NORMAS TÉCNICAS Y ESTÁNDARES QUE DEBERÁN CUMPLIR LOS PROVEEDORES DE SERVICIOS DE CERTIFICACIÓN

(Versión 3)

Managua, Agosto 2019

MINISTERIO DE HACIENDA Y CREDITO PUBLICO
DIRECCION GENERAL DE TECNOLOGIA

CUADRO DE REVISIONES

No. Revisión	Fecha	Elaborado/ Entrevistado	Revisado	Autorizado	Aprobado
0	Diciembre/ 2013	Hans Espinoza Responsable Dirección Acreditación de Firma Electrónica	Yuri Dompe Responsable Departamento Supervisión e Inspección Daysi Romero Responsable Departamento de Acreditación y Registro	Ana Aguilera Responsable Dirección de Normas y Planes Tecnológicos	Esperanza Meza Directora General DGTEC
1	Enero / 2016	Hans Espinoza Responsable Dirección Acreditación de Firma Electrónica Daysi Romero Responsable Departamento de Acreditación y Registro	Yuri Dompe Responsable Departamento Supervisión e Inspección	Hans Espinoza Responsable Dirección Acreditación de Firma Electrónica Ana Aguilera Responsable Dirección de Normas y Planes Tecnológicos	Esperanza Meza Directora General DGTEC
2	Agosto / 2017	Yuri Dompe Responsable Departamento Supervisión e Inspección Daysi Romero Responsable Departamento de Acreditación y Registro	Hans Espinoza Responsable Dirección Acreditación de Firma Electrónica	Hans Espinoza Responsable Dirección Acreditación de Firma Electrónica	Esperanza Meza Directora General DGTEC
3	Agosto / 2019	Yuri Dompe Responsable Departamento Supervisión e Inspección Daysi Romero Responsable Departamento de Acreditación y Registro	Hans Espinoza Responsable Dirección Acreditación de Firma Electrónica	Hans Espinoza Responsable Dirección Acreditación de Firma Electrónica	Esperanza Meza Responsable Dirección General de Tecnología

CONTENIDO

I. INTRODUCCIÓN

La Dirección General de Tecnología - DGTEC del Ministerio de Hacienda y Crédito Público - MHCP a través de la Dirección de Acreditación de Firma Electrónica ha elaborado el documento "Normas Técnicas y Estándares que deberán cumplir los Proveedores de Servicios de Certificación", el cual servirá de base y consulta de los estándares internacionales que deben cumplir e implementar los interesados en ser acreditados como Proveedores de Servicios de Certificación.

Toda recomendación que modifique este documento debe ser notificada a través del Departamento de Atención al Cliente a la Dirección de Acreditación de Firma Electrónica - DAFE, quien es la responsable de su elaboración y actualización.

Este documento es propiedad de la Dirección General de Tecnología.

II. JUSTIFICACIÓN

Sección a actualizar	Justificación	Servidor Público/Cargo que solicitó la actualización
Capítulo VI: Normas Técnicas y Estándares.	Se realizó ajustes necesarios, actualizaciones y emisiones de nuevos estándares emitidos por Organizaciones Internacionales como: ISO/IEC, ETSI y RFC, también se agregó nuevos estándares no considerados en la versión anterior y se eliminaron estándares que fueron reemplazados por otros que ya están obsoletos. Se realizó reorganizó la clasificación de los estándares en el presente documento.	Hans Espinoza – Resp. Dirección Acreditación de Firma Electrónica. Daysi Romero – Resp. Departamento de Acreditación y Registro. Yuri Dompe – Resp. Dpto. de supervisión e Inspección.
Capítulo VII: Anexos.	Se realizó ajustes en el Anexo No. 1, se actualizaron los estándares y se reorganizó la estructura de la tabla. Se eliminó el Anexo No. 2 del documento anterior. Se modificaron y se reenumeraron los Anexos No. 3 y Anexo No.4 del documento anterior.	Hans Espinoza – Resp. Dirección Acreditación de Firma Electrónica. Daysi Romero – Resp. Departamento de Acreditación y Registro. Yuri Dompe – Resp. Dpto. de supervisión e Inspección.

III. OBJETIVO

Orientar al solicitante para ser acreditado como Proveedor de Servicio de Certificación acerca del análisis, aplicación y cumplimiento de los estándares que garanticen la seguridad y confianza.

IV. BASE LEGAL

- Ley No.729 Ley de Firma Electrónica, publicada en la Gaceta Diario Oficial No. 165 el 30 de Agosto del 2010:

  - Art.15 Entidad Rectora de Acreditación de Firma Electrónica: Se designa a la Dirección General de Tecnología, conocida en adelante como DGTEC, dependencia del Ministerio de Hacienda y Crédito Público, como Ente Rector del proceso de acreditación de firma electrónica.

- Reglamento de Ley 729, Decreto Presidencial 57-2011 publicado en la Gaceta Diario Oficial No. 211 el 8 de Noviembre del 2011:

  - Art. 9 inciso 4, mandata a la DGTEC a "Dictar normas técnicas, con el objeto de implementar la Ley y su Reglamento".

- Art.14 establece que “Las normas técnicas que dicte la Entidad Rectora para la aplicación e implementación del presente Reglamento son de obligatorio cumplimiento para los Proveedores acreditados de Servicios de Certificación y los usuarios de los mismos”.

- Art. 20 este indica en el segundo párrafo que “Además se deberán acreditar los siguientes requisitos relativos a la seguridad física, lógica y de la plataforma tecnológica utilizada, que sean determinados por la Entidad Rectora a través de normas técnicas de conformidad con estándares internacionales reconocidos”.

V. ACRÓNIMOS[1]

Acrónimo	Definición
AC	Autoridad Certificadora.
AR	Autoridad de Registro.
CSR	Certificate Signing Request o Solicitud de Firma de Certificado.
DPC	Declaración de Prácticas de Certificación.
ESI	Electronic Signatures and Infrastructures.
ETSI	European Telecommunications Standards Institute."Instituto Europeo de Normas de Telecomunicaciones", es una organización de estandarización de la industria de las telecomunicaciones (fabricantes de equipos y operadores de redes) de Europa, con proyección mundial.
FIPS	Federal Information Processing Standards. "Estándares Federales de Procesamiento de la Información", son estándares anunciados públicamente desarrollados por el Gobierno de los Estados Unidos para la utilización por parte de todas las agencias del Gobierno no militares y por los contratistas del Gobierno. Muchos estándares FIPS son versiones modificadas de los estándares usados en las comunidades más amplias (ANSI, IEEE, ISO, etc.).
ICP	Infraestructura de Clave Pública.
IEC	International Electrotechnical Commission. "Comisión Electrotécnica Internacional".
INCP	Infraestructura Nicaragüense de Clave Pública.
ISO	International Organization for Standardization."Organización Internacional de Normalización" es el organismo encargado de promover el desarrollo de normas internacionales de fabricación, comercio y comunicación para todas las ramas industriales a excepción de la eléctrica y la electrónica.
ITU	International Telecommunication Union."Unión Internacional de Telecomunicaciones" es el organismo especializado de la Organización de las Naciones Unidas encargado de regular las telecomunicaciones a nivel internacional entre las distintas administraciones y empresas operadoras.
ITU-T	Sector de Normalización de las Telecomunicaciones de la UIT.
LDAP	Lightweight Directory Access Protocol."Protocolo Ligero de Acceso a Directorios".
LCR	Lista de Certificados Revocados.
NTN	Norma Técnica Nicaragüense.
OCSP	Online Certificate Status Protocol. "Protocolo de Validación de Certificados En-Línea".
PC	Política de Certificación.
PKCS	“Public-Key Cryptography Standards”.
PSC	Proveedor de Servicios de Certificación.
RFC	Request For Comments. O’ Petición de Comentarios, son notas sobre Internet.
RUC	Registro Único de Contribuyente.
SGSI	Sistema de Gestión de Seguridad de la Información.

