# GUÍA DE ESTÁNDARES TECNOLÓGICOS Y LINEAMIENTOS DE SEGURIDAD PARA LA ACREDITACIÓN Y RENOVACIÓN COMO PROVEEDOR DE SERVICIOS DE CERTIFICACIÓN O CASOS ESPECIALES

## CONTROL DE VERSIONES

| VERSIÓN (EDICIÓN) | MOTIVO DEL CAMBIO | PUBLICACIÓN |
|---|---|---|
| 1 | Creación | Agosto- 2006 |
| 2 | Actualización General (incluido estándares) | Julio- 2007 |
| 2.1 | Actualización General | Abril- 2008 |
| 3 | Actualización General (incluido estándares) | Agosto- 2011 |
| 3.1 | Actualización General (Inclusión de Casos Especiales) | Enero - 2012 |
| 4.0 | Actualización General (inclusión estándares ETSI y CA/BR) | Mayo- 2015 |
| 4.1 | Firma electrónica para garantizar su integridad por las autoridades actuales | Junio 2017 |
| 5.0 | Actualización General (Reemplazo del algoritmo de firma electrónica RSA a Curva Elíptica, longitud de clave pública y actualización de estándares) | Noviembre - 2024 |

**Versión del Documento:** **Noviembre 12, 2024 11:30**

# ÍNDICE

## ELABORACIÓN

### DIRECTORIO

| NOMBRE | CARGO SUSCERTE |
|---|---|
| Gerardo Gómez | Superintendente |
| Juan Carlos Monsalve S | Gerente de Estandarización Acreditación y Fiscalización |
| Kevins Rangel | Gerente de Seguridad Informática |
| Monica Lugo | Consultora Juridica |

### EDICIÓN Y REVISIÓN

Nohely Coronado, Alberto Rodríguez, Andrys Archila, Charlotte Giannotti

## 1. OBJETO Y CAMPO DE APLICACIÓN

El propósito de esta guía es orientar al solicitante acerca de la aplicación de los estándares desarrollados para el análisis de los requisitos tecnológicos, seguridad y confianza que debe cumplir para obtener la acreditación o renovación como PSC o CE de acuerdo a lo establecido en LSMDFE y su Reglamento.

## 2. REFERENCIAS NORMATIVAS

**2.1.** Ley de Infogobierno

**2.2.** Decreto N.º 1.204 con Fuerza de Ley Sobre Mensajes de Datos y Firmas Electrónicas.

**2.3.** Reglamento Parcial de la Ley Sobre Mensajes de Datos y Firmas Electrónicas.

**2.4.** Providencia Administrativa N° 016 “Normas técnicas de la infraestructura nacional de la certificación electrónica”. Gaceta Oficial de la República Bolivariana de Venezuela Nº 38.636 de fecha 2 de marzo de 2007.

**2.5.** Norma SUSCERTE N° 022 “Manual de actualización y aprobación de políticas y prácticas de certificación”.

**2.6.** Norma SUSCERTE N°. 032 “Infraestructura Nacional de Certificación Electrónica: Estructura, Certificados y Lista de Certificados Revocados”.

**2.7.** ISO/IEC 15408:2023 Common Criteria for Information Technology Security Evaluation, Versión 3.

**2.8.** FIPS PUB 140-1:1994 Security Requirements for Cryptographic Modules.

**2.9.** FIPS PUB 140-2:2002 Security Requirements for Cryptographic Modules.

**2.10.** FIPS PUB 140-3:2019 Security Requirements for Cryptographic Modules.

**2.11.** ETSI TS 102 042:2013 Policy requirements for certification authorities issuing public key certificates V2.4.1.

**2.12.** ISO/IEC 9594-8:2020 Information Tecnology – Open Systems Interconnection – The Directory: Public-key and Attribute Certificate Frameworks.

**2.13.** ITU-T Rec. X.509:2008 Tecnología de la información. Interconexión de sistemas abiertos – El directorio – Marco de autenticación.

**2.14.** ITU-T Rec. X.690:2002 / ISO/IEC 8825-1:2008. ASN.1 Basic Encoding Rules

**2.15.** RFC 2559:2002 Boeyen, S. et al. Internet X.509 Public Key Infrastructure.

**2.16.** RFC 3647:2003 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework

**2.17.** CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates v2.0.5 (CA/BR B)

**2.18.** RFC 5280:2008 PKIX Certificate and CRL Profile y sus actualizaciones.

**2.19.** RFC 6818:2013 Updates to the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

**2.20.** ISO/IEC 27001:2022 Tecnología de la Información. Técnicas de Seguridad – Sistema de Gestión de la Seguridad de la Información - Requisitos.

**2.21.** ISO/IEC 27002:2022 Seguridad de la información, ciberseguridad y protección de la privacidad. Controles de seguridad de la información.

**2.22.** RCF 2560 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP.

## 3. DEFINICIONES Y TERMINOLOGÍAS

A los efectos de este código, se establecen las siguientes definiciones y terminologías:

| | |
|---|---|
| **ACREDITACIÓN** | Título que otorga la Superintendencia de Servicios de Certificación Electrónica a los Proveedores de Servicios de Certificación para proporcionar certificados electrónicos, una vez |

| | |
|---|---|
| | cumplidos los requisitos y condiciones establecidos en el Decreto-Ley 1.204. |
| **CAPTCHA** | (Completely Automated Public Turing test to Tell Computers and Humans Apart) (prueba de Turing completamente automática y pública para diferenciar ordenadores de humanos) es una prueba desafío-respuesta controlada por máquinas que son utilizadas para determinar cuándo el usuario es un humano o un programa automático |
| **CASO ESPECIAL** | Son entidades de Certificación excepcionales para Proyectos de Interés Nacional que son acreditados por SUSCERTE. |
| **CERTIFICADO DE VALIDACIÓN EXTENDIDA** | Certificado emitido y administrado en cumplimiento a las políticas de Validación Extendida de la CA/Browser Forum. |
| **CIBERSEGURIDAD** | Es el conjunto de procedimientos y |

herramientas que se implementan para proteger la información que se genera y procesa a través de computadoras, servidores, dispositivos móviles, redes y sistemas electrónicos, de los ataques digitales.

**CLAVE DEL SIGNATARIO**

Conjunto de caracteres alfanuméricos que permite el uso de un certificado electrónico. Esta clave sólo deberá ser conocida por el signatario.

**CLAVE PRIVADA**

Una clave privada es una variable criptográfica que se utiliza para cifrar y descifrar datos. Es una clave matemática que se mantiene en secreto por el titular y que se usa junto con un algoritmo.

**CLAVE PÚBLICA**

Es una clave matemática que tiene disponibilidad pública y que es utilizada por las aplicaciones para verificar las firmas digitales creadas con su correspondiente clave privada.

| | |
|---|---|
| **CURVA ELÍPTICA** | Es una rama de la criptografía de clave pública que se basa en las matemáticas y ofrece una forma segura de realizar operaciones criptográficas, como el intercambio de claves, las firmas digitales y el cifrado |
| **FIREWALLS** | Son sistemas y/o equipos de seguridad de red que restringe el tráfico de Internet entrante y saliente dentro de una red privada o pública. |
| **FUNCIÓN HASH** | Es una función computable mediante un algoritmo, que tiene como entrada un conjunto de elementos, que suelen ser cadenas, y los convierte (mapea) en un rango de salida finito, normalmente cadenas de longitud fija. |
| **HASH** | Es una sucesión alfanumérica (letras y números) de longitud fija, que identifica o representa a un conjunto de datos determinados. |

| | |
|---|---|
| **HONEYPOTS** | Es un mecanismo de ciberseguridad que simula un objetivo de ataque diseñado para alejar a los ciberdelincuentes de los objetivos legítimos y recopilar información sobre su identidad y métodos con el fin último de mejorar la seguridad de las redes. |
| **LISTA DE CERTIFICADOS REVOCADOS** | Documento mantenido y publicado por una Autoridad de Certificación (AC) que enumera los certificados revocados por ella. |
| **MALWARE** | Es cualquier código de software o programa informático, escrito intencionadamente para dañar los sistemas informáticos o a sus usuarios. |
| **PHISHING** | Es una forma de ciberdelincuencia en la que los delincuentes intentan obtener información confidencial de usted a través del correo electrónico con enlaces fraudulentos, incitándole a rellenar un formulario con su información personal |

| | |
|---|---|
| | identificable. |
| **SIGNATARIO** | Entidad identificada en un certificado electrónico, quien usa la clave privada que se encuentra asociada con clave pública del certificado. |
| **SNIFFER** | Es un software o hardware que se utiliza para monitorizar, capturar y analizar en tiempo real los paquetes de datos que pasan por una red, sin redirigirlos ni alterarlos. |
| **SOLICITANTE** | Es la persona jurídica de Derecho Público o Derecho Privado en el ámbito de las TIC para acreditarse como PSC, PSC Acreditado o Caso Especial. |
| **SUPERINTENDENCIA DE SERVICIOS DE CERTIFICACIÓN ELECTRÓNICA** | Superintendencia de Servicios de Certificación Electrónica adscrito a la autoridad<br><br>nacional con competencia en materia de ciencia, tecnología e innovación. |

| | |
|---|---|
| **SUSCRIPTOR** | Persona que contrata la generación de un certificado electrónico con un PSC. |

## 4. SÍMBOLOS Y ABREVIATURAS

A los efectos de esta norma, se establecen los siguientes símbolos y abreviaturas:

| | |
|---|---|
| **AC / CA** | Autoridad de Certificación/Certification Authority |
| **AR / RA** | Autoridad de Registro/Registration Authority |
| **BYOD / TTPD** | Bring your own device / Trae tu Propio Dispositivo |
| **CA/BR B** | CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates v 2.0.5 |
| **CA/BR G** | CA/Browser Forum Guidelines For The Issuance And Management of Extended Validation Certificates v 2.0.1 |
| **CE** | Casos Especiales |
| **DPC / CPS** | Declaración de Prácticas de Certificación/Certification Practices Statement |
| **ECDSA / AFDCE** | Elliptic Curve Digital Signature Algorithm/Algoritmo de Firma Digital de Curva Elíptica |
| **GEAF** | Gerencia de Estandarización Acreditación y Fiscalización |

| | |
|---|---|
| **GSI** | Gerencia de Seguridad Informática |
| **LCE / SQL** | Lenguaje de Consulta Estructurada/Structured Query Language |
| **LCR / CRL** | Lista de Certificados Revocados/Certificate Revocation List |
| **LSMDFE** | Ley Sobre Mensajes de Datos y Firmas Electrónicas. |
| **MSH / HSM** | Módulo de Seguridad de Hardware/Hardware Security Module |
| **OCSP** | On - line Certificate Status Protocol |
| **PC** | Política de Certificados. |
| **PII / IIP** | Personally Identifiable Information / Información de Identificación Personal |
| **PSC** | Proveedor de Servicios de Certificación. |
| **RPLSMDFE** | Reglamento Parcial de Ley Sobre Mensajes de Datos y Firmas Electrónicas. |
| **SGSI** | Sistema de gestión de la seguridad de la información |
| **SUSCERTE** | Superintendencia de Servicios de Certificación Electrónica. |
| **TIC** | Tecnologías de Información y Comunicación |
| **UCP / CPU** | Unidad Central de Procesamiento/Central Processing Unit |

## 5. PROCEDIMIENTO

### 5.1 Principio Básico

La Guía tiene como función principal establecer los estándares tecnológicos y lineamientos de seguridad, que debe cumplir todo solicitante para obtener su acreditación o renovación como PSC o CE ante SUSCERTE.

### 5.2 Consideraciones Generales

**5.2.1** El objetivo de la acreditación o renovación para los PSC o CE es asegurar la existencia de un sistema de certificación de firma electrónica confiable, que garantice su continuidad en el tiempo y que sirva de base para el desarrollo tecnológico del país.

**5.2.2** Como criterios generales de la acreditación o renovación, se tienen:

**5.2.2.1** Los requerimientos del proceso de acreditación o renovación deben garantizar la compatibilidad de la Infraestructura Nacional de Certificación Electrónica con los estándares internacionales, permitiendo así la interoperabilidad entre los sistemas.

**5.2.2.2** Los niveles de exigencia del proceso de acreditación o renovación deben ajustarse a las mejores prácticas y los estándares internacionales.

**5.2.2.3** Se considera fundamental promover el desarrollo tecnológico de los servicios de certificación electrónica, sin preferencia hacia una tecnología en particular. Además los PSC o CE podrán introducir cambios tecnológicos siempre que estos cumplan con la normativa establecida, se notifique a SUSCERTE y sean aprobados por ella.

**5.2.2.4** El contenido de estos criterios puede cambiar en el tiempo, dependiendo de los avances de la tecnología y consideraciones de seguridad nacional. Si el cambio es considerado significativo, el proceso de revisión se incorporará a la normativa interna.

**5.2.2.5** Los PSC o CE acreditados deberán ser notificados de los cambios de esta norma. Si existiera alguna duda respecto a la actualización de estos criterios, deberá contactarse con la Superintendencia.

**5.2.2.6** Los lineamientos aquí establecidos corresponden al cumplimiento de los estándares tecnológicos internacionales, los cuales son los siguientes:

**a) En cuanto a prácticas de certificación:**

- ETSI TS 102 042: "Policy requirements for certification authorities issuing public key certificates". V2.4.1 (2013-02)
- RFC 3647. "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework". Noviembre 2003.
- CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates v 2.0.5
- CA/Browser Forum Guidelines For The Issuance And Management Of Extended Validation Certificates v 2.0.1

**b) Respecto a seguridad:**

- ISO/IEC 27001:2013 Tecnología de la Información. Técnicas de Seguridad – Sistema de Gestión de la Seguridad de la Información. (2013)
- ISO/IEC 27002:2013 Tecnología de la Información. Técnicas de Seguridad – Código de buenas prácticas para controles de seguridad de la información
- ISO/IEC 15408 Common Criteria for Information Technology Security Evaluation, Versión 3
- FIPS PUB 140-2 Security Requirements for Cryptographic Modules

**c) Referentes a Estructura de Certificados:**

- ITU-T Rec. X.509 Tecnología de la información. Interconexión de sistemas abiertos – El directorio – Marco de autenticación (2001)
- ITU-T Rec. X.690 (07/2002) / ISO/IEC 8825-1:1998. ASN.1 Basic Encoding Rules

**d) Para Repositorio de Información:**

- [RFC 2559] Boeyen, S. , "Internet X.509 Public Key Infrastructure. Abril 2002
- [RFC 4386] Boeyen, S. , "Internet X.509 Public Key Infrastructure repository location services. Febrero 2006

**e) En cuanto a criptografía**

- [RFC 5280] Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile (2008) y actualizaciones.

**5.2.3** Los recaudos técnicos, estándares tecnológicos y lineamientos de seguridad a aplicar para la acreditación o renovación como PSC o CE, se resumen en el Anexo No 1.

## 5.3. Consideraciones Específicas

### 5.3.1 Infraestructura de Clave Pública. Perfiles de Certificado y Servicios de Publicación

#### 5.3.1.1 Estructura e Información del Certificado Electrónico

##### 5.3.1.1.1 Objetivo

Comprobar los aspectos mínimos que dispone el estándar ITU-T Rec. X.509, contenidos mínimos, incorporación de los requisitos mínimos obligatorios, límites y atributos del certificado de firma electrónica.

##### 5.3.1.1.2 Descripción

**1.** La estructura de datos que conforma el certificado de firma electrónica emitido por el PSC o CE debe estar en conformidad al estándar ITU-T Rec. X.509.

**2.** El certificado de firma electrónica emitido por el PSC o CE debe contener al menos los siguientes datos:

a) Un código de identificación único del certificado.

b) Identificación del PSC o CE, con indicación de su nombre o razón social, RIF, dirección de correo electrónico, y, en su caso, los antecedentes de su acreditación y su propia firma electrónica.

c) Los datos de la identidad del signatario, entre los cuales deben necesariamente incluirse su nombre, dirección de correo electrónico y cédula de identidad.

d) Plazo de vigencia (fecha de inicio y de vencimiento).

**3)** El PSC o CE debe incorporar en sus certificados el RIF propio y la identificación del signatario de acuerdo a la estructura e identificadores que se especifica por la Superintendencia de acuerdo al caso.

**4)** Los PSC o CE deben indicar en forma explícita, que el certificado emitido corresponde a una política de certificados con los límites de uso (ej. de firma electrónica). Esta indicación debe quedar inserta en el campo Certificate Policies de las extensiones del certificado del formato X.509 versión 3.

**5)** El PSC o CE 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 de la Infraestructura Nacional de Certificación Electrónica.

**6)** Los límites de uso que se incorporen en los certificados, deben ser reconocibles por terceros de la Infraestructura Nacional de Certificación Electrónica.

**7)** Los datos de creación de firma del PSC o CE acreditado para emitir certificados, no deben ser utilizados más allá de lo establecido en la DPC aprobada por SUSCERTE.

#### 5.3.1.1.3 Estándares de Evaluación

- ITU-T Rec. X.509 / ISO/IEC 9594-8
- ITU-T X.690

-Modelo de Certificado de firma electrónica, emitido por el PSC o CE en evaluación.

-Modelo de solicitud de firma del certificado (CSR), en caso de acreditación.

-Modelo de certificados electrónicos emitidos por el PSC o CE (40360 y PC).

#### 5.3.1.1.4 Detalles de la Evaluación

| Aspectos | Evaluación |
|---|---|
| **Conformidad con el estándar ITU-T Rec. X.509 Norma SUSCERTE No.** | Se verificará que la estructura básica del certificado esté en conformidad a la norma y que la gramática utilizada tanto en la estructura básica como en las extensiones obligatorias para incluir el RIF o CI, puedan ser leídos por cualquier aplicación que cumpla |

| | |
|---|---|
| **032.** | dicho estándar. |
| **Contenido básico del certificado de firma electrónica emitido por el PSC o CE (Norma SUSCERTE No. 032)** | Se confirmará que el certificado contiene la siguiente información:<br>a) Un código de identificación único del certificado<br>b) Identificación del PSC o CE, con indicación de su nombre o razón social, RIF, dirección de correo electrónico, y, en su caso, los antecedentes de su acreditación y su propia firma electrónica<br>c) Los datos de la identidad del signatario, entre los cuales deben necesariamente incluirse su nombre, dirección de correo electrónico, su RIF O CI, y<br>d) El tiempo de vigencia. |
| **Método de incorporación de identificación del signatario (Norma SUSCERTE No. 032)** | Se verificará que el PSC o CE incorpore en sus certificados el identificador según sea el caso, como por ejemplo que el signatario sea persona jurídica se debe incluir el RIF. |
| **Lectura y reconocimiento del contenido mínimo cuando existen atributos adicionales en el certificado** | Se validará que el PSC o CE estructure sus certificados, de forma que los atributos adicionales que introduzca, con el fin de incorporar límites al uso del certificado, si los hay, no impidan la lectura ni su reconocimiento por terceros. |
| **Reconocimiento de límites de uso del certificado de firma electrónica por terceros** | Se verificará que el PSC o CE 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 o CE acreditado para emitir certificados no sean utilizados más allá de lo establecido en la DPC aprobada por SUSCERTE. |
| **Algoritmos de firma** | Se validará que el PSC o CE utilice algoritmos de firma estándares establecidos por el RFC 5280 que provean el adecuado nivel de seguridad aprobado por SUSCERTE tanto para su propia firma como para la firma del signatario. |
| **Tamaño de las claves** | Se comprobará que el PSC o CE utilice el tamaño de clave pública y privada, de mínimo 256 y máximo 521 (ECDSA) para su propia firma y para la firma del signatario; o en su defecto se establecerá una longitud acorde a los estándares internacionales y conforme con las normativas emitidas por SUSCERTE. |
| **Funciones Hash** | Se verificará que el PSC o CE utilice funciones Hash de última generación para el proceso de firma, debidamente elegida a través de un estudio de factibilidad por la Superintendencia, que provean |

| | |
|---|---|
| | el nivel de seguridad, tanto para su propia firma como para la firma del signatario.<br>El uso de funciones de hash debe actualizarse cada año, posterior a la creación de esta norma, ya que al cumplirse el lapso, se debe haber superado cualquier problema de interoperabilidad de algoritmos de mayor complejidad. |

#### 5.3.1.2 Estructura de la Lista de Certificados Revocados (LCR) y Servicio OCSP – Online Certificate Status Protocol

##### 5.3.1.2.1 Objetivo

Verificar que las listas de certificados revocados tengan el formato y contenido establecido en el estándar, y permita al signatario identificar plenamente al PSC o CE emisor de la LCR y se verificará la integridad y funcionalidad del servicio OCSP, el cual sirve para determinar el estado de revocación de un certificado electrónico, como método alternativo a la LCR. Este protocolo se describe en el RFC 2560.

##### 5.3.1.2.2 Descripción

La lista de certificados revocados (LCR) debe contener la información y estructura que especifica el RFC 6818 y RFC 5280.

Estos RFC especifican 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 podrá ser almacenada y enviada en medios inseguros, debe estar debidamente firmada por el PSC o CE emisor.

Para el Servicio OCSP se verificará que el PSC o CE:

- Garantice la existencia de un servicio seguro de consulta de la validez de los certificados electrónicos a través del servicio OCSP
- Provea acceso al servicio a partes interesadas por medios electrónicos de manera continua y regular.

- Use sistemas y productos confiables que garanticen la seguridad de su sistema.
- Posea procedimientos para informar a los signatarios las características generales del servicio.

#### 5.3.1.2.3 Estándares de Evaluación

- RFC 6818
- RFC 5280
- RFC 2560
- Norma SUSCERTE No 032

#### 5.3.1.2.4 Documentación Solicitada

- DPC y PC del PSC o CE.
- LCR emitida por el PSC o CE en evaluación y el certificado de firma electrónica de la AC que la emite.
- Reportes de solicitudes y/o peticiones al servicio OCSP

#### 5.3.1.2.5 Detalles de la Evaluación

| Aspectos | Evaluación |
|---|---|
| **Contenido Mínimo** | Se verificará que la LCR contenga al menos la siguiente información:<br>● Versión. Debe tener el valor 2<br>● Algoritmo de firma. Este campo debe contener la identificación del algoritmo de firma utilizado, siguiendo el RFC 6818 y RFC 5280.<br>● Nombre del emisor. Este campo debe contener el nombre de la entidad que emitió y firmó la lista de certificados revocados.<br>● Fecha actual. Este campo debe contener la fecha y hora en que fue emitida la lista de certificados revocados (LCR).<br>● Próxima actualización. Se deberá incluir en este campo la fecha en que se emitirá la próxima lista de certificados revocados.<br>● 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. |
| **Comprobación de firma** | Se comprobará que la lista de certificados revocados esté debidamente firmada por el PSC o CE 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 o CE 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.<br>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 la 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. |

**5.3.1.3 Registro de Acceso Público.** (Servicios, contenido y accesibilidad electrónica del sistema público de información del PSC o CE).

#### 5.3.1.3.1 Objetivo

Asegurar el acceso a información relevante descriptiva del sistema por parte de los signatarios y terceros, como mínimo se requiere acceso a la DPC y PC, así como a los servicios de publicación como el certificado de la AC y LCR.

#### 5.3.1.3.2 Descripción

Se verificará que el PSC o CE:

- 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 o CE acreditado o si es homologado.

- Provea acceso al registro público de certificados a los signatarios y terceros interesados por medios electrónicos de manera ininterrumpida.
- Use sistemas y productos confiables que garanticen la seguridad de su sistema de difusión de información.
- Tenga procedimientos para informar a los signatarios 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 o CE se compromete a utilizar en la prestación del servicio.
- Posea 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) la información de acceso electrónico y las resoluciones de la Superintendencia que le afecten. Esto debe realizarse como mínimo en los sitios de dominio público registrados durante el proceso de acreditación o renovación. Además, debe incluirse la DPC y PC.

#### 5.3.1.3.3 Información Necesaria

Documento descriptivo que contenga la siguiente información:

- Detalle del sitio Web donde publicará la información.
- Descripción de la tecnología.
- Disponibilidad, accesibilidad, conexión, esquemas y diagramas de funcionamiento.
- Medidas de seguridad.
- Sitio Web de prueba con las funcionalidades requeridas.
- Publicación y vigencia de DPC y PC
- Publicación y vigencia de la LCR.

#### 5.3.1.3.4 Detalles de la Evaluación

| | |
|---|---|
| **Existencia y contenido mínimo del Sitio Web de información pública** | El PSC o CE debe mantener un sitio de acceso electrónico, con información relevante para los signatarios y las partes que confían. Debe contener los siguientes documentos:<br>● Registro de certificados emitidos, indicando código de identificación único del certificado y su estado (vigente, suspendido o revocado).<br>● Copia de la LCR actualizada cada 24 horas.<br>● Indicar si el certificado ha sido traspasado de otro PSC o CE acreditado o ha sido homologado.<br>● Acceso seguro a los signatarios para realizar revocación o suspensión de certificados vigentes.<br>● DPC y PC(s). |
| **Disponibilidad de la información y servicio** | Se debe asegurar una disponibilidad del sitio no menor al 99%. anual.<br>Para esto se verificará la existencia de mecanismos redundantes o alternativos de conexión y sitios de contingencia que permitan levantar la plataforma 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. |

### 5.3.2 Infraestructura de Clave Pública. Ciclo de Vida de las Claves

**5.3.2.1 Plan de Administración de Claves Criptográficas** (Implementación y Mantenimiento)

#### 5.3.2.1.1 Objetivo

Comprobar que la organización implemente 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.

#### 5.3.2.1.2 Descripción

Las claves criptográficas son la base de una infraestructura de claves públicas (PKI), siendo el elemento principal a resguardar y administrar por el PSC o CE, y por lo tanto requiere de un plan específico para su administración.

Para la generación y resguardo de las claves de la AC, se exige el cumplimiento de las directrices establecidas en la ETSI TS 102 042 secciones 7.2.1 – 7.2.2 – 7.2.3 – 7.2.4 - 7.2.5 – 7.2.6 – 7.2.7, para el reconocimiento de los certificados electrónicos y sus firmas.

El contenido mínimo de este plan consistirá en lo siguiente:

- Documentación del ciclo de vida completo de las claves criptográficas de la AC, esto es:
  1) Generación de las claves de la Autoridad de Certificación del PSC o CE
  2) Almacenamiento, respaldo y recuperación de la clave privada de la AC.
  3) Distribución de la clave pública de la AC.
  4) Uso de la clave privada por parte de la AC.
  5) Término del ciclo de vida de la AC.
  6) Revocación del Certificado del PSC o CE
- Administración del ciclo de vida del hardware criptográfico utilizado por la AC.
- Servicios de administración de las claves de los signatarios suministradas por la AC (generación de clave, renovación y revocación de la clave)
- Preparación de los dispositivos seguros de los signatarios.
- A su vez el plan debe ser consistente con la DPC y PC.

#### 5.3.2.1.3 Estándares de Evaluación

- ETSI TS 102 042
- FIPS 140-1
- FIPS 140-2
- FIPS 140-3
- CA/BR B
- CA/BR G

#### 5.3.2.1.4 Documentación Solicitada

Documento descriptivo de la implementación del Plan de Administración de Claves Criptográficas de la Organización.

#### 5.3.2.1.5 Detalles de la Evaluación

| Aspectos | Evaluación |
|---|---|
| **Relación entre el Plan de Administración de Claves y los recursos asignados** | Verificar que el PSC o CE 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 lograr 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 mantenga 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 o CE se logran a través de la implementación del Plan de Administración de Claves. |
| **Requerimientos ETSI TS 102 042, sección 7.2.1** | Generación de Claves de la AC:<br>El PSC o CE se asegurará de que las claves CA se generen en circunstancias controladas.<br>En particular:<br>a) La generación de claves de la AC se llevará a cabo en un ambiente protegido físicamente (Véase Plan de Seguridad de la Información – Acceso Físico) por personal autorizado (Véase Documento Evaluación del Personal) bajo, al menos, el control dual. El número de personal autorizado para llevar a cabo esta función deberá mantenerse al mínimo, considerando las contingencias y ser coherentes con la DPC.<br>b) La generación de claves se llevará a cabo con una aplicación o dispositivo que asegure que las claves se generan de una manera |

| | |
|---|---|
| | confiable y no ponen en peligro la seguridad de la clave privada.<br>La generación de claves de CA se llevará a cabo dentro de un dispositivo que:<br>● Cumpla los requisitos identificados en FIPS PUB 140-2 el nivel 3 o superior;<br>● Un sistema confiable como EAL 3 (Evaluation Assurance Level) o superior, de acuerdo con la norma ISO / IEC 15408;<br>O con otros estándares de seguridad equivalentes.<br>c) La generación de claves se debe realizar utilizando un algoritmo reconocido por SUSCERTE como apto para los usos de firma.<br>d) La longitud de la clave seleccionada y algoritmo para la clave de firma de la AC, será uno que es reconocido por SUSCERTE para este fin.<br>e) Un tiempo adecuado antes de la expiración de la clave de firma, el PSC o CE deberá generar un nuevo par de claves de firma de certificado y se aplicaran todas las medidas necesarias, para evitar la interrupción de las operaciones de una entidad que puede confiar en la clave de la AC. La nueva clave de la AC será también generada y distribuida de acuerdo con esta política.<br>NOTA : Con el fin de cumplir con este requisito, estas operaciones deben realizarse oportunamente para permitir que todas las partes que tienen relación con la AC, estén informadas del cambio de clave y de implementar los procesos necesarios para evitar inconvenientes y disfunciones. Esto no se aplica a una AC que cesará sus operaciones antes de su fecha de caducidad. |
| **Requerimientos ETSI TS 102 042, sección 7.2.2** | Almacenamiento, Respaldo y Recuperación:<br>El PSC o CE se asegurará de que las claves privadas de la AC se mantienen confidenciales y mantendrán su integridad.<br>En particular:<br>a) La firma de la clave de la AC se realizará con aplicación o dispositivo que no permita comprometer la seguridad de la misma y que cumpla con los requisitos identificados en los estándares FIPS PUB 140-1, el nivel 3 o superior; o<br>● Un sistema confiable como EAL 4 o superior, de acuerdo con la norma ISO / IEC 15408;<br>● o con otros estándares de seguridad equivalentes<br>Esto se hará bajo un perfil objetivo de seguridad o de protección que cumple con los requisitos de la presente norma, basado en un análisis de riesgos, y teniendo en cuenta las medidas de seguridad de carácter no técnico. |

| | |
|---|---|
| | b) Se debe garantizar la confidencialidad de la clave privada luego del proceso de creación o firma dentro de la aplicación o dispositivo utilizado.<br>NOTA: Esto se puede lograr con la aplicación de controles de seguridad físicos y lógicos o de cifrado.<br>c) La clave privada de la AC deberá ser respaldada, almacenada y recuperada sólo por personal autorizado, al menos, con un control dual en un entorno protegido físicamente (Véase Plan de Seguridad de la Información – Acceso Físico). El número de personas autorizadas para llevar a cabo esta función, deberá mantenerse al mínimo, de acuerdo a los planes de contingencia y como lo establece la DPC.<br>d)Las copias de seguridad de las claves privadas de la AC estarán bajo las mismas o con mayores niveles de seguridad que las claves privadas que están actualmente en uso.<br>e) Cuando las claves se almacenan en un módulo de hardware criptográfico o HSM, los controles de acceso a éste deberán asegurar que las llaves no son accesibles fuera del módulo de hardware. |
| **Requerimientos ETSI TS 102 042, sección 7.2.3** | Distribución de la clave pública de la AC:<br>El PSC o CE deberá asegurar la integridad y autenticidad de la clave pública de la AC, y cualquier otro parámetro asociado al uso de la clave, durante su distribución a terceras personas.<br>En particular:<br>a) La verificación de la clave pública de la AC estará a disposición de terceras personas, de esta manera se asegurará la integridad de la misma y la autenticación de su origen.<br>b) La clave pública de la AC debe ser firmada por sí misma para su distribución. |
| **Requerimiento ETSI TS 102 042, sección 7.2.4** | Depósito de claves (Key escrow)<br>Si la clave del signatario es usada para firmar electrónicamente, el PSC o CE no puede mantener la clave del signatario, ya que esto le daría la capacidad de descifrar desde el respaldo. |
| **Requerimientos ETSI TS 102 042, sección 7.2.5** | Usos de la Clave de la AC:<br>El PSC ó CE se asegurará de que la clave privada no se utilizará de forma inadecuada.<br>En particular:<br>a) La clave de la CA utilizada para la generación de certificados, tal como se define en la sección 7.3.3 de la ETSI 102 042, y/o la emisión de la información del estado de revocación, no será utilizada |

