósito de la DPC es revelar cómo los participantes realizan sus funciones e implementan controles.

Las principales diferencias entre las PC y la DPC son:

- La ICP utiliza la PC para definir los requisitos que establecen lo que deben hacer personal participante dentro de ella. Una sola AC u Organización puede usar una DPC para revelar cómo cumple con los requisitos de una PC o cómo implementa sus prácticas y controles.

- La PC facilita la interoperación mediante certificación cruzada, certificación unilateral u otros medios. Por lo tanto, está destinado a cubrir varias AC. Por el contrario, la DPC es una declaración de una única AC u Organización, su propósito no es facilitar la interoperación (ya que hacerlo es función de una PC).

- La DPC es generalmente más detallada que la PC y especifica cómo la AC cumple los requisitos especificados en una o más PC bajo las cuales emite certificados.

VII. ESTRUCTURA DE LA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN Y POLÍTICA DE CERTIFICADO

La DPC y la PC deben estar redactadas en idioma español, así como también se debe entregar una copia de la versión en inglés correspondiente a la versión oficial exacta redactada en español, debe utilizarse de referencia el Anexo 2: “Referencia cruzada del contenido de este documento, el RFC 3647 y estándares relacionado”, la columna: RFC 3647.

Es necesario que se respete la numeración y orden de los componentes, inclusive cuando uno de ellos no sea considerado por una DPC o una PC, este debe ponerse y especificarse con un “omitido” (facilitando la información correspondiente al Ente Rector), o en otro caso indicar donde se puede encontrar la información requerida. Esto con el fin de garantizar la estandarización y de facilitar la comparación de DPC y PC con otras autoridades certificadoras nacionales e internacionales.

Los PSC nacionales deben basar su estructura en la estructura de la DPC y de la PC recomendada a continuación en el presente documento y especificar cualquier cláusula o requisito adicional según sus necesidades, adicionándolos posterior a la estructura recomendada con una numeración distinta a esta estructura, o bien puede agregar cláusulas adicionales sin numeración.

Los PSC extranjeros deberían basar su estructura de DPC y de PC con la estructura recomendada por su respectivo Ente Rector o cualquiera de las referenciadas en el Anexo 2: “Referencia cruzada del contenido de este documento, el RFC 3647 y estándares relacionados”.

La estructura de la DPC y la PC debería estar conformada con los siguientes componentes y subcomponentes, respetando la siguiente numeración:

[2] Para entender la relación entre AC y PSC refiérase al documento Modelo de Confianza para Firma Electrónica Certificada.

1. INTRODUCCIÓN

Este componente identifica e introduce el conjunto de disposiciones e indica los tipos de entidades y aplicaciones para las cuales el documento está dirigido (ya sea si se está definiendo la política de certificado o la declaración de prácticas de certificación).

1.1 Información general

Este subcomponente ofrece una introducción general al documento que se está redactando. Este subcomponente también se puede utilizar para proporcionar una sinopsis de la Infraestructura de Clave Pública a la que se aplica la Política de Certificado - PC o Declaración de Prácticas de Certificación - DPC.

1.2 Nombre e identificación del documento

Este subcomponente proporciona los nombres aplicables u otros identificadores, incluyendo los identificadores de objeto ASN.1, para identificar el documento. Debería contener como mínimo lo siguiente:

CAMPO	CONTENIDO
Nombre del documento	Para la DPC: Declaración de Prácticas de Certificación [de Nombre de la AC]. Para la PC: Política de Certificado de Nombre del Certificado.
Versión del documento	Permite identificar la cantidad de actualizaciones del documento.
Estado del documento	Para identificar la aprobación o no y la vigencia del documento.
Fecha de emisión	Fecha en que se emite el documento.
Fecha de expiración	Fecha en que expira el documento.
Localización / URL	Lugar o sitio en internet desde donde se descarga el documento.
Identificador único de objeto (OID)	Identificador único del documento, este debe de ser asignado en base a la “Normativa de Conformación de Identificadores de Objetos en Nicaragua”.

1.3 Participantes de la ICP

Este subcomponente describe la identidad o tipos de entidades que toman un rol de participante dentro de una Infraestructura de Clave Pública, nombrados:

1.3.1 Autoridades de certificación

Se identificarán a una autoridad de certificación como una autoridad emisora con respecto a los certificados que emite y es la autoridad certificadora sujeto en relación con el certificado de la autoridad de certificación que se le ha emitido.

Las autoridades de certificación dentro de la INCP deben estar organizadas de acuerdo al “Modelo de Confianza para Firma Electrónica Certificada”.

1.3.2 Autoridades de registro

Se identificarán a las entidades que establecen los procedimientos de inscripción para los solicitantes de certificados de usuario final, realiza la identificación y autenticación de los solicitantes de certificados, recibe y tramita solicitudes de revocación de certificados y realiza trámites de renovación en nombre de una autoridad de certificación.

1.3.3 Suscriptores

Se identificarán a las personas físicas o jurídicas, equipos u aplicaciones que reciben certificados de la autoridad de certificación.

1.3.4 Partes que confían

Se identifican a las personas físicas o jurídicas, entidades u organizaciones, administración pública, que de forma voluntaria aceptan y confían en los certificados electrónicos, en las firmas electrónicas provenientes de los Proveedores de Servicio de Certificación. Las partes que confían pueden o no pueden ser suscriptor dentro de la Infraestructura de Clave Pública.

1.3.5 Otros participantes

Se identificarán otras entidades que provean servicios relacionados a Infraestructura de Clave Pública, tales como los PSC.

1.4 Usos del certificado

En el caso que una PC o DPC describen diferentes niveles de seguridad, este subcomponente puede describir las aplicaciones o tipos de aplicaciones que son apropiados o inapropiados para los diferentes niveles de seguridad.

1.4.1 Usos apropiados del certificado

El Proveedor de Servicios de Certificación especifica los usos permitidos para los certificados que emite a sus suscriptores. Este subcomponente puede describir aplicaciones o tipos de aplicaciones apropiados o inapropiados para los diferentes niveles de seguridad.

1.4.2 Usos prohibidos del certificado

El PSC enlista los tipos de aplicaciones para las cuales el uso del certificado emitido es prohibido o indica que cualquier otro uso no descrito en el subcomponente 1.4.1 no es permitido.

1.5 Administración de políticas

1.5.1 Organización que administra el documento

Este subcomponente incluye información correspondiente a la organización responsable de la elaboración, el registro, mantenimiento y actualización de la DPC o la PC, como son:

- Nombre de la Organización del PSC.
- Correo electrónico.
- Dirección de la Organización.
- Número telefónico.
- Sitio Web de la Organización.

1.5.2 Persona de contacto

Este subcomponente incluye el nombre de la autoridad responsable para el registro, mantenimiento de los certificados electrónicos e incluye lo siguiente:

- Nombre del contacto.
- Correo electrónico.
- Dirección domiciliar.
- Número telefónico.
- Sitio de Internet.

1.5.3 Persona que determina la idoneidad de la DPC para la política

Este subcomponente debería de incluir información de la AP responsable de determinar si una AC puede operar dentro de la ICP o interoperar con ella, y además es responsable de aprobar que la Declaración de Práctica de Certificación es adecuada para la Política de Certificado, este subcomponente debe incluir:

- Nombre.
- Correo electrónico.
- Número de teléfono.
- Otra información generalizada.

Este subcomponente debe estar presente en la DPC y podría omitirse en la PC.

1.5.4 Procedimientos de aprobación de la DPC

Este subcomponente incluye los procedimientos mediante los cuales se aprueba la Declaración de Prácticas de Certificación, dicha aprobación avala que la AC puede operar o interoperar en una ICP.

Este subcomponente debe estar presente en la DPC, y podría omitirse en la PC

1.6 Definiciones y acrónimos

Este subcomponente contiene una lista de términos definidos que se utilizan en el documento, así como una lista de siglas con sus significados utilizados en el documento.

2. RESPONSABILIDADES DE PUBLICACIÓN Y REPOSITORIOS

Este componente contiene las disposiciones aplicables en relación con:

2.1 Publicación y responsabilidades de los repositorios

Se identificarán la entidad o entidades que son responsables de operar los repositorios dentro de la Infraestructura de Clave Pública.

2.2 Publicación de información sobre la certificación

Indicar la información a ser publicada por el PSC en el repositorio, la forma como se va a publicar la información relativa a sus prácticas, los certificados y el estado actual de tales certificados, que pueden incluir la responsabilidad de poner la Política de Certificado o Declaración de Práctica de Certificación a disposición del público mediante diversos mecanismos. Así como la identificación de los componentes, subcomponentes, y elementos del documento que existen, pero no están a disposición del público por seguridad.

2.3 Tiempo o frecuencia de publicación

Indicar cuándo la información debe ser publicada y la frecuencia de las publicaciones.

La información de la AC se publica cuando se encuentre disponible y en especial, de forma inmediata cuando se trate de menciones relativas a la vigencia, expiración o revocación de los certificados.
Los certificados deberían de ser publicados tan pronto se produzca su generación y emisión en el repositorio público del PSC.

2.4 Controles de acceso a los repositorios

Indicar los controles y restricciones que se impondrán para el acceso a la información publicada, para elementos tales como: las Políticas de Certificado, Declaración de Prácticas de Certificación, certificados, estados del certificado y la LCR.

3. IDENTIFICACIÓN Y AUTENTICACIÓN

En este componente se describen los procedimientos utilizados para autenticar la identidad y/u otros atributos de un solicitante de certificado de usuario final ante una autoridad de certificación o autoridad de registro previo a la emisión del certificado. Además, el componente establece los procedimientos para la autenticación de la identidad y los criterios para la aceptación de los solicitantes de las entidades que buscan convertirse en autoridad de certificación o autoridad de registro u otras entidades que operan o inter-operan con una Infraestructura de Clave Pública. También describe cómo los solicitantes con claves renovadas o revocadas se autentican. Este componente también aborda las prácticas de nombres, incluyendo el reconocimiento de los derechos de marca registrada en ciertos nombres.

3.1 Denominación

Este subcomponente incluye los siguientes elementos relacionados con la denominación e identificación de los suscriptores:

3.1.1 Tipos de nombres

Describir los tipos de nombres admitidos para los sujetos de los certificados emitidos en función de la política de certificado. Estos pueden ser tales como X.500 nombre distinguido; RFC-822 nombres; y X.400 nombres.

3.1.2 Necesidad de que los nombres sean significativos

Especificar cuando sea el caso que los nombres tengan significado o no. Se describen las distintas denominaciones que se utilicen para cada tipo de certificado.

3.1.3 El anonimato o seudónimos de los suscriptores

Indicar cuando o no el suscriptor puede ser anónimo o seudónimo y si ellos pueden, que nombres son asignados o pueden ser usados por suscriptores anónimos.

3.1.4 Reglas para interpretar varias formas de nombres

Incluir las reglas para interpretar las distintas clases de nombres admitidas por la política de certificado; tales como el estándar X.500 y RFC 822.

3.1.5 Unicidad de los nombres

Especificar cuando el nombre distintivo debe ser único a cada suscriptor y como logra la unicidad cuando corresponde que un certificado es emitido a un mismo suscriptor.

3.1.6 Reconocimiento, autenticación y función de las marcas registradas

Especificar el referente sobre marcas. En conflicto el Proveedor de Servicio de Certificación puede reservarse el derecho de tomar todas las decisiones referidas a posibles conflictos sobre la utilización de

nombres entre sus suscriptores conforme su normativa legal nacional vigente al respeto. En caso de conflicto, la parte que solicite debería demostrar su interés legítimo y su derecho a la utilización de un nombre en particular. Suscriptor

3.2 Validación inicial de identidad

Este subcomponente contiene los siguientes elementos para los procedimientos de identificación y autenticación para el registro inicial de cada tipo de sujeto (autoridad de certificación, autoridad de registro, suscriptor, u otro participante):

3.2.1 Método para probar posesión de la clave privada

Especificar el procedimiento para asegurar que el solicitante se encuentra en posesión de la clave privada, para el registro de la respectiva clave pública, de acuerdo a protocolos de seguridad adecuados y que dicha clave privada es para firmar un mensaje de datos.

3.2.2 Autenticación de la identidad de la Organización

Especificar los requisitos de identificación y autenticación de la identidad organizacional del suscriptor o participante (autoridad de registro, autoridad de certificación; suscriptor (en el caso de los certificados emitidos a las Organizaciones o los dispositivos controlados por una Organización), u otro participante).

3.2.3 Autenticación de la identidad individual

Se establecen los requisitos de identificación y autenticación para un suscriptor individual o una persona natural que actúe en nombre de un suscriptor de Organización o participante (autoridad de registro, autoridad de certificación, en el caso de los certificados emitidos a las Organizaciones o los dispositivos controlados por una organización, el suscriptor, u otro participante), incluyendo:

- Tipo de documentación y/o el número de credenciales de identificación son necesarios; pudiendo ser la cédula de identidad, o pasaporte válido.
- Cédula de residencia y pasaporte en caso de ciudadanos extranjeros.
- Como una autoridad de registro o autoridad de certificación autentica la identidad de la Organización o de una persona sobre la base de la documentación o credenciales proporcionadas; ya sea el número RUC.
- Si la propia persona debe presentarse personalmente a la autoridad de certificación o autoridad de registro que autentica.
- Como un represéntate legal de la organización se debe autenticar, por ejemplo, por referencia a los documentos de autorización debidamente firmados o una tarjeta de identificación corporativa.

3.2.4 Información del suscriptor no verificada

Especificar y/o listar que información de un suscriptor no es verificada, durante el registro inicial.

3.2.5 Validación de autoridad

Consiste en determinar si una persona tiene derechos, privilegios o permisos específicos, incluyendo el permiso para actuar en nombre de una Organización para obtener un certificado según el tipo de certificado. Tenerse en cuenta consideraciones especiales para personas susceptibles a riesgos o de altos cargos.

3.2.6 Criterios para la interoperación

Cuando una AC solicita operar dentro de una ICP o interoperar con ella, este subcomponente contiene los criterios por los cuales una Infraestructura de Clave Pública, autoridad de certificación o Autoridad de política determina cuando o no la autoridad de certificación es capaz de realizar dichas operaciones o interoperaciones, tales interoperaciones pueden incluir: certificación cruzada, certificación unilateral u otras formas de interoperación.

La DGTEC es la que reconoce a todas aquellas infraestructuras o ACs cuya DPC y PC estén conforme con la normativa emitida por ella como son: “Normativa de Acreditación para Proveedores de Servicios se Certificación”, “Normativa para la Certificación Cruzada”, “Normativa para el Reconocimiento de Certificados Extranjero”, para que puedan inter operar con la INCP, además se debe de estar conforme lo establecido en la Ley 729 y el Reglamento 57-211.

3.3 Identificación y autenticación para solicitudes de renovación de claves

Este subcomponente describe los procedimientos de identificación y autenticación para la renovación de la clave por cada tipo de sujeto (autoridad de certificación, autoridad de registro, suscriptor y otros participantes):

3.3.1 Identificación y autenticación para la renovación rutinaria de claves

Especificar los procedimientos de identificación y autenticación para la generación de un nuevo par de claves y su correspondiente certificado. Se requiere que la clave privada sea válida es decir que no esté ni vencida ni revocada. Así como indicar a cuáles aplica renovación y en qué caso no aplica, considerando que en determinado tiempo será necesario realizar nuevamente una verificación como la inicial.

3.3.2 Identificación y autenticación para la renovación de la clave después de una revocación

Establecer los requerimientos de identificación y autenticación para la renovación después de la revocación de certificados. Un ejemplo pudiese ser utilizar el mismo procedimiento a seguir como en la validación inicial de identidad, o establecer un mecanismo distinto en dependencia de la causa de la revocación.

3.4 Identificación y autenticación para la solicitud de revocación

En este subcomponente se describen los procedimientos de identificación y autenticación para la solicitud de revocación por cada tipo de sujeto (autoridad de certificación, autoridad de registro, suscriptor, u otro participante). Los ejemplos incluyen una solicitud de revocación firmada electrónicamente con la clave privada cuya clave pública necesita ser revocada y una solicitud firmada electrónicamente por la autoridad de registro.

4. REQUISITOS OPERATIVOS DEL CICLO DE VIDA DEL CERTIFICADO

Este componente se utiliza para especificar los requisitos impuestos a la autoridad de certificación emisora, autoridad de registro, suscriptor o de otros participantes en relación con el ciclo de vida de un certificado.

Dentro de cada subcomponente, puede ser necesario considerar de manera individual a los sujetos (autoridad de certificación, autoridad de registro, suscriptor y otros participantes).

4.1 Solicitud de certificado

Este subcomponente contiene los requerimientos y procedimientos operativos establecidos por la autoridad de certificación para recibir los requerimientos de certificados. Estos procedimientos deberían de ser cumplidos por los Proveedores de Servicios de Certificación y por los solicitantes de certificados.

4.1.1 Quién puede presentar una solicitud de certificado

Especificar quienes pueden solicitar un certificado dentro del ámbito infraestructura de clave pública, tales como la autoridad de registro, un sujeto de certificado o un representante autorizado del mismo.

4.1.2 Proceso de inscripción y responsabilidades

Proceso de inscripción es utilizado por los sujetos para presentar las solicitudes de certificados y responsabilidades en relación con este proceso. Un ejemplo de este proceso es que el sujeto genera el par de claves y envía una solicitud de certificado a la autoridad de registro. La autoridad de registro válida y firma la solicitud y la envía a la autoridad de certificación. Una autoridad de certificación o autoridad de registro puede tener la responsabilidad de establecer un proceso de inscripción para recibir las solicitudes de certificados. Del mismo modo, los solicitantes de certificados deben tener la responsabilidad de proporcionar información precisa sobre sus solicitudes de certificados. Se deberán indicar todas las formas establecidas para realizar dichos procedimientos.