[1] Las referencias a la mayoría de los acrónimos utilizados se mantienen en el idioma de origen (inglés)

VI. NORMAS TÉCNICAS Y ESTÁNDARES

Los lineamentos establecidos en este documento corresponden al cumplimiento de los estándares técnicos nacionales e internacionales para ofrecer de forma segura y confiable los servicios que ofrecerá un Proveedor de Servicio de Certificación.

Criterios Específicos

Los criterios generales se definen en base al cumplimiento del conjunto de requisitos y obligaciones definidas en la Ley 729 Firma Electrónica, el Reglamento 57-2011 y el marco normativo establecido por el Ente Rector, los estándares tecnológicos y lineamientos de seguridad a aplicar para la acreditación como Proveedor de Servicios de Certificación se resumen en el **Anexo No. 1:** Resumen de Áreas Técnicas y Estándares Tecnológicos específicos y se detallan a continuación:

1. Declaración de Prácticas de Certificación - DPC Política de Certificados - PC

Objetivo

Comprobar que el Proveedor de Servicio de Certificación defina en su política de certificados los procedimientos de gestión de ciclo de vida de los certificados y los diferentes tipos de certificados a otorgar según se establece en la Ley 729 y su reglamento 57-2011.

Descripción

El enfoque de una política de certificado es significativamente diferente al de una declaración de prácticas de certificación. Una política de certificados se define independientemente de los detalles específicos del entorno operativo específico de una entidad de certificación mientras que una declaración de prácticas de certificación se adapta a la estructura organizativa, los procedimientos de operación, instalaciones y el entorno computacional de una entidad de certificación.

Los elementos principales que debe contener la declaración de prácticas de certificación son:

- Las limitaciones de responsabilidad y las obligaciones tanto del Proveedor de Servicios de Certificación como del titular.

Los elementos principales que debe contener la Política de Certificación - PC, son:

- Los procedimientos de gestión del ciclo de vida de los certificados y los diferentes tipos de certificados que le han sido autorizados al Proveedor de Servicios de Certificación por el Ente Rector.

Estándares de evaluación

- DGTEC: “Modelo de la Declaración de Prácticas de Certificación - DPC y Políticas de Certificados – PC de los Proveedores de Servicios de Certificación - PSC”
- RFC 3647: “Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework”.
- Estándares ETSI equivalentes al RFC 3647:
  - ETSI EN 319 401: “Electronic Signatures and Infrastructures - ESI; General Policy Requirements for Trust Service Providers; 6.1 Trust Service Practice statement”.
  - ETSI EN 319 411-1: “Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements”.

- ETSI EN 319 411-2: “Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for TSP issuing EU qualified certificates”.

- ETSI EN 319 412-1: “Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures”.

- ETSI EN 319 412-2: “Electronic Signatures and Infrastructures (ESI); Part 2: Certificate profile for certificates issued to natural persons”.

- ETSI EN 319 412-3: “Electronic Signatures and Infrastructures (ESI); Part 3: Certificate profile for certificates issued to legal persons”.

- ETSI EN 319 412-5: “Electronic Signatures and Infrastructures (ESI); Part 5: QCStatements”.

Documentación solicitada

Documento de la Declaración de Prácticas de Certificación - DPC y Política de Certificados - PC con los diferentes tipos de estructura de campos de certificados.

Detalles de la evaluación

Aspectos	Evaluación
Estructura	Verificar que la Declaración de Práctica de Certificación - DPC y Política de Certificados han sido elaboradas en base a la estructura indicada en el Documento “Modelo de la Declaración de Prácticas de Certificación - DPC y políticas de certificados - PC de los Proveedores de Servicios de Certificación - PSC”.
Declaración de Prácticas de Certificación	Verificar que la DPC del PSC además de incluir las recomendaciones del “Modelo de la Declaración de Prácticas de Certificación (DPC) y políticas de certificados - PC de los Proveedores de Servicios de Certificación - PSC”, en lo conducente a las DPC: ▪ Exige a los titulares como mínimo cumplir con todos los requisitos definidos en el marco regulatorio nacional (incluido el emitido por el ente regulador de firma electrónica y las condiciones (obligaciones contractuales) establecidas por el PSC) para obtener el (o los) servicio(s) de Firma Electrónica que le han sido autorizados al PSC por la DGTEC. ▪ Establece las obligaciones y responsabilidades de la parte que confía en los servicios prestados a los Titulares, así como las obligaciones y responsabilidades de los Titulares ante la parte que confía.
Políticas de Certificación	Verificar que la(s) PC del PSC además de incluir las recomendaciones del “Modelo de la Declaración de Prácticas de Certificación - DPC y políticas de certificados - PC de los Proveedores de Servicios de Certificación - PSC”, en lo conducente a las PC, incluyen como mínimo cumplir con todas las condiciones definidas por el PSC en sus contratos de servicio conforme al marco regulatorio nacional (incluido el emitido por el ente regulador y las condiciones contractuales establecidas por el PSC.

2. Seguridad de la información

Objetivo

Comprobar que el Proveedor de Servicios de Certificación dispone de un Sistema de Gestión de Seguridad de la Información - SGSI con las medidas, infraestructuras, y todo lo necesario para garantizar la seguridad de la información.

Descripción

El Proveedor de Servicios de Certificación debe contar con la certificación del estándar NTN 21 001-13 o su equivalente/superior[2] a ISO 27001:2005 sobre el Sistema de Gestión de Seguridad de Información.

El Proveedor de Servicios de Certificación debe asegurarse que los procesos operacionales y administrativos tengan una adecuada correspondencia con el cumplimiento de los estándares establecidos por el Ente Rector y cubran por lo menos los siguientes procesos:

- Administración del riesgo (Valoración de los riesgos, tratamiento de los riesgos, mantenimiento).
- Declaración de los objetivos de seguridad.
- Continuidad de los procesos comerciales y operacionales.
- Acciones, procedimientos y mecanismos que permitan alcanzar los objetivos establecidos en la política de seguridad.
- Prevención de accesos no autorizados, daños, robos de información o interrupción de las operaciones.

Estándares de evaluación

- NTN 21 001-13: (basado en la ISO/IEC 27001: 2005) “Information Technology - Security Techniques - Information Security Management Systems – Requirements” o equivalente ISO/IEC 27001 superior.
- ISO/IEC 27002:2013: “Information Technology - Security Techniques - Code of Practice for Information Security Controls”.
- ISO/IEC 27005:2018 o superior: “Information technology -- Security Techniques -- Information Security Risk Management”.
- ISO/IEC 15408-1:2009 “Information technology -- Security techniques -- Evaluation criteria for IT Security -- Part 1: Introduction and General Model”.
- ISO/IEC 19790:2012 “Information technology -- Security Techniques -- Security Requirements for Cryptographic Modules”.
- ISO/IEC 24759:2017 “Information technology -- Security techniques -- Test requirements for cryptographic modules”.
- FIPS 140-2 Nivel 3 (o superior): “Federal Information Processing Standards”
- TIA-942-B: “Telecommunications Infrastructure Standard for Data Centers”.

Documentación solicitada

Documento que avale la certificación del estándar así como copia de todos los documentos soporte que sustentan dicha certificación, como lo son:

- Documento de Administración de riesgos.
- Documento de Política de seguridad.

[2] La norma ISO/IEC 27001:2013 (Cor 1:2014 y Cor 2:2015) fue revisada y confirmada por última vez en 2019, por lo tanto, es la versión superior vigente.

- Documento de Plan de continuidad de negocio y de recuperación de desastres.
- Documento de Plan de seguridad del sistema de información.
- Documento de Plan de seguridad física y ambiental.