| | |
|---|---|
| | para ningún otro propósito.<br>b) Las claves de firma de certificado sólo serán utilizados dentro de espacios físicamente seguros (Véase Plan de Seguridad de la Información – Acceso Físico). |
| **Requerimientos ETSI TS 102 042, sección 7.2.6** | Final del Ciclo de Vida de la Clave<br>El PSC o CE se asegurará de que la clave privada no se utilizará luego del final de su ciclo de vida.<br>En particular:<br>a) El uso de la clave privada de la AC correspondiente, se limitará a que es compatible con el algoritmo de hash, el algoritmo de firma y la longitud de clave usados en la generación del certificado, tal y como se define en la cláusula ETSI 7.2.1.<br>b) Todas las copias de las claves privadas de la AC serán destruidas al final de su ciclo de vida. |
| **Requerimientos ETSI TS 102 042, sección 7.2.7** | Ciclo de vida de la administración del hardware criptográfico usado para la firma de certificados:<br>El PSC o CE garantizará la seguridad del dispositivo criptográfico a lo largo de su ciclo de vida.<br>En particular, el PSC o CE se asegurará de que:<br>a) Los certificados y el estatus de la información de revocación que maneja el hardware criptográfico no deben ser manipulados durante la generación.<br>b) Los certificados y el estatus de la información de revocación que maneja el hardware criptográfico no deben ser manipulados mientras son almacenados.<br>c) La instalación, activación, copia de seguridad y recuperación de la clave de la AC en el hardware criptográfico deberá requerir el control simultáneo o conjunto de al menos dos (2) de los empleados autorizados.<br>d) Los certificados y el estatus de la información de revocación que maneja el hardware criptográfico deberá estar funcionando correctamente.<br>e) La clave privada de la AC que está almacenada en el hardware criptográfico debe destruirse en caso de finalizar las operaciones o funcionamiento del dispositivo. Esta destrucción no afecta a todas las copias de la clave privada. Sólo la instancia física de la clave almacenada en el hardware criptográfico en consideración será destruida. |
| **Requerimientos ETSI TS 102 042, sección** | Terminación de una AC:<br>La AC deberá garantizar que las posibles interrupciones a los |

| | |
|---|---|
| **7.4.9** | suscriptores y partes de confianza se minimicen como resultado del cese de los servicios, y debe asegurar la continuidad de mantenimiento de registros para proporcionar evidencia de certificación a los efectos de los procedimientos judiciales, que para el caso de Venezuela, la LSMDFE establece un mínimo de diez (10) años.<br>1.- Antes que la AC termine sus servicios debe asegurar como mínimo que:<br>a) El PSC o CE deberá informar la terminación de la AC a todos los suscriptores y entidades con las que tenga acuerdos u otras formas de relaciones que se establezcan, entre las cuales, las partes que confían en la AC. Adicionalmente, esta información deberá ponerla a disposición de otras partes de confianza;<br>b) La AC terminará todas las autorizaciones de los subcontratistas que habiliten sus operaciones como los que actúen en nombre de ella, en el desempeño de las funciones relacionadas con el proceso de emisión de certificados;<br>c) La AC llevará a cabo las acciones necesarias para la transferencia de las obligaciones de mantener el registro de información de sus operaciones, la información de estado de revocación y los archivos de registro de eventos, por un periodo de diez (10) años tal y como lo establece la LSMDFE.<br>d) La AC deberá destruir o retirar de su uso, sus claves privadas, como se define en la cláusula 7.2.6. de la ETSI.<br>2.- El PSC o CE llegará a un acuerdo para cubrir los costos de cumplir con estos requisitos mínimos en caso de que el cese de la AC este vinculado con una situación de quiebra o por otras razones que eviten poder cubrir los costos por sí mismos, en la medida de lo posible dentro de las limitaciones de la legislación aplicable en materia de quiebra.<br>3.- La AC deberá indicar en sus prácticas las provisiones consideradas para la interrupción del servicio. Esto incluirá:<br>a) La notificación de las entidades afectadas;<br>b) La transferencia de sus obligaciones frente a terceros;<br>c) El manejo del estado de revocación de los certificados no vencidos que se han emitido. |
| **Requerimientos CA/BR B, sección 4.9.1.2** | Razones para revocar un certificado de una CA Subordinada PSC o CE.<br>La AC emisora revocará un certificado de AC subordinada dentro de los siete (07) días siguientes si se presenta uno o más de los |

| | |
|---|---|
| | siguientes supuestos:<br>1. La AC Subordinada solicita la revocación por escrito;<br>2. La AC Subordinada notifica a la AC emisora que la solicitud de certificado original no fue autorizada y no concede retroactivamente la autorización;<br>3. La AC emisora obtiene pruebas de que la clave privada de la AC subordinada correspondiente a la clave pública en el certificado, sufrió un Compromiso de clave;<br>4. La AC emisora obtiene pruebas de que el certificado fue mal utilizado;<br>5. La entidad emisora conoce que el certificado no fue emitido de conformidad o que la AC Subordinada no ha cumplido con los requisitos de base de la Declaración de Política de Certificados o Prácticas de Certificación aplicable;<br>6. La AC emisora determina que alguna de la información que aparece en el certificado es inexacta o engañosa;<br>7. La entidad emisora o AC subordinada cesa operaciones por cualquier razón y no ha hecho arreglos para otra AC para proporcionar apoyo en la revocación del Certificado;<br>8. El derecho de emisión de AC o AC subordinada para emitir certificados bajo estos requisitos vence o es revocado o cancelado, a menos, que la entidad emisora haya hecho arreglos para continuar manteniendo el repositorio de la LCR / OCSP;<br>9. La Revocación es requerida por la Política de Certificados de la AC y/o Declaración de Prácticas de Certificación. |
| **Nivel de seguridad del dispositivo seguro de los signatarios** | Verificar que el dispositivo seguro de los signatarios cumple como mínimo con los requerimientos del estándar FIPS 140-1 nivel 3 (o Common Criteria EAL 3 ISO/IEC 15408) en sus elementos de seguridad e implementación de los algoritmos criptográficos estándar. |

#### 5.3.2.2 Modelo y Manual de Operación de la Autoridad de Certificación (AC)

##### 5.3.2.2.1 Objetivo

Comprobar a través de la documentación presentada, el cumplimiento de los aspectos operacionales mínimos que dispone la LSMDFE, el Reglamento parcial, la ETSI y

CA/BR, con relación a los requisitos de confiabilidad e interoperabilidad en la forma de operar y prestar los servicios de la AC principales y subordinadas de un PSC o CE.

#### 5.3.2.2.2 Descripción

El propósito del modelo y manual es describir la administración diaria y las prácticas operacionales de la AC principal y/o las subordinadas, del PSC o CE, y garantizar que las directrices primarias de la DPC y 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, líneas de tiempo, etc.

El Modelo y Manual de Operación de la AC principal y/o subordinadas del PSC deberá tener las siguientes características:

- Ser consistente con la DPC y PC.
- Ser consistente con el estándar ETSI y CA/BR.
- Incluir la interacción entre la AC principal y subordinada, así como con las 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.

#### 5.3.2.2.3 Estándares de Evaluación

- ETSI TS 102 042
- CA/BR
- RFC 3647

#### 5.3.2.2.4 Documentación Solicitada

- Modelo y Manual de operación de la AC principal y/o subordinadas del PSC o CE.
- Manual del Hardware Criptográfico usados para la generación y protección de las claves privadas de la(s) autoridades de certificación

#### 5.3.2.2.5 Detalles de la Evaluación

| Aspectos | Evaluación |
|---|---|
| **Asignación de funciones y responsabilidades** | Identificación del personal encargado de la operación y administración de la AC principal y/o subordinadas del PSC o CE, en relación a lo establecido en la "Evaluación del Personal". |
| **Referencias de los cargos en los planes del PSC o CE** | Referencia del personal en los planes de continuidad del negocio y los planes de recuperación de desastres y contingencias. |
| **Descripción de las Operaciones** | Descripción detallada de los siguientes procedimientos:<br>1. Generación de pares de claves<br>2. Publicación de la LCR<br>3. Publicación de la información del certificado<br>4. Distribución de claves y certificados<br>5. Renovación de certificados<br>6. Renovación de certificados luego de una revocación<br>7. Suspensión de certificados<br>8. Medidas de control de acceso<br>9. 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 modelo de interacción entre la AC principal y/o subordinadas, así como con la(s) AR(s) |
| **Requerimientos ETSI TS 102 042, sección 7.2.8** | Servicio de la AC de gestión de Certificados para signatarios<br>La AC se asegurará de que la generación de las claves de los signatarios, se lleve a cabo de forma segura y se conserve el secreto de la clave privada.<br>Generación de Certificado<br>a) Las claves de los signatarios se deben generar con un algoritmo reconocido por SUSCERTE (ECDSA) y las políticas de certificados deben estar adaptadas a los usos identificados en el algoritmo durante el tiempo que dure el certificado.<br>b) La longitud de las claves de los signatarios generadas por la AC deben ser de un tamaño (mínimo 256) y uso de acuerdo a un algoritmo de clave pública reconocido por los estándares (ECDSA) de forma que se adapte a los propósitos establecidos en las Políticas de Certificado por el tiempo que dure o de su validez.<br>c) La clave privada del signatario deberá ser entregada al mismo, |

| | |
|---|---|
| | asegurando su secreto y la integridad, a los efectos de que la misma no se vea comprometida.<br>d) Una vez entregada la clave al signatario, solo se debe mantener bajo el control y uso exclusivo del signatario. |
| **Requerimientos ETSI TS 102 042, sección 7.3.2** | Renovación y actualización de Certificados Electrónicos<br>La AC se asegurará de que las solicitudes de un signatario que ya ha sido previamente registrado en la misma AC sea completa, precisa y debidamente autorizada. Esto aplica para la renovación de certificados, la revocación y antes de una expiración, o una actualización debido a cambio a los atributos del signatario.<br>a) La AC verificará la existencia y validez del certificado que se renueva y que la información que utiliza para verificar la identidad y los atributos del signatario siguen siendo válidos.<br>b) Si alguno de los términos y condiciones de la AC han cambiado, éstas serán comunicadas y acordadas de nuevo con el suscriptor.<br>c) Si los nombres o atributos del certificado han cambiado, o el certificado anterior ha sido revocado, el registro de información debe ser verificado, grabado, acordado por el signatario de conformidad con la cláusula 7.3.1 de la ETSI apartados d) e i).<br>d) La AC deberá emitir un nuevo certificado utilizando la clave pública previamente certificadas del signatario, sólo si su seguridad criptográfica es todavía suficiente para el período de validez del nuevo certificado y no existen indicios de que la clave privada del sujeto haya sido comprometida. |
| **Requerimientos ETSI TS 102 042, sección 7.3.3** | Generación de Certificados<br>El PSC o CE deberá garantizar las condiciones de seguridad necesarias para la emisión de los certificados a objeto de asegurar su autenticidad.<br>En particular:<br>a) Los certificados deben incluir, de acuerdo a los estándares X.509 y RFC 5280 :<br>1) Identificación de la CA que emite el certificado y el país en el que está establecida;<br>2) El nombre del sujeto, o un seudónimo que lo identifique como tal;<br>3) La existencia de un atributo específico del signatario, se incluirá de ser necesario, según la función o finalidad para la que el certificado esté destinado;<br>4) La clave pública que corresponde a la clave privada bajo el control del sujeto;<br>5) Una indicación relativa a la fecha inicial y final del período de |

| | |
|---|---|
| | validez del certificado;<br>6) El número de serie del certificado;<br>7) La firma electrónica de la autoridad de certificación que lo emite;<br>8) El alcance del uso del certificado, si aplica;<br>9) Los límites del valor de las transacciones para las que puede utilizarse el certificado, si aplica;<br>a) El PSC o CE tomará medidas contra la falsificación de certificados y debe garantizar la confidencialidad durante el proceso de generación de dichos datos.<br>b) El procedimiento de emisión del certificado estará firmemente vinculado al registro asociado, de renovación o revocación, incluyendo el suministro de cualquier clave pública generada por el signatario.<br>c) Si el PSC o CE genera la clave del signatario:<br>1) El procedimiento de emisión del certificado estará firmemente ligado a la generación del par de claves del PSC o CE;<br>2) La clave privada se pasa de forma segura al signatario registrado;<br>3) El dispositivo seguro que contiene la clave privada del signatario debe almacenar con seguridad esa clave registrada por el signatario (FIPS PUB 140-2 nivel 3).<br>e) El PSC o CE se asegurará de que durante el tiempo de vida de la AC, el nombre distinguido que se ha utilizado en un certificado nunca se vuelve a asignar a otra entidad.<br>f) La confidencialidad y la integridad de los datos de registro deberán estar protegidos, especialmente cuando se intercambian entre el emisor y el signatario o entre los componentes del sistema de la AC.<br>g) El PSC o CE verificará que los datos de registro que intercambia con la Autoridad de Registro (AR), sean autenticados o validados. |
| **Requerimientos ETSI TS 102 042, sección 7.3.4** | Difusión de los términos y condiciones<br>El PSC o CE se asegurará de que los términos y condiciones estén a disposición de los suscriptores y partes de confianza.<br>En particular:<br>a) El PSC o CE pondrá a disposición de los suscriptores y partes de confianza los términos y condiciones sobre el uso de los certificados:<br>a.1) La política aplicada al certificado, incluyendo una declaración clara en cuanto a si la política es para los certificados emitidos al público o si la política es requerida para el uso de algún producto, |

| | |
|---|---|
| | aplicación o dispositivo en particular, para efectos de la aplicación del par de claves asociados al certificado expedido;<br>a.2) Cualquier limitación en el uso del certificado;<br>a.3) Las obligaciones del suscriptor como se define en la cláusula 6.2 (ETSI), incluyendo si la política requiere el uso de cualquier producto, aplicación o dispositivo en particular, para los fines de la aplicación del par de claves asociados con la emisión del certificado;<br>a.4) Información sobre cómo validar el certificado, incluyendo los requisitos para comprobar el estado de revocación del mismo, de manera que las partes que confían, consideren "una confianza razonable" en el certificado<br>a.5) Cualquier limitación de responsabilidad que el PSC o CE acepte o excluya, incluyendo los fines y usos;<br>a.6) El período de tiempo en el cual es retenida la información de registro<br>a.7) El período de tiempo en el cual se conservan los registros de eventos de la AC;<br>a.8) Los procedimientos de reclamo y solución de controversias;<br>a.9) El ordenamiento jurídico aplicable; y<br>a.10) Si el PSC ha sido evaluado conforme con la política de certificados identificada, y si es así a través de cual esquema.<br>b) La información que se indica en el apartado (a) debe estar disponible y ser pública, transmitida electrónicamente, y en un lenguaje fácilmente comprensible. |
| **Requerimientos ETSI TS 102 042, sección 7.3.5** | Difusión de los certificados<br>El PSC o CE debe asegurarse que los certificados están a disposición de los suscriptores, signatarios y terceras partes que confían.<br>En particular:<br>Se difunde<br>a) Luego de la generación, el certificado completo y exacto, deberá estar disponible para el suscriptor o signatario para el cual se emite el certificado.<br>b) Los certificados están disponibles para su consulta pública.<br>c) El PSC o CE pondrá a disposición de las partes que confían los términos y condiciones con respecto al uso del certificado<br>d) Los términos y condiciones aplicables serán fácilmente identificables para un certificado determinado.<br>e) La información indicada en las letras b) y c) anteriores deberá |

| | |
|---|---|
| | estar disponible las 24 horas al día, 7 días a la semana. En caso de fallo del sistema, servicio u otros factores que no están bajo el control del PSC o CE, deberán aplicar medidas para garantizar que el servicio de información no está disponible para un periodo mayor al establecido en la declaración de prácticas de certificación lo cual debe ir de la mano con los lapsos fijados en la LSMDFE y su Reglamento.<br>f) Si la AC emite certificados al público la información indicada en los literales b y c anteriores debe estar publicada y disponible a nivel internacional. |
| **Requerimientos ETSI TS 102 042, sección 7.3.6** | Revocación y Suspensión de certificados<br>El PSC o CE se asegurará de que los certificados que se revoquen, una vez se verifique y valide la autorización, deben ser revocados de manera oportuna y a la brevedad posible<br>Gestión de Revocación<br>a) El PSC o CE deberá documentar como parte de su declaración de prácticas de certificación los procedimientos para revocación de certificados, incluyendo:<br>a.1) Quienes pueden presentar reportes y solicitudes de revocación;<br>a.2) La forma en la que se pueden presentar;<br>a.3) Los requisitos para la posterior confirmación de los reportes y solicitudes de revocación;<br>a.4) Las razones para la suspensión de los certificados<br>a.5) El mecanismo utilizado para la distribución de la información de estado de revocación;<br>a.6) El retardo máximo entre la recepción de una solicitud de revocación o reporte y el cambio de estado al de revocación, debe estar a disposición de todas las partes que dependen de la información, que para todos los casos no puede exceder de 24 horas.<br>b) Las solicitudes y los reportes relativos a la revocación, se tramitarán en el recibo (por ejemplo, compromiso de la clave privada del signatario, la muerte del signatario, terminación inesperada de sus funciones de acuerdo o de negocios respecto al signatario o al suscriptor, la violación de obligaciones contractuales):<br>b.1) Se aplican, los requisitos de la CA/BR G, las secciones 9.3.2 (5) y 9.3.3 (5)<br>b.2) Se aplican, los requisitos de CA/BR B, sección 10.3.2 (5) |

| | |
|---|---|
| | c) Se aplican los requisitos de CA/BR G, secciones 11.2.1 y 11.3.3.<br>d) Las solicitudes y los reportes relativos a la revocación deben ser autenticados, revisando que provengan de una fuente confiable y deben estar conforme a lo dispuesto en las prácticas de la AC.<br>e) El estado de revocación de un certificado puede ser "suspendido" mientras se está confirmando las causales y los reportes de revocación. El PSC se asegurará de que el certificado no se mantenga suspendido por más tiempo del necesario a los efectos de confirmar su estado.<br>f) El signatario, y en su caso el suscriptor, de un certificado revocado o suspendido, debe ser informado del cambio de estado de su certificado.<br>g) Una vez que el certificado es revocado definitivamente (es decir, no suspendido) no podrá ser utilizado y deberá emitirse un nuevo certificado al signatario en caso de que éste lo solicite.<br>h) Cuando se utilizan listas de certificado revocado (LCR), incluyendo sus posibles variantes (por ejemplo, Delta CRL), éstas se publicarán por lo menos cada 24 horas, o cuando un certificado sea revocado;<br>i) Cuando se utilizan listas de certificados revocados (LCR) incluyendo sus posibles variantes (por ejemplo, Delta CRL) como el único de los medios de suministro de información para el estado de revocación:<br>i.1) Cada LCR deberá indicar un tiempo para la próxima edición programada de la LCR (el cual no podrá exceder de 24 horas);<br>i.2) Una nueva LCR puede ser publicada antes de la hora indicada de la próxima edición de LCR;<br>i.3) La LCR será firmada por la AC.<br>i.4) La LCR debe ser emitida cumpliendo con Recomendación UIT-T X.509<br>Estado de revocación<br>j) La información del estado de revocación, deberá estar disponible las 24 horas al día, 7 días a la semana. Si se produce un fallo del sistema, servicio u otros factores que no están bajo el control del PSC o CE, el PSC o CE deberá hacer el mejor esfuerzo para asegurar que este servicio de información esté disponible dentro de los lapsos establecidos en su declaración de prácticas de certificación y de acuerdo a lo definido en la LSMDFE y su Reglamento<br>o) Si la AC emite certificados al público, la información del estado |

| | |
|---|---|
| | de revocación debe ser pública y deberá estar disponible a nivel internacional.<br>p ) La información de revocación debe incluir la información del estado de revocación hasta que el certificado expire.<br>q ) Si se admite la firma de código, en caso de un certificado de firma de código de EV, la CA debe seguir el procedimiento de revocación que se indica en el artículo 13 de CA/BR B. |
| **Requerimientos ETSI TS 102 042, sección 7.2.7** | Ciclo de vida del hardware criptográfico utilizado para firmar certificados<br>La AC tiene la responsabilidad de mantener la seguridad del dispositivo criptográfico durante todas las etapas de su existencia, desde su creación hasta su destrucción.<br>En particular, la AC se asegurará de que:<br>a) La firma del Certificado y su información del estado de revocación realizada por el hardware criptográfico no sea manipulada durante su envío.<br>b) la firma del Certificado y su información del estado de revocación realizada por el hardware criptográfico no sea manipulada durante su almacenamiento.<br>c) La instalación, activación, copia de seguridad y recuperación de claves de firma de la AC en el hardware criptográfico deberá requerir el control simultáneo de al menos tres (3) de los empleados de confianza.<br>d) La firma del Certificado y su información del estado de revocación realizada para que el hardware criptográfico esté funcionando correctamente.<br>e) La clave privada de la Autoridad de Certificación (AC) que está almacenada en el dispositivo criptográfico debe ser eliminada de forma segura cuando el dispositivo ya no se use o vaya a desincorporarse. |
| **Requerimientos CA/BR B, sección 4.9.1.1** | Razones para Revocación de un Certificado del Suscriptor<br>El PSC o CE revocará un certificado dentro de 24 horas si se presenta uno o más de las siguientes razones:<br>1.Una solicitud del suscriptor por escrito;<br>2. El suscriptor notifica que la solicitud original de certificado no fue autorizada y no concederá retroactivamente la autorización.<br>3. El PSC o CE obtiene pruebas de que el suscriptor de la clave privada correspondiente a la clave pública en el certificado sufrió un compromiso de clave.<br>4. El PSC o CE obtiene evidencia de que el certificado ha sido mal |

| | |
|---|---|
| | utilizado.<br>5. El PSC o CE descubre que un suscriptor ha violado una o más de sus obligaciones como suscriptor o los Términos de Uso;<br>6. El PSC o CE tiene conocimiento de circunstancias que indican que el uso de un nombre de dominio o la dirección IP en el certificado ya no está legalmente permitida (por ejemplo, un tribunal o árbitro ha revocado un derecho a utilizar el nombre de dominio, un acuerdo de licencia o servicios relevantes entre el Domain Name Registrants y el solicitante ha terminado, o nombres de dominio que no han logrado renovar);<br>7. El PSC o CE conoce que un Certificado ha sido utilizado para autenticar a un subordinado de manera fraudulenta, engañosa;<br>8. El PSC o CE conoce de un cambio en la información contenida en el Certificado;<br>9. El PSC o CE conoce que el certificado no se hubiere expedido de acuerdo con estos requisitos o política de certificación de la entidad emisora o Declaración de Prácticas de Certificación;<br>10. El PSC o CE determina que alguna de la información que aparece en el certificado es inexacta o engañosa;<br>11. El PSC o CE cesa su actividad por cualquier razón y no ha hecho arreglos con otra CA para proporcionar apoyo en revocación del Certificado;<br>12. El derecho del PSC o CE para emitir certificados bajo estos requisitos expira o se revoca, a menos que el PSC o CE ha hecho arreglos para continuar manteniendo los repositorios de la LCR / OCSP;<br>13. El PSC o CE tiene conocimiento de un posible compromiso de la clave privada de la AC Subordinada utilizada para la emisión del Certificado;<br>14. La Revocación es requerida por la Política de Certificados de la CA y/o Declaración de Prácticas de Certificación;<br>15. El contenido técnico o el formato del Certificado presenta un riesgo inaceptable para el software de aplicación de los Proveedores o las Partes que Confían (por ejemplo, el CA/Browser Forum podría determinar obsoleta los algoritmos criptográficos de firma o el tamaño de las claves presentan un riesgo inaceptable y que dichos certificados deberán ser revocados y sustituidos por la misma dentro de un período de tiempo dado). |

#### 5.3.2.3 Modelo y Manual de Operación de la Autoridad de Registro (AR)

##### 5.3.2.3.1 Objetivo

Comprobar a través de la documentación presentada los aspectos operacionales mínimos que dispone la LSMDFE y su reglamento parcial con relación a los requisitos de confiabilidad e interoperabilidad de la operación del PSC o CE para realizar las funciones de Autoridad de Registro.

El PSC o CE se asegurará de constatar de que los suscriptores y signatarios sean identificados con precisión, que sus datos, sus nombres y otros asociados, sean debidamente revisados como parte del servicio, o si aplica, concluir a través de la revisión y certificación a través de fuentes confiables; y que la solicitud del certificado sea exacta, autorizada y completa.

##### 5.3.2.3.2 Descripción

El Modelo y Manual de Operación deberá describir cómo operará el servicio de registro del PSC o CE y su administración diaria. Entre otros aspectos podrá tener las siguientes características:

- Ser consistente con la 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 signatarios de los certificados. Según la norma ETSI TS 102 042, se entiende que el PSC o CE tiene la obligación de generar y entregar en forma segura la clave privada del signatario de un certificado de firma electrónica emitido por él, asegurar la fiabilidad del dispositivo seguro y los mecanismos que el signatario utiliza para firmar.
- 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 AC y AR.
- Incluir la descripción de los mecanismos a través del cual se verificará 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 signatarios, así como sus datos.

#### 5.3.2.3.3 Estándares de Evaluación

- ETSI 102 042
- CA/BR B
- CA/BR G
- RFC 3647

#### 5.3.2.3.4 Documentación Solicitada

- Modelo y Manual de Operación de la AR
- Manual técnico de los dispositivos seguros de firma electrónica

#### 5.3.2.3.5 Detalles de la Evaluación

| Aspectos | Evaluación |
|---|---|
| **Nómina y descripción de cargos** | Nómina de los cargos de personal empleado, con la descripción de los procedimientos operacionales y la forma en que los empleados realizan sus funciones. |
| **Proceso de registro** | Se verifica el registro del signatario. La autenticación, confirmación de su identidad y forma de política para comprobar el nombre y datos asociados al signatario. |
| **Entrega segura de los datos de creación de firma** | El PSC o CE debe tener implementados procedimientos y prácticas que permitan entregar en forma personal y segura los datos de creación de firma al signatario del certificado. |
| **Dispositivo seguro y mecanismos de firma del signatario** | El PSC o CE debe tener implementados procedimientos y prácticas que aseguren que una vez entregados los datos de creación de firma sólo el signatario tenga control de ellos.<br>El dispositivo seguro entregado al signatario debe firmar internamente el documento sin ser jamás accesible la clave privada |

| | |
|---|---|
| | del signatario.<br>El mecanismo de control de acceso a la clave privada sólo debe ser conocido por el signatario al momento de la entrega del dispositivo y en lo posible modificable por el mismo signatario, antes de ser utilizado por primera vez.<br>El dispositivo seguro debe contar con mecanismos que inhabiliten el dispositivo en caso de reiterados intentos fallidos de acceso.<br>El PSC o CE debe entregar al signatario herramientas, aplicaciones e instrucciones para que el signatario pueda firmar en forma segura. |
| **Capacitación y servicio al signatario** | El PSC o CE debe implementar procedimientos de capacitación que permitan al signatario manejar en forma segura e informada el dispositivo de firma, y además mantener un servicio de atención para responder y solucionar dudas de los signatarios. |
| **Referencias de los cargos en los planes de continuidad de negocios del PSC o CE** | Referencia del personal en los planes de continuidad del negocio y los planes de recuperación de desastres y contingencias. |
| **Planes de contingencia** | Descripción de planes de contingencia |
| **Descripción de las operaciones** | Descripción detallada de los siguientes eventos:<br>1. Procedimiento certificados seguro de suspensión y revocación de Medidas de control de acceso<br>2. Procedimientos de respaldo y recuperación |
| **Interacción entre AR del PSC o CE** | El documento cubre los procedimientos que involucren la interacción entre la(s) AC y la(s) AR |
| **Requerimientos ETSI TS 102 042, sección 7.3.1** | Registro del signatario<br>La AC se asegurará de que se evidencie tanto para el suscriptor como para el signatario su identificación, la precisión de sus nombres y los datos asociados a su identificación, sean debidamente examinados y sean exactos como parte del servicio de registro, y que puedan ser certificados a través de fuentes adecuadas y autorizadas.<br>En particular:<br>Se verificará la existencia legal, física y operacional de los suscriptores y signatarios según sea el caso.<br>a) Antes de entrar en una relación contractual con un suscriptor, el PSC o CE deberá informar al suscriptor respecto a los términos y condiciones relacionadas con el uso del certificado.<br>b) Si el signatario es una persona y no es el mismo que el |

| | |
|---|---|
| | suscriptor, el signatario será informado de sus obligaciones.<br>c) El PSC o CE comunicará esta información a través de medios de comunicación confiables, íntegros y disponibles, y en un lenguaje fácilmente comprensible.<br>d) El PSC o CE deberá recoger ya sea evidencia directa, o a través de fuentes adecuadas y autorizadas, la identidad (por ejemplo, nombre) y, en su caso, cualesquiera otros atributos específicos del signatario a los que se les emita un certificado. La verificación de la identidad del signatario será al momento de la inscripción por medios adecuados y de acuerdo con la legislación nacional.<br>e) Si el signatario es una persona las evidencias de su identidad (por ejemplo, nombre) deberá ser comprobada contra la presencia de la persona física, ya sea directa o indirectamente utilizando medios que proporcione una seguridad equivalente a la presencia física. Las evidencias para la verificación de otro tipo de entidades deberán incluir procedimientos que proporcionen el mismo grado de seguridad.<br>f) Si el signatario es una persona física, las evidencias consistirán en:<br>f.1) Nombre completo (incluyendo el apellido y nombre de conformidad con la ley aplicable a nivel nacional en prácticas de identificación).<br>f.2) La fecha y lugar de nacimiento, la referencia a un documento de identidad reconocido a nivel nacional, u otros atributos que puede ser utilizado para, en la medida de lo posible, distinguir la persona de otros con el mismo nombre.<br>g) Si el signatario es una persona física que es identificado en asociación con una persona jurídica, o entidad de organización (por ejemplo, el suscriptor), las evidencias consistirá en:<br>g.1) Nombre completo (incluyendo el apellido y nombre, en consonancia con la ley aplicable a nivel nacional en prácticas de identificación) del signatario;<br>g.2) La fecha y lugar de nacimiento, la referencia a un documento de identidad reconocido a nivel nacional, o de otros atributos del suscriptor que puede ser utilizado para, en la medida de lo posible, distinguir la persona de otros con el mismo nombre;<br>g.3) El nombre completo y la situación jurídica de la persona jurídica asociada u otra entidad organizativa (por ejemplo, el suscriptor);<br>g.4) Cualquier información relevante de registro existente (por |

| | |
|---|---|
| | ejemplo, registro de la empresa) de la persona jurídica asociada u otra entidad organizativa;<br>g.5) Pruebas de que el signatario se asocia con la persona jurídica u otra entidad organizativa.<br>h) Si el signatario es una organización, se proporcionará la siguiente evidencia:<br>h.1) Del nombre completo de la entidad u organización (organización privada, entidad gubernamental o no comercial);<br>h.2) Referencia a un registro reconocido a nivel nacional, u otros atributos que pueden utilizarse en la medida de lo posible, distinguiendo la entidad u organización de los demás con el mismo nombre.<br>h.3) Si el sujeto es un dispositivo o sistema operado por o en nombre de una entidad u organizativa, las evidencias consistirán en:<br>h.3.1) Identificador del dispositivo por el cual se puede hacer referencia (por ejemplo, nombre de dominio de Internet);<br>Se verificará exhaustivamente el control y registro exclusivo del dominio. Nombre, cargo del contratante del dominio. Nombre, cargo del solicitante y quien aprobó el certificado electrónico.<br>El contratante del dominio debe estar vinculado en los registros legales del suscriptor o del signatario.<br>Se verificará el cumplimiento de: CA/BR G sección 10.6;<br>h.3.2) El nombre completo de la entidad u organización;<br>Requisitos CA/BR G secciones 10.2 y 10.6<br>h.3.3) Un número de identidad reconocido a nivel nacional, u otros atributos que pueden utilizarse para, en la medida de lo posible, distinguir la entidad u organización de los demás con el mismo nombre.<br>i) El PSC o CE deberá registrar toda la información necesaria para verificar la identidad del signatario y, en su caso, cualquier atributo específico de la materia, incluyendo cualquier número de referencia en la documentación utilizada para la verificación, y cualquier limitación sobre su validez.<br>j) Si una entidad que no sea el signatario está suscribiendo los servicios de AC (es decir, el suscriptor y signatarios están en entidades separadas), entonces se debe proporcionar evidencia de que el suscriptor está autorizado para actuar en nombre del signatario (por ejemplo, está autorizado para todos los miembros de la organización identificada). |

| | |
|---|---|
| | k) El suscriptor deberá proporcionar una dirección física, u otros atributos, que indique cómo puede ser él contactado.<br>l) El PSC o CE deberá registrar el acuerdo firmado con el suscriptor, incluyendo:<br>l.1) La aceptación de las obligaciones del suscriptor<br>l.2) El acuerdo del suscriptor respecto al uso seguro del dispositivo<br>l.3) El consentimiento para que el PSC o CE (bien sea suscriptor o signatario):<br>● Mantenga la información utilizada en el registro<br>● El derecho de proveer el dispositivo del signatario<br>● Cualquier revocación posterior<br>● La identidad y los atributos específicos ubicados en el certificado<br>Traspaso de dicha información a terceros en las mismas condiciones, si así lo requieren las políticas, en el caso de terminación de los servicios de la AC;<br>l.4) Bajo qué condiciones, el suscriptor requiere que el sujeto consienta la publicación del certificado;<br>l.5) La confirmación de que la información contenida en el certificado es correcta.<br>l.6) Los requisitos CA/BR G las secciones 10.8 y 10.9;<br>l.7) Los Requisitos de la CA/BR B sección 10.3.2<br>m) Los registros identificados anteriormente se conservarán durante el periodo de tiempo establecido en la LSMDFE (10 años) y según sea necesario, para aportar pruebas de certificación en procedimientos judiciales.<br>n) El PSC o CE se asegurará de que los requisitos de la legislación nacional de protección de datos se cumplen (incluyendo el uso de seudónimos en su caso) dentro de su proceso de registro.<br>o) La política de verificación del PSC o CE sólo exigirá la toma de pruebas de identidad suficiente para satisfacer los requisitos de la utilización prevista para el certificado.<br>p) Los requisitos CA/BR G sección 10.11.1 y 10.11.2<br>q) Los requisitos CA/BR G sección 12.1.3.<br>r) Los requisitos CA/BR G sección 7.2.<br>s) Los requisitos CA/BR G sección 9.2.<br>t) Los requisitos CA/BR B secciones 10.1, 10.2, 11.3, 11.4, 11.5 y 11.6<br>u) Los requisitos CA/BR G 6.2.1 punto 1) y 2)<br>v) Los requisitos CA/BR B sección 7.1 |

| | |
|---|---|
| **Requerimientos ETSI TS 102 042, sección 7.2.9** | Preparación segura del dispositivo de usuario<br>El PSC o CE se asegurará de que si se distribuyen dispositivos a usuarios finales el mismo debe ser revisado e inicializado, de forma que se pueda garantizar la seguridad y confianza en su uso<br>Para el caso de firma de código con Certificados de Validación Extendida se debe seguir las recomendaciones del Apéndice H , de la CA/BR G.<br>a) La preparación dispositivo del usuario será controlada por el PSC o CE<br>b) El dispositivo de usuario se debe almacenar y distribuir de forma segura.<br>c ) La desactivación y reactivación debe ser controlada de forma segura<br>d) Cuando el aseguramiento del dispositivo está asociado a la activación de la data (por ejemplo de código PIN), los datos de activación deben ser preparados de forma segura y distribuidos de forma separada al módulo de creación de firma. |
| **Requerimientos CA/BR G 13.1.5** | Razones para Revocación de un Certificado del Suscriptor<br>El PSC o CE revocará un certificado dentro de 24 horas si se presenta uno o más de los siguientes supuestos:<br>1. Solicitudes de revocación por escrito del suscriptor a la AC.<br>2. El suscriptor notifica a la AC que la solicitud de certificado original no fue autorizada y no puede conceder retroactivamente autorización<br>3. El PSC o CE obtiene pruebas de que la clave privada del signatario correspondiente a la clave pública en el Certificado sufrió un compromiso o ya no cumple con los requisitos acordados.<br>4. El PSC o CE obtiene pruebas de que el certificado fue mal utilizado;<br>5. El PSC o CE descubre que un Suscriptor o Signatario ha violado una o más de sus obligaciones de uso acordadas en las condiciones y términos.<br>6. El PSC o CE tiene conocimiento de circunstancias que indican que el uso de un nombre de dominio completo o la IP dirección en el certificado ya no está legalmente permitida (por ejemplo, un tribunal o árbitro ha revocado un dominio, o el derecho del Titular de utilizar el nombre de dominio, un acuerdo de licencia o servicios relevantes entre el Nombre de dominio y el Solicitante ha terminado, o el “Domain Name Registrante” ha fallado en renovar el nombre de dominio); |

| | |
|---|---|
| | 7. El PSC o CE se hace consciente de que un Certificado se ha utilizado para autenticar de forma fraudulenta o engañosa Nombres de Dominio Fully-Qualified.<br>8. El PSC o CE observa un cambio material en la información contenida en el Certificado;<br>9. El PSC o CE observa que el certificado no fue emitido de acuerdo con los requisitos de la Política de Certificado de la AC o Declaración de Prácticas de Certificación<br>10. El PSC o CE observa o determina que la información que aparece en el Certificado es inexacta o engañosa;<br>11. El PSC o CE cesa operaciones por cualquier motivo y no ha hecho arreglos para otro PSC pueda proporcionar apoyo, se revoca el Certificado;<br>12. El derecho del PSC o CE para emitir certificados bajo los requisitos iniciales expira, se revocan o terminan, a menos que el PSC haya hecho arreglos para continuar manteniendo el Repositorio LCR / OCSP;<br>13. El PSC o CE observa un posible compromiso de la clave privada de la AC utilizada para la emisión del Certificado;<br>14. La revocación es requerida por la Política de Certificados de la AC y/o Declaración de Prácticas de Certificación;<br>15. El contenido técnico o el formato del Certificado presenta un riesgo inaceptable para Software o Aplicación provista por terceras partes (por ejemplo, el CA / Browser Forum podrían determinar que el algoritmo criptográfico o el tamaño de las claves presenta un riesgo inaceptable y que dichos Certificados deben ser revocados y sustituidos por las AC en un plazo de tiempo determinado). |

#### 5.3.2.4 Modelo de Confianza

##### 5.3.2.4.1 Objetivo

Verificar que el PSC o CE provea a los signatarios de certificados de firma electrónica emitidos por él, un mecanismo de confianza que le permita comprobar la validez de cualquier certificado que reciba.

