Gobierno de Reconciliación y Unidad Nacional

El Pueblo, Presidente!

MHCP

DIRECCIÓN GENERAL DE TECNOLOGÍA

REQUISITOS ESPECÍFICOS PARA EMITIR CERTIFICADOS PARA FIRMA ELECTRÓNICA CERTIFICADA

Managua, julio del 2022

CONTROL DE REVISIÓN Y ACTUALIZACIÓN (VERSIONES)

Nº	Fecha	Elaborado/ Entrevistado	Revisado	Aprobado	Autorizado
01	Julio / 2022	Yuri Dompe Responsable Departamento de Supervisión e Inspección	Daysi Romero Responsable Departamento de Acreditación y Registro	Hans Espinoza Responsable Dirección Firma Electrónica	José Diaz Responsable Dirección General de Tecnología

ÍNDICE

I. INTRODUCCIÓN

La Dirección General de Tecnología - DGTEC del Ministerio de Hacienda y Crédito Público a través de la Dirección Firma Electrónica ha elaborado el presente documento "Requisitos específicos para emitir certificados para Firma Electrónica Certificada", a fin de establecer la normativa que regule los requisitos específicos que deberá cumplir todo Proveedor Servicios de Certificación - PSC que solicite autorización para brindar el servicio de emisión de certificados de firma electrónica certificada como parte de su cartera de servicios en el territorio nacional, o que ya haya sido autorizado para brindar ese servicio.

II. OBJETIVO

Complementar los requisitos específicos relacionados con la emisión de certificados de firma electrónica certificada que debe cumplir todo Proveedor de Servicios de Certificación - PSC que pretenda ser autorizado a operar en Nicaragua, o que ya haya sido autorizado por el Ente Rector de Firma Electrónica, para emitir "Certificados de Firma Electrónica Certificada".

III. 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.

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

  - Art.9, en los incisos 1, 4 establece las potestades de la Entidad Rectora relacionados con definir y dictar normas técnicas.

  - Art. 14, establece el obligatorio cumplimiento por parte de los Proveedores de Servicios de Certificación de las normas técnicas que dicte la Entidad Rectora.

IV. GLOSARIO DE TÉRMINOS Y SIGLAS

Los siguientes términos son definidos o complementados en esta normativa:

Marco Normativo de Firma Electrónica: Ley 729 "Ley de Firma Electrónica", Decreto 57-2011 "Reglamento de la Ley 729", Normas Técnicas emitidas por el Ente Rector de Firma Electrónica - DGTEC y otras relacionadas (NTN).

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

AC: Autoridad de Certificación.

CRL: Lista de Revocación de Certificados.

CSS: Servicio de Estado de Certificados.

DGTEC: Dirección General de Tecnología, dependencia del Ministerio de Hacienda y Crédito Público.

DPC: Declaración de Prácticas de Certificación (o Practicas de certificación o Practicas del Servicio de certificación o Practicas del PSC). Es un documento que debe elaborar el PSC, basado en las recomendaciones del RFC 3647.

Entidad Rectora o Ente Rector: Entidad Rectora de Acreditación de Firma Electrónica, que para fines del presente documento y en base a la ley 729, tal designación recae en la Dirección General de Tecnología, dependencia del Ministerio de Hacienda y Crédito Público.

ETSI: European Telecommunications Standars Institute – Instituto Europeo de Estándares de Telecomunicaciones.

IEC: International Electrotechnical Commission - Comisión Electrotécnica Internacional.

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

ISO: International Organization for Standardization - Organización Internacional de Estandarización.

ITU: International Telecommunications Union – Unión Internacional de Telecomunicaciones.

NCP+: Política de Certificación Normalizada que requiere un dispositivo criptográfico seguro.

NTN: Norma Técnica Nicaragüense.

OVR: Requisito General (requisito aplicable a más de un componente)

PC: Política de Certificados. Es un documento que debe elaborar el PSC, basado en las recomendaciones del RFC 3647.

PSC: Proveedor de Servicios de Certificación.

QCP-n: Política de Certificado Cualificado de la Unión Europea, emitido a una persona natural.

QCP-n-qscd: Política de Certificado Cualificado de la Unión Europea, emitido a una persona natural donde la clave privada y el certificado relacionado residen en un QSCD.

QSCD: Dispositivo calificado de creación de Firma.