Detalles de la evaluación

Aspectos	Evaluación
Certificación del SGSI del PSC con el estándar ISO 27001:2005 (o superior).	Verificar la existencia y validez de la certificación del SGSI del PSC con los objetivos de control establecidos en el estándar ISO 27001:2005 (o superior) y que son ampliados en el estándar ISO 27002 forma parte de los documentos soporte.
Administración de Riesgos (Valoración de Riesgos)	La valoración del riesgo debe estar basada al menos en las recomendaciones del estándar ISO 27005 (o superior), de tal forma que permita: ▪ Verificar la adecuada identificación de los riesgos. ▪ Verificar que los riesgos considerados sean reales. ▪ Validar que riesgos relevantes no hayan sido omitidos. ▪ Verificar la valoración adecuada de los riesgos. ▪ Constatar si hay un plan de mantenimiento de la valoración. ▪ Verificar que la evaluación de los riesgos esté en términos y en consecuencia con el negocio del PSC. ▪ Verificar la adecuada estimación de la probabilidad de su ocurrencia. ▪ Verificar el establecimiento de un orden de prioridad para el tratamiento de los riesgos. ▪ Verificar que se haya priorizado las acciones para reducir la ocurrencia de los riesgos. ▪ Verificar que se haya considerado la participación de los interesados cuando se toman las decisiones sobre gestión del riesgo. ▪ Verificar la eficacia del monitoreo del tratamiento del riesgo. ▪ Verificar el monitoreo y revisión con regularidad del riesgo y los procesos de gestión de riesgos.
Política de Seguridad	La política de Seguridad debe estar basada en las recomendaciones del estándar ISO 27001:2005 (o superior) y que son ampliados en el estándar ISO 27002 en particular en el Objetivo de Control 5 ”Políticas de Seguridad de la Información”.
Plan de continuidad del negocio y Recuperación de Desastres	Verificar que el plan incluye al menos los requerimientos del Objetivo de Control 17 de la ISO/IEC 27002, además: ▪ El PSC debe definir y mantener un plan de continuidad del negocio en caso de un desastre. ▪ El plan de continuidad de negocios del PSC deberá considerar los escenarios en que se comprometa o sospeche que la clave privada de firma del PSC ha sido comprometida (dejando de ser de dominio exclusivo y seguro del PSC), por lo que los procesos de recuperación deben estar disponibles y probados. ▪ A continuación de un desastre el PSC deberá, en la medida que sea posible, tomar las medidas que eviten su repetición. ▪ En el caso de verse comprometida su clave privada, el PSC deberá como mínimo tomar las siguientes medidas: - Informar de la situación a todos los suscriptores y sus contrapartes, así como a los otros PSC con quienes tiene acuerdos de interoperabilidad, certificación cruzada u otras formas de colaboración. - Indicar que los certificados e información del estado de revocación emitida usando la clave del PSC puede no ser válida, porque ha sido comprometida.

Aspectos	Evaluación
Plan de seguridad del sistema de información	El plan de seguridad debe considerar al menos los controles 6 al 14, 16, 17 y 18 del estándar ISO 27002. Sin embargo, en este requisito se evalúan en particular los siguientes aspectos: ▪ Organización de la Seguridad de la Información (control 6). ▪ Seguridad Ligada a los Recursos Humanos (control 7). ▪ Gestión de activos (control 8). ▪ Control del acceso (control 9). ▪ Criptografía (control 10). ▪ Seguridad Física y del Ambiente (control 11). ▪ Seguridad de las Operaciones (control 12). ▪ Gestión de las comunicaciones (control 13). ▪ Adquisición, desarrollo y mantenimiento de los sistemas de información (control 14). ▪ Gestión de incidentes de seguridad de la información (control 16). ▪ Aspectos de seguridad de la información en la gestión de la continuidad del negocio (control 17). ▪ Cumplimiento (control 18).
Plan de seguridad física y ambiental	El plan de seguridad física y ambiental debe considerar al menos los objetivos de control conducentes establecidos en el estándar ISO 27002. Verificando en particular la existencia de los controles de seguridad física, funcionales, de seguridad personal, los procedimientos de control de seguridad, los archivos de informaciones y registros.
Evaluación de la Plataforma Tecnológica	La evaluación de la Plataforma Tecnológica debe considerar la evaluación de los estándares (ISO/IEC 15408-1; ISO/IEC 19790; ISO/IEC 24759; FIPS 140-2 Nivel 3 o superior; TIA-942-B sobre los siguientes elementos: ▪ Módulo criptográfico. ▪ Módulo AC (Autoridad de Certificación). ▪ Módulo AR (Autoridad de Registro). ▪ Módulo de Almacenamiento y Publicación de Certificados. ▪ Protocolos de comunicación entre AC y AR. ▪ Elementos de administración de logs y Auditoría. ▪ Arquitectura de Red.

3. Infraestructura de Clave Pública

3.1. Estructura e Información del Certificado de Firma Electrónica

Objetivo

A continuación se expone un modelo de referencia de campos mínimos basado en los estándares vigentes: RFC 5280, RFC 3647, ITU-T X.509, ISO/IEC 9594-8 y complementados por el marco normativo nacional Ley 729 y Modelo de la Declaración de Prácticas de Certificados - DPC y Políticas de Certificados - PC que actualmente rigen los sistemas de Firma Electrónica Certificada.

Descripción

La estructura de datos que conforma el certificado de firma electrónica emitido por el PSC debe estar conforme la RFC 5280.

En este apartado se describen los campos básicos que deben conformar los diferentes perfiles de los certificados de servicios de firma electrónica que ofrecerán el Proveedor de Servicios de Certificación

(certificados de firma electrónica para persona natural, certificados de firma electrónica para persona jurídica, certificados de firma electrónica para servidores públicos y certificados de sello electrónico de tiempo).

Versión: Numero de versión (Constante, X-509 Versión 3).

Serial Number: Un código identificación único del certificado.

Issuer: Identificación del PSC, con indicación de su nombre o razón social, RUC, dirección de correo electrónico.

Signature: Firma de la Autoridad Certificadora del PSC.

Subject: Los datos de identidad del titular, entre los cuales deben necesariamente incluirse su nombre o razón social (en caso de ser persona jurídica), dirección de correo electrónico y cedula de identidad o RUC (en caso de ser persona jurídica).

Validity: Plazo de Vigencia (fecha de inicio y fecha de vencimiento).

Subject Public Key Info: Información de la llave publica del usuario (Algoritmo y Valor de llave pública).

Unique Identifiers: Identificador único de la entidad emisora.

La estructura anterior no limita la incorporación de otros campos (extensiones del certificado) que sea necesario integrar en el certificado en dependencia del tipo de servicio para el cual se emite el mismo, y de la correspondiente DPC del PSC que sea debidamente aprobada por la DGTEC.

Como reglas generales también se deben de considerar los siguientes elementos:

- El Proveedor de Servicio de Certificación interesado debe estructurar los certificados que emite de forma que los atributos adicionales que introduce, así como la incorporación de límites al uso del certificado no impidan la lectura del mismo ni su reconocimiento por terceros u otro Proveedor de Servicio de Certificación.

- Los datos de creación de firma del Proveedor de Servicios de Certificación acreditado para emitir certificados no deben ser utilizados más allá de lo establecido en la Declaración de Prácticas de Certificación aprobada por la DGTEC.

- El Perfil del Certificado debe estar acorde a lo establecido en el “Modelo de la Declaración de Prácticas de Certificación - DPC y Políticas de Certificados - PC de los Proveedores de Servicios de Certificación - PSC“.

- El tamaño de las claves deben ser acordes a lo establecido en el “Modelo de la Declaración de Prácticas de Certificación y Políticas de Certificados de los Proveedores de Servicios de Certificación“.

Estándares de evaluación

- ITU-T X.509: “Information technology – Open Systems Interconnection – The Directory: Public key and attribute certificate frameworks”.