##### 5.3.2.4.2 Descripción

El certificado de firma electrónica emitido por un PSC o CE acreditado debe permitir a su receptor verificar, en forma directa o mediante consulta electrónica, todos los certificados que reciba, con la finalidad de comprobar la validez del mismo.

De esta forma es factible asegurar la interoperabilidad en el sistema y la propagación de la confianza depositada por el signatario en su PSC o CE hacia el resto del sistema.

#### 5.3.2.4.3 Estándares de Evaluación

Este apartado no aplica

#### 5.3.2.4.4 Documento Solicitado

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

#### 5.3.2.4.5 Detalles de la Evaluación

| Aspectos | Evaluación |
|---|---|
| **Modelo de confianza** | El modelo de confianza es el esquema por el cual un signatario de un certificado de firma electrónica emitido por un PSC o CE acreditado puede confiar en dicho certificado.<br>El esquema definido en la LSMDFE y su reglamento parcial, deja en manos del PSC implementar el mecanismo por el cual un signatario que confíe en él, pueda confiar en cualquier otro PSC o CE acreditado.<br>El mecanismo propuesto consiste en que cada PSC o CE mantenga en su repositorio de acceso público los certificados de todos los Proveedores acreditados, de tal manera que los signatarios que confíen en él puedan instalar en sus aplicaciones estos certificados.<br>El método debe incluir mecanismos de seguridad para evitar que se puedan reemplazar los certificados en el repositorio o durante su transmisión, sin que ello no pueda ser detectado por el signatario.<br>Este modelo tiene la finalidad de mostrar a los signatarios la cadena de confianza que brinda la Infraestructura Nacional de Certificación Electrónica de Venezuela, es decir, este modelo debe mostrar al signatario toda la estructura de Certificación Electrónica de nuestro país que respalda y le da el valor jurídico a los certificados emitidos por el PSC o CE acreditado. |
| **Efectividad** | Se verifica el mecanismo utilizado para implementar el modelo |

| | |
|---|---|
| | de Confianza en forma práctica en la Infraestructura Nacional de Certificación Electrónica. |
| **Requerimientos ETSI TS 102 042, sección 7.2.3** | Distribución de claves públicas<br>Generación y distribución de los certificados<br>La AC se asegurará la verificación de la integridad y la autenticidad de la clave pública, la AC la firma asegurando de esta forma lo anterior, así como cualquier parámetro asociado que se mantenga durante su distribución a las partes que confían.<br>En particular:<br>a) La AC verifica y firma las claves públicas poniéndola de esta forma a disposición de las partes que confían. De esta manera se asegura la integridad de las mismas y se autentica su origen a los efectos de garantizar su distribución confiable. |

### 5.3.3 Administración, Operación y Seguridad de la Infraestructura de Clave Pública

El PSC o CE debe asegurarse que los procesos operacionales y administrativos tengan una adecuada correspondencia con el cumplimiento de estándares.

Los procesos operativos y de control deben ser documentados, implementados y mantenidos.

El SGSI del PSC o CE no puede ser tercerizado, reside bajo su responsabilidad la Seguridad de sus operaciones.

La información manejada por el PSC o CE debe estar clasificada y de esta forma asegurarse que reciba el adecuado nivel de protección.

#### 5.3.3.1 Revisión de la Evaluación de Riesgos

##### 5.3.3.1.1 Objetivo

Determinar la consistencia del análisis de riesgos y amenazas de la Infraestructura Técnica y Operativa del PSC o CE

##### 5.3.3.1.2 Descripción

Dado que el producto principal de un PSC o CE es la “confianza”, el requerimiento fundamental para un PSC o CE es demostrar una clara comprensión de las amenazas

de seguridad enfrentadas por el negocio y poder mostrar planes efectivos para reducir el riesgo a un nivel aceptable.

La Evaluación de Riesgos es parte de un proceso más amplio denominado Administración del Riesgo. El objetivo principal de un proceso de administración del riesgo en una organización debe ser proteger la organización y su capacidad de cumplir con su misión, y no sólo sus activos IT.

**La Administración del Riesgo incluye tres procesos:**

1. **Valoración de los riesgos,** incluye la identificación y evaluación de los riesgos e impactos de los riesgos, y medidas recomendadas para reducirlos.
2. **Tratamiento de los riesgos,** se refiere a la priorización, implementación y mantenimiento de las medidas de reducción de riesgo apropiadas recomendadas por el proceso de valoración de riesgos. Este proceso conduce a la definición de un Plan de Seguridad.
3. **Mantenimiento,** corresponde al proceso de evaluación continua para adecuar la valoración de riesgos a condiciones cambiantes del entorno o del negocio.

El resultado debe ser un compromiso razonable entre los costos económicos y operacionales de las medidas de protección, y obtener mejoras en la capacidad de lograr la misión de la organización.

Se debe seguir un proceso similar al descrito en los documentos indicados en las referencias, para realizar el proceso de evaluación de riesgos.

Los esfuerzos de seguridad podrán abordar los riesgos de una manera eficaz y oportuna, donde y cuando sean necesarios. La gestión del riesgo en la seguridad de la información podrá ser una parte integral de todas las actividades de gestión de seguridad de la información y se podrán aplicar tanto a la implementación como al funcionamiento continuo de un SGSI.

La gestión del riesgo en la seguridad de la información debe ser un proceso continuo.

El reporte de la valoración de los riesgos debe tener lineamientos dados en la siguiente estructura (ejemplo en el Anexo No 2).

#### 5.3.3.1.3 Estándares de Evaluación

Puede considerarse como referencia normativa la ISO 27005, el Magerit u otro estándar ampliamente conocido.

#### 5.3.3.1.4 Documentación Solicitada

- Copia del documento correspondiente a la Evaluación de Riesgos o documento equivalente.

#### 5.3.3.1.5 Detalles de la Evaluación

| Aspectos | Evaluación |
|---|---|
| **Reporte de la valoración de riesgos** | ● Verificar la adecuada identificación de los riesgos;<br>● Verificar que los riesgos considerados sean reales.<br>● Validar que riesgos relevantes no hayan sido omitidos.<br>● Verificar la valoración adecuada de los riesgos.<br>● Constatar si hay un plan de mantenimiento de la valoración.<br>● Verificar que la evaluación de los riesgos esté en términos y en consecuencia con el negocio del PSC o CE<br>● Verificar la adecuada estimación de la probabilidad de su ocurrencia<br>● Verificar el establecimiento de un orden de prioridad para el tratamiento de los riesgos;<br>● Verificar que se haya priorizado las acciones para reducir la ocurrencia de los riesgos;<br>● Verificar que se haya considerado la participación de los interesados cuando se toman las decisiones sobre gestión del riesgo<br>● Verificar la eficacia del monitoreo del tratamiento del riesgo<br>● Verificar el monitoreo y revisión con regularidad del riesgo y los procesos de gestión de riesgos |
| **Estructura del proceso de valoración de riesgos** | Verificar si el proceso de valoración ha sido realizado o auditado por un ente externo, independiente y calificado.<br>Verificar que el proceso de valoración de riesgo haya sido revisado y reevaluado al menos una (1) vez al año. |

#### 5.3.3.2 **Política de Seguridad de la Información** (Documentación y mantenimiento)

##### 5.3.3.2.1 Objetivo

Comprobar a través de este documento que la organización tiene claros los objetivos de seguridad relevantes para el negocio y que las instancias de gestión del PSC o CE apoyan formalmente esta política.

##### 5.3.3.2.2 Descripción

La política de seguridad es una declaración de objetivos de seguridad. Sólo contiene aquellos que son factibles de lograr a través de acciones, procedimientos y mecanismos implementados por el PSC o CE. Si el PSC o CE tiene en otra organización algún aspecto de seguridad o confianza, entonces debe indicarse claramente.

La política de seguridad debe cumplir al menos con los siguientes requerimientos:

**1.** Los objetivos de seguridad deben ser consecuencia de la Evaluación de Riesgos, de forma tal que los objetivos de la política de seguridad y sus defensas asociadas correspondan al nivel de riesgo requerido para que un PSC o CE sea un ente de confianza.

**2.** Debe estar basada en las recomendaciones del estándar ISO 27002:2022 control 5, los cuales se transcriben en el Anexo No 3 de esta norma.

**3.** Los objetivos de la política son de alto nivel y no técnicos, por tanto debe ser lo suficientemente general para permitir alternativas de implementación tecnológica.

**4.** Si la complejidad de los objetivos así lo requieren, la política puede estar conformada por más de un documento; es decir, puede haber una política general soportada por políticas específicas.

**5.** En esta política de seguridad deben estar incluidos los elementos contenidos en la DPC y PC

**6.** Este documento debe identificar los objetivos de seguridad relevantes y las amenazas potenciales relacionadas a los servicios suministrados, así como las medidas tomadas para evitar o limitar los efectos de estas amenazas.

**7.** Adicionalmente, la documentación debe describir las reglas, directivas y procedimientos que indican cómo son provistos los servicios específicos y las medidas de seguridad asociadas.

En el Anexo No 4 de esta norma se describen los principales aspectos que una política de seguridad debe considerar.

Para los propósitos de la acreditación o renovación de un PSC o CE, algunos de los aspectos más relevantes han sido incorporados en criterios separados para así facilitar el proceso de evaluación y donde estos se detallan completamente. Por ello, este documento puede expresar en forma general aquellos aspectos de la seguridad organizacional que se tratan en documentos específicos.

#### 5.3.3.2.3 Estándares de Evaluación

– ISO/IEC 27002:2022

#### 5.3.3.2.4 Documentación Solicitada

- Copia del documento correspondiente a la política de seguridad de la organización.

- Documento en el cual se describa formalmente la estructura organizativa del PSC o CE, aprobada por las autoridades del mismo.

#### 5.3.3.2.5 Detalles de la Evaluación

| Aspectos | Evaluación |
|---|---|
| **Conformidad con el estándar ISO 27002:2022 control 5.1** | Verificar que los requerimientos del control 5.1 descritos en el Anexo No 3, están incorporados. |
| **Consistencia entre la política de seguridad y la DPC y PC** | Constatar la consistencia de la política de seguridad con la DPC y PC. |
| **Relación entre la Evaluación de Riesgos y la política de seguridad** | Verificar que los principales aspectos de la política de seguridad son coherentes con los niveles de riesgo determinados en la evaluación formal de riesgos. |

| | |
|---|---|
| **Inclusión de lo indicado en el Anexo 4** | Chequear que los elementos fundamentales de una política de seguridad que apliquen al PSC o CE, están incluidos en el documento. |
| **Claridad de los objetivos de seguridad** | Verificar que se establezcan objetivos de seguridad claros relacionados con la protección de los procesos de negocio, activos y servicios del PSC o CE. |

#### 5.3.3.3 Plan de Continuidad del Negocio y Recuperación ante Desastres

##### 5.3.3.3.1 Objetivo

Comprobar a través de este documento que la organización tiene planes establecidos para disminuir a un nivel aceptable el efecto de interrupciones del servicio del PSC o CE, mediante una combinación de controles preventivos y planes de contingencia.

##### 5.3.3.3.2 Descripción

El Plan de Continuidad del Negocio y de Recuperación de Desastres, debe describir cómo los servicios serán restaurados en el evento de desastre, una caída de los sistemas o fallas de seguridad.

Dicho plan debe ser mantenido, probado periódicamente y debiera ser parte integral de los procesos de la organización.

En particular, el documento describe la prioridad de restauración para asegurar la continuidad de los negocios de terceros que sean dependientes de la operación del PSC o CE.

Este documento debe seguir los lineamientos brindados por:

- Estándar ISO 27002:2022 en su control 5
- Estándar ETSI TS 102 042 V2.4.1 en su sección 7.4.

Este documento también debe describir los procedimientos de contingencia a ser seguidos en al menos los siguientes eventos:

- Desastre que afecte el funcionamiento de los productos de software, en el cual el PSC o CE basa sus servicios.

- Incidente o posible incidente de seguridad que afecte la operación del sistema, en el cual el PSC o CE basa sus servicios.
- Compromiso de la clave privada de firma del PSC o CE.
- Falla de los mecanismos de Auditoría.
- Falla en el hardware donde se ejecuta el producto, en el cual el PSC o CE basa sus servicios, este debe incluir los servidores, dispositivos criptográficos, dispositivos de seguridad y dispositivos de comunicaciones.

Se debe identificar los eventos que pueden causar interrupciones a los procesos comerciales y operacionales, junto con la probabilidad y el impacto de dichas interrupciones y sus consecuencias para la seguridad de la información, esto según la ISO 27002:2022.

El plan debe además incluir mecanismos para la preservación de evidencias de mal uso de los sistemas, cuyo propósito es ser usado en caso de ser necesario.

**5.3.3.3.3 Estándares de Evaluación**

- ISO 27002:2022
- ETSI TS 102 042

**5.3.3.3.4 Documentación Solicitada**

- Documento de Planes de Continuidad del Negocio y Recuperación de Desastres.
- Documento de Evaluación de Riesgo.

**5.3.3.3.5 Detalles de la Evaluación**

| Aspectos | Evaluación |
|---|---|
| **Conformidad con el estándar ISO 27002:2022 controles 5.29** | Verificar que los requerimientos del control 5 indicados en el Anexo No 3, están incorporados.<br>El PSC o CE debe asegurar que las operaciones deben restaurarse tan pronto como sea posible ante la ocurrencia de un desastre, incluyendo el caso del compromiso de la clave privada utilizada para la firma de certificados.<br>Otras situaciones de desastre incluyen la falla de componentes críticos de los sistemas del PSC o CE, incluyendo hardware y |

| | |
|---|---|
| | software.<br>En particular:<br>a) El PSC O CE debe definir y mantener un plan de continuidad del negocio en caso de un desastre<br>b) El plan de continuidad de negocios del PSC o CE deberá considerar como un desastre el compromiso o sospecha de compromiso de la clave privada de firma del PSC o CE y los procesos de recuperación deben estar disponibles y probados.<br>c) A continuación de un desastre el PSC o CE deberá, en la medida que sea posible, tomar las medidas que eviten su repetición.<br>d) En el caso de compromiso de su clave privada, el PSC o CE deber como mínimo tomar las siguientes medidas:<br>1. Informar del compromiso a todos los suscriptores y sus contrapartes así como a los otros PSC o CE con quienes tiene acuerdos de interoperabilidad, certificación cruzada u otras formas de colaboración.<br>2. Indicar que los certificados e información del estado de revocación emitidos usando la clave del PSC o CE, pueden no ser válidas, porque han sido comprometidas.<br>Se recomienda a los terceros con los que se tiene un acuerdo de colaboración, sean informados del compromiso de la clave privada.<br>El PSC o CE podrá revocar cualquier certificado de la AC que haya sido emitido. |
| **Evaluación del riesgo** | Esta evaluación podrá considerar los procedimientos comerciales y operacionales y no se podrá limitar a los medios de procesamiento de la información. También se debe verificar que la evaluación del riesgo identifique, cuantifique y establezca prioridad de los riesgos en comparación con los criterios y objetivos relevantes para la organización, incluyendo los recursos críticos, impactos de las interrupciones, tiempos de desabastecimiento permitidos y prioridades de recuperación. |
| **Viabilidad de las facilidades computacionales alternativas** | Chequear que las facilidades computacionales alternativas consideradas en el plan, cumplen con los requerimientos mínimos para la operación del PSC o CE. |
| **Elementos de Auditoría** | Verificar que el sistema en el cual el PSC o CE basa sus servicios provee mecanismos de preservación de los elementos de auditoría. |

#### 5.3.3.4 Plan de Seguridad de la Información

#### 5.3.3.4.1 Objetivo

Comprobar a través de este documento que la organización tiene un plan de seguridad coherente con su Política de Seguridad, que permita mostrar un nivel de confianza consistente con los objetivos del negocio.

#### 5.3.3.4.2 Descripción

El Plan de Seguridad de la información tiene como propósito describir los requerimientos de seguridad de la información y los controles desplegados o planificados para satisfacer dichos requerimientos. Adicionalmente, debe delinear las responsabilidades y conductas esperadas de los individuos que acceden a los sistemas.

Por lo tanto, el Plan de Seguridad de la información debe describir las acciones operacionales, procedimientos y mecanismos que permitan lograr los objetivos indicados en la Política de Seguridad del PSC o CE.

El plan de seguridad debe considerar al menos los controles 5 al 8 del estándar ISO 27002:2022. Sin embargo, en este requisito se evalúan en particular los siguientes aspectos:

- Controles Organizacionales (control 5)
- Controles de Personas ( control 6)
- Controles Físicos ( control 7)
- Controles Tecnológicos( control 8)

En el anexo No. 5 se mencionan otros elementos a considerar para la evaluación del plan de seguridad de la información. Se considera que este Plan es una declaración de intenciones del PSC o CE, por lo que la evaluación bajo este requisito no es una certificación de su nivel de seguridad. El proceso de evaluación bajo este requisito indica el nivel de confiabilidad del PSC o CE si éste cumple con el plan de seguridad de la información.

El PSC o CE debe asegurar que el acceso físico y lógico a los servicios que manejan información sensible esté controlado y los riesgos físicos para los activos estén

reducidos a su valor residual. Esto debe estar basado en el estándar ETSI 102 042 secciones 7.4.4 y 7.4.6.

**ACCESO FÍSICO**

**Ubicación de las instalaciones**

La ubicación de los sistemas de certificación no debe estar públicamente identificada. No debe haber ambientes compartidos que permitan la visibilidad de las operaciones críticas de emisión o revocación de certificados. Esas operaciones deberán ser realizadas en espacios cerrados, que no permitan visibilidad desde el exterior y estar físicamente protegidos.

El PSC o CE se asegurará de que el acceso físico a los servicios críticos deben estar controlados y debe reducir al mínimo el riesgo de sus activos.

**Acceso físico a las instalaciones**

a) El acceso físico a las instalaciones que están relacionadas con el ciclo de vida del certificado, deberán limitarse a personas debidamente autorizadas.

b) Se debe aplicar controles para evitar la pérdida, el daño o el compromiso de los activos o la interrupción de las actividades del negocio; y

c) Se deben aplicar controles para evitar el compromiso o el robo de información.

En base a lo dicho anteriormente se recomienda: Zonas de acceso físico:

**Zona 1:** Las instalaciones destinadas a la gestión del ciclo de vida de los certificados, deberán encontrarse en un ambiente protegido físicamente con la finalidad de evitar el compromiso de los servicios a través del acceso no autorizado a los sistemas o datos. En esta zona todas las personas ajenas a las operaciones deberán ingresar acompañadas de personal autorizado, así como el personal autorizado debe ser identificado.

**Zona 2:** La protección física de esta zona se logra a través de la creación de perímetros de seguridad claramente definidos (es decir, barreras físicas). No se permite compartir con otras organizaciones esta zona, por lo que deberán estar fuera

de este perímetro cualquier otra actividad no relacionada con la AC. El acceso del personal autorizado debe quedar registrado y debe contar con al menos un (1) factor de seguridad (tarjeta electrónica, biometría y/o clave)

**Zona 3:** Los controles de seguridad física y ambiental se aplicarán para proteger los sistemas y las instalaciones, por lo que se deberán tener controles de protección contra desastres naturales, controles de seguridad contra incendios, controles ante fallas de servicios públicos (por ejemplo, energía, telecomunicaciones), colapso de la estructura, fugas en las tuberías, protección contra el robo, allanamiento de las instalaciones, etc. El acceso del personal autorizado y las actividades que en la misma se desarrollen, deben estar registradas con un sistema de circuito cerrado de TV. Así mismo el acceso debe quedar registrado y debe contar con al menos un (1) factor de seguridad (tarjeta electrónica, biometría y/o clave).

**Zona 4:** En esta zona se llevan a cabo las actividades críticas del PSC o CE, las funciones de la AC(s) y AR(s), la instalación física de la infraestructura de clave pública y equipos de comunicación, hardware criptográfico de la AC(s), hardware criptográfico de los signatarios. El acceso del personal autorizado a esta zona debe quedar registrado y debe ser dual, al menos contar con dos (2) factores de autenticación simultáneos (tarjeta electrónica, biometría y clave). Debe quedar registrada la actividad a través de circuito cerrado de TV.

Para entrar a la Zona 1 todo individuo deberá ser identificado y su ingreso registrado por personal autorizado.

**Acceso Lógico a los sistemas**

Los controles se llevarán a cabo para proteger los equipos, información, medios de comunicación y el software relacionado con la Servicios de la AC. El PSC o CE se asegurará de que el acceso al sistema se limite a las personas debidamente autorizadas. Debe quedar registrados los accesos y actividades en los sistemas, deben

habilitarse los logs de auditorías en base de datos y servicios relacionados a la ICP. Los mismos deben resguardarse como parte de la política de respaldo.

Los controles (por ejemplo, servidores de seguridad) se aplicarán para proteger a los dominios de la red interna de la ICP de accesos no autorizados por terceros en la red. Se recomienda configurar los cortafuegos para evitar accesos no autorizados dentro de las operaciones de la AC.

a) Los datos sensibles deberán estar protegidos contra el acceso o modificación no autorizada. Los datos sensibles serán protegidos (Por ejemplo, mediante el cifrado y un mecanismo de integridad) cuando se intercambian a través de redes que no son seguras. Los datos sensibles incluyen información de registro.

b) La AC deberá asegurar una gestión eficaz del usuario, esto incluye a los operadores, administradores y cualquier usuario que tiene acceso directo a los sistemas para mantener su seguridad, se recomienda incluir la gestión de cuentas de usuario, auditoría y la modificación puntual o eliminación del acceso en caso de ser necesario.

c) La AC deberá garantizar que el acceso a la información, sistemas o aplicaciones estén restringidos de acuerdo con la política de control de acceso y controles de seguridad informática, suficientes para la separación de funciones según los roles identificados en las prácticas de AC, incluyendo el administrador de seguridad y operación. En particular, el uso de programas o aplicaciones estará restringido y estrechamente controlado. Se limitará sólo a permitir el acceso a los recursos necesarios para llevar a cabo las funciones asignadas a ese usuario.

d) El personal de la AC deberá estar identificado y autenticado antes de utilizar aplicaciones críticas relacionadas con la gestión de certificados.

e) El personal de la AC deberán rendir cuentas de sus actividades (por ejemplo mediante el registro de eventos).

f) Los datos sensibles deberán estar protegidos de usuarios no autorizados, en caso de ser revelados a través de objetos de almacenamiento reutilizados (por ejemplo archivos borrados).

**Implementación del Sistema de Confianza y Mantenimiento**

El sistema de la AC debe asegurarse de usar sistemas y productos que aseguren la protección a alteraciones.

a) Un análisis de los requisitos de seguridad se llevará a cabo en la etapa de diseño y la especificación de los requisitos de cualquier proyecto de desarrollo de sistemas, realizado para la AC o en nombre de la AC para garantizar la seguridad.

b) Deben existir procedimientos de control de cambios para nuevas versiones, modificaciones y correcciones de software operacional.

**Cumplimiento de normas legales**

El PSC o CE deberá garantizar que se cumplen todos los requisitos legales aplicables de acuerdo al marco normativo nacional establecido. Algunos registros pueden necesitar ser retenidos de manera segura para cumplir con los requisitos legales.

**Resguardo de la información relacionada con el PSC o CE**

El PSC o CE se asegurará de que toda la información relevante al ciclo de vida de los certificados electrónicos sea resguardada por al menos diez (10) años, de acuerdo a lo establecido en el marco legal vigente (LSMDFE y su Reglamento), así como aquella que pueda servir como evidencia y/o prueba para propósitos legales.

#### 5.3.3.4.3 Estándares de Evaluación

- ISO/IEC 27002:2022

- ETSI 102 042 V 2.4.1

#### 5.3.3.4.4 Documentación Solicitada

Copia del documento correspondiente al Plan de Seguridad de Información.

#### 5.3.3.4.5 Detalles de la Evaluación

| Aspectos | Evaluación |
|---|---|

| | |
|---|---|
| **Relación entre el Plan de Seguridad y los recursos asignados** | Verificar que el PSC o CE pueda justificar la disponibilidad de los recursos y capacidades, para implementar los mecanismos y los recursos asignados por el procedimiento de seguridad |
| **Relación entre el Plan de Seguridad y Evaluación de Riesgos** | Comprobar que los procedimientos y mecanismos de seguridad permiten lograr el riesgo residual determinado en la Evaluación de Riesgos |
| **Relación entre Plan de Seguridad y Política de Seguridad** | Confirmar que los procedimientos y mecanismos de seguridad permiten lograr los objetivos de la Política de Seguridad |
| **Mantenimiento del Plan de seguridad** | Verificar que el Plan de Seguridad incluya los procedimientos que garanticen que la seguridad del PSC o CE, se mantienen en el tiempo ante cambios en: amenazas, personal, servicios, componentes tecnológicos, etc. |
| **Relación del Plan de Seguridad con las prácticas y política de certificación** | Verificar que los objetivos de seguridad enunciados en la DPC y PC del PSC o CE se logran a través del Plan de Seguridad |
| **Requerimientos ISO 27002:2022, Control 5** | Confirmar que los controles organizacionales del estándar ISO 27002:2022 están considerados (indicados en el Anexo N° 3) |
| **Requerimientos ISO 27002:2022, Control 6** | Verificar que se han tomado en cuenta los controles de personas del estándar ISO 27002:2022 (ver Anexo N° 3) |
| **Requerimientos ISO 27002:2022, Control 7** | Verificar que se han tomado en cuenta los controles físicos del estándar ISO 27002:2022 (ver Anexo N° 3) |
| **Requerimientos ISO 27002:2022, Control 8** | Verificar la inclusión de los controles tecnológicos del estándar ISO 27002:2022 (indicados en el Anexo N° 3) |
| **Administración de claves Criptográficas** | Verificar que el Plan de Seguridad contiene un Plan de Administración de Claves Criptográficas para todo el ciclo de vida de estas claves |
| **Protección del repositorio de acceso público** | Verificar que el Plan de Seguridad contiene medidas especiales de protección del repositorio público de certificados |
| **Protección de información privada** | Asegurarse de que el plan incluye medidas de protección de información privada recaudada durante el proceso de registro |
| **Acceso a la información** | Cumplimiento de los lineamientos sobre acceso físico y lógico |

#### 5.3.3.5 Implementación del Plan de Seguridad de la Información

##### 5.3.3.5.1 Objetivo

Comprobar que la organización tiene implementado un plan de seguridad coherente con su Política de Seguridad, que permita mostrar un nivel de confianza consistente con los objetivos del negocio.

#### 5.3.3.5.2 Descripción

El PSC o CE debe mostrar que sus procedimientos de administración de la seguridad y la capacidad de disponer de las instalaciones, están de acuerdo con el Plan de Seguridad.

Se evalúan:

- Acciones operacionales, procedimientos y mecanismos que permiten lograr los objetivos indicados en el Plan de Seguridad del PSC o CE.
- Controles desplegados o planificados para satisfacer dichos requerimientos.
- Que estos controles sean coherentes con los requerimientos del estándar ISO 27002:2022.

La evaluación combinará entrevistas con el personal del PSC o CE y auditorías que incluirán visitas a las instalaciones del PSC o CE para verificar la implementación práctica del plan.

#### 5.3.3.5.3 Estándares de Evaluación

- ISO 27002:2022

#### 5.3.3.5.4 Documentación Solicitada

- Documento descriptivo de la implementación del Plan de Seguridad de la Información del solicitante a PSC o CE, el cual será validado al momento de la auditoría.

#### 5.3.3.5.5 Detalles de la Evaluación

| Aspectos | Evaluación |
|---|---|
| **Relación entre el Plan de Seguridad y los recursos asignados** | Verificar que el PSC o CE dispone de los recursos y capacidades para implementar los mecanismos y procedimientos de seguridad |
| **Relación entre el plan de seguridad y política de seguridad** | Comprobar que los procedimientos y mecanismos de seguridad implementados permiten lograr los objetivos de la política de seguridad |

| | |
|---|---|
| **Relación entre Plan de Seguridad y Evaluación de Riesgos** | Verificar que los procedimientos y mecanismos de seguridad implementados permiten lograr el riesgo residual determinado en la Evaluación de Riesgos |
| **Mantenimiento del Plan de Seguridad** | Confirmar que la implementación del Plan de Seguridad incluye los procedimientos que garanticen que la seguridad del PSC o CE se mantiene en el tiempo ante cambios en: amenazas, personal, servicios, componentes tecnológicos, etc. |
| **Relación del Plan de Seguridad con la Declaración de Prácticas y la Política de Certificados** | Verificar que los objetivos de seguridad enunciados en la DPC y PC del PSC o CE se logran a través del Plan de Seguridad. |
| **Requerimientos ISO 27002:2022, Control 5** | Verificar que los controles organizacionales recomendados por el estándar ISO 27002:2022 están implementados (indicados en el Anexo N° 3) |
| **Requerimientos ISO 27002:2022, Control 6** | Verificar que los controles de personas recomendados por el estándar ISO 27002:2022 están implementados (ver Anexo N° 3) |
| **Requerimientos ISO 27002:2022, Control 7** | Confirmar la implementación de los controles físicos recomendados por el estándar 27002:2022 (ver Anexo N° 3) |
| **Requerimientos ISO 27002:2022, Control 8** | Comprobar que los controles tecnológicos recomendados por el estándar ISO 27002:2022 están implementados (ver Anexo N° 3) |
| **Protección del repositorio de acceso público** | Verificar que la implementación del Plan de Seguridad contiene medidas especiales de protección del repositorio público de certificados |
| **Protección de información privada** | Comprobar que la implementación del plan incluye medidas de protección de información privada recolectada durante el proceso de registro |

#### 5.3.3.6 Evaluación de la Plataforma Tecnológica

##### 5.3.3.6.1 Objetivo

Evaluar los elementos de seguridad de la plataforma tecnológica utilizada para la generación, publicación y administración de certificados de firma electrónica y LCR.

