Gobierno de Reconciliación y Unidad Nacional

El Pueblo, Presidente!

MHCP

DIRECCIÓN GENERAL DE TECNOLOGÍA

REQUISITOS GENERALES DE PROVEEDORES DE SERVICIOS DE CERTIFICACIÓN

Managua, abril del 2022

CONTROL DE REVISIÓN Y ACTUALIZACIÓN (VERSIONES)

Nº	Fecha	Elaborado/ Entrevistado	Revisado	Aprobado	Autorizado
0	Abril / 2022	Yuri Dompe Responsable Departamento de Supervisión e Inspección	Hans Espinoza Responsable Dirección Firma Electrónica Daysi Romero Responsable Departamento de Acreditación y Registro	Hans Espinoza Responsable Dirección Firma Electrónica	Jose Diaz Responsable Dirección General de Tecnología (a.i)

MINISTERIO DE HACIENDA Y CRÉDITO PÚBLICO
DGTEC-MHCP
DIRECCIÓN GENERAL

INDICE

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 generales de Proveedores de Servicios de Certificación", a fin de estandarizar la operación y funcionamiento de los Proveedores de Servicios de Certificación interesados en ofrecer servicios de firma electrónica certificada, estampado cronológico (sellos de tiempo), archivo confiable de mensaje de datos (conservación de documentos electrónicos) u otros servicios como parte de su cartera de servicios en el territorio nacional.

II. OBJETIVO

Armonizar los requisitos generales (criterios) que debe cumplir todo Proveedor de Servicios de Certificación - PSC con los estándares internacionales más comúnmente aceptados, como parte de los requerimientos para poder ser autorizados y operar en Nicaragua.

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:

Acreditación: Es el acto administrativo mediante el cual el Ente Rector de Firma Electrónica (Dirección General de Tecnología - DGTEC) autoriza a un Proveedor de Servicios de Certificación - PSC a operar y prestar sus servicios al público en general, este acto administrativo es emitido a través de una resolución administrativa.

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 - Dirección General de Tecnología y otras relacionadas (NTN).

Política de Seguridad: Es un documento que debe elaborar el Proveedor de Servicios de Certificación - PSC, basado 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".

Roles de acceso: Son los privilegios de acceso que se le asignan a una persona para poder acceder a una aplicación, o a un sistema, o a una red, o a un área física delimitada. Estos privilegios de acceso deben delimitar claramente que es lo que puede o no puede hacer la persona en esa aplicación, sistema, red o área física.

Servicio de registro: Verifica la identidad y, si corresponde, cualquier atributo específico de un sujeto. Los resultados de este servicio se pasan al servicio de generación de certificados.

Servicio de generación de certificados: Crea y firma certificados basados en la identidad y otros atributos verificados por el servicio de registro. Esto puede incluir la generación de claves.

Servicio de difusión: Distribuye certificados a los sujetos y, si el sujeto da su consentimiento, los pone a disposición de las partes que confían. Este servicio también pone a disposición de los suscriptores y partes que confían los términos y condiciones del Proveedor de Servicios de Certificación - PSC, y cualquier información sobre prácticas y políticas publicadas.

Servicio de gestión de revocaciones: Procesa las solicitudes e informes relativos a la revocación para determinar las medidas necesarias a tomar. Los resultados de este servicio se distribuyen a través del servicio de estado de revocación.

Servicio de estado de revocación: Proporciona información sobre el estado de revocación del certificado a las partes que confían.

Servicio de provisión de dispositivos al sujeto: Prepara y proporciona o pone a disposición de los sujetos dispositivos criptográficos seguros u otros dispositivos seguros.

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

AC: Autoridad de Certificación.

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

DPC: Declaración de Prácticas de Certificación (o Prácticas de Certificación o Prácticas del servicio de Certificación o Prácticas del Proveedor de Servicios de Certificación - PSC). Es un documento que debe elaborar el Proveedor de Servicios de Certificación - 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 Normas de Telecomunicaciones.

ICP: Infraestructura de Clave Pública - Es una infraestructura capaz de soportar la gestión de Claves Públicas, capaces de soportar servicios de autenticación, cifrado, integridad y no repudio.

IEC: International Electrotechnical Commission - Comisión Electrotécnica Internacional.

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

INCP: Infraestructura Nicaragüense de Clave Pública.

IP: Protocolo 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.

OID: Identificadores de Objeto.

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.

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.

TI: Tecnología de la Información.

UTC: Coordinated Universal Time, o Tiempo Universal Coordinado es el principal estándar de tiempo por el cual el mundo regula los relojes y el tiempo.

V. EQUIVALENCIA NORMATIVA ACEPTADA

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

1. Web trust for Certification Authorities (Version 2.2.1).

2. ETSI 319 411-1 V1.3.1 (2021-05) Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements.

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 GENERALES

1. Documentación aplicable a los Servicios de Certificación

1.1 Declaración de Prácticas de Certificación

1.1.1. El Proveedor de Servicio de Certificación - PSC debe estructurar su Declaración de Prácticas de Certificación - DPC de acuerdo con la IETF RFC 3647.