- RFC 5280: “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile”.

- ISO/IEC 9594-8:2017: “Information technology - Open Systems Interconnection - The Directory: - Part 8: Public-key and attribute certificate frameworks”.
- RFC 3647: “Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework”.
- RFC 3628: “Policy Requirements for Time-Stamping Authorities”.
- RFC 3161: “Internet X.509 Public Key Infrastructure Time Stamp Protocol - TSP”.
- ETSI TS 319 421 “Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps”.
- ETSI EN 319 422 “Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles”.
- DGTEC: “Modelo de la Declaración de Prácticas de Certificación - DPC y Políticas de Certificados – PC de los Proveedores de Servicios de Certificación - PSC”.

Documentación solicitada

Ejemplos de certificados de firma electrónica emitida por el Proveedor de Servicio de Certificación en evaluación y el ejemplo de la Solicitud de Firma del Certificado - CSR.

Detalles de la evaluación

Aspectos	Evaluación
Conformidad con el estándar ITU-T X.509 V3	Se verificará que la estructura básica del certificado esté en conformidad a la norma vigente y que la gramática utilizada tanto en la estructura básica como en las extensiones obligatorias puedan ser leídos por cualquier aplicación que cumpla el estándar ITU-T Rec X.509. V3.
Contenido básico del certificado de firma electrónica emitido por el PSC.	Se confirmará que el certificado contiene la siguiente información: ▪ Un código de identificación único del certificado. ▪ Identificación del PSC, con indicación de su nombre o razón social, RUC, dirección de correo electrónico, y, en su caso, los antecedentes de su acreditación y su propia firma electrónica. ▪ Los datos de la firma de la AC del PSC. ▪ Los datos de identidad del titular, entre los cuales deben necesariamente incluirse su nombre o razón social, dirección de correo electrónico y cedula de identidad o RUC. ▪ Plazo de vigencia del certificado ▪ Información de la clave pública del titular. ▪ Identificador único de la entidad emisora.
Método de incorporación de identificación del titular	Se verificará que el PSC incorpore en sus certificados el identificador que venga al caso, Numero de Cedula para Nacionales o No. de pasaporte en caso de Extranjeros en caso de que el suscriptor sea una persona jurídica entonces se pondrá el No. RUC esto de conformidad a lo señalado en el Subcomponente del “Modelo de la Declaración de Prácticas de Certificación - DPC y Políticas de Certificados – PC de los Proveedores de Servicios de Certificación - PSC“.
Lectura y reconocimiento del contenido mínimo cuando existen atributos adicionales en el certificado	Se validará que el PSC estructure sus certificados de forma que los atributos adicionales que se introduzcan con el fin de incorporar límites al uso del certificado, si los hay, no impidan la lectura ni su reconocimiento por terceros.

Aspectos	Evaluación
Reconocimiento de límites de uso del certificado de firma electrónica	Se verificará que el PSC estructure sus certificados de manera que los límites de uso, si los hay, sean reconocibles por terceros.
Uso de clave pública acreditada	Se verificará que los datos de creación de firma del PSC acreditado para emitir certificados no sean utilizados más allá de lo establecido en la DPC aprobada por la DGTEC.
Algoritmos de firma	Se validará que el PSC utilice algoritmos de firma estándares de la industria (establecidos por el IETF PKIX RFC 5280) que provean el adecuado nivel de seguridad aprobado por la DGTEC tanto para su propia firma como para la firma del titular, o en su defecto cualquier tamaño de clave que sea aprobado debida y formalmente por la DGTEC, utilizando como mínimo de referencia el SHA256RSA.
Tamaño de las claves	Se comprobará que el PSC utilice el tamaño de clave pública y privada, de mínimo RSA 4096 bits para su propia firma y RSA 2048 bits para la firma del titular; o en su defecto cualquier tamaño de clave que sea aprobado debida y formalmente por la DGTEC.
Funciones Hash	Se verificará que el PSC utilice funciones Hash de última generación para el proceso de firma, debidamente elegidas por la DGTEC (utilizando como mínimo de referencia el SHA256) que provean el nivel de seguridad tanto para su propia firma como para la firma del titular. El uso de funciones de hash debe revisarse cada año, posterior a la creación de este documento.

3.2. Estructura de la Lista de Certificados Revocados – LCR y Servicio Online Certificate Status Protocol - OCSP

Objetivo

Verificar que las listas de certificados revocados tengan el formato y contenido especificado en el estándar, y permita al titular identificar plenamente al PSC emisor de la Lista de Certificados Revocados - LCR; y verificar la integridad y funcionalidad del servicio Protocolo de Estado del Certificado en Línea - OCSP, el cual sirve para determinar el estado de revocación de un certificado electrónico, como método alternativo a la Lista de Certificados Revocados - LCR. Este protocolo se describe en el RFC 6960.

Descripción

La Lista de Certificados Revocados - LCR debe contener la información y estructura que especifica el estándar ISO/IEC 9594-8 y del RFC 5280. Este estándar especifica que la lista debe contener al menos la identificación del emisor, fecha de su emisión e identificación de los certificados revocados a dicha fecha.

Ya que la lista podría ser almacenada y enviada en medios inseguros, debe estar debidamente firmada por el PSC emisor.

Estándares de evaluación

- ITU-T X.509: “Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks”.
- RFC 5280: “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile”.
- ISO/IEC 9594-8:2017: “Information technology - Open Systems Interconnection - The Directory: Part 8: Public-key and attribute certificate frameworks”.

- RFC 6960: “X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP”.
- RFC 6818: “Updates to the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.”

Documentación solicitada

- DPC y PC del PSC.
- Lista de Certificados Revocados - LCR emitida por el Proveedor de Servicios de Certificación en evaluación y el certificado de firma electrónica de la AC que la emite.
- Reportes de solicitudes y/o peticiones al servicio Protocolo de Estado de Certificados en Línea - OCSP.

Detalles de la evaluación

Aspectos	Evaluación
Para el Servicio LCR	
Contenido Mínimo	Se verificará que la LCR contenga al menos la siguiente información: ▪ Versión: Debe tener el valor 2. ▪ Nro. LCR: número que identifica de forma única a cada LCR emitida por el PSC. ▪ Algoritmo de firma: Este campo debe contener la identificación del algoritmo de firma utilizado, siguiendo el RFC 6818. El algoritmo de firma debe ser como mínimo SHA 256 RSA. ▪ Nombre del emisor: Este campo debe contener el nombre de la entidad que emitió y firmó la lista de certificados revocados. ▪ Última actualización: Este campo debe contener la fecha y hora en que fue emitida la lista de certificados revocados. ▪ Próxima actualización: Se deberá incluir en este campo la fecha en que se emitirá la próxima lista de certificados revocados ▪ Certificados revocados. En este campo se deben incluir los números de serie de los certificados revocados por el emisor, indicando además la fecha y hora de revocación correspondiente, y el motivo de la revocación.
Comprobación de firma	Se comprobará que la lista de certificados revocados esté debidamente firmada por el PSC emisor.
Mecanismo de suspensión de certificados	Se verificará que la lista de certificados revocados incluya la información necesaria para indicar el estado de suspensión de un certificado.
Para el Servicio OCSP:	
Pruebas de las peticiones	El PSC debe mantener un sitio de acceso electrónico, el servicio del OCSP el cual debe aceptar peticiones respecto a la vigencia o no de los certificados electrónicos por él emitidos. Se debe asegurar una disponibilidad del sitio no menor al 99%.
Comprobación del contenido de las consultas	Debe revisarse el contenido de las respuestas esperadas. Los estatus de las respuestas deben ser: válido, revocado y desconocido.
Seguridad	Se debe proteger la integridad y disponibilidad de la información mediante el uso de tecnología y medidas de seguridad tanto físicas como lógicas que reduzcan los riesgos y consecuencias de ataques maliciosos tanto internos como externos en contra del sitio.