4.2 Procesamiento de solicitud de certificado

Este subcomponente se utiliza para describir el procedimiento para tramitar las solicitudes de certificados. Por ejemplo, la autoridad de certificación y la autoridad de registro pueden realizar procedimientos de identificación y autenticación para validar la solicitud de certificado. Siguiendo este proceso, la autoridad de certificación o autoridad de registro aprobará o rechazará la solicitud del certificado, tal vez por la aplicación de ciertos criterios. Finalmente, este subcomponente establece un límite de tiempo durante el cual una autoridad de certificación y/o autoridad de registro debe actuar y procesar una solicitud de certificado. Especificado con el siguiente esquema:

4.2.1 Realización de funciones de identificación y de autenticación

Describa sus prácticas para la identificación y autenticación de los solicitantes de certificados, las prácticas existentes empleadas por usted para identificar y autenticar las Organizaciones pueden utilizarse como base para la emisión de certificados a estos solicitantes. Puede hacerse referencia a la documentación de tales prácticas existentes.

4.2.2 Aprobación o rechazo de las solicitudes de certificado

Describa sus prácticas para la aprobación o el rechazo de las solicitudes. Tenga en cuenta que, de acuerdo con la política de certificado, las solicitudes de certificados serán aprobadas en base a las prácticas de negocios normales de la entidad que opera la autoridad de certificación, basándose en los registros de autoridad de certificación de suscriptores. La política de certificado también dice que cada autoridad de certificación seguirá el procedimiento especificado en la Sección 3.2.1 “Método para probar posesión de la clave privada” para verificar que el solicitante tiene la clave privada correspondiente a la clave pública que estará vinculada al certificado que la autoridad de certificación emite al solicitante.

4.2.3 Tiempo para procesar las solicitudes de certificados

Especifique aquí el período de tiempo máximo esperado para procesar las solicitudes de certificados.

4.3 Emisión del certificado

Establecer los requerimientos y procedimientos establecidos por los Proveedores de Servicios de Certificación para la emisión del certificado y para la notificación de dicha emisión al solicitante.

En este subcomponente se describen los siguientes elementos relacionados con la emisión del certificado:

4.3.1 Acciones de la autoridad de certificación durante la emisión del certificado

Acciones realizadas por la autoridad de certificación durante la emisión del certificado, por ejemplo, un procedimiento por el cual la autoridad de certificación valida las firmas de la autoridad de registro y posteriormente la autoridad de registro genera un certificado.

4.3.2 Notificación al suscriptor por la AC de la emisión del certificado

Mecanismos de notificación, si lo hubiese, utilizados por la autoridad de certificación para notificar al suscriptor de la emisión del certificado, es decir, es un procedimiento por el cual la autoridad de certificación genera un correo electrónico dirigido a la autoridad de registro o al suscriptor donde indique que se ha emitido un certificado a su nombre. El procedimiento debería de establecer en dependencia del tipo de certificado a emitir un mecanismo seguro de generación del certificado en un dispositivo seguro de creación de firma para entregar el certificado a la autoridad de registro o al suscriptor.

4.4 Aceptación del certificado

Se recomiendan establecer los requerimientos y procedimientos referidos a la publicación del certificado y a la aceptación del mismo por su suscriptor. El subcomponente contiene lo siguiente:

4.4.1 Conducta que constituye aceptación de certificados

Definir los procedimientos para la aceptación del certificado por el solicitante. Dichas conductas pueden incluir medidas positivas para indicar la aceptación, acciones implicando aceptación o la incapacidad de oponerse a la certificación o su contenido. Un suscriptor puede enviar un mensaje firmado aceptando el certificado o un suscriptor puede enviar un mensaje firmado para rechazar el certificado donde el mensaje incluye el motivo del rechazo y se identifican los campos en el certificado que son incorrectos o incompletos.

4.4.2 Publicación del certificado por la autoridad de certificación

Determinar los diversos medios que se utilizan para publicar un certificado. Por ejemplo, la autoridad de certificación podría publicar el certificado en un repositorio X.500 o protocolo ligero de acceso a directorios.

4.4.3 Notificación de la emisión del certificado por la AC a otras Entidades

Se recomienda incluir los procedimientos establecidos para notificar a las Entidades, Instituciones del Gobierno, personas naturales y empresas privadas de la emisión del certificado en caso que aplique. Por ejemplo, la autoridad de certificación puede enviar el certificado a la autoridad de registro.

4.5 Uso del par de claves y del certificado

Este subcomponente describe la responsabilidad relacionada con el uso de las claves y certificados emitidos por el Proveedor de Servicios de Certificación, incluyendo:

4.5.1 Uso de la clave privada y del certificado por el suscriptor

Se describe la responsabilidad del suscriptor relacionadas con el uso apropiado de la clave privada y su certificado, autorizados en esta Declaración de Práctica de Certificación y en consistencia con el contenido aplicable del certificado. Por ejemplo, se le puede solicitar al suscriptor que use una clave privada y el certificado sólo para aplicaciones apropiadas como se establece en la Política de Certificado y de acuerdo con el contenido del certificado aplicable (por ejemplo: el campo “keyUsage” del certificado). El uso de una clave privada y el certificado están sujetos a los términos del acuerdo suscrito, el uso de una clave privada sólo se permite después de que el suscriptor ha aceptado el certificado correspondiente o el suscriptor deberá dejar de usar la clave privada después del vencimiento o revocación del certificado.

4.5.2 Uso de la clave pública y del certificado por la parte que confía

Se describe la responsabilidad de la parte que confía para el uso de la clave pública y el certificado. Por ejemplo, una parte que confía puede estar obligada a confiar en los certificados sólo para aplicaciones apropiadas como se establece en la Política de Certificado y de acuerdo con el contenido del certificado correspondiente (por ejemplo, el campo de “keyUsage” en el certificado), realizar con éxito operaciones de claves públicas como condición para confiar en un certificado, asumir la responsabilidad de verificar el estado de un certificado utilizando uno de los mecanismos requeridos o permitidos establecidos en la Política de Certificado o Declaración de Práctica de Certificación (vea la sección 4.9), y aplicar los términos del acuerdo de la parte que confía como una condición para confiar en el certificado.

4.6 Renovación del certificado

Este subcomponente es usado para describir los siguientes elementos relacionados a la renovación del certificado. La renovación del certificado significa la emisión de un nuevo certificado al suscriptor sin cambiar el suscriptor u otro participante de la clave pública, o cualquier otra información en el certificado.

La renovación de certificado incorporará la misma clave pública del certificado anterior (si es necesario renovar el par de claves deberá aplicar el componente 4.7) estableciéndolo en el siguiente contexto:

4.6.1 Circunstancias para la renovación de certificados

Circunstancias bajo las cuales se lleva a cabo la renovación del certificado, como cuando la vida útil del certificado ha expirado, pero la política permite que se reutilice el mismo par de claves.

4.6.2 Quién puede solicitar la renovación

Quien puede solicitar la renovación de un certificado, por ejemplo, el suscriptor, la autoridad de registro o la autoridad de certificación estos pueden renovar automáticamente un certificado de suscriptor de usuario final.

4.6.3 Procesamiento de solicitudes de renovación de certificado

Los procedimientos de una autoridad de certificación o autoridad de registro para procesar solicitudes de renovación para emitir el nuevo certificado, por ejemplo, el uso de un token, como una contraseña, para

volver a autenticar al suscriptor, o procedimientos que son iguales a los procedimientos de la emisión del certificado inicial.

4.6.4 Notificación de la emisión de un nuevo certificado al suscriptor

En este subcomponente se determinará el proceso para notificar al suscriptor la emisión del nuevo certificado, que puede ser distinto o igual a la sección 4.3.2.

4.6.5 Conducta que constituye la aceptación de la renovación del certificado

El cual puede ser conforme a la sección 4.4.1. o mediante un método distinto.

4.6.6 Publicación del certificado renovado por la AC

En este subcomponente se determina el proceso de la AC para publicar el nuevo certificado, el cual puede ser el mismo al apartado 4.4.2.

4.6.7 Notificación de la emisión del certificado por la AC a otras Entidades

En este subcomponente se establece el procedimiento de la AC para notificar a otras Entidades sobre la emisión del certificado nuevo en caso que aplique.

4.7 Renovación de las claves del certificado

Este subcomponente es usado para describir los siguientes elementos relacionados a un suscriptor u otro participante en la generación de un nuevo par de claves y la solicitud de emisión de un nuevo certificado que certifica la nueva clave pública. Estableciéndolo en el siguiente contexto:

4.7.1 Circunstancias para renovación de las claves del certificado

Circunstancias bajo las cuales puede o debe tener lugar la renovación de la clave del certificado, como después de que un certificado es revocado por razones de compromiso clave o después de que un certificado haya expirado y el período de uso del par de claves también haya expirado.

4.7.2 Quién puede solicitar certificación de una nueva clave pública

Este puede ser distinto o igual a lo estipulado en 4.6.2, según las consideraciones de tiempo y el caso.

4.7.3 Procedimiento de solicitudes de cambio de clave del certificado

Procedimientos de una autoridad de certificación o autoridades de registro para procesar las solicitudes de renovación de claves, para emitir el nuevo certificado, tales como los procedimientos que son los mismos para de la emisión del certificado inicial. Puede ser igual o distinto a lo estipulado en 4.6.3.

4.7.4 Notificación de la emisión de un nuevo certificado al suscriptor

Describe la política para notificar al suscriptor acerca de la disponibilidad del nuevo certificado renovado. Esto debería ser consistente con el proceso de notificación para cualquier nueva emisión de certificado (ver sección 4.3.2).

4.7.5 Conducta que constituye la aceptación de un certificado con clave renovada

Cuando se emite un certificado renovado, la autoridad de certificación lo publicará en el repositorio y notificará al suscriptor. Consulte la Sección 4.4.1.

4.7.6 Publicación del certificado con clave renovada por la AC

Describe la política con respecto a la publicación del nuevo certificado. Se recomienda que sea coherente con el proceso de publicación de cualquier nuevo certificado (ver sección 4.4.2).

4.7.7 Notificación de la emisión del certificado por la AC a otras Entidades

Este componente puede ser conforme la sección 4.4.3.

4.8 Modificación de certificado

Este subcomponente es usado para describir los siguientes elementos relacionados a la emisión de un nuevo certificado, debido a cambios en la información del certificado que no sea la clave pública del suscriptor:

4.8.1 Circunstancias para la modificación del certificado

Circunstancias bajo las cuales puede ocurrir la modificación del certificado, tales como cambio de nombre, cambio de rol, reorganización que resulte en un cambio en el nombre distinguido (DN) de certificado.

4.8.2 Quién puede solicitar modificación de un certificado

Pueden ser, por ejemplo: suscriptores, personal de recursos humanos, la autoridad de registro o según corresponda el caso.

4.8.3 Procesamiento de solicitudes de modificación de un certificado

Los procedimientos de la autoridad de certificación o autoridad de registro para procesar solicitudes de modificación para emitir el nuevo certificado, tales como procedimientos que son los mismos que los de la emisión inicial de certificados.

4.8.4 Notificación de la emisión de un nuevo certificado al suscriptor

Describe el procedimiento para notificar al suscriptor sobre la emisión de un certificado modificado. Esto debería ser coherente con el proceso de notificación para cualquier nuevo certificado (ver sección 4.3.2).

4.8.5 Conducta que constituye aceptación del certificado modificado

Cuando se emite un certificado modificado, la autoridad de certificación lo publicará en el repositorio y notificará al suscriptor. Este puede ser conforme a la sección 4.4.1. o mediante un método distinto.

4.8.6 Publicación del certificado modificado por la AC

Describe el procedimiento para la publicación de un certificado modificado. Esto debe ser consistente con el proceso de publicación de cualquier nuevo certificado (ver sección 4.4.2).

4.8.7 Notificación de la emisión del certificado por la AC a otras Entidades

Este componente puede ser conforme la Sección 4.4.3.

4.9 Revocación y suspensión del certificado

En este componente se especifican los procedimientos de los Proveedores de Servicios de Certificación para asegurar que los certificados sean revocados de una manera oportuna, basadas en una solicitud de revocación de certificado autorizada y validada.

Este subcomponente es usado para describir los siguientes elementos relacionados a la suspensión o revocación de un certificado, debido a diferentes escenarios. En el siguiente contexto:

4.9.1 Circunstancias para la revocación

Se indican las circunstancias bajo las cuales un certificado podrá ser suspendido y aquellos casos en los cuales la revocación deberá ser obligatoria. Ejemplo, en caso de que un suscriptor haya sido suscriptor de un certificado de una organización y su contrato como empleado haya terminado. Otro ejemplo pudiese ser, la pérdida del token criptográfico, o sospechas de que la clave privada se haya visto comprometida.

4.9.2 Quién puede solicitar la revocación

Especifica quién puede solicitar la revocación del certificado del participante, por ejemplo, el suscriptor, autoridad de registro o autoridad de certificación en el caso de un certificado de suscriptor de usuario final.

4.9.3 Procedimientos para la solicitud de revocación

Especifica los procedimientos establecido para la solicitud de revocación de certificados, como puede ser: un mensaje firmado electrónicamente de la autoridad de registro, un mensaje firmado electrónicamente del suscriptor o una llamada telefónica de la autoridad de registro.

Se garantizará que los procedimientos de revocación se encontrarán disponibles en su correspondiente política de certificado, a disposición de los autorizados en el apartado anterior.

4.9.4 Periodo de gracia de la solicitud de revocación

Este subcomponente especifica el período de gracia disponible para el suscriptor, dentro del cual el suscriptor debe hacer una solicitud de revocación.

De conceder o no periodo de gracia, debería indicar en qué casos y las razones para el establecimiento de dicho periodo.

4.9.5 Tiempo dentro del cual la AC debe procesar la solicitud de revocación

Este subcomponente describe la política sobre el período dentro del cual procesará una solicitud de revocación.

La solicitud de revocación correctamente efectuada debería ser procesada, siempre siguiendo el procedimiento de verificación y autenticación de la solicitud presentada de forma inmediata a partir del procedimiento descrito en la sección 4.9.3.

Establecer aquí el plazo máximo entre la recepción de la solicitud de revocación y el cambio de la información de estado del certificado, indicando la revocación, disponible para las partes que confían. Si la solicitud de revocación requiere revocación a fecha futura, la fecha acordada será considerada como la fecha de confirmación.

4.9.6 Requisito de verificación de revocación para las partes que confía

Este subcomponente describe los mecanismos, si los hay, que una parte que confía puede utilizar o debe utilizar para verificar el estado de los certificados en los que desea confiar, que pueden estar basados en el Protocolo de Estado del Certificado en Línea - PECL, acceso y descarga de las listas de certificados revocados LCR.

4.9.7 Frecuencia de emisión de LCR

Define la frecuencia con que se emite la lista de certificados revocados que publica.

4.9.8 Latencia máxima de LCR

Este subcomponente especifica si es usado un mecanismo de lista de certificados revocados, aquí se establecerá el tiempo máximo admisible entre la generación de la lista de certificados revocados y su publicación en el repositorio (en otras palabras, la cantidad máxima de retrasos relacionados con el procesamiento y la comunicación en la publicación de la lista de certificados revocados en el repositorio después de que se generen las listas de certificados revocados).

4.9.9 Disponibilidad de comprobación en línea de Revocación/Estado

Se establece si se posee un servicio de revocación de certificados en línea y de verificación de su estado. Se refiere al uso del PECL y de un sitio web en el cual se pueden consultar los estados de los certificados.

Se debería poner a disposición de las partes que confían:

- La información relativa a las características operacionales de los servicios de verificación de estado.
- La disponibilidad de tales servicios y cualquier política aplicable en caso de no disponibilidad.
- Cualquier característica opcional de tales servicios.

4.9.10 Requisitos de comprobación en línea de la revocación

Se definen los requisitos para que una parte que confía pueda realizar la comprobación en línea de la información de revocación de certificados.

4.9.11 Otras formas de divulgación de revocación disponibles

Se define, de existir, otras formas utilizadas para divulgar la información sobre revocación de certificados.

4.9.12 Requisitos especiales de renovación de clave por compromiso

Cualquier variación de las estipulaciones anteriores para las cuales la suspensión o revocación es el resultado del compromiso de la clave privada (a diferencia de otras razones para la suspensión o la revocación).

4.9.13 Circunstancias para la suspensión

Circunstancias bajo las cuales un certificado puede ser suspendido, su gestión y en los casos que no aplica.

4.9.14 Quién puede solicitar la suspensión

Especifica quienes pueden solicitar la suspensión de un certificado, por ejemplo, el suscriptor, el personal de recursos humanos, un supervisor del suscriptor o la autoridad de registro en el caso de un certificado de suscriptor de usuario final. Puede basarse en la sección 4.9.2.

4.9.15 Procedimientos para la solicitud de suspensión

Especifica los procedimientos para solicitar la suspensión del certificado, como un mensaje firmado electrónicamente del suscriptor o autoridad de registro, una comunicación oral o escrita previamente autenticada, desde un sitio web o cualquier otro.

4.9.16 Límites en período de suspensión

Especifica cuánto tiempo puede durar la suspensión de un certificado según sea el caso.

4.10 Servicios de estado del certificado

Este subcomponente se refiere a los servicios de comprobación del estado de los certificados, disponible para las partes que confían, incluyendo:

4.10.1 Características operacionales

Especifica las características operativas de los servicios de comprobación del estado de los certificados.

4.10.2 Disponibilidad del servicio

Describe la disponibilidad de los servicios de comprobación del estado de los certificados, y cualquier política aplicable sobre la no disponibilidad de los mismos.

4.10.3 Características opcionales

Establecer otras características adicionales sobre el servicio de comprobación del estado de los certificados.

4.11 Fin de suscripción

Este subcomponente especifica los procedimientos usados por el suscriptor para finalizar la suscripción a un servicio de una autoridad de certificación, incluyendo:

La revocación del certificado al final de la suscripción (el cual puede diferir, dependiendo de si el fin de la suscripción es debido a la expiración del certificado o por finalización del servicio).