##### 5.3.3.6.2 Descripción

Evaluar la seguridad de los elementos que constituyen la plataforma tecnológica del PSC o CE. Se debe considerar los componentes de tipo hardware y software que

conforman la infraestructura PKI del PSC o CE, así como, todos los elementos de apoyo a su operación e interrelación, como protocolos y servicios.

Los elementos a considerar son:

- Módulo criptográfico.
- Módulo de Operación AC (Autoridad de Certificación)
- Módulo de Operación 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.

#### 5.3.3.6.3 Estándares de Evaluación

- FIPS 140-2

- ISO/IEC 15408 o equivalente.

#### 5.3.3.6.4 Documentación Solicitada

- 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 poder 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.

#### 5.3.3.6.5 Detalles de la Evaluación

| Aspectos | Evaluación |
|---|---|
| **Módulo criptográfico** | 1. Funcionalidad y operación:<br>● Generar pares de clave privada y pública con claves en los rangos 256/384/521 bits<br>● Capacidad de FIPS 140-2 Nivel 3<br>● Capacidad de firma y cifrado<br>2. Seguridad<br>● Existencia de sistema de control de acceso para acceder a la |

| | |
|---|---|
| | clave privada<br>● Existencia de controles de acceso para acceder a funcionalidades de firma y cifrado<br>3. Ciclo de vida<br>● Capacidad de respaldar la clave privada, en forma segura<br>● Capacidad de recuperar la clave privada de respaldo (back-up)<br>4. Auditoría<br>● Capacidad de generar logs auditables para administración de contingencia y accesos maliciosos<br>5. Documentación<br>● Manuales de operación, configuración y puesta en marcha<br>● Procedimiento de recuperación ante contingencia |
| **Módulo de Operación AC (Autoridad de Certificación)** | 1. Funcionalidad y operación:<br>● Servicios que presta la AC<br>● Interrelación de los servicios<br>● Capacidad para generar certificados con claves de al menos 256/384/521 bits, según corresponda al tipo de certificado emitido<br>● Capacidad de suspensión y revocación de certificados<br>● Capacidad para generar LCRs<br>● Indicar fecha de publicación y de nueva renovación de la LCR<br>● Capacidad para generar certificados de firma electrónica<br>● Capacidad de generar certificados de comunicación segura, entre AC y AR, si corresponde a la arquitectura (Specifies The Functions Needing A Trusted Channel CC P2 FTP_ITC.1)<br>● Capacidad de entregar certificados y LCR a directorios públicos X500<br>2. Seguridad.<br>● Existencia de sistema control de acceso para acceder a la generación de certificados (Generation of Secrets CC P2 FIA_SOS.2)<br>● Existencia de sistema de control de acceso para acceder a los sistemas de administración y auditoría (User authentication before any action CC P2 FIA_UAU.2)<br>3. Ciclo de vida.<br>● Capacidad de emitir, suspender y revocar certificados<br>● Capacidad de revocar certificado raíz y generar uno nuevo<br>4. Auditoría. |

| | |
|---|---|
| | ● Capacidad de generar log para administración de contingencia<br>● Actividades del personal autorizado y accesos maliciosos<br>5. Documentación<br>● Manuales de operación, configuración y puesta en marcha<br>● Procedimiento de recuperación ante contingencia |
| **Módulo de Operación AR (Autoridad de Registro)** | 1. Funcionalidad y operación:<br>● Servicios que presta la AC<br>● Interrelación de los servicios<br>● Capacidad de recibir requerimientos de certificados (Cryptographic key distribution CC P2 FCS_CKM.2)<br>● Solicitar certificado a la AC<br>2. Seguridad:<br>● Existencia de sistema control de acceso para acceder a la generación de certificados<br>● Existencia de sistema de control de acceso para acceder a los sistemas de administración y auditoría<br>3. Ciclo de vida:<br>● Capacidad de validación de datos de los certificados y solicitud de certificados a la AC<br>4. Auditoría:<br>● Capacidad de generar logs auditables para administración de contingencia y accesos maliciosos<br>5. Documentación:<br>● Manuales de operación, configuración y puesta en marcha<br>● Procedimiento de recuperación ante contingencia |
| **Módulo de Almacenamiento y Publicación de Certificados** | Almacenamiento de certificados en base de datos X500, y publicación a través de protocolos LDAP v2.0 y/o OCSP v1.0 |
| **Protocolos de comunicación entre AR y AC** | Capacidad de generar certificados de comunicación segura, entre AC y AR, si corresponde a la arquitectura, utilizando un protocolo estándar de SUSCERTE (Inter-TSF trusted channel CC P2 FTP_ITC.1) |
| **Elementos de administración de logs y auditoría** | Deben existir módulos de logs y de auditoría, que permitan verificar los intentos de acceso, los accesos y las operaciones dañinas, sean éstas intencionadas o no |

## 5.3.4.- Declaración de Prácticas de Certificación y Políticas de Certificado

### 5.3.4.1 Declaración de Prácticas de Certificación (DPC) y Políticas de Certificados (PC)

#### 5.3.4.1.1 Objetivo

Verificar que el PSC o CE disponga de un documento que señale los procedimientos de gestión de certificados y los diferentes tipos de certificados a otorgar, según se establecen en las normas SUSCERTE y los estándares internacionales. El enfoque de una Política de Certificado es significativamente diferente al de una Declaración de Prácticas de Certificación. Una Política de Certificados estructura los procedimientos de operación, instalaciones y el entorno computacional de una entidad de certificación. 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.

#### 5.3.4.1.2 Descripción

Los elementos principales que debe contener la DPC, son las delimitaciones de responsabilidad y las obligaciones tanto del PSC o CE, como del signatario.

Además debe quedar explícito, tanto el ciclo de vida de los certificados, desde su solicitud hasta el término de su vida útil, como el ciclo de vida del PSC o CE, desde el inicio hasta el fin del mismo.

Este requisito es relevante no sólo para el signatario del certificado sino para todas las entidades involucradas, incluyendo quienes reciben un documento firmado electrónicamente.

La DPC y PC deben ser revisadas y actualizadas anualmente, y aprobadas por las autoridades del PSC.

#### 5.3.4.1.3 Estándares de Evaluación

- RFC 3647

- ETSI TS 102 042
- CA/BR B
- CA/BR G

#### 5.3.4.1.4 Documentación Solicitada

Documento de la Declaración de Prácticas de Certificación (DPC) y Políticas de Certificados (PC) con los diferentes tipos de estructura de certificados (Norma SUSCERTE N° 022 y Norma SUSCERTE N° 032).

#### 5.3.4.1.5 Detalles de la Evaluación

| Aspectos | Evaluación |
|---|---|
| **Verificar estructura** | Verificar que la DPC contiene al menos los tópicos indicados en la Norma SUSCERTE N° 022 y la Norma SUSCERTE N° 032 |
| **Signatarios** | Se debe indicar a quién se le puede otorgar un certificado de firma electrónica |
| **Usos del certificado** | Se debe indicar los propósitos para el cual fue emitido el certificado y sus limitaciones, indicando cuáles usos son permitidos y cuáles no |
| **Publicación de información de la AC y Repositorios de los Certificados** | Se debe verificar la publicación de los certificados, LCR, y DPC, su frecuencia de publicación, así como la disponibilidad de los repositorios y sus controles de acceso |
| **Identificación y Autenticación** | Se debe comprobar el registro del nombre del signatario, la validación inicial de su identidad, así como la identificación y autenticación de las solicitudes de renovación y revocación de la clave |
| **Ciclo de vida de los certificados** | Confirmar que para cada etapa del ciclo de vida de los certificados (emisión/revocación/suspensión/renovación) estén establecidos los procedimientos y deberes del PSC o CE |
| **Controles de seguridad física, de gestión y de operaciones** | Se debe comprobar la existencia de los controles de seguridad física, funcionales, de seguridad personal, los procedimientos de control de seguridad, los archivos de informaciones y registros.<br>Además se debe contemplar que exista la documentación de procedimientos de la recuperación en caso de desastre y en caso del cese de la actividad del PSC o CE, que incluyan los |

| | |
|---|---|
| | procedimientos de término y de traspaso a otro PSC u organismo que asuma la responsabilidad de mantener la continuidad de los servicios, en tanto existan certificados vigentes |
| **Controles de Seguridad técnica** | Comprobar la existencia de las medidas de seguridad adoptadas por el PSC o CE para la generación e instalación de las claves privada y pública, la protección de la clave privada, los datos de activación.<br>Además se debe verificar los siguientes controles de seguridad: del computador, del ciclo de vida y de la red, así como los controles de ingeniería de los módulos criptográficos |
| **Perfiles de certificados, OCSP y LCR** | Se verificará que el perfil de los certificados cumpla con los estándares internacionales vigentes, aplicables para las infraestructuras de claves públicas y los certificados electrónicos.<br>En forma similar se verificará que el perfil de la LCR y el OCSP se adapten al estándar correspondiente |
| **Auditoría de conformidad** | Se debe verificar que el PSC o CE cumpla con la frecuencia de la realización de auditorías internas |
| **Aranceles y responsabilidad financiera** | Se refiere a las tasas establecidas para la emisión, renovación y revocación de certificados |
| **Confidencialidad de la información de los signatarios / protección de datos** | Existencia de procedimientos de protección de la información de los signatarios |
| **Obligaciones AC, AR, signatario** | Descripción de las obligaciones que contraen las entidades involucradas en la emisión y utilización de un certificado |
| **Las obligaciones y responsabilidades del PSC o CE** | Comprobar que exista una declaración de las obligaciones y deberes del PSC o CE |
| **Las obligaciones y responsabilidades del signatario** | Verificar que existan definiciones de los deberes y obligaciones de los signatarios |
| **Renuncias de garantías y limitación de responsabilidades** | Concordancia de la DPC y PC con los procedimientos operacionales |
| **Modificaciones** | Entre los requisitos comerciales y legales, todo PSC o CE |

| | |
|---|---|
| | debe tener procedimientos que especifiquen una autoridad que apruebe los cambios aplicables a su DPC, así como su publicación y notificación |
| **Validación Extendida** | La Declaración de Prácticas de Certificación de la AC, deberá incluir los puntos relacionados a "Implementación" y "Compromiso" correspondientes a las políticas de validación extendida del Estándar de la CA/Browser Forum (CA/Browser Forum Baseline Requirements) |
| **Organizaciones externas** | La Declaración de Prácticas de Certificación de la AC deberá identificar las obligaciones de todas las organizaciones externas de apoyo a los servicios de AC, incluyendo las políticas y prácticas aplicables |
| **Actualización y aprobación** | La Declaración de Prácticas de Certificación y las Políticas de Certificados serán revisadas y actualizadas una vez al año, así mismo debe ser aprobada por los representantes legales de la organización o aquella persona que tenga bajo su responsabilidad legal a la AC |

### 5.3.5. Organización

#### 5.3.5.1 Evaluación del Personal

##### 5.3.5.1.1 Objetivo

Verificar que el PSC o CE emplee personal calificado para la prestación de los servicios ofrecidos, en el ámbito de la firma electrónica y los procedimientos de seguridad y de gestión, con el fin de minimizar los riesgos de errores humanos, robos o mal uso de los atributos del cargo.

##### 5.3.5.1.2 Descripción

Se evaluará en conformidad al análisis de riesgos del PSC o CE que el personal que maneje o tenga acceso a sistemas e información sensible cumpla al menos con las siguientes condiciones:

a) Que tenga la calificación técnica o profesional requerida para el cargo o función que desempeña

b) Que tenga la experiencia mínima requerida para el cargo y función que desempeña

c) Que esté instruido en los procedimientos mínimos de seguridad que debe guardar en su función

Se evalúa el procedimiento que utiliza el PSC o CE para reclutar, seleccionar, evaluar y contratar personal crítico.

El personal de operaciones y sistemas no podrá tener acceso a funciones de confianza, hasta que todos sus antecedentes hayan sido verificados.

Los empleados que manejen información sensible, deben ser personal fijo, y deben existir contratos de confidencialidad que se extiendan más allá de la vigencia del contrato del empleado y/o empresa externa. Este documento debe estar basado en el estándar ETSI TS 102 042, sección 7.4.3.

#### 5.3.5.1.3 Estándares de Evaluación

- ISO 27002:2022
- ETSI TS 102 042

#### 5.3.5.1.4 Documentación Solicitada

- Perfiles de los cargos del personal que maneje información o sistemas sensibles
- Currículos de las personas que ocupan los cargos y funciones sensibles
- Evidencia de Identificación del personal calificado como crítico, durante la visita del experto designado por SUSCERTE, en la forma que él lo solicite (Presentación de CV, foto, huella biométrica, etc.)

#### 5.3.5.1.5 Detalles de la Evaluación

| Aspectos | Evaluación |
|---|---|
| **Experiencia profesional del personal crítico** | Se valida la experiencia del personal crítico que trabaja para el PSC o CE, verificando la concordancia de los perfiles en cada cargo y función, con el análisis de riesgos |
| **Capacitación del personal crítico en aspectos de seguridad acorde a su función y cargo.** | Se confirma que el personal crítico esté capacitado en las prácticas de seguridad que debe observar de acuerdo a su cargo y función |
| **Procedimiento de** | Se valida el procedimiento definido por el PSC o CE para la |

| | |
|---|---|
| **contratación del personal crítico** | contratación del personal crítico |
| **Requerimientos ETSI TS 102 042, sección 7.4.3** | Seguridad del Personal:<br>El PSC o CE se asegurará que el personal y las prácticas de contratación apoyarán a mejorar la fiabilidad de las operaciones de la AC.<br>En particular:<br>a) El PSC o CE deberá emplear un número suficiente de personas que posean el conocimiento y la experiencia necesaria para garantizar la calidad en los servicios que ofrecen y que sean calificados para la funciones de trabajo<br>El personal del PSC o CE puede cumplir con el requisito de "conocimiento experto, experiencia y calificación" a través de capacitación formal, experiencia actualizada o la combinación de ambas<br>b) Deberán existir sanciones disciplinarias apropiadas que se aplicarán al personal que viole las políticas o procedimientos de la AC<br>c) Las funciones y responsabilidades sobre seguridad, tal como se especifican en la política de seguridad de la AC, se documentan en la descripción del cargo. Las funciones sobre tareas de confianza, en el que la seguridad de la operación de la AC es dependiente, deberán ser claramente identificadas<br>d) El personal de la AC (fijos y contratados) deberán tener las descripciones de sus cargos definidos desde el punto de vista de: separación de funciones y los mínimos privilegios, determinación de la sensibilidad del cargo basadas en sus funciones y niveles de acceso, investigación de antecedentes y conocimientos del empleado. En su caso, éstas establecerán diferencias entre las funciones generales y las funciones específicas en la AC. Las descripciones de trabajo pueden incluir habilidades y requisitos de experiencia<br>e) El personal deberá ejercer la administración y gestión de procedimientos que están en línea con los procesos de seguridad de la información<br>Nota: véase la norma ISO/IEC 27002:2022 para la orientación.<br>El registro, generación de certificados, prestación de servicios con dispositivos, gestión de la revocación<br>f) El personal directivo deberá emplear o contratar a quienes posean experiencia o capacitación en tecnología de firma |

| | |
|---|---|
| | electrónica y estén familiarizados con los procedimientos de seguridad para el personal con responsabilidades de protección, seguridad de la información y la evaluación del riesgo suficiente para llevar a cabo las funciones de gestión<br>g) Todo el personal del PSC o CE en los roles de confianza deberán estar libres de intereses que pudieran perjudicar la imparcialidad de las operaciones<br>h) Los roles de confianza incluyen roles relacionados con las siguientes responsabilidades:<br>1) Oficiales de Seguridad: la responsabilidad general de la administración de la aplicación de las prácticas de seguridad. Adicionalmente aprobar la generación/revocación/suspensión de certificados<br>2) Los administradores del sistema: autorización para instalar, configurar y mantener los sistemas de la AC para el registro, generación de certificados, la provisión y prestación de servicios con dispositivos, gestión de la revocación<br>3) Los operadores del sistema: responsables de la operación diaria de los sistemas de la AC. Está autorizado para realizar la copia de seguridad y recuperación del sistema<br>4) Los auditores del sistema: autorizado para ver los archivos y registros de auditoría de los sistemas de la AC.<br>i) La alta dirección será la responsable de nombrar oficialmente al personal con roles de confianza.<br>j) El PSC o CE no nombrará en roles de confianza a personas que tengan una condena por un delito grave u otro delito que afecte a su idoneidad para el cargo. El personal no tendrá acceso a las funciones de confianza hasta que se completen todas las comprobaciones necesarias.<br>En algunos países no puede ser posible para la AC obtener información sobre las condenas anteriores. Cuando sea así, se recomienda que el empleador le pida al candidato proporcionar dicha información y rechazar la solicitud en caso de que sea negativa. |

### 5.3.6 Reconocimiento de los Certificados de la Cadena de Confianza

#### 5.3.6.1 Inclusión de Certificado Raíz de PSC o CE en Herramientas Tecnológicas

##### 5.3.6.1.1 Objetivo

Verificar el cumplimiento por parte del PSC o CE en la inclusión del Certificado Raíz en herramientas y aplicaciones tecnológicas, que permita establecer confianza en la identidad de los certificados utilizados.

#### 5.3.6.1.2 Descripción

Dado que el producto principal de un PSC o CE es la confianza en la identidad digital, esta se debe garantizar en el ámbito nacional al momento del empleo de herramientas y aplicaciones para navegar en páginas web, procesamiento de palabras, correo electrónico, entre otras; que implementen certificados emitidos por los PSC o CE.

La inclusión del Certificado Raíz en herramientas y aplicaciones tecnológicas requiere lo siguiente:

**1.** Estudio de factibilidad de inclusión en las distintas herramientas y aplicaciones tecnológicas, tanto privativas como no privativas, garantizando así el cumplimiento de la Ley Infogobierno en materia de Tecnologías Libres

**2.** Contar con la validación de SUSCERTE, para continuar con el proceso de incorporación en las herramientas y aplicaciones validadas

**3.** Crear la petición de solicitud de inclusión en cada herramienta o aplicación requerida

**4.** Someterse a un proceso de verificación de las políticas, estándares y documentación relacionada con el Certificado Raíz del PSC o CE, por parte de la organización donde se desea incluir el Certificado de la AC

**5.** Reunir los requisitos exigidos por parte de la organización donde se solicita la inclusión, tales como:

**1.** **Generales**. Información sobre el PSC o CE: creación, naturaleza, misión, visión, objetivos, sector atendido, entre otros.

**2.** **Técnicos.** Información sobre el Certificado Raíz, Nombre del Certificado, Nombre Común, Resumen, URL del Certificado, Huella, Validez, Versión, Parámetros de las llaves de firma, URL página web, Certificados de ejemplo, CRL, OCSP, Solicitud de bits de confianza, Validación SSL, Jerarquía, Firmas Cruzadas, entre otros

3. **Documentación de políticas y prácticas.** Información referente a la operación del PSC o CE, disponible tanto en idioma nativo como en idioma inglés que incluye: DPC, PC, acuerdos para firmas cruzadas, auditorías, procedimientos de verificación de SSL y de correo electrónico, procedimientos de firma de código, entre otros; así como cualquier otro que sea requerido por la organización donde se procese la inclusión
4. **Informar mensualmente a SUSCERTE** sobre el estatus del reporte, a partir de la creación de la petición de inclusión
5. **Disponer del recurso humano y tecnológico**, para el logro de la meta en el tiempo mínimo dispuesto por la organización referente para la inclusión; así como para la consecución de los objetivos del Estado, en materia de certificación electrónica
6. **Cumplir con todas las condiciones** que no se encuentren en este apartado, pero que sean exigidas por la organización a quien se solicita la inclusión, siempre y cuando no se contradiga lo dispuesto en las normativas legales y sublegales que apliquen en materia de certificación electrónica

#### 5.3.6.1.3 Estándares de Evaluación

**1.** X.509v3
**2.** ETSI 102 042 v2.4.1
**3.** RFC 4346
**4.** CA/BR G
**5.** CA/BR B

#### 5.3.6.1.4 Documentación Solicitada

- Copia electrónica del documento correspondiente a la evaluación de la documentación del PSC o CE y pruebas técnicas requeridas.
- Copia electrónica de la tramitación, aprobación o negación, tal sea el caso, de la inclusión del Certificado Raíz en los Navegadores Web.

#### 5.3.6.1.5 Detalles de la Evaluación

| Aspectos | Evaluación |
|---|---|
| **Generales** | ● Verificar la información propia del PSC o |

| | |
|---|---|
| | CE facilitada a los navegadores web<br>● Validar la petición o solicitud de inclusión en los navegadores web |
| **Técnicos** | ● Verificar la información del Certificado Raíz suministrada por el PSC o CE a la organización que provee el navegador web.<br>● Validar la disponibilidad de la LCR y el servicio de OCSP del PSC o CE |
| **Documentación** | ● Verificar que la documentación relacionada con el Certificado Raíz del PSC o CE requerida por el navegador web esté en idioma inglés |
| **Personal** | ● Verificar que exista un personal asignado al seguimiento de la solicitud de inclusión |

## 6. PARTE FINAL

### 6.1. Disposiciones transitorias

A partir de la fecha de publicación en gaceta de esta Norma, el PSC o Caso Especial, deberá iniciar un proceso de adecuación de máximo de doce (12) meses contados a partir de la fecha de publicación. Durante ese lapso el PSC o CE debe consignar ante SUSCERTE informes trimestrales donde se evidencie el alcance y avance de esta actualización.

### 6.2 Disposiciones finales

Si los estándares y recomendaciones internacionales utilizados para la elaboración de esta norma son actualizados o reemplazados, SUSCERTE puede solicitar a los PSC o CE aplicar dichos cambios a fin de garantizar el funcionamiento óptimo de la Infraestructura Nacional de Certificación Electrónica.

## 7. ANEXOS NORMATIVOS

### Anexo No 1 Resumen de Recaudos Técnicos para la Acreditación o Renovación

| Nº | Nombre de Recaudo | Normas y Guías | Documentación Solicitada |
|---|---|---|---|
| **T01 Infraestructura de Clave Pública. Perfiles de Certificado y Servicios de Publicación** | | | |
| **T01.1** | Estructura e | - ITU-T Rec. X.509 | - Modelo de la solicitud de firma del |

| | | | |
|---|---|---|---|
| | Información del Certificado Electrónico | - ISO/IEC 9594-8<br>- ITU-T X.690<br>- Norma SUSCERTE N° 032 | certificado (CSR), en caso de acreditación. |
| **T01.2** | Estructura de la Lista de Certificados Revocados (LCR) y OCSP – Online Certificate Status Protocol | - RFC 5280 y actualizaciones<br>-Norma SUSCERTE N° 032<br>- RFC 2560 | - DPC y PC del PSC o CE<br>- LCR emitida por el PSC o CE en evaluación y el certificado de firma electrónica de la AC que la emite<br>- Reportes de solicitudes y/o peticiones al servicio(OCSP) |
| **T01.3** | Registro de acceso público | No aplica | Documento descriptivo que contenga al menos la siguiente información:<br>- Detalle del sitio Web donde publicará la información.<br>- Descripción de la tecnología.<br>- Disponibilidad, accesibilidad, conexión, esquemas y diagramas de funcionamiento.<br>- Medidas de seguridad.<br>- Sitio Web de prueba con las funcionalidades requeridas.<br>- Publicación y vigencia de DPC y PC<br>- Publicación y vigencia de la LCR |
| **T01.4** | Modelo de confianza | No aplica | Documento en el que se describe el modelo de confianza utilizado por el PSC o CE para lograr el objetivo o alternativamente la DPC y PC si contiene dicho punto. |
| **T02 Seguridad** | | | |
| **T02.1** | Evaluación de riesgos | Cualquier referencia normativa, por ejemplo: ISO 27005, NIST SP 800 30, Magerit , CRAMM, OCTAVE, MEHARI, u otro estándar reconocido | Copia del documento correspondiente a la Evaluación de Riesgos o documento equivalente. |
| **T02.2** | Política de seguridad | - ISO/IEC 27002:2022 | - Copia del documento correspondiente |

| | | | |
|---|---|---|---|
| | de la información | | a la política de seguridad de la organización.<br>- Documento en el cual se describa formalmente la estructura organizativa del PSC o CE, aprobada por las autoridades de la Institución |
| **T02.3** | Plan de continuidad del negocio y recuperación ante desastres. | - ISO/IEC 27002:2022<br>- ETSI TS 102 042 | - Documento de Planes de Continuidad del Negocio y Recuperación de Desastres.<br>- Documento de Evaluación de Riesgo |
| **T02.4** | Plan de seguridad de la información | - ISO/IEC 27002:2022<br>- ETSI TS 102 042 | Copia del documento correspondiente al Plan de Seguridad de Información. |
| **T02.5** | Implementación del plan de seguridad de la información. | - Declaración de Aplicabilidad de controles (SOA) del Anexo “A”. ISO 27002:2022 | Documento descriptivo de la implementación del Plan de Seguridad de la Información del solicitante a PSC o CE, el cual será validado al momento de la auditoría. |
| **T02.6** | Plan de administración de claves criptográficas. | - ETSI TS 102 042<br>- FIPS 140-1<br>- FIPS 140-2<br>- FIPS 140-3<br>- CABR B<br>- CABR G | Documento descriptivo de la implementación del Plan de Administración de Claves Criptográficas de la Organización |
| **T03 Plataforma Tecnológica** | | | |
| **T03.1** | Evaluación de la plataforma tecnológica | - FIPS 140-2 o FIPS 140-3<br>- ISO/IEC 15408 o equivalente | - Documento descriptivo de la implementación de la infraestructura tecnológica.<br>Este documento debe incluir al menos, planos de interconexión de sistemas, cableado de red de datos, cableado de poder principal y auxiliar, dispositivos de seguridad y control de acceso, y todo aquello relevante que permita demostrar la confiabilidad de la infraestructura tecnológica.<br>- Manuales del fabricante de los productos hardware y software relevantes.<br>- Documentación del fabricante que |

| | | | |
|---|---|---|---|
| | | | acredite el correspondiente nivel de seguridad |
| **T04 Políticas de Certificación** | | | |
| **T04.1** | Declaración de Prácticas de Certificación y Políticas de Certificado | - RFC 3647<br>- ETSI TS 102 042<br>- CA/BR B<br>- CA/BR G | Documento de la Declaración de Prácticas de Certificación (DPC) y Política de Certificados (PC) con los diferentes tipos de estructura de campos de certificados. (Norma SUSCERTE N° 022) |
| **T04.2** | Modelo y Manual de Operación de la Autoridad de Certificación (AC) del PSC o CE | - ETSI TS 102 042<br>- CA/BR<br>- RFC 3647 | - Modelo y Manual de operación de la AC principal y/o subordinadas del PSC o CE<br>- Manual del Hardware Criptográfico usados para la generación y protección de las claves privadas de la(s) autoridades de certificación |
| **T04.3** | Modelo y Manual de Operación de la Autoridad de Registro (AR) | - ETSI TS 102 042<br>- CA/BR B<br>- CA/BR G<br>- RFC 3647 | - Modelo y Manual de Operación de la AR<br>- Manual técnico de los dispositivos seguros de firma electrónica |
| **T05 Modelo Organizacional** | | | |
| **T05.1** | Estructura organizativa | - ISO/IEC 27002:2022<br>- ETSI TS 102 042 | Describiendo las unidades y cantidad de personas dedicadas a las labores relacionadas a la solicitud |
| **T05.2** | Evaluación del personal | - ISO/IEC 27002:2022<br>- ETSI TS 102 042 | - Perfiles de los cargos del personal que maneja información o sistemas sensibles Currículos de las personas que ocupan los cargos y funciones sensibles.<br>- Evidencia de Identificación del personal calificado como crítico, durante la visita del experto designado por la Superintendencia, en la forma que él lo solicite (Presentación de CV, foto, huella biométrica, etc.) |

## Anexo N° 2 Ejemplo Matriz de Riesgos

| Matriz de Evaluación de riesgos | | ID | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | Amenazas | Allanamiento (ilegal, legal) | Persecución (civil, fiscal, penal) | Orden de secuestro / Detención | Sabotaje (ataque físico y electrónico) | Daños por vandalismo | Extorsión | Fraude / Estafa | Robo / Hurto (físico) | Robo / Hurto de información electrónica | Intrusión a Red interna |
| **Activos** | **Clasificación** | | 2 | 1 | 1 | 3 | 3 | 2 | 1 | 3 | 3 | 3 |
| Documentos Institucionales (Proyectos, Planes de recuperación ante desastre, informes de auditoría, etc.) | **De Uso Interno** | 2 | | | | | | | | | | |
| Base de datos AC | **Confidencial** | 3 | | | | | | | | | | |
| Base de datos AR | **Confidencial** | 3 | | | | | | | | | | |
| Portal web interno | **De Uso Interno** | 2 | | | | | | | | | | |
| Portal web externo | **De Uso Público** | 3 | | | | | | | | | | |
| Correo electrónico | **Confidencial** | 2 | | | | | | | | | | |
| Respaldos | **Confidencial** | 3 | | | | | | | | | | |

## Anexo N° 3 Controles del Estándar ISO/IEC 27002:2022, Controles del 5 al 8, Aplicables

### CONTROL 5 Controles Organizacionales

#### 5.1 Política de Seguridad de la Información

**Control**: La política de seguridad de la información y las políticas específicas del tema deben ser definidas, aprobadas por la gerencia, publicadas, comunicadas, reconocidas por el personal relevante, las partes interesadas, revisadas a intervalos planificados y si ocurren cambios significativos.

**Objetivo:** Garantizar la idoneidad, la adecuación y la eficacia continua de la dirección de gestión y el apoyo a la seguridad de la información de acuerdo con los requisitos comerciales, legales, estatutarios, reglamentarios y contractuales.

#### 5.2 Roles y Responsabilidades de Seguridad de la Información

**Control**: Los roles y responsabilidades de seguridad de la información deben definirse y asignarse de acuerdo con las necesidades de la organización.

**Objetivo:** Establecer una estructura definida, aprobada y entendida para la implementación, operación y gestión de la seguridad de la información dentro de la organización.

#### 5.3 Segregación de Funciones

**Control**: Deben segregarse los deberes conflictivos y las áreas conflictivas de responsabilidad.

**Objetivo**: Reducir el riesgo de fraude, error y elusión de los controles de seguridad de la información.

#### 5.4 Responsabilidades de la Dirección

**Control:** La gerencia debe exigir a todo el personal que aplique la seguridad de la información de acuerdo con la Política de Seguridad de la Información establecida, las políticas y los procedimientos específicos del tema de la organización.

**Objetivo**: Asegurar que la Gerencia comprenda su papel en la seguridad de la información y

emprender acciones destinadas a garantizar que todo el personal conozca y cumpla con sus responsabilidades de seguridad de la información.

### 5.5 Contacto con las Autoridades

**Control**: La organización debe establecer y mantener contacto con las autoridades pertinentes.

**Objetivo**: Garantizar que se produzca un flujo de información adecuado con respecto a la seguridad de la información entre la organización y las autoridades legales, reguladoras y de supervisión pertinentes.

### 5.7 Inteligencia de Amenazas

**Control:** La información relacionada con las amenazas a la seguridad de la información debe recopilarse y analizarse para generar información sobre amenazas.

**Objetivo**: Proporcionar conciencia del entorno de amenazas de la organización para que se puedan tomar las medidas de mitigación adecuadas.

### 5.8 Seguridad de la Información en la Gestión de Proyectos

**Control:** La seguridad de la información debe integrarse en la gestión de proyectos.

**Objetivo**: Para garantizar que los riesgos de seguridad de la información relacionados con proyectos y entregables, se aborden de manera efectiva en la gestión de proyectos a lo largo del ciclo de vida del proyecto.

### 5.9 Inventario de Información y otros Activos Asociados

**Control**: Se debe desarrollar y mantener un inventario de información y otros activos asociados, incluidos los propietarios.

**Objetivo**: Identificar la información de la organización y otros activos asociados con el fin de preservar su seguridad de la información y asignar la propiedad adecuada.