3.3. Registro de Acceso Público

Objetivo

Asegurar el acceso a información relevante descriptiva del sistema a los titulares y terceros de forma permanente.

Descripción

Se verificará que el Proveedor de Servicios de Certificación - PSC:

- Incluya en su DPC los componentes: 2.2, 2.3 y 2.4 referidos en el “Modelo de la Declaración de Prácticas de Certificación - DPC y Políticas de Certificados - PC de los Proveedores de Servicios de Certificación - PSC”.
- Garantice la existencia de un servicio seguro de consulta remota de un registro de certificados emitidos, en el que quede constancia de los certificados emitidos indicando si el mismo se encuentra vigente, revocado o suspendido, si le ha sido traspasado de otro PSC acreditado o si es homologado.
- Provea acceso al registro público de certificados a los titulares y partes interesadas por medios electrónicos de manera continua y regular.
- Use sistemas y productos confiables que garanticen la seguridad de su sistema de difusión de información.
- Cuente con procedimientos para informar a los titulares las características generales de los procesos de creación y verificación de firma electrónica, así como de las reglas sobre prácticas de certificación que el PSC se comprometa a utilizar en la prestación del servicio.
- Tenga procedimientos para dejar sin efecto temporal o definitivamente (suspender o revocar) los certificados.
- Cuente con procedimientos para publicar y actualizar en su(s) sitio(s) web la información de acceso electrónico, las resoluciones de la DGTEC que le afecten. Esto debe realizarse como mínimo en los sitios de dominio público registrados durante el proceso de acreditación. Además, debe incluirse la DPC y PC.
- Provea de los manuales y software (controladores) necesarios para la operación de los dispositivos de firma electrónica certificada que proporcione a sus usuarios.

Estándares de evaluación

- RFC 3647: “Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework”.
- DGTEC: “Modelo de la Declaración de Prácticas de Certificación - DPC y Políticas de Certificados – PC de los Proveedores de Servicios de Certificación - PSC”; Componentes: 2.2, 2.3 y 2.4.

Documentación solicitada

Documento descriptivo que contenga al menos la siguiente información:

- Detalle del sitio Web donde publicara la información.
- Descripción de la tecnología utilizada.

- Disponibilidad, accesibilidad, conexión, esquemas y diagramas de funcionamiento.
- Medidas de seguridad implementadas para asegurar que solo el personal autorizado pueda modificar el sitio.
- Sitio Web de prueba con las funcionalidades requeridas.
- Documento de pruebas de penetración, realizado por una empresa auditora calificada.

Detalles de la evaluación

Aspectos	Evaluación
Existencia y contenido mínimo del Sitio Web de información pública	El PSC debe mantener un sitio de acceso electrónico, con información relevante para los titulares y las partes que confían. Al menos debe contener los siguientes documentos: ▪ DPC y PC que implementan. ▪ Certificado de la AC Raíz ▪ Certificado del PSC. ▪ Publicación del De-lta LCR cada 24hs. (si es que esta implementado). ▪ Lista de certificados vigentes y revocados. ▪ La proforma de contrato de suscriptor. ▪ Las resoluciones que habilitan, suspenden o revocan al PSC. ▪ La información relevante de la última auditoría que fueran objeto. ▪ Leyes, decretos, reglamentos y resoluciones que rigen la actividad de la ICP Nicaragua. ▪ Identificación, domicilio y medio de contacto. ▪ Indicaciones de transferencia de certificados de otros PSC (si los hay) ▪ Acceso seguro a los titulares de certificados para poder realizar revocaciones o suspensiones de certificados vigentes.
Disponibilidad de la Información y servicio	Se debe asegurar una disponibilidad del sitio no menor al 99% y un tiempo programado de inactividad máximo de 0,5% anual. Para esto se verificará la existencia de mecanismos redundantes o alternativos de conexión y sitios de contingencia que se levanten manual o automáticamente en caso de desastres.
Seguridad	Se debe proteger la integridad y disponibilidad de la información mediante el uso de tecnologías y medidas de seguridad tanto físicas como lógicas que reduzcan los riesgos y consecuencias de ataques maliciosos tanto internos como externos en contra del sitio. El repositorio debe contar con un certificado SSL.

3.4. Plan de administración de claves criptográficas

Objetivo

Comprobar que el PSC implementa un plan de administración del ciclo de vida de sus claves criptográficas coherente con su política de seguridad que permita mostrar un nivel de confianza consistente con los objetivos del negocio y que asegure que las claves de la AC son generadas bajo circunstancias controladas.

Descripción

Las claves criptográficas son la base de una Infraestructura de Claves Públicas - ICP, siendo el elemento principal a resguardar y administrar por el Proveedor de Servicios de Certificación - PSC, y por lo tanto requiere de un plan específico para su administración.

Este Plan debe tener el siguiente contenido mínimo:

Documentación del ciclo de vida completo de las claves criptográficas, esto es:

- Generación de las claves de la Autoridad de Certificación de firma electrónica del PSC.
- Almacenamiento, respaldo y recuperación de la clave privada de la AC de firma electrónica.
- Distribución de la clave pública de la AC de firma electrónica.
- Uso de la clave privada por parte de la AC de firma electrónica.
- Término del ciclo de vida de la AC de firma electrónica.
- Revocación del Certificado del PSC.
- Administración del ciclo de vida del hardware criptográfico utilizado por la AC.
- Servicios de administración de las claves de los titulares suministrados por la AC (generación de clave, renovación después de vencimiento y revocación de la clave).
- Preparación de los dispositivos seguros de los titulares.
- A su vez el plan debe ser consistente con la Proveedor de Servicios de Certificación - PSC y la Política de Certificados - PC.

Estándares de Evaluación

- ISO/IEC 15408 (Common Criteria EAL-4 o superior) “Information technology - Security techniques - Evaluation Criteria for IT Security”.
- ISO/IEC 7816: Partes: 1 al 4, 6 al 10,12 y 15 “Identification cards - Integrated Circuit Cards - Part 1: Cards with Contacts - Physical Characteristics”.
- ISO/IEC 7810: “Identification cards - Physical characteristics”.
- ISO/IEC 14443: Partes: 1 al 4 “Cards and security devices for personal identification - Contactless proximity objects”.
- FIPS PUB 180-4: “Secure Hash Standard (SHS)”.
- FIPS 140-2 (level 3) “Federal Information Processing Standards”.
- Estándares ETSI relacionados:
    - ETSI EN 319 401 “Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers”.
    - ETSI EN 319 411 “Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers Issuing Certificates”.

Documentación Solicitada

- Documento descriptivo de la implementación del plan de administración de claves criptográficas del PSC.