4.12 Custodia y recuperación de claves

Este subcomponente contiene los siguientes elementos para identificar las políticas y prácticas relacionadas con la custodia y/o recuperación de las claves privadas donde los servicios de custodia de

clave privada están disponibles (a través de la autoridad de certificación u otro tercero de confianza), mediante los siguientes elementos:

4.12.1 Prácticas y políticas de custodia y recuperación de claves

Identificación del documento que contiene políticas y prácticas establecidas para el servicio de recuperación y custodia de la clave privada o una lista de dichas políticas y prácticas.

4.12.2 Prácticas y políticas de encapsulado y recuperación de clave de sesión

Identificación del documento que contiene la políticas y prácticas de encapsulado y recuperación de la clave de sesión o una lista de tales políticas y prácticas.

5. CONTROLES DE GESTIÓN, OPERATIVOS Y FÍSICOS

Este componente describe controles de seguridad no técnicos (es decir, los controles físicos, procedimientos y los controles de personal) utilizados por la autoridad de certificación emisora de certificados para realizar de forma segura las funciones de generación de claves, autenticación de sujeto, la emisión de certificados, revocación de certificados, auditoría y archivo.

Este componente también se puede utilizar para definir controles de seguridad no técnicos en los repositorios, autoridad de certificación, autoridad de registro, suscriptores y otros participantes. Los controles de seguridad no técnicos de las autoridades de certificación, autoridades de registro, suscriptores y otros participantes podría ser el mismo, similar o muy diferentes.

Dentro de cada subcomponente, en general, se debería realizar una consideración por separado, para cada tipo de Entidad, es decir, para la autoridad de certificación emisora, repositorio, autoridades de certificación sujeto, autoridades de registro, suscriptores y otros participantes.

5.1 Controles de seguridad física

En este subcomponente, se describen los controles físicos en las instalaciones que resguardan los sistemas de la entidad. Los temas que debe incluir son:

5.1.1 Localización y construcción de instalaciones

Este subcomponente especifica los requerimientos sobre las medidas de seguridad de protección de las instalaciones.

5.1.2 Acceso físico

Se deberían determinar los mecanismos de control para acceder a las instalaciones, así como para el acceso de un área de las instalaciones a otra, o para el acceso a zonas de mayor seguridad, como ubicar las operaciones de la autoridad de certificación en un cuarto de computo seguro monitoreado por guardias de seguridad o sistemas de alarmas y requerimientos para avanzar de una zona a otra zona logrados a través del uso de un token, lectores biométricos y/o listas de control de acceso.

5.1.3 Electricidad y aire acondicionado

Se establecen los mecanismos para asegurar el suministro de energía eléctrica y el correcto funcionamiento y mantenimiento de los sistemas de aire acondicionado.

5.1.4 Exposición al agua

Se establecen los mecanismos instalados para evitar las exposiciones al agua de las instalaciones.

5.1.5 Prevención y protección de incendios

Se definen los mecanismos con que se cuentan para la protección y prevención de incendios, con especial atención a los dispositivos criptográficos.

5.1.6 Medios de almacenamiento

Se establecen los mecanismos de almacenamiento de información relacionada, por ejemplo, lugares para almacenar los medios de respaldos en ubicaciones separadas que son físicamente seguras y protegidas de daños provocados por fuego y agua.

5.1.7 Eliminación de desechos

Se establecen los mecanismos para verificar toda la adecuada eliminación de los materiales desechables donde se almacena información sensible.

5.1.8 Copia de seguridad fuera de las instalaciones

Se establece el procedimiento de almacenamiento de copias de seguridad en sitios externos.

5.2 Controles de procedimiento

Este subcomponente aborda lo siguiente:

5.2.1 Roles de confianza

Se definen los requisitos para reconocer roles de confianza y sus responsabilidades. Es decir, se define la descripción del personal que por sus responsabilidades son sometidos a procedimientos de control.

5.2.2 Número de personas requeridas por tarea

Se determinan las responsabilidades compartidas entre los distintos roles y personas, con atención a las tareas clasificadas como sensibles o de alto riesgo.

5.2.3 Identificación y autenticación para cada rol

Se define el proceso de identificación y autenticación de cada rol.

5.2.4 Roles que requieren separación de tareas

Se determina la separación de funciones en cuanto a los roles que no pueden ser ejecutados por la misma persona.

5.3 Controles de seguridad personal

Este subcomponente aborda los siguientes controles:

5.3.1 Requisitos de calificaciones, experiencia y autorización

Se describen los antecedentes laborales, calificaciones, y autorizaciones que el personal debe tener como condición para desempeñar funciones de confianza u otras funciones importantes. Los ejemplos incluyen las credenciales, experiencia de trabajo, y las autorizaciones gubernamentales oficiales necesarias que los candidatos a estos puestos deberían tener antes de ser contratados.

5.3.2 Procedimientos de verificación de antecedentes y autorización

Se realiza la verificación de antecedentes y procedimientos de autorización que se requieran en relación con la contratación de personas que desempeñen funciones de confianza u otras funciones importantes, esas funciones pueden requerir una verificación de sus antecedentes penales, referencias y autorizaciones adicionales que un participante realiza después de que se ha tomado la decisión de contratar a una persona en particular. Dicho procedimiento debe realizarle respetando y cumpliendo con el debido proceso de protección de los datos personales en base a la Ley 787 “Ley de Protección de Datos Personales”.

5.3.3 Requisitos de capacitación

Se describen los requisitos de capacitación y procedimientos de capacitación (entrenamiento) para cada rol después de la contratación de personal.

5.3.4 Frecuencia y requisitos de reentrenamiento

Se describe la frecuencia de los procesos de actualización técnica o profesional para cada rol después de la finalización de la capacitación inicial.

5.3.5 Frecuencia y secuencia de rotación de trabajo

Se describe la frecuencia y secuencia de rotación de las tareas de cada uno de los puestos.

5.3.6 Sanciones por acciones no autorizadas

Sanciones contra la persona por acciones no autorizadas, uso no autorizado de la autoridad, y uso no autorizado de los sistemas de la entidad con el propósito de imponer responsabilidad al personal de un participante.

5.3.7 Requisitos de contratista independiente

Los controles sobre el personal que son contratistas independientes en lugar de ser empleados de la entidad; esto incluyen:

- Requisitos de depósito para el personal contratado.
- Requisitos pactados de indemnización por daños debidos a la acción del personal de la empresa contratada.
- Auditoría y supervisión del personal de la empresa contratista.
- Compromiso de confidencialidad.
- Otros controles sobre el personal contratado.

5.3.8 Documentación proporcionada al personal

Documentación que debería ser proporcionada al personal para el desempeño de sus tareas durante el entrenamiento inicial, capacitación constante, o cualquier otro tipo.

5.4 Procedimientos de registro de auditoría

El subcomponente es utilizado para describir los procedimientos de auditoria, implementados con el propósito de registrar los eventos de auditoria relacionados con la gestión de los componentes de la ICP del PSC y de mantener un ambiente seguro. Los elementos que debe incluir son:

5.4.1 Tipos de eventos registrados

Se establecen los tipos de eventos, que serán registrados en los log de auditoría, como las operaciones del ciclo de vida del certificado, los intentos de acceso al sistema, y las peticiones hechas al sistema.

5.4.2 Frecuencia de procesamiento de registro

Se establece la frecuencia con que se procesan o archivan los registros de auditoria, por ejemplo, semanal, después de una alarma o eventos anómalos, o cuando alguna vez el registro de auditoría está lleno.

5.4.3 Periodo de conservación de registros de auditoría

Se establece el período de conservación de los registros de auditoría.

5.4.4 Protección de los registros de auditoría

- Quién puede ver los registros de auditoría, por ejemplo, sólo el administrador de auditoría.
- Protección contra la modificación de los registros de auditoría, por ejemplo, un requisito que nadie puede modificar o eliminar del registro auditoría como parte de rotación de archivo de auditoria.
- Protección contra la eliminación de registros de auditoría.

5.4.5 Procedimientos de copia de respaldo de los registros de auditoria

Se determina el procedimiento de copia de respaldo de los registros de auditoría, para que en caso de pérdida o destrucción de los registros de auditoria se cuente con ellos.

5.4.6 Sistema de archivo de registros de auditoria (interno vs externo)

Se especifica si el sistema de archivo de registros de auditoría es interno o externo a la entidad.

5.4.7 Notificación al sujeto causa de eventos

Especifica si el sujeto que causó que ocurriera un evento de auditoría es notificado de la acción de auditoría y a su vez activa las notificaciones de los trabajos de auditoría. Debería indicar cómo se realiza la notificación de las incidencias a las partes relacionadas e interesadas, lo cual debe ser ampliado en el procedimiento correspondiente.

5.4.8 Evaluaciones de vulnerabilidad

Se determinan los procesos de análisis y gestión de las vulnerabilidades, debería indicar cuales son los mecanismos, procedimientos y herramientas con los cuales cuenta el PSC para la detección y evaluación de posibles vulnerabilidades que puedan atentar contra la seguridad de la información.

5.5 Archivo de registros

Este subcomponente es usado para describir de manera general la política de registros archivados (o la retención de archivos), incluyendo lo siguiente:

5.5.1 Tipos de registros archivados

Se determinan los diferentes tipos de registros que son archivados, por ejemplo:

- La emisión, revocación, y demás eventos relevantes relacionados con los certificados, así como las operaciones relacionadas con la gestión de las claves y certificados del Proveedor de Servicios de Certificación.
- Las Firmas, y demás eventos relevantes relacionados con las LCR's.
- Todas las operaciones de acceso al archivo de los certificados.
- Todas las operaciones de acceso al servicio de información sobre el estado de los certificados.
- Eventos relevantes de la generación de pares de números aleatorios y pseudoaleatorios para la generación de Claves.
- Eventos relevantes de la generación de pares de claves propias o de soporte de autenticidad.
- Todas las operaciones del servicio de archivo de claves y del acceso al archivo de claves expiradas.
- Todas las operaciones relacionadas con la actividad como parte que confía.
- Los eventos relevantes de la operación de la Autoridad de Sellado de Tiempo, especialmente las correspondientes a la sincronización de relojes y pérdidas de sincronismo. Siempre se incluirá el momento exacto en el que se produce.

5.5.2 Periodo de conservación del archivo

Se establece el período de conservación de los archivos y registros, considerando la legislación nacional aplicable.

5.5.3 Protección del archivo

Este componente debería incluir al menos, como garantiza:

- Quién puede ver el archivo.
- Protección contra la modificación del archivo.
- Protección contra la eliminación de archivo.

- Protección contra el deterioro de los medios en los que se almacenan los archivos.
- Protección contra la obsolescencia de hardware, sistemas operativos y otros softwares.

5.5.4 Procedimientos de copia de respaldo del archivo

Se establece el procedimiento de resguardo de los archivos.

5.5.5 Requisitos para el sellado de tiempo de los registros

Indicar con que fuente están fechados los registros, así de cómo se gestionan.

5.5.6 Sistema de recopilación del archivo (internos o externos)

Se definirán los medios por las cuales se realiza el repositorio de los archivos.

5.5.7 Procedimientos para obtener y verificar información del archivo

Procedimientos para obtener y verificar la información de los archivos, como el requisito de que dos copias separadas de los datos de los archivos se mantengan bajo el control de dos personas y que las dos copias sean comparadas para asegurar que la información de archivo sea precisa.

Se establece el proceso requerido para obtener información de archivos de datos para llevar a cabo verificaciones de integridad.

5.6 Cambio de clave

Este subcomponente describe el procedimiento para proporcionar una nueva clave pública a los usuarios de un certificado luego de una renovación de clave por la autoridad de certificación. Estos procedimientos pueden ser los mismos que el procedimiento para proporcionar la clave actual.

5.7 Recuperación ante compromiso y desastre

Este subcomponente describe los requisitos relacionados con los procedimientos de notificación y recuperación en caso de desastre o en los eventos que comprometan la seguridad, en especial a lo relacionado al compromiso de clave.

5.7.1 Procedimientos de manejo de incidentes y compromisos

Listado o identificación de incidentes aplicables y reportes de compromiso de la seguridad, así como el procedimiento de gestión.

Se describen los procedimientos para establecer un Plan de Continuidad que defina las acciones a realizar, recursos a utilizar y personal a emplear en caso de ocurrir un acontecimiento intencionado o accidental que utilice o degrade los recursos y servicios de certificación prestado por el PSC.

5.7.2 Daño en los recursos informáticos, software y/o datos

Se establecen los procedimientos de recuperación que se utilizan si los recursos informáticos, software y/o los datos están dañados o corrompidos, incluso si se sospecha de ello. Estos procedimientos describen cómo se reestablece un entorno seguro, los certificados que se han revocado, si se revoca la clave de

entidad, como se proporciona la nueva clave pública de la entidad a los usuarios, y cómo se vuelven a certificar los sujetos.

5.7.3 Procedimiento si la clave privada de una entidad está comprometida

Se establece el procedimiento de recuperación utilizados si la clave de entidad está comprometida. Estos procedimientos describen cómo se restablece un entorno seguro, cómo se proporciona a los usuarios la nueva clave pública de la entidad y cómo se vuelven a certificar los sujetos.

5.7.4 Capacidades de continuidad de negocios después de un desastre

Capacidad de la entidad para garantizar la continuidad del negocio después de un desastre natural o de otro tipo. Tales capacidades podrían incluir la disponibilidad de un sitio remoto un sitio de contingencia en el que las operaciones pueden ser recuperadas. También pueden incluir los procedimientos para asegurar su instalación durante el período de tiempo después de un desastre natural o de otro tipo y antes de que se restablezca un entorno seguro, ya sea en el sitio original o en el sitio remoto.

5.8 Terminación/cese de la AC o la AR

Este subcomponente describe requerimientos relacionados a los procedimientos para la terminación y notificación de terminación (finalización de servicios) de una autoridad de certificación o autoridad de registro, incluyendo la identidad del custodio de los registros y de archivos de la autoridad de certificación y/o autoridad de registro.

Se deben especificar procedimientos referidos a:

- Notificación ante la entidad rectora - DGTEC, los suscriptores, terceros que confía, otros Proveedores de Servicios de Certificación y otros usuarios vinculados.
- Revocación del certificado de Proveedor de Servicios de Certificación y de los certificados emitidos a otras AC y suscriptores.
- Transferencia de la custodia de archivos y documentación.

Se establece que el responsable de la custodia de archivos y documentación cumplirá con idénticas exigencias de seguridad que las contempladas para los Proveedores de Servicios de Certificación finalizados. Se debería de garantizar también que la transferencia incluya las responsabilidades que sean cubiertas por el seguro que tenga adquirido, el cual debería de contar con las garantías de seguro establecidas en la Ley 729 para responder ante daños a los suscriptores o ante terceros.

6. CONTROLES DE SEGURIDAD TÉCNICA

Este componente se utiliza para definir las medidas de seguridad tomadas por la autoridad de certificación emisora para proteger sus claves criptográficas y otros parámetros de seguridad críticos. Este componente también se puede utilizar para imponer restricciones en los repositorios, suscriptores, autoridad de certificación y otros participantes para proteger sus claves privadas, los datos de activación de sus claves privadas, y los parámetros de seguridad críticos. La gestión segura de claves es fundamental para garantizar que todas las claves secretas y privadas y los datos de activación están protegidos y sean utilizados únicamente por personal autorizado.

Este componente también describe otros controles de seguridad técnica utilizado por la autoridad de certificación emisora de certificados para realizar de forma segura las funciones de generación de claves, autenticación de usuario, registro de certificados, revocación de certificados, auditoría y archivo.

Los controles técnicos incluyen controles de seguridad del ciclo de vida y los controles de seguridad operativa.

Este componente también se puede utilizar para definir otros controles de seguridad técnicos en los repositorios, autoridad de certificación, autoridad de registro, suscriptores y otros participantes.

6.1 Generación e instalación del par de claves

La generación e instalación del par de claves debería ser considerado por la autoridad de certificación emisora, los repositorios, la autoridad de certificación origen, las autoridades de registro y los suscriptores. Para cada una de estas entidades, deberían contemplarse los siguientes temas:

- Responsable de la generación de claves, ¿Quién genera el par de clave pública y privada del al suscriptor? ¿Cómo es generada la clave? ¿La generación de claves es realizada por hardware o software?
- ¿Cómo es proporcionada la clave privada de manera segura al suscriptor?
- ¿Cómo es la entrega de forma segura de la clave pública de la entidad a la autoridad de certificación?
- En el caso de autoridades de certificación emisoras ¿Cómo es proporcionada la clave pública de la autoridad de certificación de forma segura a las posibles partes que confían?
- ¿De qué tamaño son las claves? ¿Algoritmo de firma utilizado? ¿Fecha de creación? ¿Fecha de vencimiento?
- ¿Quién genera los parámetros de la clave pública, y es la calidad de los parámetros revisadas durante la generación de claves?
- ¿Con qué fin se puede utilizar la clave o para qué fines se debería restringir el uso de la clave?

Todas las preguntas ordenarse y contestarse en los siguientes componentes donde correspondan.

6.1.1 Generación del par de claves

Se definen todos los aspectos relativos a la generación del par de claves de los certificados definidos en las Políticas de Certificados, del par de claves de los responsables de las Autoridades de Registro, de los servicios de información de estado de certificados, suscriptores, etc. Deberían considerarse los siguientes requerimientos mínimos:

- El par de claves debería ser generado únicamente por el suscriptor del certificado, permaneciendo su clave privada en todo momento bajo su absoluto y exclusivo control.
- El medio de generación y almacenamiento de la clave privada deberá asegurar que: La clave privada sea única y su confidencialidad se encuentre debidamente garantizada.