### 5.10 Uso aceptable de la Información y otros Activos Asociados

**Control**: Deben identificarse, documentarse e implementar reglas para el uso aceptable y procedimientos para el manejo de la información y otros activos asociados.

**Objetivo**: Para garantizar que la información y otros activos asociados se protejan, utilicen y manejen adecuadamente.

### 5.11 Devolución de Bienes

**Control:** El personal y otras partes interesadas, según corresponda, deben devolver todos los activos de la organización que estén en su poder al cambiar o terminar su empleo, contrato o acuerdo.

**Objetivo**: Para proteger los activos de la organización como parte de cambio o terminación de empleo, contrato o acuerdo.

### 5.12 Clasificación de la Información

**Control**: La información debe clasificarse de acuerdo con las necesidades de seguridad de la información de la organización en función de la confidencialidad, la integridad, la disponibilidad y los requisitos pertinentes de las partes interesadas.

**Objetivo**: Asegurar la identificación y comprensión de las necesidades de protección de la información de acuerdo con su importancia para la organización.

### 5.13 Etiquetado de la Información

**Control**: Se debe desarrollar e implementar un conjunto apropiado de procedimientos para el etiquetado de la información de acuerdo con el esquema de clasificación de la información adoptado por la organización.

**Objetivo**: Facilitar la comunicación de la clasificación de la información y apoyar la automatización del procesamiento y la gestión de la información.

### 5.14 Transferencia de Información

**Control**: Deben existir reglas, procedimientos o acuerdos de transferencia de información para

todos los tipos de instalaciones de transferencia dentro de la organización y entre la organización y otras partes.

**Objetivo**: Para mantener la seguridad de la información transferida dentro de una organización y con cualquier parte externa interesada.

### 5.15 Control de Acceso

**Control**: Las reglas para controlar el acceso físico y lógico a la información y otros activos asociados deben establecerse e implementarse en función de los requisitos comerciales y de seguridad de la información.

**Objetivo**: Para garantizar el acceso autorizado y evitar el acceso no autorizado a la información y otros activos asociados.

### 5.16 Gestión de Identidad

**Control**: Debe gestionarse el ciclo de vida completo de las identidades.

**Objetivo**: Permitir la identificación única de personas y sistemas que acceden a la información de la organización y otros activos asociados y permitir la asignación adecuada de derechos de acceso.

### 5.17 Información de Autenticación

**Control**: La asignación y gestión de la información de autenticación debe controlarse mediante un proceso de gestión, incluido el asesoramiento al personal sobre el manejo adecuado de la información de autenticación.

**Objetivo**: Para garantizar la autenticación adecuada de la identidad y evitar fallas en los procesos de autenticación.

### 5.18 Derechos de Acceso

**Control:** Los derechos de acceso a la información y otros activos asociados deben proporcionarse, revisarse, modificarse y eliminarse de acuerdo con las políticas y las reglas de

control de acceso específicas del tema de la organización.

**Objetivo**: Para garantizar que el acceso a la información y otros activos asociados se defina y autorice de acuerdo con los requisitos comerciales.

### 5.19 Abordar la seguridad de la información en los acuerdos con proveedores

**Control**: Los requisitos de seguridad de la información pertinentes deben establecerse y acordarse con cada proveedor en función del tipo de relación.

**Objetivo**: Mantener un nivel acordado de seguridad de la información en las relaciones con los proveedores.

### 5.20 Planificación preparación de la gestión de incidentes de Seguridad de la información

**Control**: La organización debe planificar y prepararse para la gestión de incidentes de seguridad de la información definiendo, estableciendo y comunicando procesos, funciones y responsabilidades de gestión de incidentes de seguridad de la información.

**Objetivo**: Garantizar una respuesta rápida, eficaz, coherente y ordenada a los incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad de la información.

### 5.21 Evaluación y decisión sobre eventos de seguridad de la información

**Control**: La organización debe evaluar los eventos de seguridad de la información y decidir si se clasifican como incidentes de seguridad de la información.

**Objetivo:** Para asegurar una categorización y priorización efectiva de los eventos de seguridad de la información.

### 5.22 Respuesta a Incidentes de seguridad de la información

**Control**: Se debe responder a los incidentes de seguridad de la información de acuerdo con los procedimientos documentados.

**Objetivo**: Garantizar una respuesta eficiente y eficaz a los incidentes de seguridad de la información.

### 5.23 Aprendiendo de los incidentes de seguridad de la información

**Control**: El conocimiento obtenido de los incidentes de seguridad de la información debe utilizarse para fortalecer y mejorar los controles de seguridad de la información.

**Objetivo**: Para reducir la probabilidad, recurrencia o las consecuencias de futuros incidentes.

### 5.24 Recopilación de pruebas

**Control**: La organización debe establecer e implementar procedimientos para la identificación, recopilación, adquisición y preservación de evidencia relacionada con eventos de seguridad de la información.

**Objetivo**: Asegurar una gestión consistente y eficaz de la evidencia relacionada con los incidentes de seguridad de la información para efectos de acciones disciplinarias y legales.

### 5.25 Seguridad de la información durante la interrupción

**Control**: La organización debe planificar cómo mantener la seguridad de la información en un nivel adecuado durante la interrupción.

**Objetivo**: Para proteger la información y otros activos asociados durante la interrupción.

### 5.26 Preparación de las TIC para la continuación del negocio

**Control**: La preparación de las TIC debe planificarse, implementarse, mantenerse y probarse en función de los objetivos de continuidad del negocio y los requisitos de continuidad de las TIC.

**Objetivo**: Para garantizar la disponibilidad de la información de la organización y otros activos asociados durante la interrupción.

### 5.27 Requisitos legales, estatutarios, reglamentarios y contractuales

**Control:** Los requisitos legales, estatutarios, reglamentarios y contractuales relevantes para la

seguridad de la información y el enfoque de la organización. Para cumplir con estos requisitos deben identificarse, documentarse y mantenerse actualizados.

**Objetivo**: Asegurar el cumplimiento de los requisitos legales, estatutarios, reglamentarios y contractuales relacionados con la seguridad de la información.

### 5.28 Derechos de propiedad intelectual

**Control**: La organización debe implementar procedimientos apropiados para proteger los derechos de propiedad intelectual.

**Objetivo**: Para garantizar el cumplimiento de los requisitos legales, estatutarios, reglamentarios y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos patentados.

### 5.29 Protección de registros

**Control**: Los registros deben protegerse contra pérdida, destrucción, falsificación, acceso no autorizado y publicación no autorizada.

**Objetivo**: Para garantizar el cumplimiento de los requisitos legales, estatutarios, reglamentarios y contractuales, así como las expectativas de la comunidad o la sociedad relacionadas con la protección y disponibilidad de los registros.

### 5.30 Privacidad y protección de la Información de Identificación Personal (PII)

**Control**: La organización debe identificar y cumplir los requisitos relacionados con la preservación de la privacidad y la protección de la PII de acuerdo con las leyes y reglamentos aplicables y los requisitos contractuales.

**Objetivo**: Para garantizar el cumplimiento de los requisitos legales, estatutarios, reglamentarios y contractuales relacionados con los aspectos de seguridad de la información de la protección de PII.

### 5.31 Revisión independiente de la seguridad de la información

**Control**: El enfoque de la organización para gestionar la seguridad de la información y su implementación, incluidas las personas, los procesos y las tecnologías, debe revisarse de forma independiente a intervalos planificados o cuando se produzcan cambios significativos.

**Objetivo**: Asegurar la idoneidad, adecuación y eficacia continuas del enfoque de la organización para gestionar la seguridad de la información.

### 5.32 Cumplimiento de políticas, normas y estándares de seguridad de la información

**Control**: El cumplimiento de la Política de Seguridad de la Información de la organización, las políticas específicas del tema, las reglas y los estándares debe revisarse periódicamente.

**Objetivo**: Para garantizar que la seguridad de la información se implemente y opere de acuerdo con la Política de Seguridad de la Información de la organización, las políticas, las reglas y los estándares específicos del tema.

### 5.33 Procedimientos operativos documentados

**Control**: Los procedimientos operativos para las instalaciones de procesamiento de información deben documentarse y ponerse a disposición del personal que los necesite.

**Objetivo**: Garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de información.

## Control 6 Controles de Personas

### 6.1 Selección

**Control**: Los controles de verificación de antecedentes de todos los candidatos para convertirse en personal deben llevarse a cabo antes de unirse a la organización y de manera continua, teniendo en cuenta las leyes, regulaciones y ética aplicables, deben ser proporcionales a los requisitos comerciales, la clasificación de la información a la que se accede y los riesgos percibidos.

**Objetivo**: Asegurar que todo el personal sea elegible y adecuado a las funciones para las que se les consideren, siga siendo elegible y adecuado durante su empleo.

### 6.2 Términos y condiciones de empleo

**Control**: Los acuerdos contractuales de empleo deben establecer las responsabilidades del personal y de la organización para la seguridad de la información.

**Objetivo**: asegurar que el personal comprenda sus responsabilidades de seguridad de la información para sus funciones.

### 6.3 Concientización, educación y capacitación en seguridad de la información

**Control**: El personal de la organización y las partes interesadas relevantes deben recibir educación y capacitación adecuadas sobre la seguridad de la información y actualizaciones regulares de la Política de Seguridad de la Información de la organización, las políticas y los procedimientos específicos del tema, según sea relevante para su función laboral.

**Objetivo**: Asegurar que el personal y las partes interesadas relevantes conozcan y cumplan con sus responsabilidades de seguridad de la información.

### 6.4 Proceso disciplinario

**Control**: Se debe formalizar y comunicar un proceso disciplinario para tomar acciones contra el personal y otras partes interesadas relevantes que hayan cometido una violación de la política de seguridad de la información.

**Objetivo**: Asegurar que el personal y otras partes interesadas relevantes entiendan las consecuencias de la violación de las política de seguridad de la información, para disuadir y tratar adecuadamente al personal y otras partes interesadas relevantes que cometieron la violación.

### 6.5 Responsabilidades después de la terminación o cambio de empleo

**Control**: Las responsabilidades y deberes de seguridad de la información que siguen siendo válidos después de la terminación o el cambio de empleo deben definirse, aplicarse y

comunicarse al personal pertinente y otras partes interesadas.

**Objetivo**: Para proteger los intereses de la organización como parte del proceso de cambio terminación de empleo o contratos.

### 6.6 Acuerdos de confidencialidad o no divulgación

**Control:** Los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información deben ser identificados, documentados, revisados regularmente y firmados por el personal y otras partes interesadas relevantes.

**Objetivo**: Para mantener la confidencialidad de la información accesible por el personal o partes externas.

### 6.7 Trabajo a distancia

**Control**: Se deben implementar medidas de seguridad cuando el personal trabaja de forma remota para proteger la información a la que se accede, procesa o almacena fuera de las instalaciones de la organización.

**Objetivo**: Para garantizar la seguridad de la información cuando el personal está trabajando de forma remota.

### 6.8 Reporte de eventos de seguridad de la información

**Control:** La organización debe proporcionar un mecanismo para que el personal informe eventos de seguridad de la información observados o sospechados a través de los canales apropiados de manera oportuna.

**Objetivo**: Para respaldar la notificación oportuna coherente y eficaz de los eventos de seguridad de la información que puedan ser identificados por el personal.

## Control 7 Controles Físicos

### 7.1 Perímetros de seguridad física

**Control**: Los perímetros de seguridad deben definirse y utilizarse para proteger las áreas que contienen información y otros activos asociados.

**Objetivo**: Para evitar el acceso físico no autorizado, el daño y la interferencia a la información de la organización y otros activos asociados.

### 7.2 Entrada física

**Control**: Las áreas seguras deben estar protegidas por controles de entrada y puntos de acceso apropiados.

**Objetivo**: Garantizar sólo el acceso físico autorizado a la información de la organización y otros activos asociados.

### 7.3 Seguridad de oficinas, Salas e instalaciones

**Control**: Debe diseñarse e implementarse la seguridad física de las oficinas, salas e instalaciones.

**Objetivo**: Prevenir el acceso físico no autorizado, el daño y la interferencia a la información de la organización y otros activos asociados en las oficinas, salas e instalaciones.

### 7.4 Supervisión de la seguridad física

**Control**: Las instalaciones deben ser monitoreadas continuamente para detectar accesos físicos no autorizados.

**Objetivo**: Para detectar y disuadir el acceso físico no autorizado.

### 7.5 Protección contra amenazas físicas y ambientales

**Control**: Se debe diseñar e implementar la protección contra amenazas físicas y ambientales, como desastres naturales y otras amenazas físicas intencionales o no intencionales a la infraestructura.

**Objetivo**: Prevenir o reducir las consecuencias de eventos originados por amenazas físicas y

ambientales.

### 7.6 Trabajar en áreas seguras

**Control**: Se deben diseñar e implementar medidas de seguridad para trabajar en áreas seguras.

**Objetivo**: Para proteger la información y otros activos asociados en áreas seguras contra daños e interferencias no autorizadas por parte del personal que trabaja en estas áreas.

### 7.7 Escritorio despejado y pantalla despejada

**Control**: Deben definirse y aplicarse adecuadamente reglas de escritorio limpio para documentos y medios de almacenamiento extraíbles y reglas de pantalla limpia para las instalaciones de procesamiento de información.

**Objetivo**: Para proteger la información y otros activos asociados en áreas seguras contra daños e interferencias no autorizadas por parte de personal que trabaja en estas áreas.

### 7.8 Ubicación y protección del equipo

**Control:** El equipo debe estar ubicado de forma segura y protegida.

**Objetivo**: Reducir los riesgos de amenazas físicas, ambientales, de accesos y daños no autorizados.

### 7.9 Seguridad de los activos fuera de las instalaciones

**Control**: Los activos fuera del sitio deben estar protegidos.

**Objetivo:** Para evitar la pérdida, el daño, el robo o el compromiso de los dispositivos externos y la interrupción de las operaciones de la organización.

### 7.10 Medios de almacenamiento

**Control**: Los medios de almacenamiento deben gestionarse a lo largo de su ciclo de vida de adquisición, uso, transporte y eliminación de acuerdo con el esquema de clasificación y los requisitos de manipulación de la organización.

**Objetivo**: Para garantizar sólo la divulgación, modificación, eliminación o destrucción autorizadas de la información almacenada.

### 7.11 Utilidades de apoyo

**Control**: Las instalaciones de procesamiento de información deben estar protegidas contra cortes de energía y otras interrupciones causadas por fallas en los servicios públicos de apoyo.

**Objetivo**: Para evitar la pérdida, el daño o el compromiso de la información y otros activos asociados o la interrupción de las operaciones de la organización debido a fallas e interrupciones de los servicios públicos de apoyo.

### 7.12 Seguridad del cableado

**Control**: Los cables que transportan energía, datos o servicios de información de apoyo deben protegerse contra intercepciones, interferencias o daños

**Objetivo**: Para evitar la pérdida, daño, robo o el compromiso de la información y otros activos asociados a la interrupción de las operaciones de la organización, relacionadas con el cableado de energía y comunicaciones.

### 7.13 Mantenimiento de equipos

**Control:** El equipo debe mantenerse correctamente para garantizar la disponibilidad, integridad y confidencialidad de la información.

**Objetivo**: Para evitar la pérdida, daño, robo o compromiso de la información y otros activos asociados, así como la interrupción de las operaciones de la organización, causadas por la falta de mantenimiento.

### 7.14 Eliminación segura o reutilización de equipos

**Control**: Los elementos del equipo que contengan medios de almacenamiento deben verificarse para garantizar que todos los datos confidenciales y el software con licencia se hayan eliminado o

sobrescrito de forma segura antes de su eliminación o reutilización.

**Objetivo**: Para evitar la fuga de información de los equipos que se desecharán o reutilizarán.

## 8 Controles Tecnológicos

### 8.1 Dispositivos de punto final de usuario

**Control**: La información almacenada, procesada o accesible a través de los dispositivos finales de los usuarios debe protegerse.

**Objetivo**: Para proteger la información contra los riesgos introducidos por el uso de dispositivos de punto final de usuario.

### 8.2 Derechos de acceso privilegiado

**Control**: La asignación y el uso de derechos de acceso privilegiado deben restringirse y gestionarse.

**Objetivo**: Para garantizar que solo los usuarios autorizados, los componentes y servicios de software reciban derechos de acceso privilegiados.

### 8.3 Restricciones de acceso a la información

**Control**: El acceso a la información y otros activos asociados debe estar restringido de acuerdo con la política específica del tema establecido sobre control de acceso.

**Objetivo**: Para garantizar sólo el acceso autorizado y evitar el acceso no autorizado a la información y otros activos asociados.

### 8.4 Acceso al código fuente

**Control**: El acceso de lectura y escritura al código fuente, las herramientas de desarrollo y las bibliotecas de software debe administrarse adecuadamente.

**Objetivo**: Para evitar la introducción de funciones no autorizadas, evitar cambios no intencionales o maliciosos y mantener la confidencialidad de la propiedad intelectual valiosa.

### 8.5 Autenticación segura

**Control**: Las tecnologías y los procedimientos de autenticación segura deben implementarse en función de las restricciones de acceso a la información y la política específica del tema sobre el control de acceso.

**Objetivo**: Para garantizar que un usuario o una entidad se autentique de forma segura cuando se otorga acceso a sistemas, aplicaciones y servicios.

### 8.6 Gestión de capacidad

**Control**: El uso de los recursos debe monitorearse y ajustarse de acuerdo con los requisitos de capacidad actuales y esperados.

**Objetivo**: Asegurar la capacidad requerida de las instalaciones de procesamiento de información, recursos humanos, oficinas y otras instalaciones.

### 8.7 Protección contra malware

**Control**: La protección contra el malware debe implementarse y respaldarse mediante la conciencia adecuada del usuario.

**Objetivo**: Para garantizar que la información y otros activos asociados estén protegidos contra malware.

### 8.8 Gestión de vulnerabilidades técnicas

**Control**: Debe obtenerse información sobre las vulnerabilidades técnicas de los sistemas de información en uso, debe evaluarse la exposición de la organización a tales vulnerabilidades y deben tomarse las medidas apropiadas.

**Objetivo**: Para prevenir la explotación de vulnerabilidades técnicas.

### 8.9 Gestión de la configuración

**Control**: Las configuraciones, incluidas las configuraciones de seguridad, de hardware, software,

servicios y redes deben establecerse, documentarse, implementarse, monitorearse y revisarse.

**Objetivo**: Para garantizar que el hardware, el software, los servicios y las redes, funcionen correctamente con la configuración de seguridad requerida y que la configuración no sea alterada por cambios no autorizados o incorrectos.

### 8.10 Eliminación de información

**Control**: La información almacenada en sistemas de información, dispositivos o en cualquier otro medio de almacenamiento debe ser eliminada cuando ya no sea necesaria.

**Objetivo**: Para evitar la exposición innecesaria de información confidencial y cumplir con los requisitos legales, estatutarios, reglamentarios y contractuales para la eliminación de información.

### 8.11 Enmascaramiento de datos

**Control**: El enmascaramiento de datos se debe utilizar de acuerdo con la política específica del tema de la organización, sobre el control de acceso y los requisitos comerciales teniendo en cuenta la legislación aplicable.

**Objetivo**: Para limitar la exposición de datos confidenciales, incluida la PII y para cumplir con los requisitos legales, estatutarios, reglamentarios y contractuales.

### 8.12 Prevención de fugas de datos

**Control**: Las medidas de prevención de fuga de datos deben aplicarse a los sistemas, redes y cualquier otro dispositivo que procese, almacene o transmita información confidencial.

**Objetivo**: Para detectar y prevenir la divulgación y extracción no autorizada de información por parte de personas o sistemas.

### 8.13 Copia de seguridad de la información

**Control**: Las copias de respaldo de la información, el software y los sistemas deben mantenerse y probarse regularmente de acuerdo con la política de respaldo específica del tema acordado.

**Objetivo**: Para permitir la recuperación de la pérdida de datos o sistemas.

### 8.14 Redundancia de las instalaciones de procesamiento de información

**Control**: Las instalaciones de procesamiento de información deben implementarse con suficiente redundancia para cumplir con los requisitos de disponibilidad.

**Objetivo**: Asegurar el funcionamiento continuo de las instalaciones de procesamiento de información.

### 8.15 Registro

**Control**: Se deben producir, almacenar, proteger y analizar sistemas que registren actividades, excepciones, fallas y otros eventos relevantes.

**Objetivo**: Para registrar eventos, generar evidencia, garantizar la integridad de la información, prevenir el acceso no autorizado, respaldar investigaciones e identificar eventos de seguridad de la información, que pueden conducir a un incidente de seguridad.

### 8.16 Actividades de seguimiento

**Control**: Las redes, los sistemas y las aplicaciones deben monitorearse para detectar comportamientos anómalos y deben tomarse las medidas apropiadas para evaluar posibles incidentes de seguridad de la información.

**Objetivo**: Para detectar comportamientos anómalos y posibles incidentes de seguridad de la información.

### 8.17 Sincronización del reloj

**Control**: Los relojes de los sistemas de procesamiento de información utilizados por la organización deben sincronizarse con las fuentes de tiempo aprobadas.

**Objetivo**: Permitir la correlación y el análisis de eventos relacionados con la seguridad, otros

datos registrados y respaldar las investigaciones sobre incidentes de seguridad de la información.

### 8.18 Uso de programas de utilidad privilegiados

**Control**: El uso de programas de utilidad que puedan anular los controles del sistema y de las aplicaciones debe restringirse y controlarse estrictamente.

**Objetivo**: Para garantizar que el uso de programas de utilidad, no dañe el sistema y los controles de aplicaciones para la seguridad de la información.

### 8.19 Instalación de software en sistemas operativos

**Control**: Deben implementarse procedimientos y medidas para gestionar de forma segura la instalación de software en los sistemas operativos.

**Objetivo**: Para garantizar la integridad de los sistemas operativos y evitar la explotación de vulnerabilidades técnicas.

### 8.20 Seguridad de redes

**Control**: Las redes y los dispositivos de red deben protegerse, administrarse y controlarse para proteger la información en los sistemas y aplicaciones.

**Objetivo**: Para proteger la información en las redes y sus instalaciones de procesamiento de información de apoyo del compromiso a través de la red.

### 8.21 Seguridad de los servicios de red

**Control**: Los mecanismos de seguridad, los niveles de servicio y los requisitos de servicio de los servicios de red deben identificarse, implementarse y monitorearse.

**Objetivo**: Para garantizar la seguridad en el uso de los servicios de red.

### 8.22 Segregación de redes

**Control**: Los grupos de servicios de información, usuarios y sistemas de información deben estar segregados en las redes de la organización.

**Objetivo**: Dividir la red en límites de seguridad y controlar el tráfico entre ellos en función de las necesidades comerciales.

### 8.23 Filtrado web

**Control**: El acceso a sitios web externos debe administrarse para reducir la exposición a contenido malicioso.

**Objetivo**: Para proteger los sistemas contra el malware y evitar el acceso a sitios web no autorizados y recursos.

### 8.24 Uso de criptografía

**Control**: Deben definirse e implementarse reglas para el uso eficaz de la criptografía, incluida la gestión de claves criptográficas.

**Objetivo**: Garantizar el uso adecuado y eficaz de la criptografía para proteger la confidencialidad, la autenticidad o la integridad de la información de acuerdo con los requisitos comerciales y de seguridad de la información, teniendo en cuenta los requisitos legales, estatutarios, reglamentarios y contractuales relacionados con la criptografía.

### 8.25 Ciclo de vida de desarrollo seguro

**Control**: Deben establecerse y aplicarse reglas para el desarrollo seguro de software y sistemas.

**Objetivo**: Garantizar que la seguridad de la información se diseñe e implemente dentro del ciclo de vida de desarrollo seguro de software y sistemas.

### 8.26 Requisitos de seguridad de la aplicación

**Control**: Los requisitos de seguridad de la información deben identificarse, especificarse y aprobarse al desarrollar o adquirir aplicaciones.

**Objetivo**: Para garantizar que todos los requisitos de seguridad de la información se identifiquen y aborden al desarrollar o adquirir aplicaciones.

### 8.27 Arquitectura del sistema seguro y principios de ingeniería

**Control**: Los principios para diseñar sistemas seguros deben establecerse, documentarse, mantenerse y aplicarse a cualquier actividad de desarrollo de sistemas de información.

**Objetivo**: Garantizar que los sistemas de información se diseñen, implementen y operen de forma segura dentro del ciclo de vida del desarrollo.

### 8.28 Codificación segura

**Control**: Los principios de codificación segura deben aplicarse al desarrollo de software.

**Objetivo**: Garantizar que el software se escriba de forma segura, reduciendo así el número de posibles problemas de seguridad de la información y vulnerabilidades en el software.

### 8.29 Pruebas de seguridad en desarrollo y aceptación

**Control**: Los procesos de prueba de seguridad deben definirse e implementarse en el ciclo de vida del desarrollo.

**Objetivo**: Para validar si se cumplen los requisitos de seguridad de la información cuando las aplicaciones o el código se implementan en el entorno de producción.

### 8.30 Desarrollo subcontratado

**Control:** La organización debe dirigir, monitorear y revisar las actividades relacionadas con el desarrollo de sistemas subcontratados.

**Objetivo**: Para garantizar que las medidas de seguridad de la información requeridas por la organización se implementen en el desarrollo de sistemas subcontratados.

### 8.31 Separación de los entornos de desarrollo, prueba y producción

**Control**: Los entornos de desarrollo, prueba y producción deben estar separados y protegidos.

**Objetivo:** Para proteger el entorno de producción y los datos contra el compromiso de las actividades de desarrollo y prueba.

### 8.32 Gestión de cambios

**Control**: Los cambios en las instalaciones de procesamiento de información y los sistemas de información deben estar sujetos a procedimientos de gestión de cambios.

**Objetivo:** Preservar la seguridad de la información al ejecutar cambios.

### 8.33 Información de prueba

**Control**: La información de las pruebas debe seleccionarse, protegerse y gestionarse adecuadamente.

**Objetivo:** Para garantizar la relevancia de las pruebas y la protección de la información operativa utilizada para las pruebas.

### 8.34 Protección de los sistemas de información durante las pruebas de auditoría

**Control**: Las pruebas de auditoría y otras actividades de aseguramiento que involucren la evaluación de los sistemas operativos deben planificarse y acordarse entre el evaluador y la gerencia correspondiente.

**Objetivo**: Minimizar el impacto de la auditoría y otras actividades de aseguramiento en los sistemas operativos y procesos comerciales.

## ANEXO N° 4 Guía de Implementación de cada Control de la ISO/IEC 27002:2022

**Controles Organizacionales**

### Políticas de Seguridad de la información

La política de seguridad de la información debe contener declaraciones relativas a:

- Definición de seguridad de la información.
- Los objetivos de seguridad de la información o el marco para establecer los objetivos de seguridad de la información.
- Principios para guiar todas las actividades relacionadas con la seguridad de la información.

- Compromiso de satisfacer los requisitos aplicables relacionados con la seguridad de la información.
- Compromiso con la mejora continua del sistema de gestión de seguridad de la información.
- Asignación de responsabilidades para la gestión de la seguridad de la información a roles definidos.
- Procedimientos para el manejo de exenciones y excepciones.
- Aprobación de cualquier cambio en la política de seguridad de la información por la alta dirección.
- La política de seguridad de la información debe comunicarse al personal relevante y a las partes interesadas en una forma que sea relevante, accesible y comprensible para el lector.

**Roles y responsabilidades de seguridad de la información**

La organización podrá definir y gestionar las responsabilidades para:

- Protección de la información y otros activos asociados.
- Realizar procesos específicos de seguridad de la información.
- Actividades de riesgos de seguridad de la información y en particular, aceptación de riesgos residuales.
- Todo el personal que utiliza la información de una organización y otros activos asociados.

**Segregación de funciones**

La segregación de deberes y áreas de responsabilidad tiene como objetivo separar los deberes en conflictos entre diferentes individuos para evitar que un individuo ejecute deberes potencialmente conflictivos por su cuenta.

La organización debe determinar qué deberes y áreas de responsabilidad requieren segregación como:

- Iniciar, aprobar y ejecutar un cambio
- Solicitar, aprobar e implementar derechos de acceso
- Diseñar, implementar y revisar código
- Desarrollar software y administrar sistemas en producción
- Usar y administrar aplicaciones
- Uso de aplicaciones y bases de datos de administración
- Diseñar, auditar y asegurar los controles de seguridad de la información

**Responsabilidades de la organización**

La gerencia debe demostrar su apoyo a la política de seguridad de la información, las políticas específicas del tema, los procedimientos y los controles de seguridad de la información.

Las responsabilidades de la gerencia debe incluir asegurar que el personal:

- Estén debidamente informados sobre sus roles y responsabilidades de seguridad de la información antes de que se les conceda acceso a la información de la organización y otros activos asociados.
- Cuentan con lineamientos que establecen las expectativas de seguridad de la información de su rol dentro de la organización.
- Tienen el mandato de cumplir con la política de seguridad de la información y las políticas específicas de la organización.
- Lograr un nivel de conciencia de la seguridad de la información relevante para sus roles y responsabilidades dentro de la organización.
- El cumplimiento de los términos y condiciones de empleo, contrato o acuerdo, incluida la política de seguridad de la información de la organización y los métodos de trabajo apropiados.
- Continuar teniendo las habilidades y calificaciones apropiadas en seguridad de la información a

través de la educación profesional continua.

- Cuando sea factible, cuenten con un canal confidencial para reportar violaciones de información política de seguridad, políticas o procedimientos específicos de un tema para la seguridad de la información.

- Cuentan con recursos adecuados y tiempo de planificación de proyectos para implementar los objetivos de la organización procesos y controles relacionados con la seguridad.

**Contacto con las autoridades**

- La organización debe especificar cuándo y quién debe contactar a las autoridades (p. ej., fuerzas del orden, organismos reguladores, autoridades de supervisión) y cómo deben informarse oportunamente los incidentes de seguridad de la información identificados.

- Los contactos con los organismos reguladores también son útiles para anticipar y prepararse para los próximos cambios en las leyes o reglamentos relevantes que afectan a la organización.

- Las organizaciones bajo ataque pueden solicitar a las autoridades que tomen medidas contra la fuente del ataque.

- Los contactos con otras autoridades incluyen servicios públicos, servicios de emergencia, proveedores de electricidad, salud y seguridad por ejemplo, departamentos de bomberos (en conexión con la continuidad del negocio), proveedores de telecomunicaciones (en relación con el enrutamiento y la disponibilidad de la línea) y proveedores de agua (en relación con las instalaciones de refrigeración para equipos).

**Contacto con grupos de interés especial**

La pertenencia a grupos o foros de intereses especiales debe considerarse como un medio para:

- Mejorar el conocimiento sobre las mejores prácticas y mantenerse actualizado con la información de seguridad relevante.

- Asegurarse de que la comprensión del entorno de seguridad de la información esté

actualizada.

- Recibir alertas tempranas de incidencias, avisos y parches relacionados con ataques y vulnerabilidades.
- Obtener acceso a asesoramiento especializado en seguridad de la información.
- Compartir e intercambiar información sobre nuevas tecnologías, productos, servicios, amenazas o vulnerabilidades.
- Proporcionar puntos de enlace adecuados cuando se trate de incidentes de seguridad de la información.

**Inteligencia de amenazas**

Las organizaciones pueden utilizar la inteligencia de amenazas para prevenir, detectar o responder a las amenazas.

La información sobre amenazas existentes o emergentes se recopila y analiza para:

- Facilitar acciones informadas para evitar que las amenazas causen daño a la organización.
- Reducir el impacto de tales amenazas.

La inteligencia de amenazas debe analizarse y utilizarse posteriormente:

- Implementando procesos para incluir información recopilada de fuentes de inteligencia de amenazas en los procesos de gestión de riesgos de seguridad de la información de la organización.
- Como entrada adicional a controles técnicos preventivos y de detección como cortafuegos, detección de intrusos sistema o soluciones antimalware.
- Como entrada a los procesos y técnicas de prueba de seguridad de la información.

**Seguridad de la información en la gestión de proyectos**

La seguridad de la información debe integrarse en la gestión del proyecto para garantizar que los riesgos de seguridad de la información se abordan como parte de la gestión del proyecto.

La gestión de proyectos en uso debe exigir que:

- Los riesgos de seguridad de la información se evalúan y tratan en una etapa temprana y periódicamente como parte de riesgos del proyecto a lo largo de su ciclo de vida.
- Los requisitos de seguridad de la información por ejemplo, requisitos de seguridad de la aplicación y requisitos para cumplir con los derechos de propiedad intelectual; se abordan en las primeras etapas de los proyectos.
- Los riesgos de seguridad de la información asociados con la ejecución de proyectos, como la seguridad de los aspectos de comunicación externa, se consideran y tratan a lo largo del ciclo de vida del proyecto.
- Se revisa el progreso en el tratamiento de riesgos de seguridad de la información y se evalúa la efectividad del tratamiento evaluado y probado.

**Inventario de información y otros activos asociados**

El inventario de información y otros activos asociados debe ser preciso, actualizado, consistente y alineado con otros inventarios.

Las opciones para garantizar la precisión de un inventario de información y otros activos asociados incluyen:

- Realizar revisiones periódicas de la información identificada y otros activos asociados contra el activo inventario.
- Hacer cumplir automáticamente una actualización de inventario en el proceso de instalación, cambio o eliminación de un activo.
- Los inventarios de información y otros activos asociados también respaldan la gestión de riesgos, las actividades de auditoría, la gestión de vulnerabilidades, la respuesta a incidentes y la planificación de la recuperación.