1.1.2. El Proveedor de Servicios de Certificación - PSC debe garantizar que su Declaración de Prácticas de Certificación - DPC y demás documentos de guía y control operacional propios están armonizados con el “Marco Normativo de Firma Electrónica” vigente para Nicaragua.

1.1.3. El Proveedor de Servicios de Certificación - PSC debe especificar el conjunto de políticas y prácticas apropiadas para los servicios de certificación que oferte al público.

1.1.4. El conjunto de políticas y prácticas debe ser aprobado por la gerencia, publicado y comunicado tanto a los empleados, suscriptores y terceros que confían según corresponda.

1.1.5. La Declaración de Prácticas de Certificación debe identificar las obligaciones de todas las organizaciones que respaldan los servicios del PSC, incluidas las políticas y prácticas aplicables.

1.1.6. El Proveedor de Servicios de Certificación - PSC no necesita revelar ningún aspecto que contenga información sensible en la documentación que se realice.

1.1.7. La Gerencia del Proveedor de Servicios de Certificación - PSC tendrá la responsabilidad de implementar la Declaración de Prácticas de Certificación - DPC.

1.1.8. El Proveedor de Servicios de Certificación - PSC debe definir un proceso de revisión de las prácticas, incluidas las responsabilidades del personal encargado de mantener actualizada la Declaración de Prácticas de Certificación - DPC.

1.1.9. Cuando el Proveedor de Servicios de Certificación - PSC realice cambios en su Declaración de Prácticas de Certificación - DPC que pudiesen afectar la aceptación del servicio por parte del suscriptor o terceros que confían, este debe notificar debidamente los cambios a los suscriptores y terceros que confían.

1.1.10. El Proveedor de Servicios de Certificación - PSC debe indicar en su Declaración de Prácticas de Certificación - DPC las disposiciones establecidas para la terminación del servicio.

1.2 Política de Certificados

1.2.1. El Proveedor de Servicios de Certificación - PSC debe estructurar su Política de Certificados - PC de acuerdo con el Internet Engineering Task Force - IETF RFC 3647.

1.2.2. El Proveedor de Servicios de Certificación - PSC debe armonizar su Política de Certificados - PC con los requisitos aplicables a la Política de Certificación Normalizada Extendida (NCP+) - (Ver ETSI EN 319 411-1 V1.3.1).

1.3 Términos y Condiciones del Proveedor de Servicios de Certificación - PSC.

1.3.1 El Proveedor de Servicios de Certificación - PSC pondrá a disposición de todos los suscriptores y terceros que confían los términos y condiciones de sus servicios.

1.3.2 Los términos y condiciones deben especificar por lo menos para cada política de servicio de certificación respaldada por el Proveedor de Servicios de Certificación - PSC lo siguiente:

1.3.2.1 La Declaración de Prácticas de Certificación - DPC que se está aplicando.

1.3.2.2 Cualquier limitación en el uso del servicio proporcionado, incluida la limitación por daños que surjan del uso de servicios que excedan dichas limitaciones. (Ej.: el tiempo de vida esperado de los certificados de clave pública).

1.3.2.3 Las obligaciones del suscriptor, si las hubiere.

1.3.2.4 Información para las partes que confían en el servicio de certificación. (Ej: Información sobre como verificar la validez del certificado).

1.3.2.5 El periodo de tiempo durante el cual se retienen los registros de eventos del Proveedor de Servicios de Certificación – PSC.

1.3.2.6 Limitaciones de responsabilidad.

1.3.2.7 El ordenamiento jurídico Nicaragüense.

1.3.2.8 Procedimientos de quejas y solución de controversias.

1.3.2.9 Si se ha evaluado que el servicio de certificación del Proveedor de Servicios de Certificación - PSC cumple con la política de servicio de certificación y, de ser así, a través de qué esquema de evaluación de la conformidad.

1.3.2.10 La información de contacto del Proveedor de Servicios de Certificación – PSC.

1.3.2.11 Cualquier compromiso en materia de disponibilidad.

1.3.3 Los suscriptores de los servicios del Proveedor de Servicios de Certificación - PSC, así como las partes que confían en los mismos deben de ser informados de los términos y condiciones precisos, antes de iniciar una relación contractual.

1.3.4 Los términos y condiciones deben de estar disponibles a través de un medio de comunicación duradero.

1.3.5 Los términos y condiciones deben de estar disponibles en un lenguaje fácilmente comprensible.

1.3.6 Los términos y condiciones podrán ser transmitidos electrónicamente.

1.4 Nombre e identificación de la Declaración de Práctica de Certificación - DPC y de la Política de Certificados del Proveedor de Servicios de Certificación - PSC

El nombre y la identificación de la Declaración de Práctica de Certificación - DPC y Política de Certificados - PC se realizará de conformidad a lo establecido en la "Guía de Administración de los Identificadores de Objeto en Nicaragua":

1.4.1 Declaración de Prácticas de Certificación:
{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 Política de Certificación:
{join-iso-itu-t(2) country(16) ni(558) incp(0) ac-privadas(1) ac-de-"acrónimo del psc" (1) pc(2) [desde (1) hasta (n)]}.

