COLIMA
Gobierno del Estado

Instituto Colimense para la Sociedad de la Información y el Conocimiento

Versión N°. 1

Manual de Seguridad Informática

Colima, Colima, 30 de abril de 2024.

Índice

	Pág.
1. CONTROL DE AUTORIZACIONES	4
2. CUERPO DEL DOCUMENTO	5
2.1. Introducción	5
2.2. Objetivo	5
2.3. Alcance	5
2.4. Marco normativo	6
2.5. Términos y definiciones	6
2.6. Organización de la Seguridad Informática	10
2.7. Políticas	11
2.7.1. Política de roles y responsabilidades	11
2.7.1.1. Titular	11
2.7.1.2. Custodio	13
2.7.1.3. Administrador	13
2.7.1.4. Usuario	14
2.7.2. Responsabilidades estratégicas	14
2.7.2.1. Responsable de definir las directrices de seguridad	14
2.7.2.2. Responsable de definir los controles para mitigar riesgos	16
2.7.3. Responsabilidades tácticas	17
2.7.3.1. Responsable de auditoría interna	17
2.7.4. Responsabilidades operativas	18
2.7.4.1. Responsable del monitoreo de la seguridad informática	18
2.7.4.2. Responsable de la administración de cuentas y asignación de privilegios	18
2.7.4.3. Responsable de la operación de tecnologías de seguridad	19
2.7.4.4. Responsable de seguridad en el desarrollo y mantenimiento de sistemas de información	20
2.8. Política de Clasificación de Información	20
2.8.1. Confidencialidad	20
2.8.2. Integridad	21
2.8.3. Disponibilidad	21
2.9. Política de inventario de activos de información	22
2.10. Política de uso adecuado de los activos de información	22
2.10.1. Protección de los activos de información	23
2.10.2. Uso indebido de los activos de información	23
2.10.3. Uso y mantenimiento de instalaciones y equipos	23
2.10.4. Uso adecuado de los equipos de cómputo	24
2.10.5. Documentación de los procedimientos operativos	24
2.11. Política de seguridad en el capital humano	25
2.11.1. Previo al empleo, cargo o comisión	26
2.11.2. Términos y condiciones	26
2.11.3. Durante el empleo	26
2.11.4. Responsabilidades de la Dependencia o Entidad	27

2.11.5. Proceso Disciplinario	28
2.11.6. Responsabilidades en la terminación del empleo o cambio de puesto	28
2.11.7. Devolución de activos de información	28
2.11.8. Eliminación de privilegios de acceso	29
2.12. Política de seguridad física y ambiental	29
2.12.1. Medidas de seguridad físicas	30
2.12.2. Áreas definidas como seguras	30
2.12.3. Centro de cómputo y/o centro de datos	30
2.12.4. Oficinas	31
2.12.5. Control de acceso físico a las instalaciones que procesan información	31
2.12.6. Protección contra amenazas externas	32
2.12.7. Protección a los centros de datos	32
2.12.8. Gestión de Medios Extraíbles	34
2.12.9. Disposición de Medios	34
2.12.10. Protección a los Medios de Almacenamiento de Información Durante su Traslado Fuera de las Instalaciones	34
2.12.11. Escritorio Limpio	36
2.13. Política de control de acceso a sistemas y aplicaciones	36
2.13.1. Registro de usuarios	36
2.13.2. Administración de privilegios	37
2.13.3. Administración de contraseñas de usuarios	37
2.13.4. Revisión de derechos de acceso	38
2.13.5. Estándares de contraseñas	38
2.13.6. Estándar de contraseñas para usuarios finales	38
2.13.7. Identificación y autenticación	39
2.13.8. Factores de autenticación	40
2.13.9. Estándar de tipos de cuentas	40
2.13.10. Restricciones de acceso a la información	41
2.13.11. Eliminación de privilegios de acceso	41
2.14. Política de uso de servicios de la red	41
2.14.1. Seguridad en redes internas	42
2.14.2. Configuración, administración y actualización de la red	42
2.14.3. Responsabilidades de la administración de la red	42
2.14.4. Monitoreo de la red	42
2.14.5. Servicios de red	43
2.14.6. Autenticación de equipos en la red	43
2.15. Política para reporte de incidentes y vulnerabilidades de seguridad de la información	43
2.15.1. Reportes de incidentes de seguridad	44
2.15.2. Respuesta a incidentes de seguridad	46
2.15.3. Reporte de vulnerabilidades de seguridad	46
2.15.4. Acciones a realizar en caso de vulneración a la seguridad	46
2.15.5. Bitácora de las vulneraciones a la seguridad	47
2.16. Política de Dispositivos Móviles y Trabajo a Distancia o Remoto	47
3. SECCIÓN DE CAMBIOS	49