6.1.2 Entrega de la clave privada al suscriptor

Debería considerarse obligatoriamente las exigencias reglamentarias impuestas por la obligación de abstenerse de generar, exigir o por cualquier otro medio tomar conocimientos o acceder a la clave privada de los suscriptores.

6.1.3 Entrega de clave pública al emisor del certificado

Se establecen los procedimientos utilizados para la entrega de la clave pública del suscriptor del certificado y al Proveedor de Servicios de Certificación responsable de la emisión del certificado.

6.1.4 Entrega de la clave pública de la AC a la parte que confía

Se definen los medios adoptados para poner el certificado de la AC, y el resto de los certificados que forma su cadena de certificación, a disposición de todos los suscriptores y a las partes que confían interesadas.

6.1.5 Tamaños de clave

Se definen los tamaños mínimos de las claves criptográficas asociadas con los certificados emitidos según las disposiciones de la DGTEC como ente rector.

6.1.6 Parámetros de generación de clave pública y comprobación de calidad

Se deberían describir los parámetros de generación de claves y los procedimientos de verificación utilizados respecto de la calidad de los parámetros de generación de claves.

6.1.7 Propósitos del uso de la clave

Se establecen los propósitos para los cuales se utilizarán las claves criptográficas de los suscriptores de los certificados, según X.509 v3 “Key usage field” campo Uso de Clave (por ejemplo, autenticación, integridad, no repudio) y las posibles restricciones en su uso.

6.2 Protección de la clave privada y controles de ingeniería del módulo criptográfico

Este subcomponente contempla los requerimientos para la protección de la clave privada y módulos criptográficos necesarios para ser considerados por la autoridad de certificación, los repositorios, las autoridades de registro, y suscriptores. Para cada uno de estos tipos de entidad, se deberán considerar desarrollar los siguientes componentes:

6.2.1 Estándares y controles para el módulo criptográfico

Se describen los estándares utilizados para los módulos de generación y almacenamiento de claves criptográficas.

6.2.2 Control multi-personal “n de m” de la clave privada

Se describen los controles empleados para la actividad de las claves, indicando cuantas personas están involucradas en el control de dicha clave.

Deben respetarse las siguientes exigencias mínimas:

- El control de la utilización de las claves criptográficas de la AC debe estar dividido de forma tal que sea necesaria la presencia de al menos 2 personas distintas (o N distintas de un total de M posibles, con N≥2 y M≥N+3).

Por ejemplo, puede requerirse la presencia de al menos dos administradores de un grupo de cinco para utilizar la clave de la AC.

6.2.3 Custodia de la clave privada

Se describen los procedimientos de custodia de la clave privada, así como también se especifica quien es el agente de custodia, en que forma está custodiada la clave y cuáles son los controles de seguridad del sistema de custodia.

6.2.4 Copia de seguridad de la clave privada

Este subcomponente describe los procedimientos y controles de seguridad empleados para la realización de copias de seguridad de las claves privadas, para cada tipo de certifico que emitan, cuando sea permitido y corresponda con el consentimiento expreso del suscriptor, así como también se especifica quien es el agente de respaldo, en que forma está respaldada la clave y cuáles son los controles de seguridad en el sistema de respaldo.

6.2.5 Archivo de clave privada

En este subcomponente se describen los procedimientos y controles de seguridad empleados para el archivo de las claves privadas, así como también se especifica quien es el agente de archivo, en que forma está archivada la clave, periodo de tiempo de conservación del archivo y cuáles son los controles de seguridad en el sistema de archivo.

En todos los casos deben establecerse procedimientos que garanticen que los niveles de seguridad de las claves no disminuyan por el proceso de archivo.

6.2.6 Transferencia de la clave privada desde o hacia un módulo criptográfico

Se establecen los requisitos para la inserción o extracción de la clave privada del suscriptor en el módulo criptográfico, describiendo bajo que circunstancia se puede realizar la operación, a quienes les está permitido realizar la operación y cuál es el formato de la clave privada utilizado durante la transferencia.

6.2.7 Almacenamiento de la clave privada en el módulo criptográfico

En este subcomponente se describe como se almacena la clave privada en el módulo criptográfico.

6.2.8 Método de activación de la clave privada

Se describen los requisitos y procedimientos necesarios para la activación de la clave privada, así como también se especifica quien puede activar (usar) la clave privada, que acciones se deben realizar para activar la clave privada y se especifica el periodo de tiempo que durará la activación de la clave.

Se exigirá la autenticación de los responsables a través de métodos adecuados.

6.2.9 Método de desactivación de la clave privada

Se describen los requisitos y procedimientos necesarios para la desactivación de la clave privada, así como también se especifica quien puede desactivar la clave privada.

Se debería exigir la autenticación de los responsables a través de métodos adecuados.

6.2.10 Método de destrucción de la clave privada

Se especifican en este subcomponente los procedimientos a seguir para la destrucción de la clave privada y de sus copias de seguridad ante cualquier hecho que motivara el final de la vida útil de un certificado, tales como su revocación o expiración.

Se definen a los responsables de realizar la destrucción, formas de autenticación, y acciones a desarrollar.

6.2.11 Calificación del módulo criptográfico

En este subcomponente se describen las capacidades del módulo criptográfico en las siguientes áreas: identificación del límite del módulo criptográfico, entrada / salida, funciones y servicios, máquina de estados finitos, seguridad física, seguridad de software, la seguridad del sistema operativo, el cumplimiento de algoritmo, la compatibilidad electromagnética, y pruebas automáticas. La capacidad puede ser expresada a través de referencia al cumplimiento de una norma como la FIPS 140-2 de EE.UU., el nivel asociado y la clasificación.

6.3 Otros aspectos de gestión del par de claves

Se deberían tener en cuenta otros aspectos de la gestión de claves para ser considerados por la autoridad de certificación emisora, los repositorios, autoridad de certificación, autoridad de registro, suscriptores y otros participantes. Para cada uno de estos tipos de entidades, se deben desarrollar los siguientes componentes:

6.3.1 Archivo de clave pública

Se describen en esta sección los procedimientos y controles de seguridad implementados para el sistema de archivo de la clave pública, el software y hardware necesarios a preservar como parte de dicho archivo para permitir la utilización de la clave pública en el tiempo y la duración en el tiempo que se mantendrá archivada la información.

Esta sección no se delimita a describir la utilización de firmas electrónicas con el archivo de datos, sino que debe dirigirse, además, a los controles de integridad utilizados para impedir la adulteración de datos (.

6.3.2 Periodos operativos de los certificados y período de uso para el par de claves

Se debería determinar que las claves privadas correspondientes a los certificados emitidos por el Proveedores de Servicios de Certificación podrían ser utilizadas por su suscriptor únicamente durante el periodo de validez de los mismos. Las correspondientes claves públicas podrían ser utilizadas durante el periodo establecido por las normas legales vigentes, a fin de posibilitar la verificación de las firmas generadas durante su periodo de validez, según se establece en el apartado anterior.

6.4 Datos de activación

En este subcomponente se establecen medidas de seguridad para proteger los datos de activación requeridos para la operación de claves privadas para todos los usuarios de certificados.

6.4.1 Generación e instalación de datos de activación

En este subcomponente especifica cómo se generan e instalan los datos de activación de las Claves Privadas en cada caso.

6.4.2 Protección de los datos de activación

Se especifican en este subcomponente los procedimientos a seguir para la adecuada protección de los datos de activación de la clave privada de los suscriptores de certificados contra usos no autorizados.

6.4.3 Otros aspectos de los datos de activación

Se incluyen otros aspectos relativos a los controles sobre los datos de activación, tales como los referidos a las claves, incluidos en los apartados 6.1 a 6.3.

6.5 Controles de seguridad informática

Se debe especificar bajo qué régimen los servicios de certificación son controlados y auditados; de manera general indicar los controles relevantes al respecto.

6.5.1 Requerimientos técnicos específicos de la seguridad del computador

Este sub-componente se utiliza para describir los controles de seguridad informática tales como: el uso del concepto de base informática de confianza, control de acceso discrecional, etiquetas, controles de acceso obligatorios, reutilización de objetos, la auditoría, la identificación y autenticación, ruta de confianza, pruebas de seguridad y pruebas de penetración. La garantía del producto también puede ser abordada.

6.5.2 Clasificación de la seguridad informática

Se establece una calificación de seguridad informática para los sistemas informáticos. La calificación podría basarse, por ejemplo, en la norma NTN 21 001-13, en la norma ISO/IEC 27001:2019 y en la norma FIPS PUB 140-2.

Este subcomponente también puede cumplir con los requisitos para el análisis de la evaluación del producto, pruebas, elaboración de perfiles, certificación de productos, y/o la actividad relacionadas a la acreditación de productos realizadas.

6.6 Controles técnicos del ciclo de vida

Este subcomponente se especifican los controles de desarrollo de sistema y los controles de gestión de seguridad.

6.6.1 Control de desarrollo del sistema

Los controles de desarrollo de sistema incluyen la seguridad del entorno de desarrollo, seguridad del personal de desarrollo, seguridad de la gestión de la configuración durante el mantenimiento del producto, las prácticas de ingeniería de software, metodología de desarrollo de software, la modularidad, el uso de

técnicas de diseño e implementación de prueba de fallas y seguridad de las instalaciones de desarrollo. Considerando además los aspectos relacionados cuando se cuenta con desarrollo externo en caso de tener.

6.6.2 Controles de gestión de seguridad

Los controles de gestión de seguridad incluyen la ejecución de herramientas y procedimientos para garantizar que los sistemas operativos y las redes se apeguen a la seguridad configurada.

6.6.3 Controles de seguridad del ciclo de vida

Este subcomponente también puede abordar las calificaciones de seguridad del ciclo de vida basada, por ejemplo, en el nivel IV y V de la Metodología de desarrollo de software confiable - (o TSDM por sus siglas en ingles), la auditoría independiente de controles de seguridad del ciclo de vida y el Modelo de madurez de capacidad del Instituto de ingeniería de software (o SEI-CMM por sus siglas en ingles).

6.7 Controles de seguridad de red

Este subcomponente se debería enfocar en los controles relacionados a la seguridad de la red, incluyendo firewalls.

6.8 Sello de tiempo

Este subcomponente debería indicar los requerimientos o practicas relacionadas al uso de Sello de tiempo en los datos. Podría también indicar cuando el sello de tiempo debe o no utilizar una fuente confiable de tiempo.

7. PERFILES DE CERTIFICADO, LRC Y PECL

Este componente es usado para especificar el formato del certificado y, si se usan lista de revocación de certificado y/o protocolo de estado del certificado en línea, así como sus respectivos formatos. Esto incluye información de perfiles, versiones, y extensiones usadas.

7.1 Perfil del certificado

Este subcomponente aborda temas como los siguientes (referida a la definición del perfil tal como lo establece el RFC 5280):

7.1.1 Número de versión

7.1.2 Extensiones del certificado

7.1.3 Identificadores de objeto del algoritmo criptográfico

7.1.4 Formato de nombres

7.1.5 Restricciones de nombres

7.1.6 Identificador de objeto de la PC

7.1.7 Uso de la extensión “Policy Constraints”

7.1.8 Sintaxis y la semántica de los calificadores de política

7.1.9 Procesamiento semántico para la extensión crítica "Certificate Policy"

7.2 Perfil de la LCR

Este subcomponente incluye temas como los siguientes (potencialmente referenciados a la definición del perfil, tal está definido en el IETF PKIX RFC 5280):

7.2.1 Número de versión

7.2.2 LCR y extensiones de entrada

7.3 Perfil del PECL

Este subcomponente incluye temas tales como los siguientes (potencialmente referenciados a la definición del perfil, tal está definido en el IETF PKIX RFC 6960):

7.3.1 Número de versión

7.3.2 Extensiones PECL y su criticidad

8. CUMPLIMIENTO DE AUDITORÍA Y OTRAS EVALUACIONES

Este componente aborda lo siguiente:

8.1 Frecuencias o circunstancias de las auditorías

Especifica la frecuencia de las auditorías de cumplimiento u otra evaluación para cada entidad que debe evaluarse de conformidad con una Política de Certificado o Declaración de Práctica de Certificación, o por las condiciones que provocaran una evaluación; Las posibilidades incluyen una auditoría anual, evaluación como condición para permitir que una entidad sea operacional o la correspondiente investigación a profundidad de un riesgo de seguridad de un compromiso posible o real de la seguridad.

8.2 Identificación/calificaciones del evaluador

La identificación y/o cualificación del personal que realiza la auditoría u otra evaluación.

8.3 Relación del evaluador con la entidad evaluada

Definir la relación funcional del evaluador con la entidad evaluada, incluyendo el grado de independencia del evaluador.

8.4 Temas cubiertos por la evaluación

La lista de los temas abordados en la evaluación y/o la metodología de evaluación utilizada para realizar la evaluación.

8.5 Acciones a tomar como resultado de una deficiencia

Define las medidas adoptadas como resultado de las deficiencias encontradas durante la evaluación, las medidas probables incluyen una suspensión temporal de las operaciones hasta que corrija las deficiencias,

la revocación de los certificados emitidos a la entidad evaluada, cambios de personal, inducción a investigaciones especiales o evaluaciones de cumplimiento posteriores más frecuentes, y reclamos por daños y perjuicios contra la entidad evaluada.

8.6 Comunicación de los resultados

Establece quién tiene derecho de ver los resultados de la auditoria, de que medio/forma y su posterior publicación.

9. OTROS ASUNTOS LEGALES Y COMERCIALES

9.1 Tarifas

Este subcomponente debería contener las disposiciones aplicables en relación con los honorarios a percibir por los distintos servicios.

9.1.1 Tarifa por emisión o renovación de certificados

9.1.2 Tarifa por acceso al certificado

9.1.3 Tarifa por acceso de información de estado o revocación

9.1.4 Tarifas por otros servicios

9.1.5 Política de reembolso

9.2 Responsabilidad financiera

Este subcomponente debería contener los requisitos o divulgaciones relacionadas con los recursos disponibles del Proveedor de Servicio de Certificación y otros participantes que presten servicios de certificación para respaldar el desempeño de sus responsabilidades operacionales de su Infraestructura de Clave Pública, y para mantener su solvencia y pagar daños y perjuicios en caso de que están obligados a pagar una sentencia o resolución en relación con un reclamo derivado de dichas operaciones. Tales disposiciones incluyen:

9.2.1 Cobertura del seguro

Describe una declaración de que el participante mantiene una cierta cantidad de cobertura de seguro para sus responsabilidades con otros participantes. Así como una especificación clara de que riesgos y que montos son cubiertos por el seguro del Proveedor de Servicio de Certificación.

9.2.2 Otros activos

Especifica una declaración de que un participante tiene acceso a otros recursos para respaldar las operaciones y pagar daños y perjuicios por posibles responsabilidades, que puede expresarse en términos de un nivel mínimo de activos necesarios para operar y cubrir las contingencias que pudieran ocurrir dentro de una Infraestructura de Clave Pública.

9.2.3 Cobertura de seguro o garantía para entidades finales

Especifica una declaración de que un participante tiene un programa que ofrece protección de garantía o seguro a los otros participantes en relación con el uso de la Infraestructura de Clave Pública.

9.3 Confidencialidad de la información del negocio

Este subcomponente contiene disposiciones relacionadas con el tratamiento de la información confidencial del Proveedor de Servicio de Certificación que los participantes pueden comunicarse entre sí, tales como planes de negocios, información de ventas, secretos comerciales e la información recibida de un tercero en virtud de un acuerdo de confidencialidad. Específicamente, este subcomponente debe contener:

9.3.1 Alcance de la información confidencial

Se especifica la información considerada confidencial por el Proveedor de Servicios de Certificación tanto de la autoridad de certificación como por las autoridades de registro vinculadas.

9.3.2 Información fuera del alcance de la información confidencial

Se especifica cuál es el tipo de información que se consideran no confidencial.

9.3.3 Responsabilidad de proteger la información confidencial

Las responsabilidades de los participantes que reciben información confidencial para protegerla de cualquier compromiso y abstenerse de usarla o divulgarla a terceros.

9.4 Privacidad de la información personal

Este subcomponente se refiere a la protección que los participantes, en particular las autoridades de certificación, las autoridades de registro y los repositorios, deberían ofrecer a la información privada de identificación personal de los solicitantes de certificados, suscriptores y otros participantes. Concretamente, este subcomponente aborda lo siguiente, en la medida en que sea pertinente en virtud de la legislación aplicable, entre ellas la Ley 787 Ley de Protección de Datos Personales:

9.4.1 Plan de privacidad

Especifica la designación y divulgación del plan de privacidad que se aplica a las actividades de un participante, si así lo requiere la ley o política aplicable.

9.4.2 Información tratada como privada

Establece los procesos de protección de la información considerada como privada.

Cualquier responsabilidad de los participantes que reciben información privada para asegurarla, y se abstengan de usarla y de divulgarla a terceros.

9.4.3 Información no considerada privada

Establece los procesos de protección de la información considerada como no privada.

9.4.4 Responsabilidad de proteger la información privada

Especifica la responsabilidad de los participantes que reciben información privada para asegurarla, y se abstengan de usarla y de divulgarla a terceros.

9.4.5 Notificación y consentimiento para utilizar información privada

Cualquier requisito de notificación o consentimiento de las personas con respecto al uso o divulgación de información privada.

9.4.6 Divulgación de conformidad con un proceso judicial o administrativo

Comunicación de la información a autoridades administrativas y/o judiciales.

Contempla cualquier circunstancia bajo la cual un participante tiene derecho o se requiere que divulgue información privada conforme a un proceso judicial, administrativo en un procedimiento privado o gubernamental, o en cualquier procedimiento legal.

9.4.7 Otras circunstancias de divulgación de información

Contempla la comunicación de la información a otras autoridades de certificación.