2. Servicios de certificación prestados por el Proveedor de Servicios de Certificación

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

2.1.1. Servicio de Registro.

2.1.2. Servicio de Generación de Certificados.

2.1.3. Servicio de Difusión.

2.1.4. Servicio de Gestión de Revocaciones.

2.1.5. Servicio de Estado de Revocaciones.

2.1.6. Servicio de provisión de dispositivos al sujeto.

2.1.7. Otros Servicios

3. Política de Seguridad de la Información

3.1. El Proveedor de Servicios de Certificación - PSC debe definir una política de seguridad de la información que será aprobada por la gerencia y que establezca el enfoque de la organización para administrar su seguridad de la información.

3.2. El Proveedor de Servicios de Certificación - PSC debe elaborar la política de seguridad de la Información que cumpla con la Norma Técnica Nicaragüense - NTN 21 001-13 o su equivalente superior más actualizada (ISO/IEC 27001 – Objetivo de Control 5 "Políticas de Seguridad de la Información).

3.3. El Proveedor de Servicios de Certificación - PSC debe asegurarse de que la Política de Seguridad de la Información este armonizada con el Marco Normativo de Firma Electrónica vigente para Nicaragua.

3.4. Los cambios a la política de seguridad de la información deben ser comunicados a terceros, cuando corresponda. Esto incluye suscriptores, partes que confían, organismos de evaluación, organismos de supervisión u organismos reguladores (Ente Rector).

3.5. La política de seguridad de la información de un Proveedor de Servicios de Certificación - PSC debe documentarse, implementarse y mantenerse actualizada; incluidos los controles de seguridad y los procedimientos operativos para las instalaciones, los sistemas y los activos de información del Proveedor de Servicios de Certificación - PSC que brindan los servicios.

3.6. El Proveedor de Servicios de Certificación - PSC debe publicar y comunicar la política de seguridad de la información a todos los empleados que son afectados por ella.

3.7. El Proveedor de Servicios de Certificación - PSC conservará la responsabilidad general por el cumplimiento de los procedimientos pre-escritos en su política de seguridad de la información, incluso cuando la funcionalidad del Proveedor de Servicios de Certificación - PSC esté a cargo de subcontratistas.

3.8. El Proveedor de Servicios de Certificación - PSC debe definir la responsabilidad de los subcontratistas y garantizar que los subcontratistas estén obligados a implementar cualquier control que sea exigido por el Proveedor de Servicios de Certificación - PSC, organismos de evaluación, organismos de supervisión u organismos reguladores (Ente Rector).

3.9. El Proveedor de Servicios de Certificación - PSC debe actualizar la política de seguridad de la información, así como el inventario de activos para la seguridad de la información, tanto a intervalos planificados, como cada vez que se produzcan cambios significativos que pudiesen alterar la idoneidad, adecuación y eficacia continua de la misma.

3.10. La configuración de los sistemas del Proveedor de Servicios de Certificación - PSC se revisará periódicamente para detectar cambios que violen las políticas de seguridad de la información del Proveedor de Servicios de Certificación - PSC.

3.11. El intervalo máximo entre dos verificaciones debe documentarse en la Declaración de Prácticas de Certificación - DPC del Proveedor de Servicios de Certificación - PSC.

4. Organización Interna

4.1 La estructura organizativa del Proveedor de Servicios de Certificación - PSC debe ser confiable.

4.1.1 Las prácticas del servicio de certificación bajo las cuales opera el Proveedor de Servicios de Certificación - PSC no serán discriminatorias.

4.1.2 El Proveedor de Servicios de Certificación - PSC debe hacer que sus servicios sean accesibles para todos los solicitantes cuyas actividades se encuentren en su campo de operación declarado y que acuerden cumplir con sus obligaciones según lo especificado en los términos y condiciones del Proveedor de Servicios de Certificación - PSC.

4.1.3 El Proveedor de Servicios de Certificación - PSC debe mantener suficientes recursos financieros y contratar un seguro de responsabilidad civil apropiado para cubrir las responsabilidades que surjan de sus operaciones y/o actividades.

4.1.4 El Proveedor de Servicios de Certificación - PSC debe contar con la estabilidad financiera y los recursos necesarios para operar de conformidad con esta política.

4.1.5 El Proveedor de Servicios de Certificación - PSC debe contar con políticas y procedimientos para la resolución de quejas y disputas recibidas de los clientes u otras partes que confían, sobre la prestación de los servicios o cualquier otro asunto relacionado.

4.1.6 El Proveedor de Servicios de Certificación - PSC debe tener (un) acuerdo(s) documentado(s) y contrato(s) vigente(s) cuando el Proveedor de Servicios de Certificación - PSC subcontrate o tercerice la provisión de servicios con terceros.