CONTROL DE AUTORIZACIONES

Autorizó

Lic. Edgar Rafael Aguirre Munguía
Director General del ICSIC

Aprobó

Ing. Carlos Rodríguez Díaz
Director de Desarrollo Telemático del ICSIC

Revisó

Lic. Ulises Alonso Arreola
Coordinador Jurídico del ICSIC

Revisó

Ing. Sergio Viera González
Encargado de la Jefatura de Seguridad Informática del ICSIC

2. CUERPO DEL DOCUMENTO

2.1 Introducción

Uno de los principales activos de la Administración Pública Estatal es la información relacionada con los ciudadanos, los servidores públicos, los trámites y servicios, las tecnologías, las configuraciones y los procedimientos que están involucrados en las operaciones que se llevan a cabo, por lo que es vital proteger la información que se trata, siendo ésta un elemento fundamental para continuar con las actividades que se realizan día con día.

Dicha información se encuentra comprendida por aquella que es pública, confidencial, reservada y privilegiada, la cual se encuentra protegida en los términos de las leyes en materia de transparencia y protección de datos personales y responsabilidades administrativas.

Si bien, los sujetos obligados deben implementar las medidas de seguridad que permitan proteger la información contra daño, pérdida, alteración, destrucción o uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad, el Instituto Colimense para la Sociedad de la Información y el Conocimiento fue creado para impulsar la Agenda Digital como una política pública, en la que se establece el Habilitador: Acceso Universal a las TIC, Estrategia 1 Reducir la brecha de infraestructura que persiste en la entidad, facilitando a los colimenses la conectividad a redes de telecomunicaciones que sean seguras, confiables y de calidad adecuada, así como la Meta 1.4. Implementar un modelo de seguridad informática.

Para tal efecto se diseña el "Manual de Seguridad Informática" que tiene como finalidad mantener la seguridad de la información; entendiéndose ésta como la preservación de su confidencialidad, integridad, disponibilidad, autenticidad, auditabilidad, protección a la duplicación, no repudio y legalidad en las redes de telecomunicaciones, en hardware y en software, el cual se desarrolla tomando como referencia la "Norma Mexicana NMX-I-27002-NYCE-2015 Tecnologías de la Información – Técnicas de Seguridad – Código de Buenas Prácticas para el Control de la Seguridad de la Información".

2.2 Objetivo

Establecer, dar a conocer e implementar un conjunto de políticas básicas de seguridad de la información en las redes de telecomunicaciones, en el hardware y en el software, cuya aplicación permita minimizar los riesgos que pudieran afectar el logro de los objetivos de las Dependencias y Entidades de la Administración Pública Estatal.

2.3 Alcance

El presente documento es aplicable a todos los servidores públicos o cualquier persona que colabore o se relacione de alguna manera con las actividades de la Administración Pública Estatal, que hagan uso y aprovechamiento de las tecnologías de la información y

comunicaciones.

La implementación del presente Manual se llevará a cabo por cada Entidad o Dependencia en la medida de lo posible atendiendo a la estructura orgánica y tecnología administrada.

2.4 Marco Normativo

N°	Normatividad Aplicable	Fecha de Publicación
1	Constitución Política de los Estados Unidos Mexicanos	05 de febrero de 1917
2	Ley General de Responsabilidades Administrativas	18 de julio de 2016
3	Ley General de Transparencia y Acceso a la Información Pública.	04 de mayo de 2015
4	Ley Federal de Protección de Datos Personales en Posesión de los Particulares.	05 de julio de 2010
5	Ley Federal de Telecomunicaciones y Radiodifusión	14 de julio de 2014
6	Código Penal Federal	14 de agosto de 1931
7	Norma Mexicana NMX-I-27002-NYCE-2015	14 de abril de 2015
8	Constitución Política del Estado Libre y Soberano de Colima	27 de diciembre de 2017
9	Ley Orgánica del Poder Ejecutivo y de la Administración Pública del Estado de Colima	09 de octubre de 2021
10	Ley del Instituto Colimense para la Sociedad de la Información y el Conocimiento.	01 de septiembre de 2012
11	Ley de Transparencia y Acceso a la Información Pública del Estado de Colima.	30 de mayo de 2016
12	Ley de Protección de Datos Personales en Posesión de los Sujetos Obligados para el Estado de Colima.	26 de julio de 2017
13	Ley de Archivos del Estado de Colima	14 de agosto de 2019
14	Agenda Digital "Impulsando la Inclusión y el Desarrollo de la Sociedad".	02 de noviembre de 2019

