Gobierno de Reconciliación y Unidad Nacional

El Pueblo, Presidente!

MHCP

DIRECCIÓN GENERAL DE TECNOLOGÍA

NORMATIVA DE DISPOSITIVOS SEGUROS DE CREACIÓN DE FIRMA

Managua, agosto del 2021

CONTROL DE REVISIÓN Y ACTUALIZACIÓN (VERSIONES)

Nº	Fecha	Elaborado/ Entrevistado	Revisado	Aprobado	Autorizado
0	Agosto/2021	Daysi Romero Responsable Departamento de Acreditación y Registro	Hans Espinoza Acuña Responsable Dirección Acreditación de Firma Electrónica Yuri Dompe Responsable Departamento de Supervisión e Inspección	Hans Espinoza Acuña Responsable Dirección Acreditación de Firma Electrónica	Jose Diaz Chow Responsable Dirección General de Tecnología (a.i)

ÍNDICE

I. INTRODUCCIÓN

La Dirección General de Tecnología - DGTEC del Ministerio de Hacienda y Crédito Público - MHCP a través de la Dirección Firma Electrónica ha elaborado el presente documento “Normativa de Dispositivos Seguros de Creación de Firma”, a fin de regular y definir los requerimientos que deben de cumplir los dispositivos seguros de creación de firma para ser permitidos en Nicaragua en la generación de Firmas Electrónicas.

II. OBJETIVO

Establecer normativa de requerimientos técnicos y de seguridad de los dispositivos seguros de creación de firma para ser autorizados.

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. 5, inciso 3, Requisitos de Validez de la Firma Electrónica Certificada.
  - Art. 23 Requisitos de los Dispositivos Seguros de Creación 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. 20, inciso V, Para el dispositivo en el cual se entregarán los certificados y datos privados de firma electrónica certificada ofrecidos por el PSC a sus clientes.

IV. GLOSARIO DE TÉRMINOS Y SIGLAS

Los siguientes términos son definidos o complementados en esta normativa:

Algoritmo Criptográfico: Procedimiento computacional bien definido que toma entradas variables, que pueden incluir claves criptográficas, y produce una salida.

Dispositivo de Creación de Firma: Es un software o hardware que ha sido configurado para crear firma electrónica.

Dispositivo Seguro de Creación de Firma: Es un dispositivo de creación de firma que cumple con los requerimientos de la presente normativa.

Límite Criptográfico: Perímetro continúo definido explícitamente que establece los límites físicos y/o lógicos de un módulo criptográfico y contiene todos los componentes de hardware, software y/o firmware de un módulo criptográfico.

Módulo Criptográfico: Conjunto de hardware, software y/o firmware que implementa funciones de seguridad y está contenido dentro del límite criptográfico.

El siguiente término se encuentra definido en la Ley No.729 Ley de Firma Electrónica:

Dispositivos de Creación de Firma: Es un mecanismo que sirve para aplicar los datos de creación de firma.

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

CC: Common Criteria - Common Criteria for Information Technology Security Evaluation - Criterios comunes para la evaluación de la seguridad de la tecnología de la información.

EAL: Common Criteria Evaluation Assurance Level- Nivel de garantía de evaluación de criterios comunes.

ECDSA: Elliptic Curve Digital Signature Algorithm – Algoritmo de Firma Digital de Curva Elíptica.

FIPS: Federal Information Processing Standard - Estándares Federales de Procesamiento de la Información.

IEC: International Electrotechnical Commission - Comisión Electrotécnica Internacional.

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

IT: Information Technology-Tecnología de la Información.

NIST: National Institute of Standards and Technology - Instituto Nacional de Estándares y Tecnología.

RSA: Algoritmo Criptográfico Rivest, Shamir y Adleman.

SHA: Secure Hash Algorithm - Algoritmo Hash Seguro.

V. NORMATIVAS DE REQUERIMIENTOS TÉCNICOS

1. Módulo criptográfico de tipo hardware

Los dispositivos seguros de creación de firma de las personas firmantes deberán cumplir en su módulo criptográfico con una certificación activa de al menos uno de los siguientes estándares:

- FIPS 140-2[1] de nivel 3 o superior.
- FIPS 140-3 de nivel 3 o superior.
- ISO/IEC 19790:2012 “Information technology - Security Techniques - Security Requirements for Cryptographic Modules” (Tecnología de la información - Técnicas de Seguridad - Requisitos de Seguridad para Módulos Criptográficos), con nivel de seguridad 3 o superior.

[1] A partir del 22 de septiembre del 2026 todas las certificaciones vigentes basadas en FIPS 140-2 pasarán a formar parte del listado histórico del Programa de Validación de Módulos Criptográficos (CMVP), según el National Institute of Standards and Technology (NIST), por lo que no serán reconocidas por esta Entidad Rectora.

- Common Criteria EAL4 o superior en Perfiles de Protección para Dispositivos Seguros de Creación de Firma.

- ISO/IEC 15408 “Information technology - Security Techniques - Evaluation Criteria for IT Security” - "Tecnología de la información - (Técnicas de seguridad - Criterios de evaluación para la seguridad de TI), con EAL4 o superior en Perfiles de Protección para Dispositivos Seguros de Creación de Firma.