4.2 Segregación de funciones:

4.2.1 El Proveedor de Servicios de Certificación - PSC debe definir, asignar y fijar los límites de las autoridades y segregación de las funciones y responsabilidades.

4.2.2 El Proveedor de Servicios de Certificación - PSC debe segregar claramente todas las actividades de registro, aprobación y aprobación de transacciones en las políticas y procedimientos.

5. Recursos Humanos

5.1 El Proveedor de Servicios de Certificación - PSC se asegurará que los empleados y contratistas respalden la confiabilidad de las operaciones del PSC.

5.2 El Proveedor de Servicios de Certificación - PSC debe emplear personal y, cuando sea el caso, subcontratistas, que cuenten con los conocimientos, confiabilidad, experiencia y calificación necesarios para desempeñar las funciones para las que fueron contratados.

5.3 El Proveedor de Servicios de Certificación - PSC debe garantizar que el personal empleado o subcontratado sea capacitado mediante actualizaciones periódicas (al menos cada 12 meses) sobre nuevas amenazas y prácticas de seguridad.

5.4 Las funciones y responsabilidades de seguridad, como se especifica en la política de seguridad del Proveedor de Servicios de Certificación - PSC, deben ser documentadas en descripciones de trabajo o en documentos disponibles para todo el personal involucrado.

5.5 Los roles de acceso tanto a los sistemas, como a la información física o a las áreas físicas, de los cuales depende la seguridad operacional del Proveedor de Servicios de Certificación - PSC, deben ser claramente identificados.

5.6 El personal del Proveedor de Servicios de Certificación - PSC (tanto permanente como temporal) debe tener descripciones de trabajo definidas desde el punto de vista de los roles cumplidos con segregación de funciones y privilegios mínimos, determinando la sensibilidad de la posición con base en las funciones y niveles de acceso, verificación de antecedentes y capacitación de empleados.

5.7 El personal gerencial del Proveedor de Servicios de Certificación - PSC debe poseer experiencia o capacitación con respecto a los servicios que se brindan, debe estar familiarizado con los procedimientos de seguridad para el personal con responsabilidades de seguridad; y experiencia en seguridad de la información y evaluación de riesgos suficiente para desempeñar funciones gerenciales.

5.8 Todo el personal del Proveedor de Servicios de Certificación - PSC en roles de acceso debe estar libre de conflicto de intereses que pueda perjudicar la imparcialidad de las operaciones del Proveedor de Servicios de Certificación - PSC, así como no tener vínculos de consanguinidad (en segundo grado) o de afinidad (convivencia) con los otros miembros del personal del Proveedor de Servicios de Certificación - PSC o del Ente Rector con los que tiene que interactuar en la ejecución de sus funciones (en base a la segregación de descritas en 4.2.1 y 4.2.2); así mismo

debe presentar constancia de no encontrarse incurso en procesos de interdicción judicial y tener un record policial limpio actualizado. La información soporte debe ser actualizada cada 12 meses.

5.9 Los roles de acceso deben incluir roles que involucren las siguientes responsabilidades:

5.9.1 Oficiales de seguridad: Con la responsabilidad general de administrar la implementación de las prácticas de seguridad.

5.9.2 Administradores de sistemas: Autorizados para instalar, configurar y mantener los sistemas confiables del Proveedor de Servicios de Certificación - PSC para la administración del servicio.

5.9.3 Operadores de Sistemas: Responsables de operar los sistemas confiables del Proveedor de Servicios de Certificación - PSC en el día a día. Autorizado para realizar copias de seguridad de los Sistemas.

5.9.4 Auditores de sistemas: Autorizados para consultar archivos y registros de auditoria de los sistemas confiables del Proveedor de Servicios de Certificación - PSC, Así como para realizar pruebas de identificación de vulnerabilidades en la seguridad de los sistemas.

5.10 Al personal del Proveedor de Servicios de Certificación - PSC se le deben designar formalmente las funciones que debe realizar, por parte de la Gerencia que es responsable de la seguridad.

5.11 El personal designado debe aceptar formalmente los roles de acceso asignados para realizar sus funciones.

5.12 El personal no tendrá acceso a las funciones establecidas en los roles de acceso hasta que se completen las verificaciones que sean necesarias (ver 5.8).

6. Gestión de Activos

6.1 El Proveedor de Servicios de Certificación - PSC debe establecer controles adecuados protección de sus activos (tanto activos físicos, como activos de información).

6.2 El Proveedor de Servicios de Certificación - PSC debe mantener un inventario de todos los activos de información y debe designar una clasificación de riesgos para cada uno consistente con la evaluación de riesgos.

6.3 Los medios de uso diario o periódico que sirvan para procesar, almacenar o trasportar cualquier activo de información del Proveedor de Servicios de Certificación - PSC o de los suscriptores de sus servicios deben ser protegidos contra daños (o deterioros), robos, accesos no autorizados y obsolescencia de los mismos.