2.5 Términos y Definiciones

Para efectos de una correcta interpretación del presente manual, se establecen las siguientes definiciones, siglas y términos:

Activo de información. Toda aquella información y medio que la contiene, que por su importancia y el valor que representa para la Institución, debe ser protegido para mantener su confidencialidad, disponibilidad e integridad, acorde al valor que se le otorgue.

Activos de TIC. Los aplicativos de cómputo, bienes informáticos, soluciones tecnológicas, sus componentes, las bases de datos o archivos electrónicos y la información contenida en éstos.

Amenaza. A cualquier posible acto que pueda causar algún tipo de daño a los activos de información.

Análisis de riesgos. El uso sistemático de la información para identificar las fuentes de vulnerabilidades y amenazas a los activos de TIC, a las infraestructuras de información esenciales y/o críticas o a los activos de información, así como efectuar la evaluación de su magnitud o impacto y estimar los recursos necesarios para eliminarlas o mitigarlas.

Auditabilidad. Define que todos los eventos de un sistema deben ser registrados para su control posterior.

Autenticidad. Busca asegurar la validez de la información en tiempo, forma y distribución. Asimismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidades.

Borrado seguro. El proceso mediante el cual se elimina de manera permanente y de forma irrecuperable la información contenida en medios de almacenamiento digital.

Centro de datos. Lugar físico en el que se encuentran activos de TIC y activos de información y desde el que se proveen servicios de TIC.

Confidencialidad. Se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.

Custodio. Servidor público o tercero autorizado para tener bajo su custodia o cargo uno o más activos de información.

Derechos ARCO. Los derechos de acceso, rectificación, cancelación y oposición al tratamiento de datos personales.

Disponibilidad. Garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que así lo requieran.

ICSIC. Instituto Colimense para la Sociedad de la Información y el Conocimiento.

Impacto. Al grado de los daños y/o de los cambios sobre un activo de información, por la materialización de una amenaza.

Incidente. A la afectación o interrupción a los activos de TIC, a las infraestructuras de información esenciales y/o críticas, así como a los activos de información de la Institución, incluido el acceso no autorizado o no programado a éstos.

Información. Se refiere a toda comunicación o representación de conocimiento, datos en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales que se encuentre en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro.

En la presente definición se encuentra la información confidencial, privilegiada, pública y reservada.

Información confidencial. La que contiene datos personales concernientes a una persona física identificada o identificable. Esta información mantendrá este carácter de manera indefinida y sólo podrán tener acceso a ella los titulares de la misma, sus representantes y los servidores públicos que requieran conocerla para el debido ejercicio de sus funciones.

Así también será confidencial toda aquella información que por disposición legal, contrato, convenio, políticas, lineamientos o cualquier documento emitido por una entidad que le dé ese carácter.

En términos de la Ley Federal de Telecomunicaciones y Radiodifusión la información que se transmita a través de las redes y servicios de telecomunicaciones es confidencial, salvo aquella que por su propia naturaleza sea pública o cuando medie orden de autoridad judicial competente.

Información privilegiada. La que obtenga el servidor público con motivo de sus funciones y que no sea del dominio público.

Información pública. Por regla general toda la información que se encuentre en poder de los sujetos obligados previstos en la Ley de Transparencia y Acceso a la Información Pública del Estado de Colima, que no se encuentre clasificada como reservada, confidencial, o privilegiada de acuerdo con la Ley General de Responsabilidades Administrativas.

Información reservada. La información que se encuentra temporalmente sujeta a alguna de las excepciones de publicidad previstas en la Ley de Transparencia y Acceso a la Información Pública del Estado de Colima.

Integridad. Se salvaguarda la exactitud, totalidad de la información y los métodos de procesamiento.