9.5 Derechos de propiedad intelectual

Este subcomponente aborda los derechos de propiedad intelectual, tales como derechos de autor, patentes, marcas o secretos comerciales, que algunos participantes pueden tener o reclamar en una Política de Certificado, Declaración de Práctica de Certificación o en un certificado, sobre los nombres, y las claves, o son objeto de una licencia o para un participante. Para ello debería considerar las normativas vigentes como la “Ley de Derechos de Autor y Conexos”, la “Ley de Marcas y otros signos distintivos” y otras relacionadas.

9.6 Representaciones y garantías

Este subcomponente puede incluir representaciones y garantías de las diversas entidades que están de conformidad con la Política de Certificado o Declaración de Práctica de Certificación. Este subcomponente también puede incluir los requisitos de que las representaciones y garantías deberían de estar contenidas en algunos acuerdos, como acuerdos de suscriptores o las partes de que confía. Los participantes que pueden hacer representaciones y garantías son: la autoridad de certificación o autoridad de registro, los suscriptores, las partes que confían, y otros participantes. Por lo que deben representarse con los siguientes componentes:

9.6.1 Representaciones y garantías de la AC

9.6.2 Representaciones y garantías de la AR

9.6.3 Representaciones y garantías del suscriptor

9.6.4 Representaciones y garantías de las partes que confían

9.6.5 Representaciones y garantías de otros participantes

9.7 Renuncias de garantías

Este subcomponente puede incluir renuncias de garantías expresas que de otro modo se considera que existen en un acuerdo, y renuncias de garantías implícitas que de otro modo podrían ser impuestas por la ley aplicable, como las garantías de comerciabilidad o idoneidad para un propósito particular. La Política de Certificado o La Declaración de Prácticas de Certificación pueden imponer directamente tales renuncias

de responsabilidad, la Política de Certificado o La Declaración de Prácticas de Certificación pueden contener un requisito que establezca que las renuncias de responsabilidad sean contenidas en los acuerdos asociados, como los acuerdos de suscriptores o partes que confían. Debe armonizar con la ley de derechos de consumidor Nicaragüense y otra aplicable.

9.8 Limitaciones de responsabilidad

Este subcomponente puede incluir limitaciones de responsabilidad en una la Política de Certificado o la Declaración de Prácticas de Certificación o limitaciones que aparecen o deberían aparecer en un acuerdo asociado con la política de certificado o la declaración de prácticas de certificación, como un suscriptor o acuerdo de la parte que confía.
Estas limitaciones pueden caer en una de dos categorías: limitaciones en los elementos de daños recuperables y limitaciones en la cantidad de daños recuperables, también conocidos como límites de responsabilidad.

9.9 Indemnizaciones

Este subcomponente debería de considerar, que se cubran los riesgos de responsabilidad por daños a terceros que se pudiesen ocasionar a terceros como resultados de las actividades de certificación electrónica a cargo de la AC.

9.10 Vigencia y Terminación

Este subcomponente puede incluir el período de tiempo en el que una Política de Certificado o Declaración de Práctica de Certificación permanece vigente y las circunstancias bajo las cuales el documento, las partes del documento, o su aplicabilidad a un participante en particular pueden ser terminadas. Además, o alternativamente, la Política de Certificado o Declaración de Práctica de Certificación puede prescribir que ciertas cláusulas de vigencia y terminación aparezcan en los acuerdos, del suscriptor o partes que confían. En particular, tales condiciones deberían incluir los siguientes tópicos:

9.10.1 Vigencia

Determinar el periodo de tiempo en que una DPC, PC, documento o un acuerdo, permanecen vigentes.

9.10.2 Terminación

Definir las circunstancias en las cuales la DPC o la PC, ciertas partes de estas mismas (DPC o PC) o su aplicabilidad cesen o queden sin efecto.

9.10.3 Efecto de terminación y supervivencia

Este subcomponente contempla las consecuencias de la terminación del documento, por ejemplo, que es lo que se mantienen vigente aun después de terminado el documento.

Algunos ejemplos son los reconocimientos de los derechos de propiedad intelectual y las disposiciones sobre confidencialidad. Además, la terminación puede provocar la responsabilidad de las partes de devolver la información confidencial a la parte que la divulgó.

9.11 Notificaciones individuales y comunicaciones con los participantes

Este subcomponente debería analizar la forma en que un participante puede o debe comunicarse con otro participante en una base de uno a uno, a fin de que este tipo de comunicaciones sean jurídicamente

efectivas. Este subcomponente es diferente de las funciones de publicación y repositorio, porque a diferencia de las comunicaciones individuales que se describen en este subcomponente, publicación y anuncio a un repositorio están con el fin de comunicar a un público más amplio de destinatarios, como todas las partes de confianza. Este subcomponente puede establecer mecanismos de comunicación e indicar la información de contacto que se usa para en rutar las comunicaciones tales como las notificaciones firmadas electrónicamente por correo electrónico a una dirección específica, seguido de un correo electrónico firmado el acuse de recibo.

9.12 Enmiendas

Este subcomponente contempla las modificaciones necesarias a una Política de Certificado o Declaración de Prácticas de Certificación. Cualesquiera de estos cambios no reducen substancialmente la seguridad que proporciona una Política de Certificado o su implementación, y el administrador de la política evalúa si tienen un efecto insignificante sobre la aceptabilidad de los certificados. Tales cambios a una Política de Certificado o Declaración de Práctica de Certificación no deben exigir un cambio en el identificador de objeto de la Política de Certificado o el puntero de ubicación (URL) de la Declaración de Práctica de Certificación. Por otra parte, algunos cambios en una especificación cambiarán sustancialmente la aceptabilidad de los certificados para fines específicos, y estos cambios pueden requerir modificaciones correspondientes en el identificador de objeto (OID) de la Política de Certificado o el puntero de ubicación URL de la Declaración de Práctica de Certificación.

Este subcomponente también debe contener la siguiente información:

9.12.1 Procedimiento de enmiendas

Especifica los procedimientos por los cuales la Política de Certificado o Declaración de Prácticas de Certificación y / u otros documentos deben, pueden ser o son enmendados. En el caso de las enmiendas de la Política de Certificado o Declaración de Prácticas de Certificación, los procedimientos de cambio pueden incluir un mecanismo de notificación.

9.12.2 Mecanismo y periodo de notificación

Especifica mecanismo de notificación para notificar las enmiendas propuestas a las partes afectadas, tales como suscriptores y partes que confían, también se notifica un período de comentarios, un mecanismo por el cual los comentarios se reciben revisan e incorporan en la documentación, y un mecanismo por el cual las enmiendas se vuelven definitivas y efectivas.

9.12.3 Circunstancias bajo las cuales el identificador de objeto tiene que ser cambiado

Especifica el procedimiento y circunstancias bajo las cuales las enmiendas a la Política de Certificado o Declaración de Prácticas de Certificación requieren un cambio en el Identificador de Objeto (OID) de la Política de Certificado o el puntero (URL) de la Declaración de Prácticas de Certificación.

9.13 Disposiciones sobre resolución de diputas

Este subcomponente analiza los procedimientos utilizados para resolver las controversias que surjan de la Política de Certificado, Declaración de Práctica de Certificación y/o acuerdos.

Se especifican todas las diferencias, desavenencias y/o controversias que se produzcan entre las partes y además se identifica el ente que soluciona el conflicto y se establece la Ley para este tipo de casos.

9.14 Ley aplicable

Este subcomponente establece una declaración de que la ley de una determinada jurisdicción determinada rige la interpretación y aplicación de las Políticas de Certificado o Declaración de Prácticas de Certificación.

9.15 Cumplimiento de la ley aplicable

Este subcomponente se refiere a los requisitos establecidos de que los participantes cumplan con la ley aplicable, por ejemplo, las leyes relacionadas con el hardware y el software criptográfico que pueden estar sujeto a las leyes de control de exportación de una determinada jurisdicción. La Política de Certificado o Declaración de Prácticas de Certificación podría pretender imponer tales requisitos o puede requerir que dichas disposiciones figuran en otros acuerdos.

9.16 Disposiciones diversas

Este subcomponente contiene disposiciones diversas de los contratos. Las cláusulas cubiertas en este subcomponente pueden aparecer en una Política de Certificado, Declaración de Prácticas de Certificación, o acuerdos, e incluyen:

9.16.1 Acuerdo completo

Este subcomponente contempla una cláusula de acuerdo completo, que típicamente identifica el documento o documentos que constituyen el acuerdo completo entre las partes y establece que tales acuerdos reemplazan todos los acuerdos anteriores y contemporáneos escritos u orales relacionados con el mismo tema.

9.16.2 Asignación

Este subcomponente contempla una cláusula de asignación, que puede actuar para limitar la capacidad de una parte en un acuerdo, asignando sus derechos bajo el acuerdo a un tercero (por ejemplo, el derecho a recibir una serie de pagos en el futuro) o limitando la capacidad de una parte para delegar sus obligaciones en virtud del acuerdo.

9.16.3 Divisibilidad

Este subcomponente contempla una cláusula que establezca las intenciones de las partes en el caso de que una corte u otro tribunal determinan que una cláusula en un acuerdo es, por alguna razón, no válida o no ejecutable, y cuya finalidad es con frecuencia para evitar la inaplicabilidad de una cláusula de hacer que todo contrato no sea exigible.

9.16.4 Cumplimiento (honorarios de abogados y renuncia de derechos)

Este subcomponente contempla una cláusula de cumplimiento/ejecución, que indique que cualquier parte que prevalezca en una disputa que surja de un acuerdo tiene derecho a los honorarios de abogados como parte de su recuperación, o puede indicar que la renuncia de una parte de un incumplimiento de contrato no constituirá una renuncia continua o una renuncia futura de otros incumplimientos de contrato.

9.16.5 Fuerza mayor

Este subcomponente, es comúnmente utilizado para justificar el cumplimiento de una o más partes en un acuerdo debido a un evento fuera del control razonable de la parte o partes afectadas. Por lo general, la duración de la actuación justificada es proporcional a la duración de la demora causada por el evento. La

cláusula también puede prever la terminación del acuerdo en circunstancias y condiciones especificadas. Las cláusulas de fuerza mayor deben redactarse de manera que sea coherente con otras partes de la estructura y los acuerdos de nivel de servicio aplicables.

9.17 Otras disposiciones

Este subcomponente es un lugar en el que se pueden imponer responsabilidades y los términos adicionales a los participantes de la Infraestructura de Clave Pública que no encajan dentro de uno de los otros componentes o subcomponentes del marco. Los redactores de la Política de Certificado o Declaración de Prácticas de Certificación, pueden colocar cualquier disposición dentro de este subcomponente que no esté cubierto por otro subcomponente.

VIII. ANEXOS

Anexo 1: Estándares relacionados

A continuación, se presentan estándares relacionados al RFC 3647 los cuales presentan algunas variantes el RFC en referencia, ver también el anexo 2: "Referencia cruzada del contenido de este documento, el RFC 3647 y estándares relacionados".

1. IETF RFC 3647: Infraestructura de clave pública X.509 de internet: Marco de prácticas de certificación y política de certificados

El estándar IETF RFC 3647 presenta un marco para elaborar PC o DPC para AC, AP y comunidades de interés que deseen confiar en los certificados. El marco proporciona una lista completa de temas que potencialmente deben cubrirse en una PC o una DPC, define e indica cual es el contenido de cada cláusula de una PC o DPC.

2. ETSI EN 319 411-1: Política y requisitos de seguridad para proveedores de servicios de confianza que emiten certificados, parte 1: requisitos generales

El estándar ETSI EN 319 411-1, está estructurado en términos generales de acuerdo con el IETF RFC 3647, especifica los requisitos de control para los Proveedores de Servicios de Certificación, los cuales se deben de cumplir en cada cláusula de la estructura de la Declaración de Practicas de Certificación. Los requisitos se indican en términos de los objetivos de seguridad, seguido por requisitos más específicos para que los controles cumplan con esos objetivos cuando se considere necesario proporcionar la confianza de que se cumplirán esos objetivos.

Además de especificar los requisitos de cada cláusula de la DPC, especifica políticas y requisitos de seguridad de aplicación general para los PSC.

En la cláusula 7 establece un marco para la definición de requisitos de políticas de certificados para los PSC que emiten certificados en un contexto especifico donde se aplican requisitos particulares.

Este estándar presenta en la cláusula 5 las "Disposiciones Generales Sobre Declaración de Prácticas De Certificación Y Políticas de Certificados" lo que en el RFC corresponde a la cláusula 1. Introducción, y separado como cláusula 6 presenta las "Prácticas de los Proveedores de Servicios de Confianza" que agrupa las cláusulas que corresponden en el RFC 3647 a las cláusulas 2. Responsabilidades de publicación y repositorio, 3. Identificación y autenticación, 4. Requisitos Operativos del Ciclo de Vida del Certificado, 5. Controles de Instalaciones, Gestión y Operacionales, 6. Controles de Seguridad Técnica, 7. Perfiles de Certificados, Lista de Revocación de Certificado y Protocolo de Estado del Certificado en Línea, 8. Cumplimiento de Auditoría y Otras Evaluaciones, 9. Otros asuntos y cuestiones legales.

3. ETSI EN 319 411-2: Política y requisitos de seguridad para proveedores de servicios de confianza que emiten certificados, parte 2: Requisitos para los proveedores de servicios de confianza que emiten certificados calificados de la UE

El estándar ETSI EN 319 411-2, está estructurado en términos generales de acuerdo con el IETF RFC 3647,

El ETSI EN 319 411-2 incorpora la política general y los requisitos de seguridad como se especifica en ETSI EN 319 411-1 y agrega requisitos adicionales para cumplir con los requisitos específicos del Reglamento (UE) N° 910/2014 para los Proveedores de Servicios de Confianza que emiten certificados calificados de la Unión Europea. Estos requisitos de política y seguridad respaldan las políticas de

certificados de referencia para la emisión, el mantenimiento y la gestión del ciclo de vida de los certificados cualificados de la Unión Europea emitidos a personas físicas y a personas jurídicas.

4. ISO/IEC 27099: Tecnología de la información - infraestructura de clave pública - marco de políticas y practicas

Este estándar indica que los PSC deben de cumplir lo establecido por el RFC 3647.

Establece una estructura de requisitos para administra la seguridad de la información de la ICP de los PSC a través de PC, DPC, Objetivos de Control y Procedimientos de apoyo. La estructura de requerimientos incluye la evaluación y el tratamiento de los riesgos de la seguridad de la información.

Presenta la relación de la PC, DPC y los Sistemas de Gestión de Seguridad de la Información - SGSI, establece que la PC se enfoca en la responsabilidad de los PSC de la ICP, mientras que los SGSI su objetivo es la administración de la seguridad dentro de la organización de una ICP de los Proveedores de Servicios de Confianza, y establece que ambos están unidos por la DPC.

Establece que la PC de la AC son necesarias para controlar los procedimientos que son adecuados y que se basan en la evaluación de riesgos de la AC y cumplen con los requisitos de las políticas de certificación admitidas.

Presenta los criterios de control base con los que debe de cumplir una AC y con los que puede ser evaluada o auditada, como son: los objetivos de control en las áreas de controles físicos y ambientales de la AC, gestión del ciclo de vida de la clave de la AC, gestión del ciclo de vida del certificado y controles de la AC raíz que son presentado en las cláusulas del 7.2 al 7.17, los objetivos se abordaran mediante requisitos alternativos establecidos en la política de certificación. Los controles de la AC deben de ser descritos en la DPC.

Establece que la DPC de una AC contendrá solo los procedimientos de control que sean apropiados en función de la evaluación de riesgos de la AC para respaldar las políticas de certificación bajo las cuales se emiten los certificados.

Establece que, al evaluar la conformidad de la AC con los objetivos y procedimientos de control de la AC, el evaluador debe revisar la DPC y la PC de la AC.

En la cláusula 6.3 presenta las Directrices para la Declaración de Prácticas de Certificación, indica que las prácticas de certificación de una AC son necesarias para los procedimientos de control los que se basan en la evaluación de riesgos de la AC y cumplen con los requisitos de la PC admitida.

5. WebTrust para autoridades de certificación - principios y criterios de Webtrust para AC

Este documento proporciona un marco para evaluar la idoneidad y eficacia de los controles utilizados por las Autoridades de Certificación.

Establece que la AC divulga sus prácticas de negocio, de gestión del ciclo de vida de las claves, gestión del ciclo de vida del certificado y control ambiental de AC en su DPC, y también divulga sus prácticas de negocio, gestión del ciclo de vida de la clave, gestión del ciclo de vida del certificado y control ambiental de AC en su PC.

Establece que, la AC mantiene controles efectivos para proporcionar una seguridad razonable de que:

- La Declaración de Prácticas de Certificación de la AC es consistente con su Política de Certificación.

- La AC presta sus servicios de acuerdo con su Política de Certificación y con su Declaración de Prácticas de Certificación.

Los principios y criterios de WebTrust para las autoridades de certificación recomiendan que las AC estructuren sus documentos PC o DPC de acuerdo con IETF RFC 3647.

La AC establece sus estándares y prácticas mediante las cuales prestará los servicios en su DPC y en su Política(s) de Certificado publicadas.

Establece que los principios y criterios definidos en WebTrust son un marco de control para evaluar la idoneidad de los sistemas, políticas y procedimientos de la AC. Proporciona una base para la autoevaluación, ya sea para el desarrollo o el mantenimiento de sistemas ICP sólidos.

Establece los controles que deben evaluarse para logar cada criterio de WebTrust.

Establece en la cláusula 2.1 la gestión de la DPC en la que define que:

- La AP tiene la autoridad final y la responsabilidad de aprobar la DPC de la AC.
- Las responsabilidades para el mantenimiento de la DPC han sido formalmente asignadas.
- La DPC de la AC se modifica y aprueba de acuerdo con un proceso de revisión definido.
- La AC pone a disposición de todas las partes correspondientes su DPC.
- Las revisiones de la DPC de la AC se ponen a disposición de las partes correspondientes.
- La AC actualiza su DPC para reflejar los cambios en el entorno a medida que ocurren.