6.4 El Proveedor de Servicios de Certificación - PSC debe establecer procedimientos de gestión de medios que protejan contra la obsolescencia y el deterioro de los medios dentro del período, que, por normativa del Ente Rector, se regule el período de conservación de los registros.

6.5 El Proveedor de Servicios de Certificación - PSC debe establecer procedimientos de eliminación segura de medios y de limpiado previo de los activos de información contenidos en los mismos, cuando estos sean dados de baja de los inventarios del Proveedor de Servicios de Certificación - PSC.

7. Control de acceso

7.1 Los accesos a cualquiera de los sistemas del Proveedor de Servicios de Certificación - PSC estarán restringidos únicamente a personas previamente autorizadas ya sea por el Proveedor de Servicios de Certificación - PSC o el Ente Rector.

7.2 El Proveedor de Servicios de Certificación - PSC debe administrar el acceso de los usuarios, de los operadores, de los administradores y de los auditores de los sistemas, aplicando el principio de “privilegios mínimos” al realizar la configuración inicial de los privilegios de acceso.

7.3 El Proveedor de Servicios de Certificación - PSC debe incluir la gestión de las cuentas de usuarios, así como la modificación o eliminación oportuna de acceso a las mismas.

7.4 Los sistemas del Proveedor de Servicios de Certificación - PSC deben proporcionar suficientes controles de seguridad informática para garantizar la segregación de funciones identificadas en las practicas del Proveedor de Servicios de Certificación - PSC, incluyendo la separación de las funciones de administración y operación de seguridad de la información.

7.5 El personal del Proveedor de Servicios de Certificación - PSC debe ser identificado y autenticado antes de utilizar aplicaciones/sistemas críticos relacionados con el servicio.

7.6 El Proveedor de Servicios de Certificación - PSC debe garantizar que el registro de eventos (pistas de auditoría) de todos los sistemas se mantenga activo en todo momento, así como se realice el resguardo y almacenamiento de dichos registros por el tiempo que sea establecido por el Ente Rector.

7.7 El Proveedor de Servicios de Certificación - PSC debe establecer procedimientos para garantizar que los datos confidenciales sean debidamente protegidos de conformidad con la Ley de Protección de Datos Personales (Ley 787) y su Reglamento (Decreto No. 36-2012).

8. Controles Criptográficos

8.1 El Proveedor de Servicios de Certificación - PSC debe establecer controles criptográficos apropiados para la gestión de cualquier clave criptográfica y cualquier dispositivo criptográfico (aprobado por el Ente Rector) a lo largo de su ciclo de vida.

9. Seguridad Física y Ambiental

9.1 El Proveedor de Servicios de Certificación - PSC debe controlar el acceso físico a los componentes de los Sistemas y/o Infraestructura del Proveedor de Servicios de Certificación - PSC, cuya seguridad es crítica para la prestación de sus servicios de certificación y así minimizar los riesgos relacionados con la seguridad física.

9.2 El acceso físico a cualquiera de los componentes de los Sistemas y/o Infraestructura del Proveedor de Servicios de Certificación - PSC, estará limitada a personal debidamente autorizado, ya sea por el Proveedor de Servicios de Certificación - PSC o por el Ente Rector.

9.3 El Proveedor de Servicios de Certificación - PSC implementará controles para evitar la pérdida, daño o exposición de activos e interrupción de las actividades del negocio.

9.4 El Proveedor de Servicios de Certificación - PSC implementará controles para evitar la exposición o robo de información de las instalaciones de procesamiento.

9.5 Los componentes críticos para la operación segura de los Sistemas y/o Infraestructura del Proveedor de Servicios de Certificación - PSC, deben estar ubicados en un perímetro de seguridad protegido contra intrusión, con controles de acceso en los distintos niveles del perímetro de seguridad y alarmas para detección de intrusos y contra incendios.

10. Seguridad de la operación

10.1 El Proveedor de Servicios de Certificación - PSC debe utilizar sistemas y productos confiables, protegidos contra modificaciones, a fin de garantizar la seguridad técnica y confiabilidad de los procesos soportados por ellos.

10.2 El Proveedor de Servicios de Certificación - PSC debe realizar un análisis de los requisitos de seguridad en la etapa de diseño y especificación de requisitos, de cualquier proyecto de desarrollo de sistemas realizado por el Proveedor de Servicios de Certificación - PSC o en nombre del Proveedor de Servicios de Certificación - PSC para garantizar que la seguridad esté integrada en los Sistemas de Tecnología de la Información - TI.

10.3 El Proveedor de Servicios de Certificación - PSC debe aplicar procedimientos de control de cambios para lanzamientos, modificaciones y arreglos de software de emergencia de cualquier software operativo y cambios en la configuración que aplica la política de seguridad del Proveedor de Servicios de Certificación - PSC.

10.4 Los procedimientos deben incluir la documentación de los cambios.

10.5 La integridad de los Sistemas y la Información del Proveedor de Servicios de Certificación - PSC deben estar protegidas contra virus, software malicioso y software no autorizado.