Inventario de activos. Documento que contiene el listado de los activos de información, descripción, clasificación y responsables de los mismo.

Internet. Conjunto descentralizado de redes de telecomunicaciones en todo el mundo, interconectadas entre sí, que proporciona diversos servicios de comunicación y que utiliza protocolos y direccionamiento coordinados internacionalmente para el enrutamiento y procesamiento de los paquetes de datos de cada uno de los servicios.Estos protocolos y direccionamiento garantizan que las redes físicas que en conjunto componen Internet funcionen como una red lógica única.

Legalidad. Referido al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeta la Entidad o Dependencia.

Medidas de Seguridad. Conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permitan proteger la información.

Medidas de seguridad administrativas. Políticas y procedimientos para la gestión, soporte y revisión de la seguridad de la información a nivel organizacional, la identificación, clasificación y borrado seguro de la información, así como la sensibilización y capacitación del personal o servidores públicos.

Medidas de seguridad físicas. Conjunto de acciones y mecanismos para proteger el entorno físico de la información y de los recursos involucrados en su tratamiento.

Medidas de seguridad técnicas. Conjunto de acciones y mecanismos que se valen de la tecnología relacionada con hardware y software para proteger el entorno digital de la información y los recursos involucrados en su tratamiento.

No repudio. Se refiere a evitar que cualquier persona física o moral haya enviado o recibido información alegue ante terceros que no la envió o recibió.

Protección a la duplicación. Consiste en asegurar que una transacción sólo se realice una vez, a menos que se especifique lo contrario. Impedir que se grabe una transacción para luego reproducirla, con el objeto de simular múltiples peticiones del mismo remitente original.

Red de telecomunicaciones. Sistema integrado por medios de transmisión, tales como canales o circuitos que utilicen bandas de frecuencias del espectro radioeléctrico, enlaces satelitales, cableados, redes de transmisión eléctrica o cualquier otro medio de transmisión, así como, en su caso, centrales, dispositivos de conmutación o cualquier equipo necesario.

Responsable de Seguridad Informática. Servidor público designado por el Titular quien deberá asistir en materia de seguridad informática a los demás servidores públicos adscritos a la dependencia o entidad, verificar la aplicación de las medidas de seguridad necesarias para la protección de la información y cumplir con las demás responsabilidades establecidas en el presente Manual.

Riesgo: La posibilidad de que una amenaza pueda explotar una vulnerabilidad y causar una pérdida o daño sobre los activos de TIC, las infraestructuras de información esenciales y/o críticas y activos de información.

Seguridad informática: protección de la información que circula en la red, y que se encuentra contenida en software y hardware.

Seguridad de la información: capacidad de preservar la confidencialidad, integridad y disponibilidad de la información, así como la autenticidad, confiabilidad, trazabilidad y no repudio de la misma.

Servidor público. La persona señalada con dicho carácter en la Constitución Política del Estado Libre y Soberano de Colima y en la Ley General de Responsabilidades Administrativas.

Sistema de Información. Se refiere a un conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales.

Tecnología de la Información. Se refiere a un conjunto de activos de información operados por el responsable de la información o por un tercero que procese información en su nombre, para llevar a cabo una función propia de la dependencia o entidad, sin tener en cuenta la tecnología utilizada, ya se trate de procesamiento de datos, almacenamiento, telecomunicaciones o cualquier otro tipo de operación.

Telecomunicaciones. Toda emisión, transmisión o recepción de signos, señales, datos, escritos, imágenes, voz, sonidos o información de cualquier naturaleza que se efectúa a través de hilos, radioelectricidad, medios ópticos, físicos u otros sistemas electromagnéticos, sin incluir la radiodifusión.

Titular. Al servidor público titular de cualquier dependencia o entidad de la Administración Pública Estatal, responsable de la información, activos de TIC y activos de información, que decide sobre el tratamiento de la información que posee, así como la definición de los fines, medios, alcances y demás cuestiones relacionadas, que tiene a su cargo servidores públicos, sistemas, hardware, software y/o sistemas de comunicación que reciban, generen, procesen, almacenen o destruyan información obtenida o generada por sí, por cualquier título o por disposición legal.

Tratamiento. Cualquier operación o conjunto de operaciones aplicadas a la información, relacionadas con la obtención o recepción, generación, procesamiento, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, destrucción, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de la misma.