Establece en la cláusula 2.2 la gestión de la PC en la que define que:

- La AP tiene la responsabilidad de definir los requisitos y políticas de negocio para el uso de certificados digitales y especificarlos en una PC y acuerdos de respaldo.
- El AP tiene la autoridad y responsabilidad final para definir y aprobar las PC.
- Existe un proceso de revisión definido para evaluar que la(s) PC son compatibles con los controles especificados en la DPC.
- La AP pone a disposición de los Suscriptores y Partes que Confían las PC soportadas por la AC.

Anexo 2: Referencia cruzada del contenido de este documento, el RFC 3647 y estándares relacionados

CLAUSULAS EN ESTE DOCUMENTO	RFC 3647	ETSI EN 319 411-1 V1.3.1 y ETSI EN 319 411-2 V2.4.1	ISO/IEC 27099:2022	WebTrust for AC V2.2.2
		5. GENERAL PROVISIONS ON CPS AND CP		
1. INTRODUCCIÓN	**1.INTRODUCTIONS**	**5.1 GENERAL REQUIREMENTS**	**1.INTRODUCTION**	**1.INTRODUCTION**
1.1 Información general.	1.1 Overview.	5.2 Certification Practice Statement requirements .	1.1 Overview.	1.1 Overview.
1.2 Nombre e identificación del documento.	1.2 Document name and identification.	5.3 Certificate Policy name and identification.	1.2 Document name and identification.	1.2 Document name and identification.
1.3 Participantes de la ICP.	1.3 PKI participants.	5.4. PKI participants.	1.3 PKI participants.	1.3 PKI participants.
1.3.1 Autoridades de Certificación.	1.3.1 Certification Authorities.	5.4.1 Certification Authority.	1.3.1 Certification Authorities.	1.3.1 Certification Authorities.
1.3.2 Autoridades de registro.	1.3.2 Registration Authorities.		1.3.2 Registration Authorities.	1.3.2 Registration Authorities.
1.3.3 Suscriptores.	1.3.3 Subscribers.	5.4.2 Subscriber and subject.	1.3.3 Subscribers.	1.3.3 Subscribers.
1.3.4. Partes que confían.	1.3.4 Relying parties.		1.3.4 Relying parties.	1.3.4 Relying parties.
1.3.5 Otros participantes.	1.3.5 Other participants.	5.4.3 Others.	1.3.5 Other participants.	1.3.5 Other participants.
1.4 Usos del certificado.	1.4 Certificate usage.	5.5 Certificate usage.	1.4 Certificate usage.	1.4 Certificate usage.
1.4.1 Usos apropiados del certificado.	1.4.1 Appropriate certificate uses.		1.4.1 Appropriate certificate uses.	1.4.1 Appropriate certificate uses.
1.4.2 Usos prohibidos del certificado.	1.4.2 Prohibited certificate uses.		1.4.2 Prohibited certificate uses.	1.4.2 Prohibited certificate uses.
1.5 Administración de políticas	1.5 Policy administration.		1.5 Policy administration.	1.5 Policy administration.
1.5.1 Organización que administra el documento.	1.5.1 Organization administering the document.		1.5.1 Organization administering the document.	1.5.1 Organization administering the document.
1.5.2 Persona de contacto	1.5.2 Contact person.		1.5.2 Contact person.	1.5.2 Contact person.
1.5.3 Persona que determina la idoneidad de la DPC para la política.	1.5.3 Person determining CPS suitability for the policy.		1.5.3 Person determining CPS suitability for the policy.	1.5.3 Person determining CPS suitability for the policy.
1.5.4 Procedimientos de aprobación de la declaración de práctica de certificación.	1.5.4 CPS Approval procedures.		1.5.4 CPS Approval procedures.	1.5.4 CPS Approval procedures.
1.6 Definiciones y acrónimos.	1.6 Definitions And acronyms.		1.6 Definitions And acronyms.	1.6 Definitions And acronyms.
		6. TRUST SERVICE PROVIDERS PRACTICE		
2. PUBLICACIÓN Y RESPONSABLILIDADES DEL REPOSITORIO.	**2. PUBLICATION AND REPOSITORY RESPONSIBILITIES**	**6.1 PUBLICATION AND REPOSITORY RESPONSIBILITIES.**	**2. GENERAL PROVISIONS**	**2. GENERAL PROVISIONS**
2.1 Publicación y Responsabilidades del Repositorios	2.1 Publication and Repository Responsibilities.		2.1 Repositories.	2.1 Repositories.
2.2 Publicación de información de certificación	2.2 Publication of certification information.		2.2 Publication of certification information.	2.2 Publication of certification information.
2.3 Tiempo o frecuencia de publicación	2.3 Time or frequency of publication.		2.3 Time or frequency of publication.	2.3 Time or frequency of publication.

CLAUSULAS EN ESTE DOCUMENTO	RFC 3647	ETSI EN 319 411-1 V1.3.1 y ETSI EN 319 411-2 V2.4.1	ISO/IEC 27099:2022	WebTrust for AC V2.2.2
2.4 Controles de acceso a los repositorios	2.4 Access controls on repositories.		2.4 Access controls on repositories.	2.4 Access controls on repositories.
3. IDENTIFICACIÓN Y AUTENTICACIÓN	**3. IDENTIFICATION AND AUTHENTICATION**	**6.2 IDENTIFICATION AND AUTHENTICATION**	**3. IDENTIFICATION AND AUTHENTICATION**	**3. IDENTIFICATION AND AUTHENTICATION**
3.1 Denominación	3.1 Naming.	6.2.1 Naming.	3.1 Naming.	3.1 Naming.
3.1.1 Tipos de nombres	3.1.1 Types of names.		3.1.1 Types of names.	3.1.1 Types of names.
3.1.2 Necesidad de que los nombres sean significativos	3.1.2 Need for names to be meaningful.		3.1.2 Need for names to be meaningful.	3.1.2 Need for names to be meaningful.
3.1.3 El anonimato o seudónimos de los suscriptores	3.1.3 Anonymity or pseudonymity of subscribers.		3.1.3 Anonymity or pseudonymity of subscribers.	3.1.3 Anonymity or pseudonymity of subscribers.
3.1.4 Reglas para interpretar varias formas de nombres	3.1.4 Rules for interpreting various name forms.		3.1.4 Rules for interpreting various name forms.	3.1.4 Rules for interpreting various name forms.
3.1.5 Unicidad de los nombres	3.1.5 Uniqueness of names.		3.1.5 Uniqueness of names.	3.1.5 Uniqueness of names.
3.1.6 Reconocimiento, autenticación y función de las marcas registradas	3.1.6 Recognition, authentication, and role of trademarks.		3.1.6 Recognition, authentication, and role of trademarks.	3.1.6 Recognition, authentication, and role of trademarks.
3.2 Validación inicial de identidad	3.2 Initial identity validation.	6.2.2 Initial identity validation.	3.2 Initial identity validation.	3.2 Initial identity validation.
3.2.1 Método para probar posesión de la clave privada	3.2.1 Method To Prove possession of private key.		3.2.1 Method To Prove possession of private key.	3.2.1 Method To Prove possession of private key.
3.2.2 Autenticación de la identidad de la organización	3.2.2 Authentication of organization identity.		3.2.2 Authentication of organization identity.	3.2.2 Authentication of organization identity.
3.2.3 Autenticación de la identidad individual	3.2.3 Authentication of individual identity.		3.2.3 Authentication of individual identity.	3.2.3 Authentication of individual identity.
3.2.4 Información del suscriptor no verificada	3.2.4 Non-Verified subscriber information.		3.2.4 Non-Verified subscriber information.	3.2.4 Non-Verified subscriber information.
3.2.5 Validación de autoridad	3.2.5 Validation of authority.		3.2.5 Validation of authority.	3.2.5 Validation of authority.
3.2.6 Criterios para la interoperación	3.2.6 Criteria for interoperation.		3.2.6 Criteria for interoperation.	3.2.6 Criteria for interoperation.
3.3 Identificación y autenticación para solicitudes de renovación de claves	3.3 Identification and authentication for re-key requests.	6.2.3 Identification and authentication for Re-key requests.	3.3 Identification and authentication for re-key requests.	3.3 Identification and authentication for re-key requests.
3.3.1 Identificación y autenticación para la renovación rutinaria de claves	3.3.1 Identification and authentication for routine re-key.	6.2.3 Identification and authentication for Re-key requests. (el 3.3.1 del RFC 3647esta incluido en el 6.2.3 según el REG-6.2.3-01).	3.3.1 Identification and authentication for routine re-key.	3.3.1 Identification and authentication for routine re-key.
3.3.2 Identificación y autenticación para la renovación de la clave después de una revocación	3.3.2 Identification and authentication for re-key after revocation.	6.2.3 Identification and authentication for Re-key requests. (el 3.3.2 del RFC 3647esta incluido en el 6.2.3 según el REG-6.2.3-01).	3.3.2 Identification and authentication for re-key after revocation.	3.3.2 Identification and authentication for re-key after revocation.
3.4 Identificación y autenticación para la solicitud de revocación	3.4 Identification and authentication for revocation request.	6.2.4 Identification and authentication for revocation requests.	3.4 Identification and authentication for revocation request.	3.4 Identification and authentication for revocation request.
4. REQUISITOS OPERATIVOS DEL CICLO DE VIDA DEL CERTIFICADO	**4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS**	**6.3 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS**	**4. OPERATIONAL REQUIREMENTS**	**4. OPERATIONAL REQUIREMENTS**

CLAUSULAS EN ESTE DOCUMENTO	RFC 3647	ETSI EN 319 411-1 V1.3.1 y ETSI EN 319 411-2 V2.4.1	ISO/IEC 27099:2022	WebTrust for AC V2.2.2
4.1 solicitud de certificado.	4.1 Certificate application.	6.3.1 Certificate application.	4.1 Certificate application.	4.1 Certificate application.
4.1.1 Quién puede presentar una solicitud de certificado.	4.1.1 Who can submit a certificate application.		4.1.1 Who can submit a certificate application.	4.1.1 Who can submit a certificate application.
4.1.2 Proceso de inscripción y responsabilidades.	4.1.2 Enrollment process and responsibilities.		4.1.2 Enrollment process and responsibilities.	4.1.2 Enrollment process and responsibilities.
4.2 Procesamiento de solicitud de certificado.	4.2 Certificate application processing.	6.3.2 Certificate application processing.	4.2 Certificate application processing.	4.2 Certificate application processing.
4.2.1 Realización de funciones de identificación y de autenticación	4.2.1 Performing identification and authentication functions.		4.2.1 Performing identification and authentication functions.	4.2.1 Performing identification and authentication functions.
4.2.2 Aprobación o rechazo de las solicitudes de certificado	4.2.2 Approval or rejection of certificate applications.		4.2.2 Approval or rejection of certificate applications.	4.2.2 Approval or rejection of certificate applications.
4.2.3 Tiempo para procesar las solicitudes de certificados	4.2.3 Time to process certificate applications.		4.2.3 Time to process certificate applications.	4.2.3 Time to process certificate applications.
4.3 Emisión del certificado	4.3 Certificate issuance.	6.3.3 Certificate issuance.	4.3 Certificate issuance.	4.3 Certificate issuance.
4.3.1 Acciones de la autoridad de certificación durante la emisión del certificado	4.3.1 CA Actions during certificate issuance.		4.3.1 CA Actions during certificate issuance.	4.3.1 CA Actions during certificate issuance.
4.3.2 Notificación al suscriptor por la autoridad de certificación de la emisión del certificado	4.3.2 Notification to subscriber by the ca of issuance of certificate.		4.3.2 Notification to subscriber by the ca of issuance of certificate.	4.3.2 Notification to subscriber by the ca of issuance of certificate.
4.4 Aceptación del certificado	4.4 Certificate acceptance.	6.3.4 Certificate acceptance.	4.4 Certificate acceptance.	4.4 Certificate acceptance.
4.4.1 Conducta que constituye aceptación de certificados	4.4.1 Conduct constituting certificate acceptance.		4.4.1 Conduct constituting certificate acceptance.	4.4.1 Conduct constituting certificate acceptance.
4.4.2 Publicación del certificado por la autoridad de certificación	4.4.2 Publication of the certificate by the CA.		4.4.2 Publication of the certificate by the CA.	4.4.2 Publication of the certificate by the CA.
4.4.3 Notificación de la emisión del certificado por la autoridad de certificación a otras entidades	4.4.3 Notification of certificate issuance by the CA to other entities.		4.4.3 Notification of certificate issuance by the CA to other entities.	4.4.3 Notification of certificate issuance by the CA to other entities.
4.5 Uso del par de claves y del certificado	4.5 Key pair and certificate usage.	6.3.5 Key pair and certificate usage.	4.5 Key pair and certificate usage.	4.5 Key pair and certificate usage.
4.5.1 Uso de la clave privada y del certificado por el suscriptor	4.5.1 Subscriber private key and certificate usage.		4.5.1 Subscriber private key and certificate usage.	4.5.1 Subscriber private key and certificate usage.
4.5.2 Uso de la clave pública y del certificado por la parte que confía	4.5.2 Relying party public key and certificate usage.		4.5.2 Relying party public key and certificate usage.	4.5.2 Relying party public key and certificate usage.
4.6 Renovación del certificado	4.6 Certificate renewal.	6.3.6 Certificate renewal.	4.6 Certificate renewal.	4.6 Certificate renewal.
4.6.1 Circunstancias para la renovación de certificados	4.6.1 Circumstance for certificate renewal.		4.6.1 Circumstance for certificate renewal.	4.6.1 Circumstance for certificate renewal.
4.6.2 Quién puede solicitar la renovación	4.6.2 Who may request renewal.		4.6.2 Who may request renewal.	4.6.2 Who may request renewal.
4.6.3 Procesamiento de solicitudes de renovación de certificado	4.6.3 Processing certificate renewal requests.		4.6.3 Processing certificate renewal requests.	4.6.3 Processing certificate renewal requests.

CLAUSULAS EN ESTE DOCUMENTO	RFC 3647	ETSI EN 319 411-1 V1.3.1 y ETSI EN 319 411-2 V2.4.1	ISO/IEC 27099:2022	WebTrust for AC V2.2.2
4.6.4 Notificación de la emisión de un nuevo certificado al suscriptor	4.6.4 Notification of new certificate issuance to subscriber.		4.6.4 Notification of new certificate issuance to subscriber.	4.6.4 Notification of new certificate issuance to subscriber.
4.6.5 Conducta que constituye la aceptación de la renovación del certificado	4.6.5 Conduct constituting acceptance of a renewal certificate.		4.6.5 Conduct constituting acceptance of a renewal certificate.	4.6.5 Conduct constituting acceptance of a renewal certificate.
4.6.6 Publicación del certificado renovado por la autoridad de certificación	4.6.6 Publication of the renewal certificate by the CA.		4.6.6 Publication of the renewal certificate by the CA.	4.6.6 Publication of the renewal certificate by the CA.
4.6.7 Notificación de la emisión del certificado por la autoridad de certificación a otras entidades	4.6.7 Notification of certificate issuance by the CA to other entities.		4.6.7 Notification of certificate issuance by the CA to other entities.	4.6.7 Notification of certificate issuance by the CA to other entities.
4.7 Renovación de las claves del certificado	4.7 Certificate Re-Key.	6.3.7 Certificate Re-key.	4.7 Certificate Re-Key.	4.7 Certificate Re-Key.
4.7.1 Circunstancias para renovación de las claves del certificado	4.7.1 Circumstance for certificate Re-Key.		4.7.1 Circumstance for certificate Re-Key.	4.7.1 Circumstance for certificate Re-Key.
4.7.2 Quién puede solicitar certificación de una nueva claves pública	4.7.2 Who may request certification of a new public key.		4.7.2 Who may request certification of a new public key.	4.7.2 Who may request certification of a new public key.
4.7.3 Procedimiento de solicitudes de cambio de clave del certificado	4.7.3 Processing certificate Re-Keying requests.		4.7.3 Processing certificate Re-Keying requests.	4.7.3 Processing certificate Re-Keying requests.
4.7.4 Notificación de la emisión de un nuevo certificado al suscriptor.	4.7.4 Notification of new certificate issuance to subscriber.		4.7.4 Notification of new certificate issuance to subscriber.	4.7.4 Notification of new certificate issuance to subscriber.
4.7.5 Conducta que constituye la aceptación de un certificado con clave renovada.	4.7.5 Conduct constituting acceptance of a Re-Keyed certificate.		4.7.5 Conduct constituting acceptance of a Re-Keyed certificate.	4.7.5 Conduct constituting acceptance of a Re-Keyed certificate.
4.7.6 Publicación del certificado con clave renovada por la AC.	4.7.6 Publication Of The Re-Keyed Certificate By The CA		4.7.6 Publication Of The Re-Keyed Certificate By The CA	4.7.6 Publication Of The Re-Keyed Certificate By The CA
4.7.7 Notificación de la emisión del certificado por la autoridad de certificación a otras entidades.	4.7.7 Notification of certificate issuance by the CA to other entities.		4.7.7 Notification of certificate issuance by the CA to other entities.	4.7.7 Notification of certificate issuance by the CA to other entities.
4.8 Modificación de certificado.	4.8 Certificate modification.	6.3.8 Certificate modification.	4.8 Certificate modification.	4.8 Certificate modification.
4.8.1 Circunstancias para la modificación del certificado.	4.8.1 Circumstance for certificate modification.		4.8.1 Circumstance for certificate modification.	4.8.1 Circumstance for certificate modification.
4.8.2 Quién puede solicitar modificación de un certificado.	4.8.2 Who may request certificate modification.		4.8.2 Who may request certificate modification.	4.8.2 Who may request certificate modification.
4.8.3 Procesamiento de solicitudes de modificación de un certificado.	4.8.3 Processing certificate modification requests.		4.8.3 Processing certificate modification requests.	4.8.3 Processing certificate modification requests.
4.8.4 Notificación de la emisión de un nuevo certificado al suscriptor.	4.8.4 Notification of new certificate issuance to subscriber.		4.8.4 Notification of new certificate issuance to subscriber.	4.8.4 Notification of new certificate issuance to subscriber.
4.8.5 Conducta que Constituye aceptación del certificado modificado.	4.8.5 Conduct constituting acceptance of modified certificate.		4.8.5 Conduct constituting acceptance of modified certificate.	4.8.5 Conduct constituting acceptance of modified certificate.