10.6 El Proveedor de Servicios de Certificación - PSC debe establecer e implementar procedimientos para todos los roles de acceso que tengan un impacto en la prestación de servicios.

10.7 El Proveedor de Servicios de Certificación - PSC debe documentar las razones por las que no se aplican parches de seguridad.

11. Seguridad de la red

11.1 El Proveedor de Servicios de Certificación - PSC debe proteger su red y sus sistemas de ataques.

11.2 El Proveedor de Servicios de Certificación - PSC debe segmentar sus sistemas en redes o zonas con base en la evaluación de riesgos considerando la relación funcional, lógica y física (incluida la ubicación) entre los sistemas y servicios confiables.

11.3 El Proveedor de Servicios de Certificación - PSC debe aplicar los mismos controles de seguridad a todos los sistemas co-ubicados en la misma zona.

11.4 El Proveedor de Servicios de Certificación - PSC debe restringir el acceso y las comunicaciones entre zonas a aquellas necesarias para la operación del Proveedor de Servicios de Certificación - PSC.

11.5 El Proveedor de Servicios de Certificación - PSC prohibirá o desactivará explícitamente las conexiones y servicios innecesarios.

11.6 El Proveedor de Servicios de Certificación - PSC debe revisar periódicamente el conjunto de reglas establecidas.

11.7 El Proveedor de Servicios de Certificación - PSC debe mantener todos los sistemas que son críticos para la operación del Proveedor de Servicios de Certificación - PSC en una o más zonas seguras. (Ej.: Sistemas de AC Raíz).

11.8 El Proveedor de Servicios de Certificación - PSC debe separar la red dedicada para la administración de los Sistemas de Tecnología de la Información - TI y la red operativa del Proveedor de Servicios de Certificación - PSC.

11.9 El Proveedor de Servicios de Certificación - PSC no utilizará los sistemas para la administración de la implementación de la política de seguridad en otros fines.

11.10 El Proveedor de Servicios de Certificación - PSC debe separar los sistemas de producción para los servicios del Proveedor de Servicios de Certificación - PSC de los sistemas utilizados en desarrollo y prueba.

11.11 El Proveedor de Servicios de Certificación - PSC debe establecer la comunicación entre distintos sistemas confiables solo a través de canales confiables que estén aislados mediante separación lógica, criptográfica o física de otros canales de comunicación y proporcionen una identificación segura de sus puntos finales y protección de los datos del canal contra modificación o divulgación.

11.12 Si se requiere un alto nivel de disponibilidad de acceso externo al servicio de certificación, la conexión a la red externa debe ser redundante para garantizar la disponibilidad de los servicios en caso de una sola falla.

11.13 El Proveedor de Servicios de Certificación - PSC debe someterse o realizará un escaneo de vulnerabilidad regular en direcciones IP públicas y privadas identificadas por el Proveedor de Servicios de Certificación - PSC y registrará evidencia de que cada escaneo de vulnerabilidad fue realizado por una auditor o empresa de auditoría con las habilidades, herramientas, competencia, código de ética e independencia necesarios para proporcionar un informe confiable.

11.14 El análisis de vulnerabilidad solicitado por (11.13) debe realizarse cada 3 meses.

11.15 El Proveedor de Servicios de Certificación - PSC debe someterse a una prueba de penetración al momento de la configuración de los sistemas del Proveedor de Servicios de Certificación – PSC y después de las actualizaciones o modificaciones de la infraestructura o la aplicación que el Proveedor de Servicios de Certificación - PSC determine que son significativas.

11.16 La prueba de penetración solicitada en (11.15) debe realizarse al menos cada 12 meses.

11.17 El Proveedor de Servicios de Certificación - PSC debe registrar evidencia de que cada prueba de penetración fue realizada por un auditor o empresa de auditoría con las habilidades, herramientas, competencia, código de ética e independencia necesarios para proporcionar un informe confiable.

11.18 Los controles de Tecnología de la Información - TI implementados (Ej.: Firewalls) deben proteger los dominios de la red interna del Proveedor de Servicios de Certificación - PSC de accesos no autorizados, incluido el acceso de suscriptores y terceros.

11.19 También se deben de configurar Firewalls para evitar todos los protocolos y accesos no requeridos para la operación del Proveedor de Servicios de Certificación - PSC.

12. Administración de incidentes

12.1 Se monitorearán las actividades del sistema relacionadas con el acceso a los sistemas de Tecnología de la Información - TI, el uso de los sistemas de Tecnología de la Información - TI y las solicitudes de servicio.

12.2 Las actividades de monitoreo deben tener en cuenta la sensibilidad de cualquier información recopilada o analizada.

12.3 Las actividades anormales de los sistemas que indiquen una posible violación de la seguridad, incluida la intrusión en la red del Proveedor de Servicios de Certificación - PSC, se detectarán y reportarán como alarmas.