Detalles de la Evaluación

Aspectos	Evaluación
Relación entre el Plan de Administración de Claves y los recursos asignados	Verificar que el PSC dispone de los recursos y capacidades adecuados para implementar el plan de administración de claves.
Relación entre Plan de Administración de Claves y Evaluación de Riesgos	Verificar que los procedimientos y mecanismos de administración de claves implementados permiten alcanzar el riesgo residual determinado en la Evaluación de Riesgos.
Mantenimiento del Plan de Administración de Claves	Confirmar que los procedimientos implementados de acuerdo al Plan de Administración de Claves posibilitan que la seguridad de las claves se mantiene en el tiempo ante cambios en: amenazas, personal, servicios, componentes tecnológicos, etc.
Relación del Plan de Administración de Claves con las prácticas y Política de Certificados	Comprobar que los objetivos de seguridad enunciados en la DPC y PC del PSC se logran a través de la implementación del Plan de Administración de Claves.
Estándares ETSI relacionados	Verificar que “los requerimientos de Generación de Claves de la AC”, de los estándares ETSI relacionados, están considerados.
Estándares ETSI relacionados	Verificar que “los requerimientos de Almacenamiento, Respaldo y Recuperación de claves”, están considerados conforme los estándares ETSI relacionados.
Estándares ETSI relacionados	Confirmar que “los requerimientos de distribución de la clave pública de la AC”, están considerados conforme los estándares ETSI relacionados.
Estándares ETSI relacionados	Confirmar que “los requerimientos del Depósito de Claves (Key Escrow)”, están considerados conforme los estándares ETSI relacionados.
Estándares ETSI relacionados	Verificar que “los requerimientos de uso de clave de la AC”, están considerados conforme los estándares ETSI relacionados.
Estándares ETSI relacionados	Comprobar que “los requerimientos de fin del ciclo de vida de la clave de la AC”, están considerados conforme los estándares ETSI relacionados.
Estándares ETSI relacionados	Verificar que “los requerimientos del ciclo de vida de la administración del hardware criptográfico”, están considerados conforme los estándares ETSI relacionados.
Estándares ETSI relacionados	Verificar que “los requerimientos de terminación de una AC”, están considerados conforme los estándares ETSI relacionados.
Nivel de seguridad del dispositivo seguro de los titulares	Verificar que el dispositivo seguro de los titulares cumple como mínimo con los requerimientos del estándar FIPS 140-2 nivel 3 o Como Criterio EAL 4 ISO/IEC 15408. En sus elementos de seguridad e implementación de los algoritmos criptográficos estándares.

3.5. Manual de Operación de la Autoridad de Certificación - AC

Objetivo

Comprobar a través de la documentación presentada el cumplimiento de los requerimientos y obligaciones que dispone la Ley, el Reglamento y el marco normativo establecido por el ente rector en

relación con la confiabilidad e interoperabilidad en la forma de operar y prestar los servicios de la AC de un PSC.

Descripción

El propósito del manual es describir la administración diaria y las prácticas operacionales de la Autoridad de Certificación - AC principal y/o las Autoridad de Certificación - AC´s Subordinadas[3] y garantizar que las directrices primarias de la Declaración de Prácticas de Certificación DPC y Políticas de Certificados - PC estén implementadas operacionalmente; con el fin de facilitar al personal (de operaciones, consultores y/o auditores), la comprensión de esta información, se permite el uso de gráficos, diagramas de flujo, funcionales, líneas de tiempo, etc.

El Manual de Operación de la Autoridad de Certificación - AC principal y/o Subordinadas deberá tener al menos las siguientes características:

- Ser consistente con la Política de Certificados.
- Ser consistente con el Marco Normativo establecido por el Ente Rector.
- Incluir la interacción entra la Autoridad de Certificación - AC principal y la(s) AC´s subordinadas, así como con las Autoridad de Registro - AR.
- Describir los controles de seguridad física, de red, de recursos humanos y de procedimientos.
- Incluir los procedimientos adoptados para el manejo de claves públicas y privadas.

Estándares de Evaluación

- RFC 3647: “Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework”.
- ETSI EN 319 411 Parte: 1 y 2 “Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers Issuing Certificates”.

Documentación Solicitada

- Manual de operación de la Autoridad de Certificación - AC principal y/o AC´s subordinadas del Proveedor de Servicios de Certificación - PSC. Ver Anexo No. 2 “Estructura y Contenido mínimo del Manual de Operaciones de la Autoridad de Certificación – AC de un Proveedor de Servicio de Certificación - PSC”.
- Manual del Hardware Criptográfico usados para la generación y protección de las claves privadas de la(s) autoridades de certificación.

Detalles de la Evaluación

Aspectos	Evaluación
Nómina y descripciones de cargos	Reporte de Nómina de los cargos del personal, con las descripciones de las responsabilidades y los procedimientos en base a los cuales los empleados realizan sus funciones.

[3] En base a “Modelo de Confianza para Firma Electrónica Certificada”; Figura 5, Pág. 12.

Aspectos	Evaluación
Referencias de los cargos en los planes del PSC	Referencia del personal en los planes de continuidad del negocio y los planes de recuperación de desastres y contingencia. Descripción de las funciones del personal específico de la AC que sean responsables de las funciones críticas de la AC.
Descripción de las Operaciones	Descripción detallada de los siguientes procedimientos: ▪ Generación de pares de claves. ▪ Carga de claves y certificados en medios removibles y no removibles. ▪ Revocación de certificados. ▪ Publicación de la LCR. ▪ Publicación de la información del certificado. ▪ Distribución de claves y certificados. ▪ Renovación de certificados. ▪ Renovación de certificados luego de una revocación. ▪ Suspensión de certificados. ▪ Medidas de control de acceso a las instalaciones de la AC. ▪ Procedimientos de respaldo y recuperación.
Actualización de DPC y PC	Procedimiento de actualización de la DPC y PC de firma electrónica.
Servicios de la AC	Descripción de los servicios de la AC principal y/o subordinadas.
Interacción AC - AR	Descripción de la interacción entre la AC principal y/o subordinadas, así como con las AR´s; y las interacciones entre la AC y otras organizaciones relacionadas.
Estándares ETSI relacionados	Comprobar que los términos y condiciones “de los servicios de administración de claves de los titulares”, están considerados conforme los estándares ETSI relacionados.
Estándares ETSI relacionados	Comprobar que los términos y condiciones “para la renovación, cambio de claves y actualización de certificados electrónicos”, están considerados conforme los estándares ETSI relacionados.
Estándares ETSI relacionados	Comprobar que los términos y condiciones “para la generación de certificados”, están considerados conforme los estándares ETSI relacionados.
Estándares ETSI relacionados	Comprobar que los términos y condiciones “para la difusión de los términos y condiciones”, están considerados conforme los estándares ETSI relacionados.
Estándares ETSI relacionados	Comprobar que los términos y condiciones “para la difusión de los certificados”, están considerados conforme los estándares ETSI relacionados.
Estándares ETSI relacionados	Comprobar que los términos y condiciones “para la revocación y suspensión de certificados”, están considerados conforme los estándares ETSI relacionados.
Estándares ETSI relacionados	Comprobar que los términos y condiciones “para la gestión del ciclo de vida del hardware criptográfico utilizado para firmar certificados“, están considerados conforme los estándares ETSI relacionados.

3.6. Manual de Operación de la Autoridad de Registro - AR

Objetivo

Comprobar a través de la documentación presentada el cumplimiento de los requerimientos y obligaciones que dispone la Ley, el Reglamento y el marco normativo establecido por el ente rector en relación con la confiabilidad e interoperabilidad en la forma de operar y prestar los servicios de la Autoridad de Registro - AR de un Proveedor de Servicios de Certificación - PSC.

Descripción

El manual de operación deberá describir como operará el servicio de registro del Proveedor de Servicios de Certificación - PSC y su administración diaria. Entre otros aspectos debería tener al menos las siguientes características:

- Ser consistente con la Políticas de Certificación - PC.
- Describir el plan de entrenamiento de los empleados.
- Incluir la forma en que se verifica la identidad de las personas.
- Incluir procedimientos de entrega y uso de la clave privada por los titulares de los certificados.
- Contener la metodología adoptada para manejar los temas de:
  - Análisis de riesgos.
  - Plan de recuperación de desastres.
  - Plan de seguridad.
  - Incluir la interacción entre las unidades internas que cumplen la función de Autoridad de Certificación - AC y Autoridad de Registro - AR.
  - Incluir la descripción de los mecanismos a través del cual se constatará la solicitud del certificado, su autorización, su completitud y su veracidad.
  - Incluir la descripción de los mecanismos a través del cual se validará la identificación de los suscriptores y titulares, así como sus datos.

Estándares de Evaluación

- RFC 3647: “Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework”.
- ETSI EN 319 411: Parte 1 y 2 “Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers Issuing Certificates”.