Vulnerabilidades: Las debilidades en la seguridad de la información que potencialmente permite que una amenaza afecte a los activos de TIC, a las infraestructuras de información esenciales y/o críticas, así como a los activos de información.

Web. World Wide Web (WWW).

2.6. Organización de la Seguridad Informática

La seguridad de la información es una responsabilidad compartida por todas las áreas que integran la estructura orgánica de las Dependencias y Entidades de la Administración Pública Estatal, por lo que éstas últimas deberán revisar, aprobar y presentar a la Comisión de Infraestructura Tecnológica, por conducto de la Dirección de Desarrollo Telemático del ICSIC las propuestas o recomendaciones para que evalúen y en su caso

apruebe actualizaciones al presente Manual en respuesta a los cambios en el entorno organizacional, circunstancias o condiciones legales.

Funciones de la Comisión de Infraestructura Tecnológica en materia de seguridad informática:

1. Intercambiar información sobre nuevas tecnologías, productos, amenazas, vulnerabilidades y mejores prácticas.

2. Analizar y en su caso aprobar las iniciativas presentadas por cada dependencia o entidad para incrementar la seguridad de la información en las redes de telecomunicaciones, en el hardware o en el software, de acuerdo a las competencias y responsabilidades de las mismas.

3. Analizar y en su caso aprobar metodologías, procesos, documentos o asuntos relativos a la seguridad informática que sea sometido a su consideración.

4. Promover la difusión, capacitación y apoyo en materia de seguridad informática.

2.7. Políticas

2.7.1. Política de Roles y Responsabilidades.

Para garantizar la seguridad de la información en las redes de telecomunicaciones, en el hardware y en el software se definen y asignan los siguientes roles y responsabilidades mínimas necesarias.

2.7.1.1. Titular.

El servidor público titular de cualquier dependencia o entidad de la Administración Pública Estatal, responsable de la información, activos de TIC y activos de información, que decide sobre el tratamiento de la información que posee, así como la definición de los fines, medios, alcances y demás cuestiones relacionadas, que tiene a su cargo servidores públicos, redes, sistemas, hardware, software y/o sistemas de comunicación que reciban, generen, procesen, almacenen o destruyan información obtenida o generada por sí, por cualquier título o por disposición legal, quien deberá cumplir con las siguientes funciones:

1. Asignar a los servidores públicos por escrito los roles y responsabilidades en materia de seguridad informática.

2. Identificar y clasificar los activos de información que tenga en propiedad, en comodato o cualquier otro título, con base en la **"Política de inventario de activos de información".**

3. Aprobar los procesos de seguridad de la información en hardware, software y/o redes de telecomunicaciones.

4. Asignar y/o autorizar a los Custodios para la protección de los activos de información y de los procesos específicos de seguridad para su cumplimiento.

5. Aprobar el ciclo de vida de la información así como de los activos de información.

6. Definir y documentar los niveles de autorización en el tratamiento de la información, los fines, los medios, los alcances y demás cuestiones relacionadas.

7. Documentar las acciones realizadas para que los servidores públicos, proveedores o terceros estén debidamente informados sobre sus responsabilidades en materia de seguridad informática.

8. Velar porque los servidores públicos sean capacitados de manera anual en materia de seguridad informática, sean motivados al cumplimiento de las políticas del presente manual y se les proporcione un canal de denuncia anónima para reportar violaciones a las mismas.

9. Documentar la coordinación y supervisión de los aspectos de seguridad de la información en las relaciones con los proveedores.

10. Separar al Custodio ante el inicio de un evento que pueda comprometer la seguridad de la información que se encuentre en un activo de información.

11. Se recomienda pertenecer a grupos o foros de seguridad especializados como un medio para acrecentar el conocimiento sobre las mejores prácticas y estar al día con la información de seguridad pertinente; asegurar que la comprensión del ambiente de seguridad de la información es actual y completo; recibir notificaciones oportunas de alertas, avisos y revisiones, relativas a los ataques y vulnerabilidades; tener acceso al asesoramiento experto en seguridad de la información; compartir e intercambiar información sobre las nuevas tecnologías, productos, amenazas o vulnerabilidades; así como proporcionar enlaces adecuados cuando se traten incidentes de seguridad de la información.