Los dispositivos seguros de creación de firma utilizados por los Proveedores de Servicios de Certificación deberán cumplir en su módulo criptográfico una certificación activa de al menos uno de los siguientes estándares:

- FIPS 140-2 de nivel 3 o superior.

- FIPS 140-3 de nivel 3 o superior.

- Common Criteria EAL4 o superior en perfiles de protección para módulos criptográficos de Proveedores de Servicios de Confianza.

a. Compatibilidad de módulos criptográficos tipo hardware

Los dispositivos seguros de creación de firma basados en Hardware para las personas firmantes deberán ser compatibles y operar con los siguientes sistemas operativos:

- Microsoft Window 7 o superior.

- MacOS 10.9 o superior.

- Linux Ubuntu 16.04 LTS o superior.

Los dispositivos seguros de creación de firma basados en hardware para las personas firmantes podrán ser compatibles con los siguientes navegadores web:

- Google Chrome 43 o superior.

- Microsoft IE/Edge 11 o Superior.

- Mozilla Firefox 32 o superior.

- Safari 9 o superior.

2. Modulo criptográfico de tipo software

Los dispositivos seguros de creación de firma basados en software estarán limitados a certificados cuya vigencia no sea mayor a un año.

Los dispositivos seguros de creación de firma de las personas firmantes deberán cumplir en su módulo criptográfico una certificación activa de al menos uno de los siguientes estándares:

- FIPS 140-2 de nivel 1 o superior.

- FIPS 140-3 de nivel 1 o superior.

- ISO/IEC 19790:2012 “Information technology - Security Techniques - Security Requirements for Cryptographic Modules” con nivel de seguridad 1 o superior.

- Common Criteria en Perfiles de Protección para Dispositivos Seguros de Creación de Firma o para propósitos generales de sistemas operativos.

- ISO/IEC 15408 “Information technology - Security Techniques - Evaluation Criteria for IT Security”. en Perfiles de Protección para Dispositivos Seguros de Creación de Firma o para propósitos generales de sistemas operativos.

3. Medios remotos

Cuando se utilice un dispositivo seguro de creación de firma de forma remota, mediante un servidor de firma centralizada por parte del Proveedor de Servicios de Certificación deberá cumplir con lo estipulado en el numeral 1, garantizando el control exclusivo al firmante.

Los certificados que contengan únicamente podrán tener una vigencia menor o igual a un año.

4. Algoritmos criptográficos

Los dispositivos seguros de creación de firma deberán soportar al menos los siguientes algoritmos criptográficos:

- Elliptic Curve Digital Signature Algorithm (ECDSA) - Algoritmo de Firma Digital de Curva Elíptica.

- RSA Algorithm.

Requerimientos mínimos para los algoritmos criptográficos de uso en dispositivos seguros de creación de firma de las personas firmantes.

Algoritmo de Cifrado	Tamaño de Clave de Cifrado	Algoritmo de Hash	Algoritmo de Firma Resultante
ECDSA	Curvas P-256	SHA-256	ECDSAP256SHA256
RSA	2048 bits	SHA-256	RSA_SHA-256

Requerimientos mínimos para los algoritmos criptográficos de uso en dispositivos seguros de creación de firma por Proveedores de Servicios de Certificación.

Algoritmo de Cifrado	Tamaño de Clave de Cifrado	Algoritmo de Hash	Algoritmo de Firma Resultante
ECDSA	Curvas P-384	SHA-384	ECDSAP384SHA384
RSA	4096 bits	SHA-512	RSA_SHA-512

5. Soportes de cumplimiento de los dispositivos seguros de creación de firma

El Proveedor de Servicios de Certificación deberá garantizar el cumplimiento de los requerimientos establecidos en los puntos 1, 2 y 3, mediante la entrega a la entidad rectora de firma electrónica de los siguientes soportes:

- La certificación correspondiente del módulo criptográfico.

- La documentación técnica (incluyendo su política de seguridad) del dispositivo seguro de creación de firma emitido por el fabricante, con su copia en español en caso de estar en otro idioma.

- La guía de usuario del dispositivo seguro de creación de firma (en español).

Adicionalmente según sea el caso, el Proveedor de Servicios de Certificación deberá garantizar la entrega de los siguientes soportes cuando se trate de:

a. Dispositivo seguro de creación de firma para personas firmantes

- Todo software o driver cuando sea necesario para garantizar la compatibilidad del dispositivo seguro de creación de firma.

- Informe de compatibilidad del dispositivo seguro de creación de firma (Pruebas realizadas por el Proveedor de Servicios de Certificación demostrando la compatibilidad del dispositivo seguro de creación de firma según el numeral 1 inciso a “Compatibilidad de módulos criptográficos tipo hardware”).

b. Dispositivo seguro de creación de firma para personas firmantes y basado en modulo criptográfico de tipo hardware

- Un (01) dispositivo seguro de creación de firma, objeto de la certificación correspondiente.

c. Otros dispositivos seguros de creación de firma

- Informe de revisión en el sitio del o los dispositivos seguros de creación de firma utilizados por el Proveedor de Servicios de Certificación.