CLAUSULAS EN ESTE DOCUMENTO	RFC 3647	ETSI EN 319 411-1 V1.3.1 y ETSI EN 319 411-2 V2.4.1	ISO/IEC 27099:2022	WebTrust for AC V2.2.2
4.8.6 Publicación del certificado modificado por la autoridad de certificación.	4.8.6 Publication of the modified certificate by the CA.		4.8.6 Publication of the modified certificate by the CA.	4.8.6 Publication of the modified certificate by the CA.
4.8.7 Notificación de la emisión del certificado por la AC a otras entidades.	4.8.7 Notification of certificate issuance by the CA to other entities		4.8.7 Notification of certificate issuance by the CA to other entities	4.8.7 Notification of certificate issuance by the CA to other entities
4.9 Revocación y suspensión del certificado.	4.9 Certificate revocation and suspensión.	6.3.9 Certificate revocation and suspensión.	4.9 Certificate revocation and suspensión.	4.9 Certificate revocation and suspensión.
4.9.1 Circunstancias para la revocación.	4.9.1 Circumstances for revocation.		4.9.1 Circumstances for revocation.	4.9.1 Circumstances for revocation.
4.9.2 Quién puede solicitar la revocación.	4.9.2 Who can request revocation.		4.9.2 Who can request revocation.	4.9.2 Who can request revocation.
4.9.3 Procedimientos para la solicitud de revocación.	4.9.3 Procedure for revocation request.		4.9.3 Procedure for revocation request.	4.9.3 Procedure for revocation request.
4.9.4 Periodo de gracia de la solicitud de revocación.	4.9.4 Revocation request grace period.		4.9.4 Revocation request grace period.	4.9.4 Revocation request grace period.
4.9.5 Tiempo dentro del cual la AC debe procesar la solicitud de revocación.	4.9.5 Time within which CA must process the revocation request.		4.9.5 Time within which CA must process the revocation request.	4.9.5 Time within which CA must process the revocation request.
4.9.6 Requisito de verificación de revocación para las partes que confía.	4.9.6 Revocation checking requirement for relying parties.		4.9.6 Revocation checking requirement for relying parties.	4.9.6 Revocation checking requirement for relying parties.
4.9.7 Frecuencia de emisión de lista de certificados revocados.	4.9.7 CRL issuance frequency (if applicable).		4.9.7 CRL issuance frequency (if applicable).	4.9.7 CRL issuance frequency (if applicable).
4.9.8 Latencia máxima de LCR.	4.9.8 Maximum latency for crls (if applicable).		4.9.8 Maximum latency for crls (if applicable).	4.9.8 Maximum latency for crls (if applicable).
4.9.9 Disponibilidad de comprobación en línea de revocación/estado.	4.9.9 On-Line revocation/status checking availability.		4.9.9 On-Line revocation/status checking availability.	4.9.9 On-Line revocation/status checking availability.
4.9.10 Requisitos de comprobación en línea de la revocación.	4.9.10 On-Line revocation checking requirements.		4.9.10 On-Line revocation checking requirements.	4.9.10 On-Line revocation checking requirements.
4.9.11 Otras formas de divulgación de revocación disponibles.	4.9.11 Other forms of revocation advertisements available.		4.9.11 Other forms of revocation advertisements available.	4.9.11 Other forms of revocation advertisements available.
4.9.12 Requisitos especiales de renovación de clave por compromisos.	4.9.12 Special requirements Re Key compromise.		4.9.12 Special requirements Re Key compromise.	4.9.12 Special requirements Re Key compromise.
4.9.13 Circunstancias para la suspensión.	4.9.13 Circumstances for suspensión.		4.9.13 Circumstances for suspensión.	4.9.13 Circumstances for suspensión.
4.9.14 Quién puede solicitar la suspensión.	4.9.14 Who can request suspensión.		4.9.14 Who can request suspensión.	4.9.14 Who can request suspensión.
4.9.15 Procedimientos para la solicitud de suspensión.	4.9.15 Procedure for suspension request.		4.9.15 Procedure for suspension request.	4.9.15 Procedure for suspension request.
4.9.16 Límites en período de suspensión.	4.9.16 Limits on suspension period.		4.9.16 Limits on suspension period.	4.9.16 Limits on suspension period.
4.10 Servicios de estado del certificado.	4.10 Certificate status services.	6.3.10 Certificate status services.	4.10 Certificate status services.	4.10 Certificate status services.
4.10.1 Características operacionales.	4.10.1 Operational characteristics.		4.10.1 Operational characteristics.	4.10.1 Operational characteristics.
4.10.2 Disponibilidad del servicio.	4.10.2 Service Availability		4.10.2 Service Availability	4.10.2 Service Availability
4.10.3 Características opcionales.	4.10.3 Optional features.		4.10.3 Optional features.	4.10.3 Optional features.

CLAUSULAS EN ESTE DOCUMENTO	RFC 3647	ETSI EN 319 411-1 V1.3.1 y ETSI EN 319 411-2 V2.4.1	ISO/IEC 27099:2022	WebTrust for AC V2.2.2
4.11 Fin de suscripción.	4.11 End of subscription.	6.3.11 End of subscription.	4.11 End of subscription.	4.11 End of subscription.
4.12 Custodia y recuperación de claves.	4.12 Key Escrow and recovery.	6.3.12 Key escrow and recovery.	4.12 Key Escrow and recovery.	4.12 Key Escrow and recovery.
4.12.1 Prácticas y políticas de custodia y recuperación de claves.	4.12.1 Key escrow and recovery policy and practices.		4.12.1 Key escrow and recovery policy and practices.	4.12.1 Key escrow and recovery policy and practices.
4.12.2 Prácticas y políticas de encapsulado y recuperación de clave de sesión.	4.12.2 Session key encapsulation and recovery policy and practices.		4.12.2 Session key encapsulation and recovery policy and practices.	4.12.2 Session key encapsulation and recovery policy and practices.
5. CONTROLES DE GESTIÓN, OPERATIVOS Y FÍSICOS	**5. MANAGEMENT, OPERATIONAL, AND PHYSICAL CONTROLS**	**6.4 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS.**	**5. MANAGEMENT, OPERATIONAL, AND PHYSICAL CONTROLS**	**5. MANAGEMENT, OPERATIONAL, AND PHYSICAL CONTROLS**
		6.4.1 General.		
5.1 Controles de seguridad física.	5.1 Physical security controls.	6.4.2 Physical security controls.	5.1 Physical security controls.	5.1 Physical security controls.
5.1.1 Localización y construcción de instalaciones.	5.1.1 Site location and construction.		5.1.1 Site location and construction.	5.1.1 Site location and construction.
5.1.2 Acceso físico.	5.1.2 Physical Access.		5.1.2 Physical Access.	5.1.2 Physical Access.
5.1.3 Electricidad y aire acondicionado.	5.1.3 Power and air conditioning.		5.1.3 Power and air conditioning.	5.1.3 Power and air conditioning.
5.1.4 Exposición al agua.	5.1.4 Water exposures.		5.1.4 Water exposures.	5.1.4 Water exposures.
5.1.5 Prevención y protección de incendios.	5.1.5 Fire prevention and protection.		5.1.5 Fire prevention and protection.	5.1.5 Fire prevention and protection.
5.1.6 Medios de almacenamiento.	5.1.6 Media storage.		5.1.6 Media storage.	5.1.6 Media storage.
5.1.7 Eliminación de desechos.	5.1.7 Waste disposal.		5.1.7 Waste disposal.	5.1.7 Waste disposal.
5.1.8 Copia de seguridad fuera de las instalaciones.	5.1.8 Off-site backup.		5.1.8 Off-site backup.	5.1.8 Off-site backup.
5.2 Controles de procedimiento.	5.2 Procedural controls.	6.4.3 Procedural controls.	5.2 Procedural controls.	5.2 Procedural controls.
5.2.1 Roles de confianza.	5.2.1 Trusted Roles		5.2.1 Trusted Roles	5.2.1 Trusted Roles
5.2.2 Número de personas requeridas por tarea.	5.2.2 Number of persons required per task.		5.2.2 Number of persons required per task.	5.2.2 Number of persons required per task.
5.2.3 Identificación y autenticación para cada rol.	5.2.3 Identification and authentication for each role.		5.2.3 Identification and authentication for each role.	5.2.3 Identification and authentication for each role.
5.2.4 Roles que requieren separación de tareas.	5.2.4 Roles requiring separation of duties.		5.2.4 Roles requiring separation of duties.	5.2.4 Roles requiring separation of duties.
5.3 Controles de Seguridad Personal.	5.3 Personnel security controls.	6.4.4 Personnel controls.	5.3 Personnel security controls.	5.3 Personnel security controls.
5.3.1 Requisitos de Calificaciones, Experiencia, y Autorización.	5.3.1 Qualifications, experience, and clearance requirements.		5.3.1 Qualifications, experience, and clearance requirements.	5.3.1 Qualifications, experience, and clearance requirements.
5.3.2 Procedimientos de verificación de antecedentes y autorización.	5.3.2 Background check and clearance procedures.		5.3.2 Background check and clearance procedures.	5.3.2 Background check and clearance procedures.
5.3.3 Requisitos de capacitación.	5.3.3 Training requirements.		5.3.3 Training requirements.	5.3.3 Training requirements.
5.3.4 Frecuencia y requisitos de reentrenamiento.	5.3.4 Retraining frequency and requirements.		5.3.4 Retraining frequency and requirements.	5.3.4 Retraining frequency and requirements.

CLAUSULAS EN ESTE DOCUMENTO	RFC 3647	ETSI EN 319 411-1 V1.3.1 y ETSI EN 319 411-2 V2.4.1	ISO/IEC 27099:2022	WebTrust for AC V2.2.2
5.3.5 Frecuencia y secuencia de rotación de trabajo.	5.3.5 Job rotation frequency and sequence.		5.3.5 Job rotation frequency and sequence.	5.3.5 Job rotation frequency and sequence.
5.3.6 Sanciones por acciones no autorizadas.	5.3.6 Sanctions for unauthorized actions.		5.3.6 Sanctions for unauthorized actions.	5.3.6 Sanctions for unauthorized actions.
5.3.7 Requisitos de contratista independiente.	5.3.7 Independent contractor requirements.		5.3.7 Independent contractor requirements.	5.3.7 Independent contractor requirements.
5.3.8 Documentación proporcionada al persona.	5.3.8 Documentation supplied to personnel.		5.3.8 Documentation supplied to personnel.	5.3.8 Documentation supplied to personnel.
5.4 Procedimientos de registro de auditoría.	5.4 Audit logging procedures.	6.4.5 Audit logging procedures.	5.4 Audit logging procedures.	5.4 Audit logging procedures.
5.4.1 Tipos de eventos registrados.	5.4.1 Types of events recorded.		5.4.1 Types of events recorded.	5.4.1 Types of events recorded.
5.4.2 Frecuencia de procesamiento de registro.	5.4.2 Frequency of processing log.		5.4.2 Frequency of processing log.	5.4.2 Frequency of processing log.
5.4.3 Periodo de conservación de registros de auditoría.	5.4.3 Retention period for audit log.		5.4.3 Retention period for audit log.	5.4.3 Retention period for audit log.
5.4.4 Protección de los registros de auditoría.	5.4.4 Protection of audit log.		5.4.4 Protection of audit log.	5.4.4 Protection of audit log.
5.4.5 Procedimientos de copia de respaldo de los registros de auditoria.	5.4.5 Audit log backup procedures.		5.4.5 Audit log backup procedures.	5.4.5 Audit log backup procedures.
5.4.6 Sistema de archivo de registros de auditoria (interno vs externo).	5.4.6 Audit collection system (internal vs. external).		5.4.6 Audit collection system (internal vs. external).	5.4.6 Audit collection system (internal vs. external).
5.4.7 Notificación al sujeto causa de evento.	5.4.7 Notification to event-causing subject.		5.4.7 Notification to event-causing subject.	5.4.7 Notification to event-causing subject.
5.4.8 Evaluaciones de vulnerabilidad.	5.4.8 Vulnerability assessments.		5.4.8 Vulnerability assessments.	5.4.8 Vulnerability assessments.
5.5 Archivo de registros.	5.5 Records archival.	6.4.6 Records archival.	5.5 Records archival.	5.5 Records archival.
5.5.1 Tipos de registros archivados.	5.5.1 Types of records archived.		5.5.1 Types of records archived.	5.5.1 Types of records archived.
5.5.2 Periodo de conservación del archivo.	5.5.2 Retention period for archive.		5.5.2 Retention period for archive.	5.5.2 Retention period for archive.
5.5.3 Protección del archivo.	5.5.3 Protection of archive.		5.5.3 Protection of archive.	5.5.3 Protection of archive.
5.5.4 Procedimientos de copia de respaldo del archivo.	5.5.4 Archive backup procedures.		5.5.4 Archive backup procedures.	5.5.4 Archive backup procedures.
5.5.5 Requisitos para el sellado de tiempo de los registros.	5.5.5 Requirements for time-stamping of records.		5.5.5 Requirements for time-stamping of records.	5.5.5 Requirements for time-stamping of records.
5.5.6 Sistema de recopilación del archivo (internos o externos).	5.5.6 Archive collection system (internal or external).		5.5.6 Archive collection system (internal or external).	5.5.6 Archive collection system (internal or external).
5.5.7 Procedimientos para obtener y verificar información del archivo.	5.5.7 Procedures to obtain and verify archive information.		5.5.7 Procedures to obtain and verify archive information.	5.5.7 Procedures to obtain and verify archive information.
5.6 Cambio de clave.	5.6 Key changeover.	6.4.7 Key changeover.	5.6 Key changeover.	5.6 Key changeover.
5.7 Recuperación ante compromiso y desastre.	5.7 Compromise and disaster recovery.	6.4.8 Compromise and disaster recovery .	5.7 Compromise and disaster recovery.	5.7 Compromise and disaster recovery.
5.7.1 Procedimientos de manejo de incidentes y compromisos.	5.7.1 Incident and compromise handling procedures.		5.7.1 Incident and compromise handling procedures.	5.7.1 Incident and compromise handling procedures.
5.7.2 Daño en los recursos informáticos, software y/o datos.	5.7.2 Computing resources, software,		5.7.2 Computing resources, software,	5.7.2 Computing resources, software,

CLAUSULAS EN ESTE DOCUMENTO	RFC 3647	ETSI EN 319 411-1 V1.3.1 y ETSI EN 319 411-2 V2.4.1	ISO/IEC 27099:2022	WebTrust for AC V2.2.2
	and/or data are corrupted.		and/or data are corrupted.	and/or data are corrupted.
5.7.3 Procedimiento si la clave privada de una entidad está comprometida.	5.7.3 Entity private key compromise procedures.		5.7.3 Entity private key compromise procedures.	5.7.3 Entity private key compromise procedures.
5.7.4 Capacidades de continuidad de negocios después de un desastre.	5.7.4 Business continuity capabilities after a disaster		5.7.4 Business continuity capabilities after a disaster	5.7.4 Business continuity capabilities after a disaster
5.8 Terminación/Cese de la autoridad de certificación o la autoridad de registro.	5.8 CA or RA termination.	6.4.9 Certification Authority or Registration Authority termination.	5.8 CA or RA termination.	5.8 CA or RA termination.
6. CONTROLES DE SEGURIDAD TÉCNICA.	**6. TECHNICAL SECURITY CONTROLS**	**6.5 TECHNICAL SECURITY CONTROLS**	**6. TECHNICAL SECURITY CONTROLS**	**6. TECHNICAL SECURITY CONTROLS**
6.1 Generación e instalación del par de claves.	6.1 Key pair generation and installation.	6.5.1 Key pair generation and installation.	6.1 Key pair generation and installation.	6.1 Key pair generation and installation.
6.1.1 Generación del par de claves.	6.1.1 Key pair generation.		6.1.1 Key pair generation.	6.1.1 Key pair generation.
6.1.2 Entrega de la clave privada al suscriptor.	6.1.2 Private key delivery to subscriber.		6.1.2 Private key delivery to subscriber.	6.1.2 Private key delivery to subscriber.
6.1.3 Entrega de clave pública al emisor del certificado.	6.1.3 Public key delivery to certificate issuer		6.1.3 Public key delivery to certificate issuer	6.1.3 Public key delivery to certificate issuer
6.1.4 Entrega de la clave pública de la autoridad de certificación a la parte que confía.	6.1.4 CA public key delivery to relying parties.		6.1.4 CA public key delivery to relying parties.	6.1.4 CA public key delivery to relying parties.
6.1.5 Tamaños de clave.	6.1.5 Key sizes.		6.1.5 Key sizes.	6.1.5 Key sizes.
6.1.6 Parámetros de generación de clave pública y comprobación de calidad.	6.1.6 Public key parameters generation and quality checking.		6.1.6 Public key parameters generation and quality checking.	6.1.6 Public key parameters generation and quality checking.
6.1.7 Propósitos del uso de la clave (según x.509 v3 “key usage field”).	6.1.7 Key usage purposes (as per X.509 V3 key usage field)		6.1.7 Key usage purposes (as per X.509 V3 key usage field)	6.1.7 Key usage purposes (as per X.509 V3 key usage field)
6.2 Protección de la clave privada y controles de ingeniería del módulo criptográfico.	6.2 Private key protection and cryptographic module engineering controls	6.5.2 Private key protection and cryptographic module engineering controls.	6.2 Private key protection and cryptographic module engineering controls	6.2 Private key protection and cryptographic module engineering controls
6.2.1 Estándares y controles para el módulo criptográfico.	6.2.1 Cryptographic Module Standards And Controls		6.2.1 Cryptographic Module Standards And Controls	6.2.1 Cryptographic Module Standards And Controls
6.2.2 Control multi-persona “n de m” de la clave privada.	6.2.2 Private key (n out of m) multi-person control.		6.2.2 Private key (n out of m) multi-person control.	6.2.2 Private key (n out of m) multi-person control.
6.2.3 Custodia de la clave privada.	6.2.3 Private key escrow.		6.2.3 Private key escrow.	6.2.3 Private key escrow.
6.2.4 Copia de seguridad de la clave privada.	6.2.4 Private key backup.		6.2.4 Private key backup.	6.2.4 Private key backup.
6.2.5 Archivo de clave privada.	6.2.5 Private key archival.		6.2.5 Private key archival.	6.2.5 Private key archival.
6.2.6 Transferencia de la clave privada desde o hacia un módulo criptográfico.	6.2.6 Private key transfer into or from a cryptographic module.		6.2.6 Private key transfer into or from a cryptographic module.	6.2.6 Private key transfer into or from a cryptographic module.
6.2.7 Almacenamiento de la clave privada en el módulo criptográfico.	6.2.7 Private key storage on cryptographic module.		6.2.7 Private key storage on cryptographic module.	6.2.7 Private key storage on cryptographic module.