12.4 El Proveedor de Servicios de Certificación - PSC debe monitorear los siguientes eventos:

12.4.1 La puesta en marcha y apagado de las funciones de registro; y

12.4.2 La disponibilidad y utilización de los servicios necesarios con la red del Proveedor de Servicios de Certificación - PSC.

12.5 El Proveedor de Servicios de Certificación - PSC debe actuar de manera oportuna y coordinada para responder rápidamente a los incidentes y limitar el impacto de las brechas de seguridad.

12.6 El Proveedor de Servicios de Certificación - PSC debe designar personal calificado para dar seguimiento a las alertas de seguridad potencialmente críticos y garantizar que los incidentes relevantes se informen de acuerdo con los procedimientos del Proveedor de Servicios de Certificación - PSC.

12.7 El Proveedor de Servicios de Certificación - PSC debe establecer procedimientos para notificar a las partes correspondientes de acuerdo con las normas regulatorias aplicables, cualquier violación de seguridad o perdida de integridad que tenga un impacto significativo en los servicios proporcionados por el PSC y sobre los datos personales mantenidos en el mismo, dentro de las 24 horas posteriores a la identificación de la infracción.

12.8 Cuando haya probabilidades de que la violación de la seguridad o la pérdida de la integridad afecte negativamente a una persona natural o jurídica a la que se le haya prestado alguno de los servicios, el Proveedor de Servicios de Certificación - PSC también notificará a la persona natural o jurídica sobre la violación de la seguridad o la pérdida de la integridad sin demora alguna.

12.9 Los Sistemas del Proveedor de Servicios de Certificación - PSC deben ser monitoreados incluyendo el monitoreo o revisión regular de los registros de auditoría para identificar evidencia de actividad maliciosa implementando mecanismos automáticos para procesar los registros de auditoría y alertar al personal de posibles eventos críticos de seguridad.

12.10 El Proveedor de Servicios de Certificación - PSC debe abordar cualquier vulnerabilidad critica no abordada previamente por el Proveedor de Servicios de Certificación - PSC, dentro de un plazo de 24 horas desde su descubrimiento.

12.11 Para cualquier vulnerabilidad, dado el impacto potencial, el Proveedor de Servicios de Certificación - PSC debe elegir entre:

12.11.1 Crear o implementar un plan para mitigar la vulnerabilidad; o

12.11.2 Documentar la base de hechos para la determinación del Proveedor de Servicios de Certificación - PSC de que la vulnerabilidad no requiere reparación.

12.12 Los procedimientos de notificación y respuesta a incidentes se deben emplear de tal manera que se minimicen los daños por incidentes de seguridad y fallas en el funcionamiento.

13. Recopilación de pruebas

13.1 El Proveedor de Servicios de Certificación - PSC debe registrar y mantener accesible durante un período de tiempo apropiado, incluso después de que hayan cesado las actividades del Proveedor de Servicios de Certificación - PSC, toda la información pertinente relativa a los datos emitidos y recibidos por el Proveedor de Servicios de Certificación - PSC, en particular, con el fin de proporcionar pruebas en procedimientos judiciales y con el fin de garantizar la continuidad del servicio.

13.2 Se mantendrá la confidencialidad e integridad de los registros actuales y archivados relacionados con la operación de los servicios brindados por el Proveedor de Servicios de Certificación - PSC.

13.3 Los registros relacionados con la operación de los servicios se archivarán de manera completa y confidencial de acuerdo con las prácticas comerciales divulgadas.

13.4 Los registros relacionados con la operación de los servicios deben estar disponibles, si se requiere, para los efectos de proporcionar evidencia del correcto funcionamiento de los servicios a efectos de procedimientos judiciales.

13.5 Se registrará la hora precisa de los eventos ambientales, de gestión de claves y de sincronización de relojes significativos del Proveedor de Servicios de Certificación - PSC.

13.6 La hora utilizada para registrar eventos según lo requerido en el registro de auditoría debe sincronizarse con el Coordinated Universal Time - UTC al menos una vez al día.

13.7 Los registros relacionados con los servicios se resguardarán durante un período de tiempo según lo establecido por el Ente Rector, para proporcionar la evidencia legal necesaria y según lo notificado en los términos y condiciones del Proveedor de Servicios de Certificación - PSC.

13.8 Los eventos se registrarán de manera que no puedan borrarse o destruirse fácilmente (excepto si se transfieren de manera confiable a medios a largo plazo) dentro del periodo de tiempo que requiere para que estén resguardados.

14. Gestión de la continuidad del negocio

14.1 El Proveedor de Servicios de Certificación - PSC debe definir y mantener un plan de continuidad para implementar en caso de un desastre.

14.2 En caso de desastre, incluida la exposición de una clave de firma privada o la exposición de alguna otra credencial del Proveedor de Servicios de Certificación - PSC, las operaciones se restablecerán dentro del plazo establecido en el plan de continuidad, habiendo abordado

cualquier causa del desastre que pueda repetirse (Ej.: una vulnerabilidad de seguridad) con las medidas de remediación necesarias.