**Uso aceptable de la información y otros activos asociados**

La organización debe establecer una política específica de un tema sobre el uso aceptable de la información y otros activos asociados y comunicar a cualquier persona que use o maneje información y otros activos asociados.

Se deben elaborar procedimientos de uso aceptable para todo el ciclo de vida de la información de acuerdo con su clasificación y riesgos determinados. Se deben considerar los siguientes elementos:

- Restricciones de acceso que respaldan los requisitos de protección para cada nivel de clasificación.
- Mantenimiento de un registro de los usuarios autorizados de información y otros activos asociados.
- Protección de copias temporales o permanentes de información a un nivel consistente con la protección de la información original.
- Almacenamiento de activos asociados con la información de acuerdo con las especificaciones de los fabricantes.
- Marcado claro de todas las copias de los medios de almacenamiento (electrónicos o físicos) para la atención del destinatario autorizado.
- Autorización de disposición de información y otros activos asociados y supresión admitida.

**Devolución de bienes**

El proceso de cambio o terminación debe formalizarse para incluir la devolución de todos los activos físicos y electrónicos emitidos anteriormente que sean propiedad de la organización o estén encomendados a ella.

La organización debe identificar y documentar claramente toda la información y otros activos asociados que se devolverán, que pueden incluir:

- Dispositivos de punto extremo de usuario.
- Dispositivos portátiles de almacenamiento.

- Equipo especializado.
- Hardware de autenticación (por ejemplo, llaves mecánicas, tokens físicos y tarjetas inteligentes) para información, sistemas, sitios y archivos físicos.
- Copias físicas de la información.

**Clasificación de la información**

La organización debe tener en cuenta los requisitos de confidencialidad, integridad y disponibilidad en el esquema de clasificación.

Los resultados de la clasificación deben actualizarse de acuerdo con los cambios del valor, la sensibilidad y la criticidad de la información a lo largo de su ciclo de vida.

La clasificación brinda a las personas que manejan información una indicación concisa de cómo manejarla y protegerla.

**Etiquetado de la información**

Los procedimientos para el etiquetado de la información deben cubrir la información y otros activos asociados en todos los formatos.

Los ejemplos de técnicas de etiquetado incluyen:

- Etiquetas físicas.
- Encabezados y pies de página.
- Metadatos
- Marca de agua
- Sellos de goma.

El personal y otras partes interesadas deben conocer los procedimientos de etiquetado. Todo el personal debe recibir la capacitación necesaria para garantizar que la información se etiquete

correctamente y se manipule en consecuencia.

**Transferencia de información**

La transferencia de información puede ocurrir a través de transferencia electrónica, transferencia de medios de almacenamiento físico y transferencia verbal.

Para todo tipo de transferencia de información, las reglas, procedimientos y acuerdos deben incluir:

- Controles diseñados para proteger la información transferida de la intercepción, el acceso no autorizado, la copia, la modificación, el enrutamiento incorrecto, la destrucción y la denegación de servicio, incluidos los niveles de control de acceso acordes con la clasificación de la información involucrada y cualquier control especial que se requiera para proteger la información confidencial, como el uso de técnicas criptográficas.
- Controles para garantizar la trazabilidad y el no repudio, incluido el mantenimiento de una cadena de custodia de la información durante el tránsito.
- Identificación de los contactos apropiados relacionados con la transferencia, incluidos los propietarios de la información, el riesgo propietarios, oficiales de seguridad y custodios de la información, según corresponda.
- Responsabilidades y obligaciones en caso de incidentes de seguridad de la información, como la pérdida de medios físicos de almacenamiento o datos.
- Uso de un sistema de etiquetado acordado para información sensible o crítica, asegurando que el significado de las etiquetas se comprenda de inmediato y que la información esté debidamente protegida.
- Confiabilidad y disponibilidad del servicio de transferencia.
- La política o lineamientos específicos del tema sobre el uso aceptable de las instalaciones de transferencia de información.

- Pautas de retención y eliminación para todos los registros comerciales, incluidos los mensajes.
- La consideración de cualquier otro requisito legal, estatutario, reglamentario y contractual relevante relacionado con la transferencia de información (por ejemplo, requisitos para firmas electrónicas).

**Control de acceso**

Se debe tener en cuenta lo siguiente al definir e implementar reglas de control de acceso:

- Coherencia entre los derechos de acceso y la clasificación de la información.
- Coherencia entre los derechos de acceso, las necesidades y requisitos de seguridad del perímetro físico.
- Considerando todos los tipos de conexiones disponibles en entornos distribuidos, para que las entidades sólo proporcionen acceso a la información y otros activos asociados, incluidas las redes y la red de servicios, que están autorizados a utilizar.
- Considerar cómo se pueden reflejar los elementos o factores relevantes para el control de acceso dinámico.

**Gestión de identidad**

Los procesos utilizados en el contexto de la gestión de la identidad deben garantizar que:

- Para las identidades asignadas a personas, una identidad específica sólo se vincula a una sola persona para poder responsabilizar a la persona por las acciones realizadas con esta identidad específica.
- Las identidades asignadas a varias personas (por ejemplo, identidades compartidas) solo se permiten cuando son necesarias por razones comerciales u operativas y están sujetas a aprobación y documentación específicas.
- Las identidades asignadas a entidades no humanas están sujetas a aprobación y supervisión continua independiente.

- Las identidades se inhabilitan o eliminan de manera oportuna si no son necesarias (por ejemplo, si sus entidades asociadas se eliminan, no se utilizan, o si la persona vinculada a una identidad ha dejado la organización o ha cambiado de función).

- En un dominio específico, una sola identidad se asigna a una sola entidad, es decir, el mapeo de múltiples identidades a la misma entidad dentro del mismo contexto (identidades duplicadas) se evita.

- Registros de todos los eventos significativos relacionados con el uso y la gestión de las identidades de los usuarios y de cómo se conserva la información de autenticación.

La organización debe contar con un proceso de soporte para manejar los cambios en la información relacionada con las identidades de los usuarios. Estos procesos pueden incluir la verificación de documentos confiables relacionados con una persona.

**Información de autenticación**

Las contraseñas o frases de contraseña son un tipo de información de autenticación de uso común y son un medio común para verificar la identidad de un usuario.

- El proceso de asignación y gestión debe garantizar que: las contraseñas personales o los números de identificación personal (PIN) generados automáticamente durante los procesos de inscripción como información de autenticación secreta temporal no se pueden adivinar y son únicos para cada persona, los usuarios deben cambiarlos después del primer uso.

- Cualquier persona que tenga acceso o utilice información de autenticación debe ser advertida de que se asegure: la información de autenticación secreta, como las contraseñas, se mantiene confidencial. La información de autenticación secreta personal no debe compartirse con nadie. La información de autenticación secreta utilizada en el contexto de identidades vinculadas a múltiples usuarios o vinculadas a entidades no personales, se comparte únicamente con personas autorizadas.

- Cuando se utilizan contraseñas como información de autenticación, el sistema de

administración de contraseñas debe permitir a los usuarios seleccionar y cambiar sus propias contraseñas e incluir un procedimiento de confirmación para dirección de errores de entrada.

**Derechos de acceso**

El proceso de aprovisionamiento para asignar o revocar los derechos de acceso físico y lógico otorgados a la identidad autenticada de una entidad debe:

- Garantizar que los derechos de acceso de los usuarios que han dejado la organización se eliminen de manera oportuna.
- Se debe considerar incluir cláusulas en los contratos de personal y de servicio que especifiquen sanciones si el personal intenta acceder sin autorización a la información y otros activos asociados.

**Planificación y preparación de la gestión de seguridad de la información.**

- La organización debe establecer procesos apropiados de gestión de incidentes de seguridad de la información. Las funciones y responsabilidades para llevar a cabo los procedimientos de gestión de incidentes deben determinarse y comunicarse de manera efectiva a las partes interesadas internas y externas pertinentes.
- Los objetivos para la gestión de incidentes de seguridad de la información, deben acordarse con la gerencia y debe garantizarse que los responsables de la gestión de incidentes de seguridad de la información entiendan las prioridades de la organización para manejar los incidentes, incluido el marco de tiempo de resolución basado en las posibles consecuencias y gravedad.
- Los procedimientos de notificación deben incluir, uso de formularios de incidentes para ayudar al personal a realizar todas las acciones necesarias al informar incidentes de seguridad de la información.

**Evaluación y decisión sobre eventos de seguridad de la información.**

Se debe acordar un esquema de categorización y priorización de incidentes de seguridad de la

información para la identificación de las consecuencias y prioridad de un incidente.

- El personal responsable de coordinar y responder a los incidentes de seguridad de la información debe realizar la evaluación y tomar una decisión sobre los eventos que se presenten.
- Los resultados de la evaluación y la decisión deben registrarse en detalle para fines de futura referencia y verificación.

**Respuesta a incidentes de seguridad de la información.**

- La organización debe establecer y comunicar procedimientos sobre la respuesta a incidentes de seguridad de la información a todas las partes interesadas pertinentes.
- Los incidentes de seguridad de la información deben ser respondidos por un equipo designado con la competencia requerida.
- Garantizar que todas las actividades de respuesta involucradas se registren correctamente para su posterior análisis.
- Identificar y gestionar las vulnerabilidades así como las debilidades de la seguridad de la información, incluidas las relacionadas con los controles que han causado, contribuido o fallado en prevenir el incidente.

**Aprendiendo de los incidentes de seguridad de la información.**

La organización debe establecer procedimientos para cuantificar y monitorear los tipos, volúmenes y costos de los incidentes de seguridad de la información.

La información obtenida de la evaluación de incidentes de seguridad de la información debe utilizarse para:

- Mejorar el plan de gestión de incidentes, incluidos los escenarios y procedimientos de respuesta a incidentes.
- Identificar incidentes recurrentes o graves y sus causas para actualizar la evaluación de riesgos de seguridad de la información de la organización y determinar e implementar los controles

adicionales necesarios para reducir la probabilidad o las consecuencias de futuros incidentes similares. Los mecanismos para habilitar eso incluye recopilar, cuantificar y monitorear información sobre tipos de incidentes, volúmenes y costos.

- Mejorar la concienciación y la formación de los usuarios proporcionando ejemplos de lo que puede suceder, cómo responder a tales incidentes y cómo evitarlos en el futuro.

**Recopilación de pruebas**

Se deben desarrollar y seguir procedimientos internos al tratar con evidencia relacionada con eventos de seguridad de la información con el propósito de acciones disciplinarias y legales.

- Los procedimientos para la gestión de pruebas deben proporcionar instrucciones para la identificación, recopilación, adquisición y conservación de pruebas de acuerdo con los diferentes tipos de medios de almacenamiento, dispositivos y estado de los dispositivos (es decir, encendidos o apagados).

- Cuando se detecta por primera vez un evento de seguridad de la información, no siempre es obvio si el evento resultará o no en una acción judicial. Por lo tanto, existe el peligro de que las pruebas necesarias se destruyan intencional o accidentalmente antes de darse cuenta de la gravedad del incidente. Es aconsejable involucrar asesoramiento legal o aplicación de la ley desde el principio en cualquier acción legal contemplada y recibir asesoramiento sobre las pruebas requeridas.

**Seguridad de la información durante la interrupción.**

La organización debe determinar sus requisitos para adaptar los controles de seguridad de la información durante la interrupción.

- La seguridad de la información debe restaurarse al nivel requerido y en los plazos requeridos.

- Como parte del análisis de impacto comercial y la evaluación de riesgos realizados dentro de la gestión de continuidad comercial, se deben considerar y priorizar las consecuencias de la pérdida de

confidencialidad e integridad de la información, además de la necesidad de mantener la disponibilidad.

**Preparación de las TIC para la continuidad del negocio.**

La preparación de las TIC para la continuidad del negocio es un componente importante en la gestión de la continuidad del negocio y la gestión de la seguridad de la información para garantizar que los objetivos de la organización puedan seguir cumpliéndose durante la interrupción.

La gestión de la continuidad de las TIC constituye una parte clave de los requisitos de continuidad del negocio en relación con la disponibilidad para poder:

- Responder y recuperarse de la interrupción de los servicios de TIC, independientemente de la causa.
- Garantizar que la continuidad de las actividades prioritarias esté respaldada por los servicios de TIC requeridos.
- Responder antes de que ocurra una interrupción de los servicios de TIC y al detectar al menos un incidente que puede resultar en una interrupción de los servicios de TIC.

**Requisitos legales, estatutarios, reglamentarios y contractuales.**

La organización podrá :

- Identificar toda la legislación y los reglamentos pertinentes a la seguridad de la información de la organización para conocer los requisitos para su tipo de negocio.
- Tomar en consideración el cumplimiento en todos los países relevantes, si la organización realiza negocios en otros países o usa productos y servicios de otros países, donde las leyes y reglamentos pueden afectar la organización
- Revisar periódicamente la legislación y los reglamentos identificados a fin de mantenerse al día con los cambios e identificar nueva legislación.
- Se recomienda buscar asesoramiento legal para garantizar el cumplimiento de la legislación y

las reglamentaciones pertinentes, especialmente cuando la información cifrada o las herramientas criptográficas se mueven a través de las fronteras jurisdiccionales.

**Derechos de propiedad intelectual**

Se deben considerar las siguientes pautas para proteger cualquier material que pueda considerarse propiedad intelectual.

- Definir y comunicar una política específica sobre la protección de los derechos de propiedad intelectual.
- Adquirir software solo a través de fuentes conocidas y acreditadas, para garantizar que los derechos de autor no sean infringidos.
- Mantener prueba y evidencia de propiedad de licencias, manuales, etc.
- Llevar a cabo revisiones para garantizar que solo se instalen software autorizado y productos con licencia.
- No duplicar, convertir a otro formato o extraer de grabaciones comerciales (video, audio) que no sea permitido por la ley de derechos de autor o las licencias aplicables.
- Los derechos de propiedad intelectual incluyen derechos de autor de software o documentos, derechos de diseño, marcas registradas, patentes y licencias de código fuente.
- Los productos de software patentados generalmente se suministran bajo un acuerdo de licencia que especifica los términos y condiciones de la licencia, por ejemplo, limitando el uso de los productos a máquinas específicas o limitando la copia a la creación de copias de seguridad únicamente.
- Los requisitos legales, estatutarios, reglamentarios y contractuales pueden imponer restricciones a la copia de material patentado.
- La infracción de los derechos de autor puede dar lugar a acciones legales, que pueden implicar multas y procesos penales.

**Protección de registros**

La organización debe tomar los siguientes pasos para proteger la autenticidad, confiabilidad, integridad y usabilidad de los registros, ya que su contexto comercial y los requisitos para su gestión cambian con el tiempo. Cualquier conjunto de información, independientemente de su estructura o forma, puede gestionarse como un registro.

- Los registros deben clasificarse en tipos de registros (p. ej., registros contables, registros de transacciones comerciales, registros de personal, registros legales), cada uno con detalles sobre los períodos de retención y el tipo de medio de almacenamiento permitido, que puede ser físico o electrónico.
- Los sistemas de almacenamiento de datos deben elegirse de manera que los registros requeridos puedan recuperarse en un marco de tiempo y formato aceptables, según los requisitos que se deban cumplir.
- Cuando se elijan medios de almacenamiento electrónico, se deben establecer procedimientos para garantizar la capacidad de acceder a los registros (tanto los medios de almacenamiento como la legibilidad del formato) durante todo el período de retención para salvaguardar contra pérdidas debido a futuros cambios tecnológicos.
- Los procedimientos de almacenamiento y manipulación deben implementarse de acuerdo con las recomendaciones proporcionadas por los fabricantes de los medios de almacenamiento.

**Privacidad y protección de PII (Información de Identificación Personal)**

La organización debe desarrollar e implementar procedimientos para la preservación de la privacidad y la protección de la PII. Estos procedimientos deben comunicarse a todas las partes interesadas relevantes involucradas en el procesamiento de información de identificación personal.

- El cumplimiento de estos procedimientos y de toda la legislación y los reglamentos pertinentes

relacionados con la preservación de la privacidad y la protección de la PII requiere roles, responsabilidades y controles apropiados.

- Nombrar una persona responsable, como un oficial de privacidad, que debe brindar orientación al personal, los proveedores de servicios y otras partes interesadas sobre sus responsabilidades individuales y los procedimientos específicos que deben seguirse.
- La responsabilidad por el manejo de la PII debe abordarse teniendo en cuenta la legislación y los reglamentos pertinentes.

**Revisión independiente de la seguridad de la información**

La organización debe tener procesos para realizar revisiones independientes.

- Las revisiones deben incluir la evaluación de las oportunidades de mejora y la necesidad de cambios en el enfoque de la seguridad de la información, incluida la política de seguridad de la información, las políticas de temas específicos y otros controles.
- Las revisiones deben ser realizadas por personas independientes del área bajo revisión.
- Los resultados de las revisiones independientes deben informarse a la dirección que inició las revisiones y si procede a la alta dirección.

La organización podrá considerar la realización de revisiones cuando:

- Las leyes y reglamentos afectan el cambio de la organización.
- Ocurren incidentes significativos.
- La organización inicia un nuevo negocio o cambia un negocio actual.
- La organización comienza a usar un nuevo producto o servicio, o cambia el uso de un producto o servicio actual.
- La organización cambia significativamente los controles y procedimientos de seguridad de la información.

**Cumplimiento de políticas, normas y estándares de seguridad de la información.**

Si se encuentra algún incumplimiento como resultado de la revisión, los gerentes deben:

- Identificar las causas del incumplimiento.
- Evaluar la necesidad de acciones correctivas para lograr el cumplimiento.
- Implementar acciones correctivas apropiadas.
- Revisar las acciones correctivas tomadas para verificar su efectividad e identificar cualquier deficiencia o debilidades.
- Las acciones correctivas deben completarse de manera oportuna según corresponda al riesgo.

**Procedimientos operativos documentados**

Los procedimientos operativos deben especificar:

- Las personas responsables.
- La instalación y configuración segura de sistemas.
- Procesamiento y manejo de información, tanto automatizado como manual.
- Respaldo y resiliencia.
- Requisitos de programación, incluidas las interdependencias con otros sistemas.
- Instrucciones para el manejo de errores u otras condiciones excepcionales, que pueden surgir durante la ejecución del trabajo.
- Contactos de soporte y escalamiento, incluidos contactos de soporte externo en caso de imprevistos, dificultades operativas o técnicas.
- Instrucciones de manejo de medios de almacenamiento.
- Procedimientos de reinicio y recuperación del sistema para su uso en caso de falla del sistema.
- La gestión de la pista de auditoría y la información de registro del sistema y el monitoreo de

video.

- Procedimientos de monitoreo tales como capacidad, desempeño y seguridad.
- Instrucciones de mantenimiento.

Los procedimientos operativos documentados deben revisarse y actualizarse cuando sea necesario y deben ser autorizados.

## Controles de Personas

### Selección de personal

Se debe realizar un proceso de selección para todo el personal, incluido el personal a tiempo completo, a tiempo parcial y temporal. Debe incluir lo siguiente:

- Disponibilidad de referencias satisfactorias.
- Verificación (de integridad y exactitud) del currículum vitae del solicitante.
- Confirmación de las calificaciones académicas y profesionales reclamadas.
- Verificación de identidad independiente (por ejemplo, pasaporte u otro documento aceptable emitido por autoridades).
- Verificación más detallada, como revisión de crédito o revisión de antecedentes penales si el candidato adquiere un papel crítico.

Cuando se contrata a una persona para una función específica de seguridad de la información, debe asegurarse de que el candidato:

- Tiene la competencia necesaria para desempeñar la función de seguridad.
- Se puede confiar para asumir el rol, especialmente si el rol es crítico para la organización.

Los controles de verificación deben repetirse periódicamente para confirmar la idoneidad continua del personal, según la importancia del rol de una persona.

### Términos y condiciones de empleo

Las obligaciones contractuales para el personal deben señalar los siguientes puntos:

- Acuerdos de confidencialidad o no divulgación que el personal al que se le da acceso a información confidencial debe firmar antes de tener acceso a la información y otros activos asociados.
- Responsabilidades y derechos legales por ejemplo, con respecto a las leyes de derechos de autor o la legislación de protección de datos.
- Responsabilidades para la clasificación de la información y la gestión de la organización y otros activos asociados, instalaciones de procesamiento de información y servicios de información manipulados por el personal.
- Responsabilidades por el tratamiento de la información recibida de los interesados.
- Acciones a tomar si el personal ignora los requisitos de seguridad de la organización.

La organización debe asegurarse de que el personal esté de acuerdo con los términos y condiciones relacionados con la seguridad de la información.

**Concientización, educación y capacitación en seguridad de la información**

Se debe establecer un programa de concientización, educación y capacitación en seguridad de la información de acuerdo con la política de seguridad de la información de la organización, las políticas específicas del tema y los procedimientos relevantes sobre seguridad de la información, teniendo en cuenta la información de la organización que debe protegerse y los controles de seguridad de la información que se han implementado para proteger la información.

- Un programa de concientización sobre la seguridad de la información debe tener como objetivo que el personal sea consciente de sus responsabilidades con respecto a la seguridad de la información y los medios por los cuales se cumplen esas responsabilidades.
- La organización debe identificar, preparar e implementar un plan de capacitación adecuado

para los equipos técnicos cuyas funciones requieren conjuntos de habilidades y experiencia específicas. Los equipos técnicos deben tener las habilidades para configurar y mantener el nivel de seguridad requerido para dispositivos, sistemas, aplicaciones y servicios.

- La concientización, la educación y la capacitación en seguridad de la información pueden ser parte de, o llevarse a cabo en colaboración con otras actividades, por ejemplo, administración general de la información, TIC, seguridad, privacidad o capacitación en seguridad.

**Proceso disciplinario**

El proceso disciplinario no debe iniciarse sin la verificación previa de que se ha producido una violación de la política de seguridad de la información.

El proceso disciplinario formal debe prever una respuesta graduada que tenga en cuenta factores tales como:

- La naturaleza (quién, qué, cuándo, cómo) y la gravedad del incumplimiento y sus consecuencias.
- Si el delito fue intencional (malicioso) o no intencional (accidental)
- Si se trata o no de una primera infracción.
- Si el infractor estaba debidamente capacitado o no.

Cuando las personas demuestran un comportamiento excelente con respecto a la seguridad de la información, pueden ser recompensadas para promover la seguridad de la información y fomentar el buen comportamiento.

**Responsabilidad después de la terminación o cambio de empleo**

Los cambios de responsabilidad o empleo deben gestionarse como la terminación de la responsabilidad o empleo actual combinada con el inicio de la nueva responsabilidad o empleo.

- Las funciones y responsabilidades de seguridad de la información que tenga cualquier persona que deje o cambie de puesto deben identificarse y transferirse a otra persona.

- Debe establecerse un proceso para la comunicación de los cambios y de los procedimientos operativos al personal, otras partes interesadas y personas de contacto pertinentes (clientes y proveedores).

- El proceso de término o cambio de empleo también debe aplicarse al personal externo (proveedores) cuando se produzca una terminación del personal del contrato o del puesto con la organización, cuando haya un cambio de puesto dentro de la organización.

La función de Recursos Humanos generalmente es la responsable del proceso general de terminación y trabaja junto con el gerente supervisor de la persona en transición para administrar los aspectos de seguridad de la información de los procedimientos relevantes.

**Acuerdos de confidencialidad o no divulgación**

Los acuerdos de confidencialidad o no divulgación son aplicables a las partes interesadas y al personal de la organización.

Para identificar los requisitos para los acuerdos de confidencialidad o no divulgación, se deben considerar los siguientes elementos:

- Una definición de la información a proteger (Información Confidencial)

- La duración esperada de un acuerdo, incluidos los casos en los que puede ser necesario mantener la confidencialidad indefinidamente o hasta que la información esté disponible públicamente.

- Las acciones requeridas cuando se termina un acuerdo.

- Las responsabilidades y acciones de los signatarios para evitar la divulgación de información no autorizada.

- La propiedad de la información, los secretos comerciales y la propiedad intelectual, como esto se relaciona con la protección de la información confidencial.

- El uso permitido de la información confidencial y los derechos del firmante para usar la

información.

- El derecho a auditar y monitorear actividades que involucren información confidencial para circunstancias altamente sensibles.
- El proceso de notificación y reporte de divulgación no autorizada o fuga de información confidencial.
- Los términos para la devolución o destrucción de la información al término del contrato.
- Las acciones previstas a tomar en caso de incumplimiento del acuerdo.

Los acuerdos de confidencialidad y no divulgación protegen la información de la organización e informan a los signatarios de su responsabilidad de proteger, usar y divulgar la información de manera responsable y autorizada.

**Trabajo distancia**

Las organizaciones que permiten actividades de trabajo a distancia deben emitir una política específica sobre el tema del trabajo a distancia que defina las condiciones y restricciones pertinentes.

Considerar las siguientes directrices y medidas:

- La provisión de equipos y muebles de almacenamiento adecuados para las actividades de trabajo remoto, donde no se permite el uso de equipos de propiedad privada que no estén bajo el control de la organización.
- Una definición del trabajo permitido, la clasificación de la información que puede ser mantenida y los sistemas y servicios a los que el trabajador remoto está autorizado a acceder.
- La provisión de capacitación para quienes trabajan a distancia y quienes brindan apoyo. Esto debe incluir cómo realizar negocios de manera segura mientras se trabaja de forma remota.
- La provisión de equipos de comunicación adecuados, incluidos los métodos para asegurar el acceso remoto, como los requisitos sobre bloqueos de pantalla del dispositivo y temporizadores de

inactividad, la habilitación del seguimiento de la ubicación del dispositivo, instalación de capacidades de borrado remoto.

- Seguridad física.
- Reglas y orientación sobre el acceso de familiares y visitantes a equipos e información.
- La provisión de soporte y mantenimiento de hardware y software.
- La provisión de seguros.
- Los procedimientos de respaldo y continuidad del negocio.
- Auditoría y seguimiento de la seguridad.
- Revocación de facultades y derechos de acceso y devolución de equipos cuando finalicen las actividades de trabajo a distancia.

**Reporte de eventos de seguridad de la información**

Todo el personal y los usuarios deben ser conscientes de su responsabilidad de informar eventos de seguridad de la información lo más rápido posible, para prevenir o minimizar el efecto de los incidentes.

El mecanismo de presentación de informes debe ser lo más fácil, accesible y disponible posible.

Las situaciones a considerar para el reporte de eventos de seguridad de la información incluyen:

- Controles de seguridad de la información ineficaces.
- Incumplimiento de las expectativas de confidencialidad, integridad o disponibilidad de la información.
- Errores humanos
- Incumplimiento de la política de seguridad de la información, políticas específicas del tema o normas aplicables.

- Incumplimiento de las medidas de seguridad física.
- Cambios del sistema que no han pasado por el proceso de gestión de cambios.
- Mal funcionamiento u otro comportamiento anómalo del sistema de software o hardware.
- Infracciones de acceso.
- Vulnerabilidades.
- Sospecha de infección por malware.

Se debe advertir al personal y a los usuarios que no intenten probar vulnerabilidades de seguridad de la información sospechosas.

## Controles Físicos

### Perímetros de seguridad física

Las siguientes pautas deben considerarse e implementarse cuando corresponda.

- Definir los perímetros de seguridad, la ubicación y resistencia de cada uno de los perímetros de acuerdo con los requisitos de seguridad de la información relacionados con los activos dentro del perímetro,
- Tener perímetros físicamente sólidos para un edificio o sitio que contenga procesamiento de información (es decir, no debe haber espacios en el perímetro o áreas donde un robo pueda ocurrir fácilmente). Los techos exteriores, paredes, techos y pisos del sitio deben ser de construcción sólida y todos las puertas exteriores deben estar adecuadamente protegidas contra el acceso no autorizado con mecanismos de control (por ejemplo, rejas, alarmas, cerraduras). Las puertas y ventanas deben cerrarse con llave cuando estén desatendidas y en el exterior. se debe considerar la protección de las ventanas, particularmente a nivel del suelo; puntos de ventilación también debe ser considerado.

- Alarmar, monitorear y probar todas las puertas contra incendios en un perímetro de seguridad junto con las paredes para establecer el nivel de resistencia requerido de acuerdo con las normas adecuadas. Ellos deben operar a prueba de fallas.

La protección física se puede lograr mediante la creación de una o más barreras físicas alrededor de las instalaciones de la organización y las instalaciones de procesamiento de información.

La organización debe considerar tener medidas de seguridad física que puedan fortalecerse durante situaciones de mayor amenaza.

**Entrada física**

Los puntos de acceso como las áreas de entrega y carga y otros puntos donde personas no autorizadas pueden ingresar a las instalaciones deben controlarse y si es posible, aislarse de las instalaciones de procesamiento de información para evitar el acceso no autorizado.

Se deben considerar las siguientes pautas:

- Restringir el acceso a los sitios y edificios solo al personal autorizado. La gestión de los derechos de acceso a áreas físicas debe incluir la provisión, revisión periódica, actualización y revocación de autorizaciones.

- Mantener y monitorear de forma segura un libro de registro físico o un registro de auditoría electrónico de todos los accesos y proteger todos los registros y la información confidencial de autenticación.

- Establecer e implementar un proceso y mecanismos técnicos para la gestión del acceso a las áreas donde se procesa o almacena la información. Los mecanismos de autenticación incluyen el uso de tarjetas de acceso, biometría o autenticación de dos factores, como una tarjeta de acceso y un PIN secreto. Se deben considerar puertas de seguridad para el acceso a áreas sensibles.

- Establecer un área de recepción supervisada por personal u otros medios para controlar el acceso físico a el sitio o edificio.

- Requerir que todo el personal y las partes interesadas usen algún tipo de identificación visible y que notifiquen de inmediato al personal de seguridad si encuentran visitantes sin escolta y cualquier persona que no use una identificación visible. Se deben considerar insignias fácilmente distinguibles para identificar mejor a los empleados permanentes, proveedores y visitantes.
- Otorgar acceso restringido al personal del proveedor a áreas seguras o instalaciones de procesamiento de información solo cuando sea necesario. Este acceso debe ser autorizado y monitoreado.
- Prestar especial atención a la seguridad del acceso físico en el caso de edificios que contengan activos para múltiples organizaciones.
- Diseñar medidas de seguridad física para que puedan reforzarse cuando aumente la probabilidad de incidentes físicos.
- Proteger otros puntos de entrada, como salidas de emergencia, del acceso no autorizado.

**Visitantes**

- Autenticar la identidad de los visitantes por un medio apropiado.
- Registrar la fecha y hora de entrada y salida de los visitantes.
- Permitir el acceso de visitantes únicamente para fines específicos, autorizados y con instrucciones sobre los requisitos de seguridad del área y sobre los procedimientos de emergencia.
- Supervisar a todos los visitantes, a menos que se conceda una excepción explícita.

**Zona de entrega y carga de material**

- Restringir el acceso a las áreas de entrega y carga desde el exterior del edificio al personal identificado y autorizado.
- Diseñar las áreas de entrega y carga para que puedan cargarse y descargarse los materiales sin personal de entrega que obtiene acceso no autorizado a otras partes del edificio.

- Asegurar las puertas externas de las áreas de entrega y carga cuando las puertas a las áreas restringidas están abiertas.
- Inspeccionar y examinar las entregas entrantes en busca de explosivos, productos químicos u otros materiales peligrosos, antes de que se muevan de las áreas de entrega y carga.
- Registrar las entregas entrantes de acuerdo con los procedimientos de gestión de activos al ingresar al sitio.
- Separar físicamente los envíos entrantes y salientes, cuando sea posible.
- Inspeccionar las entregas entrantes en busca de evidencia de manipulación en el camino. Si se descubre una manipulación, debe ser informado inmediatamente al personal de seguridad.

**Seguridad de oficinas, salas e instalaciones**

Se deben considerar las siguientes pautas para asegurar oficinas, salas e instalaciones.

- Ubicar las instalaciones críticas para evitar el acceso del público.
- Cuando corresponda, asegurarse de que los edificios sean discretos y den una indicación mínima de su propósito, sin señales obvias, fuera o dentro del edificio, que identifiquen la presencia de actividades de procesamiento de información.
- Configurar instalaciones para evitar que la información o actividades confidenciales sean visibles y audibles desde el exterior. El blindaje electromagnético también debe considerarse apropiado.
- No poner a disposición de cualquier persona no autorizada directorios, guías telefónicas internas y mapas accesibles en línea que identifican ubicaciones de instalaciones de procesamiento de información confidencial.

**Supervisión de la seguridad física**

Las instalaciones físicas deben ser monitoreadas por sistemas de vigilancia, que pueden incluir guardias, alarmas contra intrusos, sistemas de monitoreo de video como un circuito cerrado de

televisión y software de gestión de información de seguridad física, ya sea administrado internamente o por un proveedor de servicios de monitoreo.