REG: Servicios de Registro.

RFC: Request for Comments - Son una serie de publicaciones del “Grupo de Trabajo de Ingeniería de Internet” que describen diversos aspectos del funcionamiento de Internet y otras redes de computadoras, como protocolos, procedimientos, etc. y comentarios e ideas sobre estos.

WebTrust: Servicio de certificación internacional que desarrolla principios y criterios para la gestión y operación de las Autoridades de Certificación.

V. EQUIVALENCIA NORMATIVA ACEPTADA

Se da por aceptado el cumplimiento de la presente normativa, cuando se acredite evidencias de cumplimiento de las siguientes normas:

1. ETSI EN 319 411-2 V2.4.1 (2021-11) Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates; (QCP-n, QCP-l-qscd policies (based on EN 319 411-1, NCP/NCP+)); o,

2. WebTrust for CA v2.1; o,

3. ISO 21188:2018 Public key infrastructure for financial services - Practices and policy framework.

El cumplimiento de cualquiera de las normativas antes referidas, debe incluir el cumplimiento de los factores o criterios propios del “Marco Normativo de Firma Electrónica” vigente para Nicaragua.

VI. REQUISITOS ESPECÍFICOS

1. Documentación aplicable a los Servicios de Certificación:

1.1. Declaración de Prácticas de Certificación.

1.1.1. El PSC debe incluir en las PC identificadas en la documentación, los requisitos relacionados con los perfiles de certificados que se utilizaran. (ver OVR-5-1.03A; ETSI EN 319 411-1 V1.3.1).

1.1.2. El PSC debe incluir en su DPC los algoritmos de firma y los parámetros empleados. (ver OVR-5-2.04; ETSI EN 319 411-1 V1.3.1) (ver Decreto 57-2011: Arto. 17, inciso 2; Arto. 20, inciso 4; Arto. 22, inciso (3).

1.1.3. Aplica (1.1.3) del documento “Requisitos Generales de Proveedores de Servicios de Certificación” (ver REQ-6.1-01; ETSI 319 401 V2.3.1).

1.1.4. Aplica (1.1.4) del documento “Requisitos Generales de Proveedores de Servicios de Certificación” (ver REQ-6-1-02; ETSI 319 401 V2.3.1).

1.1.5. No aplica.

1.1.6. Aplica (1.1.6) del documento “Requisitos Generales de Proveedores de Servicios de Certificación” (ver REQ-6.1-05A-Nota2; ETSI 319 401 v2.3.1).

1.1.7. Aplica (1.1.7) del documento “Requisitos Generales de Proveedores de Servicios de Certificación” (ver REQ-6.1-07; ETSI 319 401 v2.3.1).

1.1.8. Aplica (1.1.8) del documento “Requisitos Generales de Proveedores de Servicios de Certificación” (ver REQ-6.1-08; ETSI 319 401 v2.3.1).

1.1.9. Aplica (1.1.9) del documento “Requisitos Generales de Proveedores de Servicios de Certificación” (ver REQ-6.1-09A; ETSI 319 401 v2.3.1).

1.1.10. Aplica (1.1.10) del documento “Requisitos Generales de Proveedores de Servicios de Certificación” (ver REQ-6.1-11; ETSI 319 401 v2.3.1).

1.2. Política de Certificados

1.2.1. Aplica (1.2.1) del documento “Requisitos Generales de Proveedores de Servicios de Certificación” (ver Decreto 57-2011: Arto. 17, inciso 2) (ver OVR-5.2-02; ETSI 319 411-1 v1.3.1).

1.2.2. Aplica (1.2.2) del documento “Requisitos Generales de Proveedores de Servicios de Certificación” (ver 5.3 (b); ETSI 319 411-1 v1.3.1).

1.2.3. Estructura basada en RFC-3647 (Internet X.509 Public Key Infrastructure. Certificate Policy and Certification Practices Framework”).

1.3. Términos y Condiciones del PSC

1.3.1. Aplica (1.3.1) del documento “Requisitos Generales de Proveedores de Servicios de Certificación”.

1.3.2. Aplica (1.3.2) del documento “Requisitos Generales de Proveedores de Servicios de Certificación”.

1.3.2.1. Aplica (1.3.2.1) del documento “Requisitos Generales de Proveedores de Servicios de Certificación”.

1.3.2.2. Aplica (1.3.2.2) del documento “Requisitos Generales de Proveedores de Servicios de Certificación”
El PSC además deberá delimitar como parte del uso del certificado, que:
-Los certificados emitidos bajo estos requisitos tienen como objetivo respaldar las firmas electrónicas certificadas basadas en un certificado de firma emitido por un PSC (ver 5.5.3 QCP-n-qscd; ETSI 319 411-2 v2.4.1).