CLAUSULAS EN ESTE DOCUMENTO	RFC 3647	ETSI EN 319 411-1 V1.3.1 y ETSI EN 319 411-2 V2.4.1	ISO/IEC 27099:2022	WebTrust for AC V2.2.2
6.2.8 Método de activación de la clave privada.	6.2.8 Method of activating private key		6.2.8 Method of activating private key	6.2.8 Method of activating private key
6.2.9 Método de desactivación de la clave privada.	6.2.9 Method of deactivating private key.		6.2.9 Method of deactivating private key.	6.2.9 Method of deactivating private key.
6.2.10 Método de destrucción de la clave privada.	6.2.10 Method of destroying private key.		6.2.10 Method of destroying private key.	6.2.10 Method of destroying private key.
6.2.11 Calificación de los módulo criptográfico.	6.2.11 Cryptographic module rating.		6.2.11 Cryptographic module rating.	6.2.11 Cryptographic module rating.
6.3 Otros Aspectos de gestión del par de claves.	6.3 Other aspects of key pair management.	6.5.3 Other aspects of key pair management.	6.3 Other aspects of key pair management.	6.3 Other aspects of key pair management.
6.3.1 Archivo de clave pública.	6.3.1 Public key archival.		6.3.1 Public key archival.	6.3.1 Public key archival.
6.3.2 Periodos operativos de los certificados y período de uso para el par de claves.	6.3.2 Certificate operational periods and key pair usage periods.		6.3.2 Certificate operational periods and key pair usage periods.	6.3.2 Certificate operational periods and key pair usage periods.
6.4 Datos de activación.	6.4 Activation data.	6.5.4 Activation data.	6.4 Activation data.	6.4 Activation data.
6.4.1 Generación e instalación de datos de activación.	6.4.1 Activation data generation and installation.		6.4.1 Activation data generation and installation.	6.4.1 Activation data generation and installation.
6.4.2 Protección de los datos de activación.	6.4.2 Activation data protection.		6.4.2 Activation data protection.	6.4.2 Activation data protection.
6.4.3 Otros aspectos de los datos de activación.	6.4.3 Other aspects of activation data.		6.4.3 Other aspects of activation data.	6.4.3 Other aspects of activation data.
6.5 Controles de seguridad informática.	6.5 Computer security controls.	6.5.5 Computer security controls.	6.5 Computer security controls.	6.5 Computer security controls.
6.5.1 Requerimientos técnicos específicos de la seguridad del computador.	6.5.1 Specific computer security technical Requirements		6.5.1 Specific computer security technical Requirements	6.5.1 Specific computer security technical Requirements
6.5.2 Clasificación de la seguridad informática.	6.5.2 Computer security rating.		6.5.2 Computer security rating.	6.5.2 Computer security rating.
6.6 Controles técnicos del ciclo de vida.	6.6 Life cycle technical controls.	6.5.6 Life cycle security controls.	6.6 Life cycle technical controls.	6.6 Life cycle technical controls.
6.6.1 Control de desarrollo del sistema.	6.6.1 System development controls.		6.6.1 System development controls.	6.6.1 System development controls.
6.6.2 Controles de gestión de seguridad.	6.6.2 Security management controls.		6.6.2 Security management controls.	6.6.2 Security management controls.
6.6.3 Controles de seguridad del ciclo de vida.	6.6.3 Life cycle security controls.		6.6.3 Life cycle security controls.	6.6.3 Life cycle security controls.
6.7 Controles de seguridad de red.	6.7 Network security controls.	6.5.7 Network security controls.	6.7 Network security controls.	6.7 Network security controls.
6.8 Sello de tiempo.	6.8 Time-Stamping.	6.5.8 Timestamping.	6.8 Time-Stamping.	6.8 Time-Stamping.
7. PERFILES DE CERTIFICADO, LISTA DE REVOCACIÓN DE CERTIFICADO Y PROTOCOLO DE SERVICIO DE CERTIFICADO EN LÍNEA	**7. CERTIFICATE, CRL, AND OCSP PROFILES**	**6.6 CERTIFICATE, CRL AND OCSP PROFILES**	**7. CERTIFICATE AND CRL PROFILES**	**7. CERTIFICATE AND CRL PROFILES**
7.1 Perfil del certificado.	7.1 Certificate profile.	6.6.1 Certificate profile.	7.1 Certificate profile.	7.1 Certificate profile.
7.1.1 Número de versión.	7.1.1 Version Number(S)		7.1.1 Version Number(S)	7.1.1 Version Number(S)
7.1.2 Extensiones del certificado.	7.1.2 Certificate extensions.		7.1.2 Certificate extensions.	7.1.2 Certificate extensions.
7.1.3 Identificadores de objeto del algoritmo criptográfico.	7.1.3 Cryptographic Algorithm object identifiers.		7.1.3 Cryptographic Algorithm object identifiers.	7.1.3 Cryptographic Algorithm object identifiers.

CLAUSULAS EN ESTE DOCUMENTO	RFC 3647	ETSI EN 319 411-1 V1.3.1 y ETSI EN 319 411-2 V2.4.1	ISO/IEC 27099:2022	WebTrust for AC V2.2.2
7.1.4 Formato de nombres.	7.1.4 Name forms.		7.1.4 Name forms.	7.1.4 Name forms.
7.1.5 Restricciones de nombres.	7.1.5 Name constraints.		7.1.5 Name constraints.	7.1.5 Name constraints.
7.1.6 Identificador de objeto de la política de certificado.	7.1.6 Certificate policy object identifier.		7.1.6 Certificate policy object identifier.	7.1.6 Certificate policy object identifier.
7.1.7 Uso de la extensión “Policy Constraints”.	7.1.7 Usage of policy constraints extension.		7.1.7 Usage of policy constraints extension.	7.1.7 Usage of policy constraints extension.
7.1.8 Sintaxis y la semántica de los calificadores de política.	7.1.8 Policy qualifiers syntax and semantics.		7.1.8 Policy qualifiers syntax and semantics.	7.1.8 Policy qualifiers syntax and semantics.
7.1.9 Procesamiento semántico para la extensión crítica “Certificate Policy”.	7.1.9 Processing semantics for the critical certificate policies extension.		7.1.9 Processing semantics for the critical certificate policies extension.	7.1.9 Processing semantics for the critical certificate policies extension.
7.2 Perfil de la LCR.	7.2 CRL profile.	6.6.2 CRL profile.	7.2 CRL profile.	7.2 CRL profile.
7.2.1 Número de versión.	7.2.1 Version Number(S)		7.2.1 Version Number(S)	7.2.1 Version Number(S)
7.2.2 LCR y extensiones de entrada.	7.2.2 CRL And CRL entry extensions.		7.2.2 CRL And CRL entry extensions.	7.2.2 CRL And CRL entry extensions.
7.3 Perfil de PECL.	7.3 OCSP profile.	6.6.3 OCSP profile.	7.3 OCSP profile.	7.3 OCSP profile.
7.3.1 Número de versión.	7.3.1 Version number(s).		7.3.1 Version number(s).	7.3.1 Version number(s).
7.3.2 Extensiones protocolo de estado de certificado en línea.	7.3.2 OCSP extensions.		7.3.2 OCSP extensions.	7.3.2 OCSP extensions.
8. CUMPLIMIENTO DE AUDITORÍA Y OTRAS EVALUACIONES	**8. COMPLIANCE AUDIT AND OTHER ASSESSMENT**	**6.7 COMPLIANCE AUDIT AND OTHER ASSESSMENT**	**8. PACTICES ADMINISTRATION**	**8. PACTICES ADMINISTRATION**
8.1 Frecuencias o circunstancias de las auditorías.	8.1 Frequency or circumstances of assessment.		8.1 Frequency or circumstances of assessment.	8.1 Frequency or circumstances of assessment.
8.2 Identificación/Calificaciones del evaluador.	8.2 Identity/Qualifications of assessor.		8.2 Identity/Qualifications of assessor.	8.2 Identity/Qualifications of assessor.
8.3 Relación del evaluador con la entidad evaluada.	8.3 Assessor's relationship to assessed entity.		8.3 Assessor's relationship to assessed entity.	8.3 Assessor's relationship to assessed entity.
8.4 Temas cubiertos por la evaluación.	8.4 Topics covered by assessment.		8.4 Topics covered by assessment.	8.4 Topics covered by assessment.
8.5 Acciones a tomar como resultado de una deficiencia.	8.5 Actions taken as a result of deficiency.		8.5 Actions taken as a result of deficiency.	8.5 Actions taken as a result of deficiency.
8.6 Comunicación de los resultados.	8.6 Communication Of Results		8.6 Communication Of Results	8.6 Communication Of Results
9. OTROS ASUNTOS LEGALES Y COMERCIALES	**9. OTHER BUSINESS AND LEGAL MATTERS**	**6.8 OTHER BUSINESS AND LEGAL MATTERS**		**9. OTHER BUSINESS AND LEGAL MATTERS**
9.1 Tarifas.	9.1 Fees	6.8.1 Fees.		9.1 Fees
9.1.1 Tarifa por emisión o renovación de certificados.	9.1.1 Certificate issuance or renewal fees.			9.1.1 Certificate issuance or renewal fees.
9.1.2 Tarifa por acceso al certificado.	9.1.2 Certificate access fees.			9.1.2 Certificate access fees.
9.1.3 Tarifa por acceso de información de estado o revocación.	9.1.3 Revocation or status information access fees.			9.1.3 Revocation or status information access fees.
9.1.4 Tarifas por otros servicios.	9.1.4 Fees for other services.			9.1.4 Fees for other services.
9.1.5 Política de reembolso.	9.1.5 Refund policy.			9.1.5 Refund policy.
9.2 Responsabilidad financiera.	9.2 Financial responsibility.	6.8.2 Financial responsibility.		9.2 Financial responsibility.

CLAUSULAS EN ESTE DOCUMENTO	RFC 3647	ETSI EN 319 411-1 V1.3.1 y ETSI EN 319 411-2 V2.4.1	ISO/IEC 27099:2022	WebTrust for AC V2.2.2
9.2.1 Cobertura del seguro.	9.2.1 Insurance coverage.			9.2.1 Insurance coverage.
9.2.2 Otros activos.	9.2.2 Other assets.			9.2.2 Other assets.
9.2.3 Cobertura de seguro o garantía para entidades finales.	9.2.3 Insurance or warranty coverage for end-entities.			9.2.3 Insurance or warranty coverage for end-entities.
9.3 Confidencialidad de la información del negocio.	9.3 Confidentiality of business information.	6.8.3 Confidentiality of business information. (No policy requirement)		9.3 Confidentiality of business information.
9.3.1 Alcance de la información confidencial.	9.3.1 Scope of confidential information.			9.3.1 Scope of confidential information.
9.3.2 Información fuera del alcance de la información confidencial.	9.3.2 Information not within the scope of confidential information.			9.3.2 Information not within the scope of confidential information.
9.3.3 Responsabilidad de proteger la información confidencial.	9.3.3 Responsibility to protect confidential information.			9.3.3 Responsibility to protect confidential information.
9.4 Privacidad de la información personal.	9.4 Privacy of personal information.	6.8.4 Privacy of personal information.		9.4 Privacy of personal information.
9.4.1 Plan de privacidad.	9.4.1 Privacy plan.			9.4.1 Privacy plan.
9.4.2 Información tratada como privada.	9.4.2 Information treated as private.			9.4.2 Information treated as private.
9.4.3 Información no considerada privada.	9.4.3 Information not deemed private.			9.4.3 Information not deemed private.
9.4.4 Responsabilidad de proteger la información privada.	9.4.4 Responsibility to protect private information.			9.4.4 Responsibility to protect private information.
9.4.5 Notificación y consentimiento para utilizar información privada.	9.4.5 Notice and consent to use private information.			9.4.5 Notice and consent to use private information.
9.4.6 Divulgación de conformidad con un proceso judicial o administrativo	9.4.6 Disclosure pursuant to judicial or administrative process.			9.4.6 Disclosure pursuant to judicial or administrative process.
9.4.7 Otras Circunstancias de divulgación de información.	9.4.7 Other information disclosure circumstances.			9.4.7 Other information disclosure circumstances.
9.5 Derechos de propiedad intelectual.	9.5 Intellectual property rights.	6.8.5 Intellectual property rights. (No policy requirement)		9.5 Intellectual property rights.
9.6 Representaciones y Garantías.	9.6 Representations and warranties.	6.8.6 Representations and warranties.		9.6 Representations and warranties.
9.6.1 Representaciones y garantías de la AC.	9.6.1 CA representations and warranties			9.6.1 CA representations and warranties
9.6.2 Representaciones y garantías de la AR.	9.6.2 RA representations and warranties.			9.6.2 RA representations and warranties.
9.6.3 Representaciones y garantías del suscriptor.	9.6.3 Subscriber representations and warranties.			9.6.3 Subscriber representations and warranties.
9.6.4 Representaciones y garantías de las partes que confían.	9.6.4 Relying party representations and warranties.			9.6.4 Relying party representations and warranties.
9.6.5 representaciones y garantías de otros participantes.	9.6.5 Representations and warranties of other participants.			9.6.5 Representations and warranties of other participants.

CLAUSULAS EN ESTE DOCUMENTO	RFC 3647	ETSI EN 319 411-1 V1.3.1 y ETSI EN 319 411-2 V2.4.1	ISO/IEC 27099:2022	WebTrust for AC V2.2.2
9.7 Renuncias de garantías.	9.7 Disclaimers of warranties	6.8.7 Disclaimers of warranties .		9.7 Disclaimers of warranties
9.8 Limitaciones de responsabilidad.	9.8 Limitations of liability.	6.8.8 Limitations of liability.		9.8 Limitations of liability.
9.9 Indemnizaciones.	9.9 Indemnities.	6.8.9 Indemnities. (No policy requirement)		9.9 Indemnities.
9.10 Vigencia y terminación.	9.10 Term and termination.	6.8.10 Term and termination. (No policy requirement)		9.10 Term and termination.
9.10.1 Vigencia.	9.10.1 Term.			9.10.1 Term.
9.10.2 Terminación.	9.10.2 Termination			9.10.2 Termination
9.10.3 Efecto de terminación y supervivencia.	9.10.3 Effect of termination and survival.			9.10.3 Effect of termination and survival.
9.11 Notificaciones individuales y comunicaciones con los participantes.	9.11 Individual notices and communications with participants.	6.8.11 Individual notices and communications with participants. (No policy requirement)		9.11 Individual notices and communications with participants.
9.12 Enmiendas	9.12 Amendments.	6.8.12 Amendments. (No policy requirement)		9.12 Amendments.
9.12.1 Procedimiento de enmiendas.	9.12.1 Procedure for amendment.			9.12.1 Procedure for amendment.
9.12.2 Mecanismo y periodo de notificación.	9.12.2 Notification mechanism and period.			9.12.2 Notification mechanism and period.
9.12.3 Circunstancias bajo las cuales el identificador de objeto tiene que ser cambiado.	9.12.3 Circumstances under which OID must be changed			9.12.3 Circumstances under which OID must be changed
9.13 Disposiciones sobre resolución de diputas.	9.13 Dispute resolution provisions.	6.8.13 Dispute resolution procedures.		9.13 Dispute resolution provisions.
9.14 Ley aplicable.	9.14 Governing law.	6.8.14 Governing law.		9.14 Governing law.
9.15 Cumplimiento de la ley aplicable.	9.15 Compliance with applicable law.	6.8.15 Compliance with applicable law.		9.15 Compliance with applicable law.
9.16 Disposiciones diversas.	9.16 Miscellaneous provisions.	6.8.16 Miscellaneous provisions. (No policy requirement)		9.16 Miscellaneous provisions.
9.16.1 Acuerdo completo.	9.16.1 Entire agreement.			9.16.1 Entire agreement.
9.16.2 Asignación.	9.16.2 Assignment.			9.16.2 Assignment.
9.16.3 Divisibilidad.	9.16.3 Severability.			9.16.3 Severability.
9.16.4 Cumplimiento (honorarios de abogados y renuncia de derechos).	9.16.4 Enforcement (attorneys' fees and waiver of rights)			9.16.4 Enforcement (attorneys' fees and waiver of rights)
9.16.5 Fuerza mayor.	9.16.5 Force majeure			9.16.5 Force majeure
9.17 Otras disposiciones.	9.17 Other provisions.	6.9 Other provisions.		9.17 Other provisions.
		6.9.1 Organizational.		
		6.9.2 Additional testing.		
		6.9.3 Disabilities.		
		6.9.4 Terms and conditions.		