El acceso a los edificios que albergan sistemas críticos debe monitorearse continuamente para detectar accesos no autorizados o comportamientos sospechosos mediante:

- Instalación de sistemas de monitoreo de video, tales como, circuito cerrado de televisión para ver y registrar el acceso a áreas sensibles dentro y fuera de las instalaciones de una organización.
- Instalar, de acuerdo con las normas pertinentes aplicables, y probar periódicamente el contacto, el sonido o detectores de movimiento para activar una alarma de intrusión como:
    - Detectores de contacto que activan una alarma cuando se hace o se interrumpe su función en cualquier lugar donde se puede hacer o romper un contacto (como ventanas, puertas y debajo de objetos) para ser utilizado como alarma de pánico.
    - Detectores de movimiento basados en tecnología infrarroja que disparan una alarma cuando pasa un objeto a través de su campo de visión.
    - Sensores sensibles al sonido de cristales rotos que pueden utilizarse para activar una alarma para alertar al personal de seguridad.
    - Usar esas alarmas para cubrir todas las puertas exteriores y ventanas accesibles. Las áreas desocupadas deben ser alarmadas en todo momento. También se debe proporcionar cobertura para otras áreas (por ejemplo, informática o comunicaciones).

El diseño de los sistemas de monitoreo debe mantenerse confidencial porque la divulgación puede facilitar robos no detectados.

Los sistemas de monitoreo deben protegerse contra el acceso no autorizado para evitar que personas no autorizadas accedan a la información de vigilancia, como transmisiones de video o que

los sistemas se deshabiliten de forma remota.

El panel de control del sistema de alarma debe colocarse en una zona específica para las alarmas de seguridad, en un lugar que permita una ruta de salida fácil para la persona que activa la alarma. El panel de control y los detectores deben tener mecanismos a prueba de manipulaciones. El sistema debe probarse periódicamente para asegurarse que funciona según lo previsto, especialmente si sus componentes funcionan con baterías.

**Protección contra amenazas físicas y ambientales**

Las evaluaciones de riesgos para identificar las posibles consecuencias de las amenazas físicas y ambientales deben realizarse antes de comenzar las operaciones críticas en un sitio físico y en intervalos regulares.

Debe obtener asesoramiento especializado sobre cómo gestionar los riesgos derivados de amenazas físicas y ambientales como incendios, inundaciones, terremotos, explosiones, disturbios civiles, desechos tóxicos, emisiones ambientales y otras formas de desastres naturales o desastres causados por seres humanos.

La ubicación y la construcción de las instalaciones físicas deben tener en cuenta:

- Topografía local, como elevación adecuada, masas de agua y fallas tectónicas.
- Amenazas urbanas, como lugares con un alto perfil para atraer disturbios políticos, actividad criminal o ataques terroristas.

Con base en los resultados de la evaluación de riesgos, se deben identificar las amenazas físicas y ambientales relevantes y se deben considerar los controles apropiados en los siguientes contextos:

- Incendio: instalar y configurar sistemas capaces de detectar incendios en una etapa temprana para enviar alarmas o activar los sistemas de supresión de incendios para evitar que el fuego dañe los medios de almacenamiento y los dispositivos relacionados con los sistemas de procesamiento de

información. La supresión de incendios debe realizarse utilizando los medios más apropiados, sustancia con respecto al entorno circundante (por ejemplo, gas en espacios confinados).

- Inundaciones: instalar sistemas capaces de detectar inundaciones en una etapa temprana debajo de los pisos de las áreas que contienen medios de almacenamiento o sistemas de procesamiento de información. Bombas de agua o medios equivalentes deben estar fácilmente disponibles en caso de que ocurra una inundación.

- Sobretensiones eléctricas: adopción de sistemas capaces de proteger los sistemas de información tanto del servidor como del cliente contra sobretensiones eléctricas o eventos similares para minimizar las consecuencias de tales eventos.

- Explosivos y armas: realizar inspecciones aleatorias para detectar la presencia de explosivos o armas sobre el personal, los vehículos o las mercancías que ingresan a las instalaciones de procesamiento de información confidencial.

Las cajas fuertes u otras formas de instalaciones de almacenamiento seguras pueden proteger la información almacenada en ellas contra desastres como incendios, terremotos, inundaciones o explosiones.

**Trabajar en áreas seguras**

Las medidas de seguridad para trabajar en áreas seguras deben aplicarse a todo el personal y cubrir todas las actividades que se desarrollen en el área segura.

Se deben considerar las siguientes pautas:

- Informar al personal solo de la existencia de actividades dentro de un área segura en caso de necesidad de saber.

- Evitar el trabajo sin supervisión en áreas seguras tanto por razones de seguridad como para reducir las posibilidades de actividades maliciosas.

- Cerrar físicamente e inspeccionar periódicamente las áreas seguras vacantes.

- No permitir equipos fotográficos, de video, de audio u otros equipos de grabación, como cámaras en el usuario, a menos que estén autorizados.
- Controlar adecuadamente el transporte y uso de los dispositivos de punto final del usuario en áreas seguras.
- Publicar los procedimientos de emergencia de manera fácilmente visible o accesible

**Escritorio despejado y pantalla despejada**

La organización debe establecer y comunicar una política específica del tema sobre escritorio despejado y pantalla despejada a todas las partes interesadas relevantes.

Se deben considerar las siguientes pautas:

- Guardar bajo llave la información comercial confidencial o crítica cuando no se requiera, especialmente cuando el cargo quede vacante.
- Proteger los dispositivos de punto final del usuario mediante cerraduras con llave u otros medios de seguridad cuando no estén en uso o desconectados.
- Dejar los dispositivos de punto final de usuario desconectados o protegidos con un mecanismo de bloqueo de pantalla y teclado controlado por un mecanismo de autenticación de usuario cuando están desatendidos. Todas las computadoras y sistemas deben configurarse con una función de tiempo de espera o cierre de sesión automático.
- Hacer que el originador recopile los resultados de las impresoras o dispositivos multifunción de inmediato. El uso de impresoras con una función de autenticación, de modo que los creadores sean los únicos que puedan obtener sus impresiones y solo cuando estén parados al lado de la impresora.
- Almacenar de forma segura documentos y medios de almacenamiento extraíbles que contengan información confidencial y cuando ya no se necesiten, desecharlos mediante

mecanismos seguros de eliminación.

- Establecer y comunicar reglas y orientación para la configuración de ventanas emergentes en las pantallas (desactivar las nuevas ventanas emergentes de correo electrónico y mensajería, si es posible, durante presentaciones, pantallas compartidas o en un área pública).

- Borrar información sensible o crítica en pizarras y otros tipos de pantallas cuando ya no sea requerido.

**Ubicación y protección de equipos**

Se deben considerar las siguientes pautas para proteger el equipo:

- Ubicar el equipo para minimizar el acceso innecesario a las áreas de trabajo y para evitar acceso.

- Ubicar cuidadosamente las instalaciones de procesamiento de información que manejan datos confidenciales para reducir el riesgo de información que es vista por personas no autorizadas durante su uso.

- Adoptar controles para minimizar el riesgo de posibles amenazas físicas y ambientales (como robo, incendio, explosivos, humo, agua o falla en el suministro de agua, polvo, vibración, efectos químicos, interferencia en el suministro eléctrico, interferencia en las comunicaciones, radiación electromagnética y vandalismo).

- Establecer pautas para comer, beber y fumar en la proximidad del procesamiento de la información.

- Monitorear las condiciones ambientales, tales como la temperatura y la humedad, en busca de condiciones que puedan afectar negativamente el funcionamiento de las instalaciones de procesamiento de información.

- Aplicar protección contra rayos a todos los edificios y colocar filtros de protección contra rayos en todas las entradas de las líneas eléctricas y de comunicaciones.

- Considerar el uso de métodos especiales de protección, tales como membranas de teclado, para equipos en ambientes industriales.
- Proteger los equipos que procesan información confidencial para minimizar el riesgo de fuga de información debido a la emanación electromagnética.
- Separar físicamente las instalaciones de procesamiento de información gestionadas por la organización de aquellas no gestionadas por la organización.

**Seguridad de los activos fuera de las instalaciones**

Cualquier dispositivo utilizado fuera de las instalaciones de la organización que almacene o procese información, incluidos los dispositivos propiedad de la organización y los dispositivos de propiedad privada y utilizados en nombre de la organización (su propio dispositivo (BYOD)) necesita protección.

Se deben considerar las siguientes pautas para la protección de dispositivos que almacenan o procesan información fuera de las instalaciones de la organización.

- No dejar el equipo y los medios de almacenamiento retirados de las instalaciones desatendidos en público y en lugares sin seguridad.
- Observar las instrucciones del fabricante para proteger el equipo en todo momento (protección contra exposición a fuertes campos electromagnéticos, agua, calor, humedad, polvo).
- Cuando se transfiere equipo fuera de las instalaciones entre diferentes personas o partes interesadas, mantener un registro que defina la cadena de custodia del equipo que incluya al menos los nombres y organizaciones de quienes son responsables del equipo. La información que no necesita transferirse con el activo debe eliminarse de forma segura antes de la transferencia.
- Cuando sea necesario y práctico, solicitar autorización para retirar equipos y medios de las instalaciones de la organización, así como, mantener una bitácora de tales retiros para garantizar un registro de auditoría.

- Protección contra la visualización de información en un dispositivo (móvil o portátil) en el transporte público, y los riesgos asociados con la navegación.
- Implementar el seguimiento de la ubicación y la capacidad para el borrado remoto de dispositivos.

**Medios de almacenamiento**

Se deben considerar las siguientes pautas para la gestión de medios de almacenamiento extraíbles:

- Establecer una política específica sobre la gestión de medios de almacenamiento extraíbles y comunicar dicha política específica a cualquier persona que use o manipule medios de almacenamiento extraíbles.
- Cuando sea necesario y práctico, solicitar autorización para que los medios de almacenamiento se retiren de la organización, así como, mantener una bitácora de tales retiros para garantizar un registro de auditoría.
- Resguardar todos los medios de almacenamiento en un entorno seguro y protegido de acuerdo con su clasificación de información y protegerlos contra amenazas ambientales (como calor, humedad, campo electrónico o deterioro), de acuerdo con las especificaciones de los fabricantes.
- Si la confidencialidad o la integridad de la información son consideraciones importantes, usar técnicas criptográficas para proteger la información en medios de almacenamiento extraíbles.
- Mitigar el riesgo de degradación de los medios de almacenamiento mientras aún se necesita la información almacenada, transfiriendo la información a nuevos medios de almacenamiento antes de volverse ilegible.
- Almacenar múltiples copias de información valiosa en medios de almacenamiento separados para reducir aún más el riesgo de daño o pérdida de información coincidente.
- Considerar el registro de medios de almacenamiento extraíbles para limitar la posibilidad de pérdida de información.

- Solo habilitar puertos de medios de almacenamiento extraíbles (ranuras para tarjetas Secure Digital (SD) y serie universal puertos de bus (USB)) sí existe una razón organizativa para su uso.
- Cuando sea necesario utilizar medios de almacenamiento extraíbles, monitorear la transferencia de información a tales medios de almacenamiento.
- La información puede ser vulnerable al acceso no autorizado, mal uso o corrupción durante el transporte, por ejemplo, cuando se envían medios de almacenamiento a través del servicio postal o de mensajería.

**Reutilización o eliminación segura**

Deben establecerse procedimientos para la reutilización o eliminación segura de los medios de almacenamiento, para minimizar el riesgo de fuga de información confidencial a personas no autorizadas.

Se deben considerar los siguientes elementos:

- Si los medios de almacenamiento que contienen información confidencial deben reutilizarse dentro de la organización, eliminar datos de forma segura o formatear los medios de almacenamiento antes de reutilizarlos.
- Deshacerse de medios de almacenamiento que contengan información confidencial de forma segura cuando ya no se necesiten (destruyendo, triturando o eliminando de forma segura el contenido).
- Contar con procedimientos para identificar los artículos que pueden requerir una eliminación segura.
- Muchas organizaciones ofrecen servicios de recogida y eliminación de medios de almacenamiento. Se debe tener cuidado en la selección de un proveedor externo adecuado con controles y experiencia adecuada.
- Registrar la eliminación de elementos sensibles para mantener un registro de auditoría.

- Acumular medios de almacenamiento para su eliminación.
- Tomar en cuenta que el efecto de agregación, puede hacer que una gran cantidad de información no confidencial se convierta en confidencial.

Se debe realizar una evaluación de riesgos en los dispositivos dañados que contengan datos confidenciales para determinar si los elementos deben destruirse físicamente en lugar de enviarse a reparar o desecharse.

Cuando la información confidencial en los medios de almacenamiento no está encriptada, se debe considerar la protección física adicional de los medios de almacenamiento.

**Utilidades de apoyo**

Las organizaciones dependen de los servicios públicos (por ejemplo, electricidad, telecomunicaciones, suministro de agua, gas, alcantarillado, ventilación y aire acondicionado) para respaldar sus instalaciones de procesamiento de información.

Por lo tanto, la organización debe:

- Asegurar que el equipo de apoyo a los servicios públicos esté configurado, operado y mantenido de acuerdo con las especificaciones del fabricante correspondiente.
- Garantizar que las empresas de servicios públicos sean evaluadas regularmente por su capacidad para satisfacer el crecimiento y las interacciones comerciales con otras empresas de servicios públicos de apoyo.
- Asegurarse de que el equipo de apoyo a los servicios públicos sea inspeccionado y probado periódicamente para garantizar su correcto funcionamiento.
- Si es necesario, activar alarmas para detectar fallas en los servicios públicos.
- Si es necesario, asegúrese de que las empresas de servicios públicos tengan múltiples alimentaciones con diversas rutas físicas.
- Asegurarse de que el equipo de apoyo a los servicios públicos esté en una red separada de las

instalaciones del procesamiento de información, si está conectado a una red.

- Asegurarse de que el equipo de apoyo a los servicios públicos esté conectado a internet solo cuando sea necesario y de manera segura.

Se debe proporcionar iluminación de emergencia y comunicaciones. Los interruptores y válvulas de emergencia para cortar la energía, el agua, el gas u otros servicios públicos deben ubicarse cerca de las salidas de emergencia o las salas de equipos.

Los detalles de los contactos de emergencia deben registrarse y estar disponibles para el personal en caso de un apagón.

**Seguridad del cableado**

Se deben considerar las siguientes pautas para la seguridad del cableado:

- Las líneas eléctricas y de telecomunicaciones a las instalaciones de procesamiento de información son subterráneas donde sea posible, o sujeto a una protección alternativa adecuada, como protector de cable de piso y poste de electricidad; si los cables son subterráneos, protegerlos de cortes accidentales (con blindaje conductos o señales de presencia).
- Separar los cables de alimentación de los cables de comunicaciones para evitar interferencias.
- Para sistemas sensibles o críticos, los controles adicionales a considerar incluyen:
    - Instalación de conductos blindados, cuartos o cajas cerradas y alarmas en los puntos de inspección y terminación.
    - Uso de blindaje electromagnético para proteger los cables.
    - Barridos técnicos periódicos e inspecciones físicas para detectar dispositivos no autorizados unido a los cables.
    - Acceso controlado a paneles de conexión y salas de cables (con llaves mecánicas o PIN).

- Uso de cables de fibra óptica.
- Etiquetar los cables en cada extremo con suficientes detalles de origen y destino para permitir la identificación física y la inspección del cable.

Se debe buscar el asesoramiento de especialistas sobre cómo gestionar los riesgos derivados de incidentes o mal funcionamiento del cableado.

**Mantenimiento de equipos**

Se deben considerar las siguientes pautas para el mantenimiento del equipo:

- Mantener el equipo de acuerdo con la frecuencia de servicio recomendada por el proveedor y especificaciones.
- Implementación y seguimiento de un programa de mantenimiento por parte de la organización.
- Solo personal de mantenimiento autorizado será el que realice reparaciones y mantenimiento en el equipo.
- Mantener registros de todas las fallas sospechadas o reales y de todo mantenimiento preventivo y correctivo.
- Implementar controles apropiados cuando el equipo esté programado para mantenimiento, teniendo en cuenta si este mantenimiento es realizado por personal en el sitio o externo a la organización; someter al personal de mantenimiento a un adecuado acuerdo de confidencialidad.
- Supervisar al personal de mantenimiento al realizar el mantenimiento en el sitio.
- Autorizar y controlar el acceso para el mantenimiento remoto.
- Aplicar medidas de seguridad para activos fuera de las instalaciones, si el equipo que contiene información es sacado de las instalaciones para mantenimiento.
- Cumplir con todos los requisitos de mantenimiento impuestos por el seguro.
- Antes de volver a poner en funcionamiento el equipo después del mantenimiento, inspeccionar

para asegurarse de que el equipo no ha sido manipulado y funciona correctamente.

- Aplicar medidas para la eliminación o reutilización segura del equipo si se determina que se va a desechar el mismo.

**Eliminación segura o reutilización de equipos**

El equipo debe verificarse para asegurarse de que los medios de almacenamiento estén o no contenidos antes de su eliminación o reutilización.

Los medios de almacenamiento que contengan información confidencial o con derechos de autor deben destruirse físicamente o la información debe destruirse, eliminarse o sobrescribirse utilizando técnicas para hacer que la información original no se pueda recuperar en lugar de utilizar la función de eliminación estándar.

Las etiquetas y marcas que identifiquen a la organización o que indique la clasificación, el propietario, el sistema o la red deben retirarse antes de su eliminación, incluida la reventa o la donación a organizaciones benéficas.

La organización debe considerar la eliminación de los controles de seguridad, como los controles de acceso o el equipo de vigilancia, al final del contrato de arrendamiento o al mudarse de las instalaciones.

Esto depende de factores como:

- Su contrato de arrendamiento para devolver la instalación a su condición original.
- Minimizar el riesgo de dejar los sistemas con información confidencial para el próximo inquilino (listas de acceso de usuarios, archivos de video o imagen).
- La capacidad de reutilizar los controles en la siguiente instalación.

Los equipos dañados que contienen medios de almacenamiento pueden requerir una evaluación de riesgos para determinar si los elementos deben destruirse físicamente en lugar de enviarse a reparar o desecharse. La información puede verse comprometida por la eliminación descuidada o la

reutilización del equipo.

Además de la eliminación segura del disco, el cifrado de disco completo reduce el riesgo de divulgación de información confidencial cuando el equipo se desecha o se vuelve a implementar, siempre que:

- El proceso de cifrado es lo suficientemente sólido y cubre todo el disco (incluido el espacio de holgura, el archivo de intercambio)
- Las claves criptográficas son lo suficientemente largas para resistir ataques de fuerza bruta.
- Las claves criptográficas se mantienen confidenciales ( nunca se almacenan en el mismo disco).

Las técnicas para sobrescribir de forma segura los medios de almacenamiento, difieren según la tecnología de los medios de almacenamiento y el nivel de clasificación de la información en los mismos. Las herramientas de sobrescritura deben revisarse para asegurarse de que sean aplicables a la tecnología de los medios de almacenamiento.

**Controles tecnológicos**

**Dispositivos de punto final de usuario**

La organización debe establecer una política específica del tema sobre la configuración y el manejo seguros de los dispositivos de punto final del usuario.

La política específica del tema debe comunicarse a todo el personal pertinente y considerar lo siguiente:

- El tipo de información y el nivel de clasificación que pueden manejar los dispositivos de punto final del usuario, procesar, almacenar o soportar.
- Registro de dispositivos de punto final de usuario.
- Requisitos de protección física.

- Restricción de la instalación de software (controlado de forma remota por los administradores del sistema).
- Requisitos para el software del dispositivo de punto final del usuario (incluidas las versiones de software) y para aplicar actualizaciones (actualización automática activa).
- Reglas para la conexión a servicios de información, redes públicas o cualquier otra red fuera de las instalaciones, que requiera el uso de un cortafuegos personal.
- Controles de acceso.
- Cifrado del dispositivo de almacenamiento.
- Protección contra malware.
- Deshabilitación, borrado o bloqueo remoto.
- Copias de seguridad.
- Uso de servicios web y aplicaciones web.
- Análisis del comportamiento del usuario final.
- El uso de dispositivos extraíbles, incluidos los dispositivos de memoria extraíbles, y la posibilidad de desactivar puertos físicos (puertos USB).
- El uso de capacidades de particionamiento, si es compatible con el dispositivo de punto final del usuario, que puede separar la información de la organización y otros activos asociados (como software) y otros activos asociados a la información en el dispositivo.

**Responsabilidad del usuario**

Todos los usuarios deben ser conscientes de los requisitos y procedimientos de seguridad para proteger los dispositivos de punto final de los usuarios, así como de sus responsabilidades para implementar dichas medidas de seguridad.

Se debe recomendar a los usuarios que:

- Cerrar sesiones activas y cancelar servicios cuando ya no se necesiten.

- Proteger los dispositivos de punto final del usuario del uso no autorizado con un control físico (bloqueo de teclas o bloqueos especiales) y control lógico (acceso mediante contraseña) cuando no se utiliza; no deje los dispositivos que llevan información comercial importante, sensible o crítica desatendidos.

- Usar dispositivos con especial cuidado en lugares públicos, oficinas abiertas, lugares de reunión y otros lugares desprotegidos (evite leer información confidencial si las personas pueden leer desde atrás, use privacidad filtros de pantalla).

- Proteger físicamente los dispositivos de punto final del usuario contra el robo (en automóviles y otras formas de transporte, habitaciones de hotel, centros de conferencias y lugares de reunión).

Debe establecerse un procedimiento específico que tenga en cuenta los requisitos legales, estatutarios, reglamentarios, contractuales (incluidos los seguros) y otros requisitos de seguridad de la organización para casos de robo o pérdida de dispositivos de punto final de usuario.

**Uso de dispositivos personales**

Cuando la organización permite el uso de dispositivos personales (a veces conocidos como BYOD), además de la orientación proporcionada en este control, se debe considerar lo siguiente:

- Separación del uso personal y comercial de los dispositivos, incluido el uso de software para respaldar dicha separación y proteger los datos comerciales en un dispositivo privado.

- Proporcionar acceso a la información comercial solo después de que los usuarios hayan reconocido sus funciones (protección física , actualización de software, etc.), renunciando a la propiedad de los datos comerciales, permitiendo el borrado remoto de datos por parte de la organización en caso de robo o pérdida del dispositivo o cuando ya no esté autorizado para su uso el servicio. En tales casos, se debe considerar la legislación de protección de PII.

- Políticas y procedimientos específicos del tema para prevenir disputas relacionadas con los

derechos de propiedad intelectual desarrollado en equipo de propiedad privada.

- Acceso a equipos de propiedad privada (para verificar la seguridad de la máquina o durante una investigación), que pueden ser prevenidos por la legislación.

- Acuerdos de licencia de software que son tales, que las organizaciones pueden ser responsables de la concesión de licencias para software de cliente en dispositivos de punto final, de usuario propiedad privada, de uso personal o usuarios externos.

**Conexiones inalámbricas**

La organización debe establecer procedimientos para:

- La configuración de conexiones inalámbricas en dispositivos (desactivación de protocolos vulnerables).

- Usando conexiones inalámbricas o cableadas con el ancho de banda apropiado de acuerdo con las políticas específicas del tema (porque se necesitan copias de seguridad o actualizaciones de software).

**Derecho de acceso privilegiado**

La asignación de derechos de acceso privilegiado debe controlarse a través de un proceso de autorización de acuerdo con la política de control de acceso específica del tema relevante.

Se debe considerar lo siguiente:

- Identificar a los usuarios que necesitan derechos de acceso privilegiado para cada sistema o proceso (sistemas, sistemas de gestión de bases de datos y aplicaciones).

- Asignar derechos de acceso privilegiado a los usuarios, según sea necesario y caso por caso de acuerdo con la política específica del tema sobre el control de acceso (es decir, solo a personas con la necesaria competencia para realizar actividades que requieran un acceso privilegiado y en base a los mínimos requisito para sus roles funcionales).

- Mantener un proceso de autorización (es decir, determinar quién puede aprobar derechos de

acceso privilegiado, o no otorgar derechos de acceso privilegiado hasta que se complete el proceso de autorización) y un registro de todos los privilegios asignados.

- Definir e implementar los requisitos para la expiración de los derechos de acceso privilegiado.
- Tomar medidas para garantizar que los usuarios conozcan sus derechos de acceso privilegiado y cuándo se encuentran en el modo de acceso privilegiado. Las posibles medidas incluyen el uso de identidades de usuario específicas, configuraciones de interfaz de usuario o incluso equipos específicos.
- Los requisitos de autenticación para los derechos de acceso privilegiado pueden ser más altos que los requisitos para los derechos de acceso normales. Puede ser necesario volver a autenticarse o aumentar la autenticación antes de trabajar con derechos de acceso privilegiados.
- Regularmente y después de cualquier cambio organizacional, revisar a los usuarios que trabajan con derechos de acceso privilegiado para verificar si sus deberes, roles, responsabilidades y competencia aún los califican para trabajar con derechos de acceso privilegiado.
- Establecer reglas específicas para evitar el uso de identificaciones de usuario de administración genéricas (como “root”), dependiendo de las capacidades de configuración de los sistemas. Administrar y proteger la información de autenticación de tales identidades.
- Otorgar acceso privilegiado temporal solo durante el período de tiempo necesario para implementar cambios o actividades aprobadas (para actividades de mantenimiento o algunos cambios críticos), en lugar de otorgar derechos de acceso privilegiado de forma permanente. Esto a menudo se conoce como procedimiento de rotura de cristal y a menudo, se automatiza mediante tecnologías de gestión de acceso privilegiado.
- Registrar todos los accesos privilegiados a los sistemas con fines de auditoría.
- No compartir o vincular identidades con derechos de acceso privilegiado a múltiples personas, asignando a cada persona una identidad separada que permita asignar derechos de acceso privilegiado específicos. Las identidades se pueden agrupar (definiendo un grupo de

administradores) para simplificar la gestión de los derechos de acceso privilegiado.

- Usar únicamente identidades con derechos de acceso privilegiado para realizar tareas administrativas y no para tareas generales del día a día, es decir, revisar el correo electrónico, acceder a la web (los usuarios deben tener una identidad de red normal separada para estas actividades)

Los roles de administrador del sistema generalmente requieren derechos de acceso privilegiado. El uso inapropiado de los privilegios del administrador del sistema (cualquier característica o instalación de un sistema de información que permita al usuario anular los controles del sistema o de la aplicación) es un factor importante que contribuye a las fallas o violaciones de los sistemas.

**Restricciones de acceso a la información**

El acceso a la información y otros activos asociados debe estar restringido de acuerdo con las políticas específicas del tema.

Se debe considerar lo siguiente para respaldar los requisitos de restricción de acceso:

- No permitir el acceso a información sensible por parte de usuarios con identidades desconocidas o de forma anónima. El acceso público o anónimo sólo debe otorgarse a lugares de almacenamiento que no contengan información confidencial.
- Proporcionar mecanismos de configuración para controlar el acceso a la información en sistemas, aplicaciones y servicios.
- Controlar a qué datos puede acceder un usuario en particular.
- Controlar qué identidades o grupo de identidades tienen qué acceso, tales como lectura, escritura, eliminación y ejecución.
- Proporcionar controles de acceso físicos o lógicos para el aislamiento de aplicaciones sensibles, datos de aplicaciones o sistemas.

Los sistemas de gestión de acceso dinámico deben proteger la información mediante:

- Exigir autenticación, credenciales apropiadas o un certificado para acceder a la información.
- Restringir el acceso, por ejemplo, en un período de tiempo específico.
- Usar cifrado para proteger la información.
- Definir los permisos de impresión de la información.
- Registrar quién accede a la información y cómo se utiliza la información.
- Generar alertas si se detectan intentos de mal uso de la información.

**Acceso al código fuente**

Se deben considerar las siguientes pautas para controlar el acceso a las bibliotecas de fuentes de programas a fin de reducir una potencial corrupción de los programas de computadora:

- Administrar el acceso al código fuente del programa y las bibliotecas fuente del programa de acuerdo con procedimientos establecidos.
- Conceder acceso de lectura y escritura al código fuente en función de las necesidades empresariales, gestionado para abordar riesgos de alteración o mal uso, de acuerdo con los procedimientos establecidos.
- Actualización del código fuente, elementos asociados y otorgamiento de acceso al código fuente de acuerdo con los procedimientos de control de cambios, esto solo debe realizarse después que la autorización apropiada ha sido recibida.
- No otorgar a los desarrolladores acceso directo al repositorio de código fuente, sino a través de herramientas para desarrolladores que controlan las actividades y autorizaciones sobre el código fuente.
- Mantener listados de programas en un entorno seguro, donde el acceso de lectura y escritura debe ser adecuadamente administrado y asignado.
- Mantener un registro de auditoría de todos los accesos y de todos los cambios en el código

fuente.

**Autenticación segura**

La información de autenticación debe ir acompañada de factores de autenticación adicionales para acceder a los sistemas de información crítica (también conocida como autenticación de múltiples factores). El uso de una combinación de múltiples factores de autenticación, reduce las posibilidades de accesos no autorizados.

Los procedimientos y tecnologías de inicio de sesión deben implementarse teniendo en cuenta lo siguiente:

- No mostrar información confidencial del sistema o de la aplicación hasta que se haya completado el proceso de inicio de sesión con éxito, para evitar proporcionar a un usuario no autorizado cualquier información innecesaria.
- Mostrar un aviso general advirtiendo que el sistema, aplicación o el servicio solo debe ser accedido por usuarios autorizados.
- No proporcionar mensajes de ayuda durante el procedimiento de inicio de sesión que guiarán a un usuario no autorizado (si surge una condición de error, el sistema no debe indicar qué parte de los datos es correcta o incorrecta).
- Validar la información de inicio de sesión solo al completar todos los datos de entrada.
- Protección contra intentos de inicio de sesión de fuerza bruta en nombres de usuario y contraseñas (usando complementos como, Prueba de Turing pública automatizada para diferenciar computadoras y humanos “CAPTCHA”, que requiera restablecer contraseña después de un número predefinido de intentos fallidos o bloquear al usuario después de un número máximo de errores).
- Registrar intentos fallidos y exitosos.
- Generar un evento de seguridad si se detecta un intento potencial o una violación exitosa de los controles de inicio de sesión (por ejemplo, enviar una alerta al usuario y a los administradores del

sistema de la organización cuando se ha alcanzado un número determinado de intentos de contraseña incorrectos).

- Mostrar o enviar la siguiente información en un canal separado al completarse con éxito

1) Fecha y hora del inicio de sesión exitoso.

2) Detalles de cualquier intento fallido de inicio de sesión desde el último inicio de sesión exitoso.

- No mostrar una contraseña en texto claro cuando se ingresa; en algunos casos, puede ser necesario desactivar esta funcionalidad para facilitar el inicio de sesión del usuario (por razones de accesibilidad o para evitar el bloqueo de usuarios por errores repetidos).

- No transmitir contraseñas en texto claro a través de una red para evitar ser capturado por una red programa "sniffer".

- Finalizar sesiones inactivas después de un período definido de inactividad, especialmente en ubicaciones de alto riesgo tales como áreas públicas o externas fuera de la gestión de seguridad de la organización o dispositivos de punto final en el usuario.

- Restringir los tiempos de duración de la conexión para proporcionar seguridad adicional para aplicaciones de alto riesgo y reducir la ventana de oportunidad para el acceso no autorizado.

**Gestión de capacidad**

La organización podrá realizar pruebas de estrés de los sistemas y servicios para confirmar que hay suficiente capacidad del sistema disponible para cumplir con los requisitos de rendimiento máximo.

Se debe considerar lo siguiente para aumentar la capacidad:

- Contratación de nuevo personal.

- Obtención de nuevas instalaciones o espacios.

- Adquirir sistemas de procesamiento, memoria y almacenamiento más potentes.

- Hacer uso de la computación en la nube, que tiene características inherentes que abordan

directamente cuestiones de capacidad. La computación en la nube tiene elasticidad y escalabilidad que permiten una rápida expansión bajo demanda y reducción de los recursos disponibles para aplicaciones y servicios particulares.

Se debe considerar lo siguiente para reducir la demanda de los recursos de la organización:

- Eliminación de datos obsoletos (espacio en disco).
- Eliminación de registros impresos que hayan cumplido su período de retención (liberar espacio en los estantes).
- Desmantelamiento de aplicaciones, sistemas, bases de datos o entornos.
- Optimizar procesos por lotes y cronogramas.
- Optimizar el código de la aplicación o las consultas de la base de datos.
- Denegar o restringir el ancho de banda para los servicios que consumen recursos si estos no son críticos ( vídeo transmitido en vivo).

**Protección contra malware**

La protección contra el malware debe basarse en el software de detección y reparación de malware, la conciencia de seguridad de la información, el acceso adecuado al sistema y los controles de gestión de cambios.

Se debe considerar la siguiente orientación:

- Implementar reglas y controles que prevengan o detecten el uso de software no autorizado.
- Implementar controles que prevengan o detecten el uso de sitios web maliciosos conocidos o sospechosos (listas de bloqueo).
- Reducir las vulnerabilidades que pueden ser explotadas por malware (a través de vulnerabilidades técnicas de gestión).

- Llevar a cabo una validación automatizada periódica del software y el contenido de datos de los sistemas, especialmente para los sistemas que soportan procesos comerciales críticos; investigar la presencia de archivos no aprobados o enmiendas no autorizadas.

- Establecer medidas de protección contra los riesgos asociados con la obtención de archivos y software ya sea desde o a través de redes externas o en cualquier otro medio.

- Instalar y actualizar regularmente software de detección y reparación por malware para escanear computadoras y medios de almacenamiento electrónicos. Realización de escaneos regulares que incluyen:

- Escanear cualquier dato recibido a través de redes o mediante cualquier forma de medio de almacenamiento electrónico, en busca de malware antes de su uso.