Documentación Solicitada

- Manual de operación de la Autoridad de Certificación - AC principal y/o AC´s subordinadas del Proveedor de Servicios de Certificación - PSC. Ver **Anexo No. 3** “Estructura y Contenido mínimo del Manual de Operaciones de la Autoridad de Registro – AC de un Proveedor de Servicio de Certificación – PSC”.
- Manual técnico de los dispositivos seguros de firma electrónica.

Detalles de la Evaluación-

Aspectos	Evaluación
Nómina y descripción de cargos	Reporte de Nómina solo de los nombres y cargos del personal, con la descripción de las responsabilidades y los procedimientos en base a los cuales los empleados realizan sus funciones.
Procesos de registro	Se verifica los procesos de registro, verificación, autenticación y validación del Solicitante, así como el proceso de comprobación de identidad aplicado por la AR a los solicitantes de Certificados de servicios de firma electrónica.

Aspectos	Evaluación
Entrega segura de los datos de creación de firma	El PSC (o la AR) debe tener procedimientos y prácticas implementadas que permitan la entrega de forma personal y segura de los datos de creación de firma a los titulares de los certificados.
Dispositivo seguro y mecanismos de firma del titular	El PSC (o la AR) debe tener implementados procedimientos y prácticas que aseguren que una vez entregados los datos de creación de firma, sólo el titular tenga control de ellos. El dispositivo seguro entregado al titular debe firmar internamente el documento sin ser jamás accesible la clave privada del titular. El mecanismo de control de acceso a la clave privada sólo debe ser conocido por el titular al momento de la entrega del dispositivo y en lo posible modificable por el mismo titular, antes de ser utilizado por primera vez. El dispositivo seguro debe contar con mecanismos que inhabiliten el dispositivo en caso de reiterados intentos fallidos de acceso. El PSC debe entregar al titular herramientas, aplicaciones e instrucciones para que el titular pueda firmar en forma segura.
Capacitación y servicio al titular	El PSC debe implementar procedimientos de capacitación que permitan al titular manejar en forma segura e informada el dispositivo de firma, y además mantener un servicio de atención a usuarios para responder y solucionar dudas de los titulares.
Referencias de los cargos en los planes de continuidad de negocios del PSC	Referencia del personal en los planes de continuidad del negocio y los planes de recuperación de desastres y contingencia.
Planes de contingencia	Descripción de planes de contingencia y respuestas a incidentes de seguridad, evaluación de vulnerabilidad y procesos de gestión de cambios.
Descripción de las operaciones	Descripción detallada de los siguientes eventos: ▪ Procedimientos de control de acceso hacia las instalaciones de la AR ▪ Procedimientos de respaldo y recuperación ▪ Difusión de información al personal sobre prácticas operativas. ▪ Gráficos y diagramas de flujo relacionados con las operaciones.
Interacción entre AC y AR del PSC	La descripción de los procedimientos que involucren la interacción entre la AC y AR
Estándares ETSI relacionados	Comprobar que “los procedimientos de registro de los titulares” están considerados conforme los estándares ETSI relacionados.
Estándares ETSI relacionados	Comprobar que “los procedimientos de revisión e inicialización de dispositivos distribuidos a usuarios finales” están considerados conforme los estándares ETSI relacionados.
Seguridad de la Información	Detalles de todas las operaciones consistentes con las descritas en la Documentación de seguridad de la información Procesos y procedimientos en vigor para: ▪ Mantener la información de identidad recolectada, y, ▪ Renovaciones de certificados digitales, revocaciones y solicitudes de suspensión.
Auditorias	Requisitos de auditoria (internas y externas).
Estándares	Estándares relevantes referenciados en el documento.

3.7. Modelo de Confianza

Objetivo

Comprobar que el Proveedor de Servicios de Certificación - PSC describa con claridad a los Titulares los componentes del modelo de confianza (tecnológicos, operacionales y legales) que utilizan en su sistema de gestión y que aplican en los certificados (y/o servicios) que ellos ofertan al público.

Descripción

El modelo de confianza del Proveedor de Servicios de Certificación - PSC permite a los titulares (y/o terceros que confían) que los documentos que ellos envíen o reciban firmados con los certificados de firma electrónica emitidos por los Proveedor de Servicios de Certificación - PSC, cumplen con las garantías de autenticidad, confidencialidad, integridad y no repudio; y que en base a lo anterior cuenta con la debida fuerza probatoria legal equivalente a su formato alterno escrito.

El modelo de confianza de la Infraestructura Nicaragüense de Clave Pública - INCP se fundamenta en un modelo jerárquico (bajo la jerarquía de un certificado raíz nacional), que permite que los documentos que hayan sido firmados con certificados de firma electrónica emitidos por PSC´s que sean autorizados por el ente regulador, cuenten con el mismo valor jurídico que los firmados de forma manuscrita.

El modelo a su vez permite que los titulares puedan realizar consultas (comprobaciones) de validez del estado de los certificados con los que se hayan firmado los documentos enviados o recibidos.

Estándares de Evaluación

- Documento DGTEC: “Modelo de Confianza para Firma Electrónica Certificada”.

Documentación Solicitada

- Documento en el que se describe el modelo de confianza utilizado por el PSC para lograr el objetivo o alternativamente la DPC y/o PC si contienen dicho punto.

Detalles de la Evaluación

Aspectos	Evaluación
Modelo de Confianza	Verificar que el PSC se apega al modelo de confianza establecido por el ente rector de firma electrónica en el documento “Modelo de Confianza para Firma Electrónica Certificada”. Verificar que los certificados faciliten a los titulares la posibilidad de que puedan verificar la cadena de confianza que brinda la Infraestructura Nicaragüense de Clave Pública - INCP.

VII. ANEXOS

Anexo No. 1: Resumen de Áreas Técnicas y Estándares Tecnológicos Específicos

No.	Nombre	Normas y Estándares	Documentación Solicitada
AT01. Declaración de Prácticas de Certificación - DPC y Política de Certificados - PC			
1	Declaración de Prácticas de Certificación. Política de Certificados.	▪ "Modelo de la Declaración de Prácticas de Certificación - DPC y Políticas de Certificados - PC de los Proveedores de Servicios de Certificación - PSC." ▪ RFC 3647 o su equivalente. ▪ ETSI EN 319 401. ▪ ETSI EN 319-411 Parte:1-2. ▪ ETSI EN 319-412 Parte: 1 al 3 y 5.	Documento de la Declaración de Practica de Certificación - DPC. Con el contenido tal como lo indica el RFC 3647 o su equivalente ETSI. Documento de la Política de Certificados - PC con los diferentes tipos de estructura de campos de certificados. Con el contenido tal como lo indica el RFC 3647 o su equivalente ETSI.
AT02. Seguridad de la Información			
1	Seguridad de la Información: Certificado de Cumplimiento de Norma NTN 21 001-13 o ISO 27001: 2013 (incluyendo Cor 1:2014 y Cor 2:2015) o superior.	▪ NTN 21 001-13 / ISO 27001:2005 (ver Equivalente/superior). ▪ ISO/IEC 27002:2013.	Documento que avale la certificación estándar, así como toda la documentación soporte que sustenta dicha certificación: ▪ Ver inciso (2) del Área Técnica No. 2 de "Criterios Específicos" de este documento: "2. Seguridad de la Información /Documentación Solicitada".
2	Administración de Riesgos.	▪ ISO 27005:2018 (o superior).	Documento de Administración de Riesgos
3	Plan de Continuidad del Negocio y Recuperación de Desastres.	▪ ISO 27001:2005 (o Superior).	Documento Plan de Continuidad del negocio y Recuperación de Desastres
4	Plan de Seguridad del Sistema de Información.	▪ ISO 27002:2013.	Documento de Plan de Seguridad del Sistema de Información
5	Plan de seguridad física y ambiental.	▪ ISO 27002:2013.	Documento de Plan de seguridad física y ambiental
6	Evaluación de la Plataforma Tecnológica.	▪ ISO/IEC 15408-1. ▪ ISO/IEC 19790. ▪ ISO/IEC 24759. ▪ FIPS 140-2 Nivel 3 (o Superior). ▪ TIA-942-B.	Documento descriptivo de la implementación de la infraestructura tecnológica. Este documento debe incluir al menos: ▪ Planos de interconexión de sistemas, cableado de red de datos, cableado de fuente de alimentación de energía eléctrica (principal y auxiliar), dispositivos de seguridad y control de acceso, y todo aquello relevante que permita demostrar la confiabilidad de la infraestructura tecnológica. ▪ Manuales del fabricante de los productos hardware y software relevantes. Documentación del fabricante que acredite el correspondiente nivel de seguridad. ▪ Manuales descriptivos del diseño físico y lógico de la red. Con detalle de servicios implementados.