15. Cierre de Proveedor de Servicios de Certificación - PSC y planes de cierre

15.1 Se minimizarán las interrupciones potenciales para los suscriptores y otras partes relacionadas como resultado del cese de los servicios del Proveedor de Servicios de Certificación - PSC, y en particular, se proporcionará el mantenimiento continuo de la información requerida para verificar la exactitud de los servicios de certificación.

15.2 El Proveedor de Servicios de Certificación - PSC debe contar con un plan de cierre actualizado.

15.3 Antes que el Proveedor de Servicios de Certificación - PSC de por finalizados sus servicios, el Proveedor de Servicios de Certificación - PSC debe informar a las siguientes partes del cierre: Todos los suscriptores y otras entidades con las que el Proveedor de Servicios de Certificación - PSC tiene acuerdos u otra forma de relación establecida, entre las que se encuentran las partes que confían, los Proveedores de Servicios de Certificación - PSC y las autoridades pertinentes como el Ente Rector.

15.4 Antes de que el Proveedor de Servicios de Certificación - PSC de por finalizados sus servicios, el Proveedor de Servicios de Certificación - PSC debe poner la información de la terminación a disposición de las otras partes que confían.

15.5 Antes que el Proveedor de Servicios de Certificación - PSC de por finalizados sus servicios, el Proveedor de Servicios de Certificación - PSC debe rescindir la autorización de todos los subcontratistas para actuar en nombre del Proveedor de Servicios de Certificación - PSC en el desempeño de cualquier función relacionada con el proceso de emisión de tokens de los servicios brindados por el Proveedor de Servicios de Certificación - PSC.

15.6 Antes que el Proveedor de Servicios de Certificación - PSC de por finalizados sus servicios, el Proveedor de Servicios de Certificación - PSC debe transferir las obligaciones a una parte confiable para resguardar toda la información necesaria para proporcionar evidencias de las operaciones del Proveedor de Servicios de Certificación - PSC por el período de tiempo que determine el Ente Rector, a menos que se pueda demostrar que el Proveedor de Servicios de Certificación - PSC no posee tal información.

15.7 Antes que el Proveedor de Servicios de Certificación - PSC de por finalizados sus servicios, las claves privadas del Proveedor de Servicios de Certificación - PSC, incluidas las copias de seguridad, se destruirán o dejarán de utilizarse de tal manera que las claves privadas no puedan recuperarse.

15.8 Antes que el Proveedor de Servicios de Certificación - PSC de por finalizados sus servicios, el Proveedor de Servicios de Certificación - PSC debe hacer arreglos para transferir la provisión de servicios de certificación para sus clientes a otro Proveedor de Servicios de Certificación - PSC, en caso de que esto no sea posible, debe transferirlos al Ente Rector realice las gestiones de intermediación correspondientes.

15.9 El Proveedor de Servicios de Certificación - PSC debe tener un mecanismo de previsión contable o un seguro para cubrir los costos para cumplir con estos requisitos mínimos en caso de que el Proveedor de Servicios de Certificación - PSC quiebre o por cualquier otra razón no pueda cubrir los costos por sí mismo, en la media de lo posible dentro de las limitaciones de las normas aplicables (legislación en materia de quiebras).

15.10 El Proveedor de Servicios de Certificación - PSC debe hacer constar en sus prácticas las disposiciones realizadas para la finalización de sus servicios. Esto debe incluir:

15.10.1 Notificación de las entidades afectadas; y

15.10.2 En su caso, transferir las obligaciones del Proveedor de Servicios de Certificación - PSC a otras partes.

15.11 El Proveedor de Servicios de Certificación - PSC debe mantener o transferir a una parte confiable sus obligaciones de poner a disposición de las partes que confían su clave pública o sus tokens (de los servicios que presta) durante el período que indique el Ente Rector.

16. Cumplimiento Legal

16.1 El Proveedor de Servicios de Certificación - PSC debe proporcionar evidencia de como cumple con los requisitos legales aplicables.

16.2 Los servicios prestados por el Proveedor de Servicios de Certificación - PSC y los productos de usuario final utilizados en la prestación de estos servicios deben ser accesibles para las personas con discapacidad cuando sea posible.

16.3 Se deben tomar las medidas técnicas y organizativas apropiadas contra accesos no autorizados o procesamiento ilegal de datos personales y contra la pérdida o destrucción accidental o daño a los datos personales.

VII. EXCEPCIONES

Cuando un Proveedor de Servicios de Certificación - PSC, únicamente pretenda ofrecer el servicio de “Archivo Confiable de Mensaje de Datos (o Conservación de documentos)” u otro servicio que no involucre ninguno de los “Servicios de Certificación” mencionados en el acápite (2.1.) del Capítulo VI del presente documento se exime al Proveedor de Servicios de Certificación - PSC de la evaluación de cumplimiento de los siguientes acápites del Capítulo V:

1. Documentación aplicable a los Servicios de Certificación, y

2. Servicios de Certificación prestados por el Proveedor de Servicios de Certificación - PSC.