- Escanear archivos adjuntos y descargas de correo electrónico y mensajería instantánea en busca de malware antes de su uso. Llevar a cabo este escaneo en diferentes lugares (en servidores de correo electrónico, computadoras de escritorio) y al ingresar a la red de la organización.

- Escanear páginas web en busca de malware cuando se accede a ellas.

- Determinar la ubicación y configuración de las herramientas de detección y reparación de malware en función de los riesgo resultados de la evaluación y considerando:

- Principios de defensa en profundidad donde serían más efectivos. Por ejemplo, esto puede conducir a la detección de malware en una puerta de enlace de red (en varios protocolos de aplicación, como correo electrónico, transferencia de archivos y web), así como en servidores y dispositivos de punto final de usuario.

- Las técnicas evasivas de los atacantes (el uso de archivos cifrados) para entregar malware o el uso de protocolos de encriptación para transmitir malware.

- Tener cuidado de protegerse contra la introducción de malware durante los procedimientos de mantenimiento y emergencia, que pueden eludir los controles normales contra el malware.

- Implementar un proceso para autorizar la desactivación temporal o permanente de algunas o todas las medidas contra el malware, incluidas las autoridades de aprobación de excepciones, la justificación documentada y la fecha de revisión. Esto puede ser necesario cuando la protección contra malware provoca la interrupción de las operaciones normales.
- Aislar ambientes donde puedan ocurrir consecuencias catastróficas.
- Definir procedimientos y responsabilidades para tratar la protección contra malware en los sistemas, incluida la capacitación en su uso, informes y recuperación de ataques de malware.
- Brindar conciencia o capacitación a todos los usuarios sobre cómo identificar y mitigar potencialmente la recepción, el envío o la instalación de correos electrónicos, archivos o programas infectados con malware.
- Implementar procedimientos para recopilar regularmente información sobre nuevo malware, como suscribirse a listas de correo o revisar sitios web relevantes.
- Verificar que la información relacionada con el malware, como los boletines de advertencia, provenga de fuentes calificadas y acreditadas (sitios de Internet confiables o proveedores de software de detección de malware) y que sea precisa e informativa.

**Gestión de vulnerabilidades técnicas**

La organización debe tener un inventario preciso de los activos como requisito previo para la gestión eficaz de la vulnerabilidad técnica; el inventario debe incluir el proveedor del software, el nombre del software, los números de versión, el estado actual de implementación (por ejemplo, qué software está instalado en qué sistemas) y la(s) persona(s) dentro de la organización responsable del software.

Para identificar vulnerabilidades técnicas, la organización debe considerar:

- Definir y establecer los roles y responsabilidades asociadas a la gestión técnica de vulnerabilidades, incluido el monitoreo, el riesgo, la actualización, el seguimiento de activos y

cualquier responsabilidad de coordinación requerida.

- Para software y otras tecnologías (basado en la lista de inventario de activos), identificando recursos de información que se utilizarán para identificar vulnerabilidades técnicas y manteniendo la conciencia sobre ellos. Actualizar la lista de recursos de información en función de los cambios en el inventario o cuando se encuentran otros recursos nuevos o útiles.
- Exigir a los proveedores del sistema de información (incluidos sus componentes) que garanticen la notificación, el manejo y divulgación, incluidos los requisitos en los contratos aplicables.
- Usar herramientas de escaneo de vulnerabilidades adecuadas para las tecnologías en uso para identificar y verificar si el parcheo fue exitoso.
- Realizar pruebas de penetración o evaluaciones de vulnerabilidad planificadas, documentadas y repetibles por personas competentes y autorizadas para apoyar la identificación de vulnerabilidades. Tener precaución ya que tales actividades pueden comprometer la seguridad del sistema.
- Rastrear el uso de bibliotecas de terceros y código fuente en busca de vulnerabilidades.

**Gestión de la configuración**

La organización debe definir e implementar procesos y herramientas para hacer cumplir las configuraciones definidas (incluidas las configuraciones de seguridad) para el hardware, el software, los servicios ( servicios en la nube) y las redes, tanto para los sistemas recién instalados como para los sistemas operativos durante su vida útil.

Las plantillas estándar para la configuración segura de hardware, software, servicios y redes deben definirse:

- Utilizando orientación disponible públicamente (plantillas predefinidas de proveedores y de organizaciones de seguridad independientes).

- Considerar el nivel de protección necesario para determinar un nivel suficiente de seguridad.
- Respaldar la política de seguridad de la información de la organización, las políticas específicas del tema, los estándares y otros requisitos de seguridad, considerando la factibilidad y aplicabilidad de las configuraciones de seguridad en el contexto de la organización.

Las plantillas deben revisarse periódicamente y actualizarse cuando sea necesario abordar nuevas amenazas o vulnerabilidades, o cuando se introduzcan nuevas versiones de software o hardware.

**Eliminación de información**

La información confidencial no debe conservarse más tiempo del necesario para reducir el riesgo de divulgación no deseada.

Al eliminar información sobre sistemas, aplicaciones y servicios, se debe considerar lo siguiente:

- Seleccionar un método de eliminación (sobrescritura electrónica o borrado criptográfico) de acuerdo con los requisitos comerciales y teniendo en cuenta las leyes y regulaciones pertinentes.
- Registrar los resultados de la eliminación como prueba.
- Al utilizar proveedores de servicios de eliminación de información, obtener evidencia de borrado de información de ellos.

**Enmascaramiento de datos**

El enmascaramiento de datos es un conjunto de técnicas para ocultar, sustituir u ofuscar elementos de datos confidenciales.

Las técnicas adicionales para el enmascaramiento de datos incluyen:

- Encriptación (que requiere que los usuarios autorizados tengan una clave).
- Anular o eliminar caracteres (evitando que los usuarios no autorizados vean los mensajes completos).
- Números y fechas variables.

- Sustitución (cambiar un valor por otro para ocultar datos sensibles).
- Reemplazar valores con su hash.

**Prevención de fuga de datos**

Las herramientas de prevención de fuga de datos están diseñadas para identificar, monitorear el uso y el movimiento de datos y tomar medidas para evitar la fuga.

La organización podrá considerar lo siguiente para reducir el riesgo de fuga de datos:

- Identificar y clasificar la información para protegerla contra fugas ( información personal, modelos de precios y diseños de productos).
- Monitorear los canales de fuga de datos (correo electrónico, transferencias de archivos, dispositivos móviles y dispositivos portátiles de almacenamiento ).
- Actuar para evitar que se filtre información (poner en cuarentena correos electrónicos que contengan información).

Las acciones de prevención de fuga de datos deben estar orientadas a confundir las decisiones del adversario, este tipo de acciones son la ingeniería social inversa o el uso de honeypots para atraer a los atacantes.

**Copia de seguridad de la información**

Se deben desarrollar e implementar planes sobre cómo la organización respaldará la información, el software y los sistemas, para abordar la política específica del tema sobre respaldo.

Al diseñar un plan de respaldo, se deben tener en cuenta los siguientes elementos:

- Producir registros precisos y completos de las copias de seguridad y los procedimientos de restauración documentados.
- Reflejar los requisitos comerciales de la organización (el objetivo del punto de recuperación), los requisitos de seguridad de la información involucrada y la criticidad de la información para la

operación continua de la organización en la medida y frecuencia de las copias de seguridad.

- Almacenar las copias de seguridad en un lugar remoto seguro y protegido, a una distancia suficiente para escapar de cualquier daños por un desastre en el sitio principal.
- Dar a la información de respaldo un nivel adecuado de protección física y ambiental consistente con los estándares aplicados en el sitio principal.
- Probar regularmente los medios de respaldo para garantizar que se pueda confiar en ellos para uso de emergencia cuando sea necesario. Probar la capacidad de restaurar datos respaldados en un sistema de prueba, sin sobrescribir el medio de almacenamiento original en caso de que el proceso de copia de seguridad o restauración falle y cause daños o pérdidas irreparables de datos.
- Proteger las copias de seguridad mediante encriptación de acuerdo con los riesgos identificados (en situaciones donde la confidencialidad es de importancia).
- Asegurarse de que se detecte la pérdida inadvertida de datos antes de realizar la copia de seguridad.

Las medidas de respaldo para sistemas y servicios individuales deben probarse regularmente para garantizar que cumplan con los objetivos de respuesta a incidentes y planes de continuidad del negocio.

**Redundancia de las instalaciones de procesamiento de información.**

La organización podrá planificar e implementar procedimientos para la activación de los componentes redundantes y las instalaciones de procesamiento.

La organización debe considerar lo siguiente al implementar sistemas redundantes:

- Contratación con dos o más proveedores de redes e instalaciones de procesamiento de información crítica como proveedores de servicios de Internet.
- Usar redes redundantes.
- Utilizar dos centros de datos separados geográficamente con sistemas duplicados.

- Utilizar fuentes de alimentación físicamente redundantes.
- Usar múltiples instancias paralelas de componentes de software, con equilibrio de carga automático entre ellos (entre instancias en el mismo centro de datos o en diferentes centros de datos).
- Tener componentes duplicados en sistemas (CPU, discos duros, memorias) o en redes (cortafuegos, enrutadores, conmutadores).

Muchas de las medidas de redundancia pueden formar parte de las estrategias y soluciones de continuidad de las TIC.

**Registro**

La organización debe determinar el propósito para el cual se crean los registros, qué datos se recopilan y registran y cualquier requisito específico del registro para proteger y manejar los datos de registro.

Los siguientes eventos deben ser considerados para el registro:

- Intentos de acceso al sistema exitosos y rechazados.
- Datos exitosos y rechazados y otros intentos de acceso a recursos.
- Cambios en la configuración del sistema.
- Uso de privilegios.
- Uso de programas de utilidad y aplicaciones.
- Los archivos a los que se accede y el tipo de acceso, incluida la eliminación de archivos de datos importantes.
- Alarmas emitidas por el sistema de control de acceso.
- Activación y desactivación de sistemas de seguridad, como sistemas antivirus y sistemas de

detección de intrusos.

- Creación, modificación o supresión de identidades.
- Transacciones ejecutadas por los usuarios en las aplicaciones. En algunos casos, las aplicaciones son un servicio o producto proporcionado o administrado por un tercero.

El registro de eventos sienta las bases para los sistemas de monitoreo automatizados que son capaces de generar informes consolidados y alertas sobre la seguridad del sistema.

**Actividades de seguimiento**

El alcance y el nivel de monitoreo deben determinarse de acuerdo con los requisitos de seguridad de la información y del negocio y teniendo en cuenta las leyes y regulaciones pertinentes.

Lo siguiente debe ser considerado para su inclusión dentro del sistema de monitoreo.

- Tráfico de red, sistema y aplicación entrante y saliente.
- Acceso a sistemas, servidores, equipos de red, sistema de monitoreo, aplicaciones críticas, etc.
- Archivos de configuración de red y sistema de nivel crítico o administrativo.
- Registros de herramientas de seguridad (antivirus, IDS, sistema de prevención de intrusiones (IPS), filtros web, firewalls, prevención de fuga de datos).
- Registros de eventos relacionados con la actividad del sistema y de la red.
- Comprobar que el código que se está ejecutando está autorizado para ejecutarse en el sistema y que no ha sido manipulado (mediante la recopilación para agregar código adicional no deseado).
- Uso de los recursos (CPU, discos duros, memoria, ancho de banda) y su rendimiento.

Las actividades de monitoreo a menudo se realizan utilizando software especializado, como los sistemas de detección de intrusos.

**Sincronización del reloj**

La configuración correcta de los relojes de las computadoras es importante para garantizar la precisión de los registros de eventos, que pueden ser necesarios para investigaciones o como evidencia en casos legales y disciplinarios.

**Uso de programas de utilidad privilegiados**

Se deben considerar las siguientes pautas para el uso de programas de utilidad que pueden anular los controles del sistema y de la aplicación:

- Limitación del uso de programas de utilidad al número mínimo práctico de usuarios autorizados de confianza.
- Uso de procedimientos de identificación, autenticación y autorización para programas de utilidad, incluyendo la identificación única de la persona que usa el programa de utilidad.
- Definición y documentación de niveles de autorización para programas de servicios públicos.
- Autorización para uso cuando sea necesario para programas utilitarios.
- No poner programas de utilidad a disposición de los usuarios que tienen acceso a aplicaciones en sistemas donde se requiere segregación de funciones.
- Eliminar o deshabilitar todos los programas de utilidad innecesarios.
- Como mínimo, separación lógica de los programas de utilidad del software de aplicación. Cuando sea práctico, segregar las comunicaciones de red para dichos programas del tráfico de aplicaciones.
- Limitación de la disponibilidad de los programas de utilidad (durante la duración de un cambio autorizado).
- Registro de todos los usos de los programas de utilidad.

La mayoría de los sistemas de información tienen uno o más programas de utilidad que pueden anular los controles del sistema y de las aplicaciones, por ejemplo, diagnósticos, parches, antivirus, desfragmentadores de disco, depuradores, copias de seguridad y herramientas de red.

**Instalación de software en sistemas operativos**

Se deben considerar las siguientes pautas para administrar de forma segura los cambios y la instalación de software en los sistemas operativos:

- Realizar actualizaciones del software operativo solo por parte de administradores capacitados según corresponda autorización de gestión.
- Asegurarse de que solo se instale código ejecutable aprobado y ningún código de desarrollo o compiladores en sistemas operativos.
- Solo instalar y actualizar el software después de pruebas extensas y exitosas.
- Actualizar todas las bibliotecas fuente de programas correspondientes.
- Usar un sistema de control de configuración para mantener el control de todo el software operativo, así como la documentación del sistema.
- Definir una estrategia de reversión antes de que se implementen los cambios.
- Mantener un registro de auditoría de todas las actualizaciones del software operativo.
- Archivar versiones antiguas de software, junto con toda la información y los parámetros requeridos, procedimientos, detalles de configuración y software de soporte como medida de contingencia y para siempre que el software sea necesario para leer o procesar datos archivados.

Cuando los proveedores estén involucrados en la instalación o actualización de software, el acceso físico o lógico sólo debe otorgarse cuando sea necesario y con la debida autorización.

La organización debe definir y hacer cumplir reglas estrictas sobre qué tipos de software pueden instalar los usuarios.

**Seguridad en redes**

Se deben implementar controles para garantizar la seguridad de la información en las redes y para proteger los servicios conectados del acceso no autorizado.

se deben considerar los siguientes elementos:

- El tipo y nivel de clasificación de la información que la red puede soportar.
- Establecer responsabilidades y procedimientos para la gestión de equipos y dispositivos de red.
- Mantener actualizada la documentación, incluidos los diagramas de red y los archivos de configuración de dispositivos (enrutadores, conmutadores).
- Separar la responsabilidad operativa de las redes de las operaciones del sistema TIC cuando corresponda.
- Establecer controles para salvaguardar la confidencialidad e integridad de los datos que pasan por redes públicas, redes de terceros o redes inalámbricas y para proteger los sistemas y aplicaciones conectadas. También se pueden requerir controles adicionales para mantener la disponibilidad de los servicios de red y las computadoras conectadas a la red.
- Registro y seguimiento adecuados para permitir el registro y la detección de acciones que pueden afectar o son relevantes para la seguridad de la información.
- Coordinar estrechamente las actividades de gestión de la red para optimizar el servicio a la organización y para asegurar que los controles se aplican en forma coherente en toda la infraestructura de procesamiento de la información.
- Sistemas de autenticación en la red.
- Restringir y filtrar la conexión de los sistemas a la red (usando firewalls).
- Detectar, restringir y autenticar la conexión de equipos y dispositivos a la red.
- Endurecimiento de los dispositivos de red.
- Segregar los canales de administración de red de otro tráfico de red.
- Aislar temporalmente subredes críticas (con puentes levadizos) si la red está bajo ataque.

- Deshabilitar protocolos de red vulnerables.

La organización debe garantizar que se apliquen los controles de seguridad adecuados al uso de redes virtualizadas.

**Seguridad de los servicios de red**

Las medidas de seguridad necesarias para servicios particulares, tales como características de seguridad, niveles de servicio y requisitos de servicio, deben ser identificadas e implementadas (por proveedores de servicios de red internos o externos).

Las reglas sobre el uso de redes y servicios de red deben formularse e implementarse para cubrir:

- Las redes y los servicios de red a los que se permite acceder.
- Requisitos de autenticación para acceder a diversos servicios de red.
- Procedimientos de autorización para determinar a quién se le permite acceder a qué redes y servicios en red.
- Gestión de la red, controles y procedimientos tecnológicos para proteger el acceso a conexiones de red y servicios de red.
- Los medios utilizados para acceder a redes y servicios de red (uso de red privada virtual (VPN) o red inalámbrica).
- Hora, ubicación y otros atributos del usuario al momento del acceso.
- Seguimiento del uso de los servicios de red.

Los servicios de red incluyen la provisión de conexiones, servicios de red privada y soluciones de seguridad de red administrada, como firewalls y sistemas de detección de intrusos.

**Segregación de redes**

La organización podrá considerar la gestión de la seguridad de las grandes redes dividiéndolas en

dominios de red, segmentos de red y separándolas de la red pública (es decir, Internet).

Los criterios para la segregación de redes en dominios y el acceso permitido a través de las puertas de enlace deben basarse en una evaluación de los requisitos de seguridad de cada dominio.

**Filtrado web**

La organización debe identificar los tipos de sitios web a los que el personal debe o no tener acceso.

La organización podrá considerar bloquear el acceso a los siguientes tipos de sitios web:

- Sitios web que tienen una función de carga de información a menos que esté permitido por razones comerciales válidas.
- Sitios web maliciosos conocidos o sospechosos (aquellos que distribuyen malware o contenido de phishing).
- Servidores de mando y control.
- Sitio web malicioso adquirido por inteligencia de amenazas.
- Sitios web que comparten contenido ilegal.

El filtrado web puede incluir una variedad de técnicas que incluyen firmas, heurística, lista de sitios web o dominios aceptables, lista de sitios web o dominios prohibidos y configuración personalizada para ayudar a evitar que el software malicioso y otras actividades maliciosas ataquen la red y los sistemas de la organización.

**Uso de criptografía**

Al usar criptografía, se debe considerar lo siguiente:

- La política específica del tema sobre criptografía definida por la organización, incluida la política general
- Una política específica del tema sobre el uso de la criptografía, es necesaria para maximizar los beneficios y minimizar los riesgos y evitar un uso inapropiado o incorrecto de la información.

- Identificar el nivel de protección requerido y la clasificación de la información estableciendo en consecuencia el tipo, fuerza y calidad de los algoritmos criptográficos requeridos.
- El uso de criptografía para la protección de la información contenida en los dispositivos terminales de los usuarios móviles o medios de almacenamiento, transmitida a través de redes a dichos dispositivos o medios de almacenamiento.
- El enfoque de la gestión de claves, incluidos los métodos para hacer frente a la generación y protección de claves criptográficas y la recuperación de información cifrada en caso de pérdida, compromiso o llaves dañadas.
- Roles y responsabilidades para:
    - La implementación de las reglas para el uso efectivo de la criptografía.
    - La gestión de claves, incluida la generación de claves.
    - Los estándares a adoptar, así como algoritmos criptográficos, fuerza de cifrado, criptografía, soluciones y prácticas de uso aprobadas o requeridas para su uso en la organización.
    - El impacto del uso de información cifrada en los controles que se basan en la inspección de contenido (malware detección o filtrado de contenido).

La gestión adecuada de claves requiere procesos seguros para generar, almacenar, archivar, recuperar, distribuir, retirar y destruir claves criptográficas.

Un sistema de gestión de claves debe basarse en un conjunto acordado de normas, procedimientos y métodos para:

- Generar claves para diferentes sistemas criptográficos y diferentes aplicaciones.
- Emitir y obtener certificados de clave pública.
- Distribuir claves a las entidades previstas, incluido cómo activar las claves cuando se reciben.

- Almacenar claves, incluida la forma en que los usuarios autorizados tienen acceso a las claves.
- Cambiar o actualizar las claves, incluidas las reglas sobre, cuándo cambiar las claves y cómo se hará.
- Tratar con claves comprometidas.
- Revocación de claves, incluido cómo retirar o desactivar claves (cuando las claves se han visto comprometidas o cuando un usuario deja una organización, en cuyo caso las claves también deben archivarse).
- Recuperar claves perdidas o dañadas.
- Realizar copias de seguridad o archivar claves.
- Destrucción de llaves.
- Registro y auditoría de actividades claves relacionadas con la gestión.
- Establecer fechas de activación y desactivación de claves para que sólo se puedan usar durante el período de tiempo de acuerdo con las reglas de la organización sobre gestión de claves.
- Gestionar solicitudes legales de acceso a claves criptográficas (la información cifrada debe estar disponible en forma no cifrada como evidencia en un caso judicial).

La criptografía se puede utilizar para lograr diferentes objetivos de seguridad de la información:

- Confidencialidad: uso de cifrado de información para proteger información sensible o crítica, ya sea almacenada o transmitida.
- Integridad o autenticidad: uso de firmas digitales o códigos de autenticación de mensajes para verificar la autenticidad o integridad de la información sensible o crítica almacenada o transmitida. Usar algoritmos con el fin de verificar la integridad de los archivos.
- No repudio: utilizando técnicas criptográficas para proporcionar evidencia de la ocurrencia o no ocurrencia de un evento o acción.

- Autenticación: uso de técnicas criptográficas para autenticar usuarios y otras entidades del sistema, solicitar acceso o realizar transacciones con usuarios, entidades y recursos del sistema.

**Ciclo de vida de desarrollo seguro**

El desarrollo seguro es un requisito para crear un servicio, arquitectura, software o un sistema seguro.

- Para lograrlo, se deben considerar los siguientes aspectos:
    - Separación de los entornos de desarrollo, prueba y producción.
    - Orientación sobre la seguridad en el ciclo de vida del desarrollo de software.
    - Seguridad en la metodología de desarrollo de software.
    - Pautas de codificación segura para cada lenguaje de programación utilizado.
    - Requisitos de seguridad en la fase de especificación y diseño.
    - Puntos de control de seguridad en proyectos.
    - Pruebas de sistema y seguridad, como pruebas de regresión, escaneo de código y pruebas de penetración.
    - Repositorios seguros para el código fuente y la configuración.
    - Seguridad en el control de versiones.
    - Conocimiento y capacitación en seguridad de la aplicación requeridos.
    - La capacidad de los desarrolladores para prevenir, encontrar y reparar vulnerabilidades.
    - Requisitos de licencia y alternativas para garantizar soluciones rentables y evitar futuros problemas de licencias.

Si se subcontrata el desarrollo, la organización debe asegurarse de que el proveedor cumpla con las reglas de la organización para el desarrollo seguro.

**Requisitos de seguridad de la aplicación.**

Deben identificarse y especificarse los requisitos de seguridad de las aplicaciones.

Los requisitos de seguridad de la aplicación deben incluir:

- Nivel de confianza en la identidad de las entidades (mediante autenticación ).
- Identificar el tipo de información y el nivel de clasificación a ser procesado por la aplicación.
- Necesidad de segregación de acceso y nivel de acceso a datos y funciones en la aplicación.
- Resiliencia contra ataques maliciosos o interrupciones no intencionales (protección contra desbordamiento o inyecciones de lenguaje de consulta estructurado (SQL)).
- Requisitos legales, estatutarios y reglamentarios en la jurisdicción donde se genera la transacción, procesada, completada o almacenada.
- Necesidad de privacidad asociada con todas las partes involucradas.
- Los requisitos de protección de cualquier información confidencial.
- Protección de datos en proceso, en tránsito y en reposo.
- Necesidad de cifrar de forma segura las comunicaciones entre todas las partes involucradas.
- Controles de entrada, incluidas verificaciones de integridad y validación de entrada.
- Controles automatizados (límites de aprobación o aprobaciones dobles).
- Controles de salida, considerando también quién puede acceder a las salidas y su autorización.
- Restricciones en torno al contenido de los campos de "texto libre", ya que pueden conducir al almacenamiento incontrolado de datos confidenciales (datos personales).
- Requisitos derivados del proceso de negocio, tales como registro y seguimiento de transacciones, requisitos de no repudio.
- Requisitos exigidos por otros controles de seguridad (interfaces para registro y monitoreo o

sistemas de detección de fuga de datos).

- Manejo de mensajes de error.

Los controles requeridos a menudo incluyen métodos criptográficos para la autenticación y la seguridad de la transferencia de datos.

**Arquitectura del sistema seguro y principios de ingeniería**

Los principios de ingeniería segura brindan orientación sobre las técnicas de autenticación de usuarios, el control seguro de sesiones, la validación y desinfección de datos.

Los principios de ingeniería de seguridad podrán tener en cuenta:

- La necesidad de integrarse con una arquitectura de seguridad.
- Infraestructura de seguridad técnica (infraestructura de clave pública (PKI), gestión de acceso e identidad (IAM), prevención de fuga de datos y gestión de acceso dinámico).
- Capacidad de la organización para desarrollar y soportar la tecnología elegida.
- Costo, tiempo y complejidad de cumplir con los requisitos de seguridad.
- Buenas prácticas actuales.

Los principios de ingeniería de seguridad y los procedimientos de ingeniería establecidos deben revisarse periódicamente para garantizar que permanezcan actualizados en términos de combatir cualquier nueva amenaza potencial y seguir siendo aplicables a los avances en las tecnologías y soluciones que se aplican.

**Codificación segura**

La organización debe monitorear las amenazas del mundo real y actualizar el asesoramiento y la información sobre las vulnerabilidades del software para guiar los principios de codificación segura de la organización a través de la mejora y el aprendizaje continuos.

Durante la codificación se debe incluir:

- Prácticas de codificación seguras específicas para los lenguajes y técnicas de programación que se utilizan.
- Utilizar técnicas de programación seguras, como programación en pares, refactorización, revisión por pares, iteraciones de seguridad y desarrollo basado en pruebas.
- Utilizando técnicas de programación estructurada.
- Documentar el código y eliminar los defectos de programación, lo que puede permitir que se exploten las vulnerabilidades de seguridad de la información.
- Prohibir el uso de técnicas de diseño inseguras (el uso de contraseñas codificadas, muestras de código y servicios web no autenticados).

El código de la aplicación se diseña mejor asumiendo que siempre está sujeto a ataques, por error o acción maliciosa.

**Pruebas de seguridad en desarrollo y aceptación**

Las pruebas de seguridad deben ser una parte integral de las pruebas de sistemas o componentes.

Las pruebas de seguridad deben incluir pruebas de:

- Funciones de seguridad por ejemplo, autenticación de usuario, restricción de acceso y uso de criptografía.
- Codificación segura.
- Configuraciones seguras incluyendo la de sistemas operativos, firewalls y otros componentes de seguridad.

El alcance de las pruebas debe ser proporcional a la importancia, la naturaleza del sistema y el impacto potencial del cambio que se está introduciendo.

Se deben considerar las pruebas y el monitoreo de los entornos de prueba, las herramientas y las tecnologías para garantizar la eficacia de las pruebas.

**Desarrollo subcontratado**

Cuando se subcontrata el desarrollo del sistema, la organización debe comunicar y acordar los requisitos, expectativas, además debe monitorear y revisar continuamente si la entrega del trabajo subcontratado cumple con estas expectativas.

Se deben considerar los siguientes puntos en toda la cadena de suministro externa de la organización:

- Acuerdos de licencia, propiedad del código y derechos de propiedad intelectual relacionados con el contenido subcontratado.
- Requisitos contractuales para prácticas seguras de diseño, codificación y pruebas.
- Provisión del modelo de amenaza a considerar por desarrolladores externos.
- Pruebas de aceptación para la calidad y precisión de los entregables.
- Provisión de evidencia de que los niveles mínimos aceptables de seguridad y capacidades de privacidad son establecidos (informes de aseguramiento).
- Provisión de evidencia de que se han realizado suficientes pruebas para proteger contra la presencia de contenido malicioso (tanto intencional como no intencional) en el momento de la entrega.
- Provisión de evidencia de que se han aplicado pruebas suficientes para protegerse contra la presencia de vulnerabilidades conocidas.
- Acuerdos de depósito en garantía para el código fuente del software (si el proveedor cierra).
- Derecho contractual a auditar procesos y controles de desarrollo.
- Requisitos de seguridad para el entorno de desarrollo.
- Teniendo en cuenta la legislación aplicable (sobre protección de datos personales).

**Separación de los entornos de desarrollo, prueba y producción**

Debe identificarse e implementarse el nivel de separación entre los entornos de producción, prueba y desarrollo que es necesario para evitar problemas de producción.

Se deben considerar los siguientes elementos:

- Separar adecuadamente los sistemas de desarrollo y producción para así operarlos en diferentes dominios (en entornos físicos o virtuales separados).
- Definir, documentar e implementar reglas y autorizaciones para el despliegue de software del estado de desarrollo al estado de producción.
- Probar los cambios en los sistemas de producción y las aplicaciones en un entorno de pruebas antes de aplicarlos a los sistemas de producción.
- No probar en ambientes de producción excepto en circunstancias que han sido definidas y aprobadas.
- Compiladores, editores y otras herramientas de desarrollo o programas de utilidad que no sean accesibles desde sistemas de producción cuando no se requiera.
- Mostrar etiquetas de identificación del entorno adecuadas en los menús para reducir el riesgo de error.
- No copiar información confidencial en los entornos del sistema de desarrollo y prueba a menos que se proporcionen controles equivalentes para los sistemas de desarrollo y prueba.

Es deseable separar los entornos de desarrollo, prueba y producción para reducir el riesgo de cambio accidental o acceso no autorizado al software de producción y los datos comerciales.

**Gestión de cambios**

Los procedimientos de control de cambios deben documentarse y aplicarse para garantizar la confidencialidad, integridad y disponibilidad de la información en las instalaciones de procesamiento de información y los sistemas de información, durante todo el ciclo de vida del desarrollo del sistema, desde las primeras etapas de diseño hasta todos los esfuerzos de mantenimiento posteriores.

Los procedimientos de control de cambios deben incluir:

- Planificar y evaluar el impacto potencial de los cambios considerando todas las dependencias.

- Autorización de cambios.
- Comunicar los cambios a las partes interesadas pertinentes.
- Pruebas y aceptación de pruebas para los cambios.
- Implementación de cambios, incluidos los planes de implementación.
- Consideraciones de emergencia y contingencia, incluidos los procedimientos de respaldo.
- Mantener registros de cambios que incluyan todo lo anterior.
- Asegurar que la documentación operativa y los procedimientos del usuario se cambien según sea necesario para seguir siendo apropiado.
- Garantizar que se cambien los planes de continuidad de las TIC y los procedimientos de respuesta y recuperación, según sea necesario para seguir siendo apropiado.

Las buenas prácticas incluyen la prueba de los componentes de las TIC en un entorno separado de los entornos de producción y desarrollo.

**Información de prueba**

La información de prueba debe seleccionarse para garantizar la confiabilidad de los resultados de las pruebas y la confidencialidad de la información operativa relevante.

Se deben aplicar las siguientes pautas para proteger las copias de la información operativa, cuando se utilizan con fines de prueba, ya sea que el entorno de prueba se construya internamente o en un servicio en la nube:

- Aplicar los mismos procedimientos de control de acceso a los entornos de prueba que los aplicados a los ambientes operativos.
- Tener una autorización separada cada vez que se copia información operativa a un entorno de prueba.
- Registrar la copia y el uso de información operativa para proporcionar una pista de auditoría.
- Proteger la información confidencial mediante eliminación o enmascaramiento si se utiliza para pruebas.

- Eliminar correctamente la información operativa de un entorno de prueba, inmediatamente después de que se complete la prueba para evitar el uso no autorizado de la información de la prueba.

La información de la prueba debe almacenarse de forma segura (para evitar la manipulación, que de lo contrario puede generar resultados no válidos) y sólo debe usarse para fines de prueba.

**Protección de los sistemas de información durante las pruebas de auditoría**

Se deben observar las siguientes pautas:

- Acordar solicitudes de auditoría para el acceso a sistemas y datos con la gestión adecuada.
- Acordar y controlar el alcance de las pruebas de auditoría técnica.
- Limitar las pruebas de auditoría al acceso de sólo lectura al software y los datos. Si el acceso de solo lectura no está disponible para obtener la información necesaria, ejecutar la prueba por un administrador experimentado que tenga los derechos de acceso necesarios en nombre del auditor.
- Si se otorga el acceso, establecer y verificar los requisitos de seguridad (antivirus y parches) de los dispositivos utilizados para acceder a los sistemas (computadoras portátiles o tabletas) antes de permitir el acceso.
- Solo permitir el acceso que no sea de solo lectura para copias aisladas de archivos del sistema, eliminándolos cuando se complete la auditoría, o brindándoles la protección adecuada si existe la obligación de mantener dichos archivos bajo los requisitos de documentación de auditoría.
- Identificar y acordar solicitudes de procesamiento especial o adicional, así como ejecutar herramientas de auditoría.
- Ejecutar pruebas de auditoría que puedan afectar la disponibilidad del sistema fuera del horario comercial.
- Supervisar y registrar todos los accesos con fines de auditoría y prueba.

Las pruebas de auditoría y otras actividades de aseguramiento también pueden ocurrir en los sistemas de prueba y desarrollo, donde tales pruebas pueden afectar, por ejemplo, la integridad del código o conducir a la divulgación de cualquier información confidencial que se encuentre en dichos entornos.