AT03. Infraestructura de Clave Pública			
1	Estructura e Información del Certificado de Firma Electrónica.	▪ ITU-T X.509 ▪ RFC 5280 ▪ ISO/IEC 9594-8:2017 ▪ RFC 3647. ▪ RFC 3628. ▪ RFC 3161. ▪ ETSI TS 319 421. ▪ ETSI EN 319 422. ▪ "Modelo de la Declaración de Prácticas de Certificación - DPC y Políticas de Certificados - PC de los Proveedores de Servicios de Certificación - PSC."	Ejemplos de Certificados tipo de firma electrónica y ejemplo de la solicitud de firma del certificado (CSR).
2	Estructura e Información de la Lista de Certificados de Firma Electrónica Revocados - LCR y Servicio OCSP.	▪ ITU-T X.509 ▪ RFC 5280 ▪ ISO/IEC 9594-8:2017 ▪ RFC 6960 ▪ RFC 6818	Lista de Certificados Revocados (LCR) emitida por el PSC y el Certificado de firma electrónica de la AC que la emite. Reportes de solicitudes y/o peticiones al servicio OCSP.
3	Registro de Acceso Público.	▪ RFC 3647. ▪ "Modelo de la Declaración de Prácticas de Certificación - DPC y Políticas de Certificados - PC de los Proveedores de Servicios de Certificación - PSC."	Documento descriptivo que contenga al menos: ▪ DPC ▪ Detalle del sitio web donde se publicará la información. ▪ Descripción de la tecnología utilizada. ▪ Disponibilidad, accesibilidad, conexión, esquemas y diagramas de funcionamiento. ▪ Medidas de seguridad implementadas para asegurar que solo el personal autorizado pueda modificar el sitio. ▪ Sitio web (de prueba en caso de ser la 1ra. Acreditación) con las funcionalidades requeridas. Documentación de pruebas de penetración, realizado por una empresa auditora calificada.
4	Plan de Administración de Claves Criptográficas.	▪ ISO 15408 Common Criterial EAL 4+ (o superior). ▪ ISO/IEC 7816 Partes:1 al 4, 6 al 10, 12 y 15. ▪ ISO/IEC 7810. ▪ ISO/IEC 14443 Partes:1 al 4. ▪ FIPS PUB 180-4. ▪ FIPS 140-2 (nivel 3 o superior). ▪ Estandares ETSI relacionados: - ETSI EN 319 401. - ETSI EN 319 411-1.	Documento descriptivo de la implementación del plan de administración de claves criptográficas de la organización.
5	Manual de Operación de la Autoridad de Certificación del PSC.	▪ RFC 3647. ▪ ETSI EN 319 411-1. ▪ ETSI EN 319 411-2.	Manual de Operación de la AC de un PSC.

6	Manual de Operación de la Autoridad de Registro.	▪ RFC 3647 ▪ ETSI EN 319 411-1 ▪ ETSI EN 319 411-2	Manual de Operación de la AR de un PSC. Manual Técnico de los dispositivos seguros de Firma Electrónica.
7	Modelo de Confianza.	▪ Documento Emitido por el Ente Rector DGTEC: "Modelo de Confianza para Firma Electrónica Certificada V2_20160701".	Alternativamente la DPC y PC, si describe el modelo de confianza utilizado por el PSC para lograr el objetivo.

Anexo No. 2: Estructura y Contenido mínimo del Manual de Operaciones de la Autoridad de Certificación - AC de un Proveedor de Servicio de Certificación - PSC.

El Manual de Operaciones debe seguir la misma estructura del "Modelo de Declaración de Prácticas de Certificación y Políticas de Certificados" que es coherente con el RFC 3647

En base a lo anterior el Manual de Operaciones de una Autoridad Certificadora (AC) debería contener como mínimo la siguiente información:

- Procedimientos operacionales que describan la manera en que todo el personal empleado de la Autoridad Certificadora realiza cualquier tarea dentro de la AC.

- Referencia al "Plan de continuidad de negocio y de recuperación de desastres" y cualquier otro procedimiento de emergencia.

- Descripciones detalladas de los procedimientos seguidos para los siguientes eventos:

  - Generación de claves;
  - Carga de claves y certificados en medios seguros extraíbles;
  - Revocación del certificado;
  - Publicación de la lista de revocación de certificados;
  - Publicación de información del Certificado;
  - Método de distribución de claves y certificados de entidades finales;
  - Renovación rutinaria de certificado;
  - Renovación del certificado después de la revocación;
  - Medidas de control de acceso y procedimientos para las instalaciones de CA; y
  - Procedimientos de copia de seguridad y archivo;

- Detalles de todas las funciones de la CA consistentes con las descritas en el CPS y el CP

- Descripciones de las funciones del personal específico de CA responsable de las funciones críticas de CA

- Detalles de toda la interacción entre la CA y la RA

- Detalles de las interacciones entre la CA y las Organizaciones de Clientes Conocidos, las Organizaciones de Riesgo / Amenaza y las Organizaciones de Relación según corresponda

- Un glosario completo de términos utilizados en el documento.

Anexo No. 3: Estructura y Contenido mínimo del Manual de Operaciones de la Autoridad de Registro – AR de un Proveedor de Servicio de Certificación - PSC.

El Manual de Operaciones debe seguir la misma estructura del "Modelo de Declaración de Prácticas de Certificación y Políticas de Certificados" que es coherente con el RFC 3647.

En base a lo anterior el Manual de Operaciones de una Autoridad de Registro (AR) debería contener como mínimo la siguiente información:

- Roles y responsabilidades de la RA y del personal asociado (es decir, operadores de RA).
- El proceso y los procedimientos establecidos para respaldar la prueba de identidad.
- Los procedimientos utilizados para registrar, verificar, autenticar y validar a un Solicitante (y un Suscriptor) que solicitan un certificado digital.
- Procedimientos operativos que describen la manera en que todo el personal designado empleado dentro de la RA realiza cualquier tarea realizada con la RA.
- Vista general de los planes de respuesta a incidentes de seguridad de emergencia (incluidos los derrames de datos), evaluación de la vulnerabilidad y procesos de gestión de cambios.
- El grado de registro del sistema utilizado y los tipos de eventos capturados.
- Descripciones detalladas de los procedimientos seguidos para:
  - Medidas de control de acceso y procedimientos para las instalaciones de AR.
  - Procedimientos de copia de seguridad y archivo.
  - Publicación de información al personal sobre prácticas operativas.
- Detalles de todas las interacciones entre la RA y la CA;
- Detalles de todas las operaciones consistentes con las descritas en la Documentación de seguridad de la información;
- Procesos y procedimientos en vigor para:
  - Mantener la información de identidad recolectada.
  - Renovaciones de certificados digitales, revocaciones y solicitudes de suspensión.
- Gráficos y diagramas de flujo funcionales para mejorar la presentación de la información en el documento.
- Requisitos de auditoría (internos y externos).
- Un glosario completo de términos utilizados en el documento.
- Normas relevantes referenciadas en el documento.