1.3.2.3. Aplica (1.3.2.3) del documento “Requisitos Generales de Proveedores de Servicios de Certificación”.

1.3.2.4. Aplica (1.3.2.4) del documento “Requisitos Generales de Proveedores de Servicios de Certificación”.

1.3.2.5. Aplica (1.3.2.5) del documento “Requisitos Generales de Proveedores de Servicios de Certificación”.

1.3.2.6. Aplica (1.3.2.6) del documento “Requisitos Generales de Proveedores de Servicios de Certificación”.

1.3.2.7. Aplica (1.3.2.7) del documento “Requisitos Generales de Proveedores de Servicios de Certificación”.

1.3.2.8. Aplica (1.3.2.8) del documento “Requisitos Generales de Proveedores de Servicios de Certificación”.

1.3.2.9. Aplica (1.3.2.9) del documento “Requisitos Generales de Proveedores de Servicios de Certificación”.

1.3.2.10. Aplica (1.3.2.10) del documento “Requisitos Generales de Proveedores de Servicios de Certificación”.

1.3.2.11. Aplica (1.3.2.11) del documento “Requisitos Generales de Proveedores de Servicios de Certificación”.

1.3.3. Aplica (1.3.3) del documento “Requisitos Generales de Proveedores de Servicios de Certificación”.

1.3.4. Aplica (1.3.4) del documento “Requisitos Generales de Proveedores de Servicios de Certificación”.

1.3.5. Aplica (1.3.5) del documento “Requisitos Generales de Proveedores de Servicios de Certificación”.

1.3.6. Aplica (1.3.6) del documento “Requisitos Generales de Proveedores de Servicios de Certificación”.

1.4. Nombre e identificación de la Declaración de Practica de Certificación y de la Política de Certificados del PSC:

El nombre y la identificación de las DPC y PC se realizará de conformidad a lo establecido en el documento “Normativa de Conformación de Identificadores de Objetos en Nicaragua” y la “Guía de Administración de los Identificadores de Objeto en Nicaragua”:

1.4.1. Aplica (1.4.1) del documento “Requisitos Generales de Proveedores de Servicios de Certificación” (ver Anexo B.2.3; ISO 21188:2018) (ver el documento “Normativa de Conformación de Identificadores de Objetos en Nicaragua” y la “Guía de Administración de los Identificadores de Objeto en Nicaragua”).
Estructura modelo de la identificación OID de la DPC de un PSC en Nicaragua:
{join-iso-itu-t(2) country(16) ni(558) incp(0) ac-privadas(1) ac-de-“acrónimo del psc” (1) dpc(1) [desde (1) hasta (n)]}.

1.4.2. Aplica (1.4.1) del documento “Requisitos Generales de Proveedores de Servicios de Certificación” (ver Anexo B.2.3; ISO 21188:2018) (ver el documento “Normativa de Conformación de Identificadores de Objetos en Nicaragua” y la “Guía de Administración de los Identificadores de Objeto en Nicaragua”).
Ejemplo de identificación OID de la PC de un PSC en Nicaragua:
{join-iso-itu-t(2) country(16) ni(558) incp(0) ac-privadas(1) ac-de-“acrónimo del psc” (1) pc-de-“nombre del certificado”(2) [desde (1) hasta (n)] versión [desde (1) hasta (n)]}.
Aclaración: en <<pc-de-“nombre del certificado”>>se identificaran de forma separada todos los tipos de certificados que el PSC sea autorizado a ofertar, bien pueden ser por ejemplo: “certificados de persona natural” o “certificados de persona jurídica” o “certificados de empleado público” o de fines más específicos como los “certificados para firma de código EV”.

1.4.3. Cualquier otra asignación de OID relacionadas a certificados de firma electrónica, que no sean contemplados en el documento “Normativa de Conformación de Identificadores de Objetos en Nicaragua” y la “Guía de Administración de los Identificadores de Objeto en Nicaragua”; deberá

armonizarse con el encargado de la rama (o nodo) OID correspondiente al árbol OID pertinente a Nicaragua.

2. Servicios de Certificación prestados por el PSC

2.1. Los servicios de certificación se desglosan en los siguientes componentes a efectos de clasificación de requisitos:

2.1.1. Aplica (2.1.1) del documento “Requisitos Generales de Proveedores de Servicios de Certificación” (ver 4.3; ETSI 319 411-1 V1.3.1).

El PSC además deberá:

a) Verificar la identidad de la persona natural solicitante del servicio (ver REG-6.2.2-02 [QCP-n (a)]; ETSI 319 411-2 V2.4.1).

b) Verificar la identidad de la persona jurídica solicitante del servicio (ver REG-6.2.2-02 [QCP-l-qscd (a)]; ETSI 319 411-2 V2.4.1).

2.1.2. Aplica (2.1.2) del documento “Requisitos Generales de Proveedores de Servicios de Certificación” (ver 4.3; ETSI 319 411-1 V1.3.1).

2.1.3. Aplica (2.1.3) del documento “Requisitos Generales de Proveedores de Servicios de Certificación” (ver 4.3; ETSI 319 411-1 V1.3.1).

2.1.4. Aplica (2.1.4) del documento “Requisitos Generales de Proveedores de Servicios de Certificación” (ver 4.3; ETSI 319 411-1 V1.3.1).

Cuando el PSC proporciona CRL:

a) El PSC no debe eliminar de la CRL los certificados revocados después de que hayan expirado (ver CSS-6.3.10-03; ETSI 319 411-2 V2.4.1);

b) Si el PSC presta el servicio de CRL y El PSC no elimina de la CRL los certificados revocados después de que hayan expirado, la CRL deberá incluir la extensión X.509 “ExpiredCertsOnCRL” como se define en ISO/IEC 9594-8/Recomendación UIT-T X.509.

c) La terminación de una CRL puede ocurrir cuando no hay más certificados validos en el alcance de la CRL y, por ejemplo, cuando el certificado de la entidad firmante de la CRL expire o cuando la clave privada de la entidad firmante de la CRL se desactive (ver CSS-6.3.10-07 [Nota 3]; ETSI 319 411-2 V2.4.1)

d) El PSC debe preservar la integridad y disponibilidad de la última CRL al menos durante el periodo especificado en la DPC (ver CSS-6.3.10-08; ETSI 319 411-2 V2.4.1).

e) El Ente Rector establece los formatos para la conservación a largo plazo de datos firmados (ver CSS-6.3.10-08 [Nota 4]; ETSI 319 411-2 V2.4.1).

2.1.5. Aplica (2.1.5) del documento “Requisitos Generales de Proveedores de Servicios de Certificación” (ver 4.3; ETSI 319 411-1 V1.3.1).

El PSC además deberá documentar de forma precisa:

a) El periodo durante el cual la información del estado de revocación está disponible (ver CSS-6.3.10-12 (a); ETSI 319 411-2 V2.4.1);

b) Como se proporciona la información del estado de revocación en el caso de que la clave de la Autoridad Certificadora se encuentre expuesta (haya sido comprometida) (ver CSS-6.3.10-12 (b); ETSI 319 411-2 V2.4.1);

c) Como se proporciona la información del estado de revocación en el caso de terminación del PSC (ver CSS-6.3.10-12 (c); ETSI 319 411-2 V2.4.1);

2.1.6. Aplica (2.1.6) del documento “Requisitos Generales de Proveedores de Servicios de Certificación” (ver 4.3; ETSI 319 411-1 V1.3.1).

2.1.7. Aplica (2.1.7) del documento “Requisitos Generales de Proveedores de Servicios de Certificación” (ver 4.3; ETSI 319 411-1 V1.3.1).

Si el PSC brinda el servicio de resguardo de claves para sus usuarios, el PSC deberá garantizar que:

a) la clave privada del usuario se utilizará bajo el control exclusivo del sujeto (ver SPD-6.3.5.03 [QCP-n-qscd]; ETSI 319 411-2 V2.4.1).

b) b) el par de claves del usuario debe utilizarse solo para firmas electrónica (ver SPD-6.3.5.05 [QCP-n-qscd]; ETSI 319 411-2 V2.4.1).