12. Podrá celebrar convenios para la cooperación y coordinación en cuestiones de seguridad informática, siempre que no se comprometa información confidencial o reservada y se lleve a cabo en los términos del marco normativo aplicable, de acuerdo a las atribuciones y facultades que las leyes le confieren.

2.7.1.2. Custodio.

El Custodio de activos de información tiene la responsabilidad de establecer y mantener los controles de seguridad adecuados para los mismos con base al nivel de protección requerido por el Titular y deberá de cumplir con las siguientes funciones:

1. Asegurarse de que sus activos de información estén inventariados, debidamente clasificados y protegidos.
2. Definir y revisar periódicamente las restricciones de acceso y clasificaciones a los activos de información.
3. Tener cuidado de que ninguna persona pueda acceder, modificar o utilizar los activos de información sin autorización o detección.
4. Permitir accesos a los activos de información sólo al servidor público o tercero previamente autorizado por el Titular.
5. Informar a los usuarios la información sobre los controles establecidos.
6. Llevar a cabo las acciones delegadas por el Titular para brindar seguridad a los activos de información.
7. Asegurar el manejo adecuado del activo de información que sea eliminado o destruido.
8. Establecer el ciclo de vida de los activos de información que tenga bajo su cuidado.

2.7.1.3. Administrador.

Administrará los sistemas o aplicaciones donde radica la información, y deberá de cumplir con las siguientes funciones:

1. Revisar periódicamente la infraestructura a su cargo para detectar amenazas o vulnerabilidades de seguridad.
2. Llevar a cabo el aseguramiento de equipos y actualización de parches de seguridad.
3. Dar soporte para respuesta a incidentes de seguridad y vulnerabilidades.
4. Mantener la confidencialidad, integridad y disponibilidad de los sistemas de información e infraestructura tecnológica.
5. Realizar un monitoreo constante de la red para detectar cualquier incidente de seguridad en los servicios de la misma.
6. Dar el mantenimiento periódico de los componentes de red con base en las recomendaciones del fabricante.

7. Asegurarse de que los componentes de la red interna, tengan asignada una dirección de red autorizada.

2.7.1.4. Usuario.

Servidor Público que requiere de autorización para accesar a los sistemas o aplicaciones y poder realizar su función a través de los recursos asignados y de la normatividad existente, quien debe de cumplir con las siguientes funciones:

1. Hacerse responsable del uso de su cuenta o usuario, contraseña y equipo de cómputo asignado, así como de los medios de transmisión y almacenamiento de la información.
2. Obtener la autorización formal del Titular o Custodio, antes de intentar accesar a cualquier activo de información.
3. Utilizar los sistemas sólo para actividades propias de sus funciones.
4. No divulgar información clasificada como privilegiada, confidencial o reservada.
5. Conocer la clasificación de la información y los activos de información que maneja.
6. Apegarse al presente Manual y normatividad aplicable en la materia.
7. Proteger la información y sistemas de información bajo su uso o custodia.
8. Reportar cualquier sospecha o incidente de seguridad, así como vulnerabilidades al área responsable para atenderlos y resolverlos.

2.7.2. Responsabilidades estratégicas.

El Titular de la dependencia o entidad deberá designar las siguientes responsabilidades estratégicas a un servidor público que se encuentre adscrito a la misma.

2.7.2.1. Responsable de definir las directrices de seguridad.

Debe de cumplir con las siguientes funciones:

1. Elaborar, revisar y/o validar el plan general de seguridad.
2. Elaborar, revisar y/o validar los proyectos sobre seguridad de la información.

3. Elaborar, revisar y/o validar los roles y responsabilidades específicos adicionales a los establecidos en el presente manual, y que se relacionen a la seguridad de la información.

4. Asegurar que se promueva la seguridad de la información.

5. Elaborar, revisar y/o validar las normas, políticas, estándares, procedimientos, reglas y/o lineamientos de seguridad informática en el diseño de bases de datos, de plataformas de desarrollo y técnicas de programación para su implementación.

6. Asesorar en materia de seguridad informática a los mandos superiores y unidades administrativas de la dependencia o entidad a la que se encuentre adscrito.

7. Participar como enlace técnico ante las instancias de seguridad informática que sean necesarias.

8. Elaborar, revisar y/o validar protocolos de seguridad informática.

9. Elaborar un directorio de emergencia que contenga por lo menos los números telefónicos de policía en general y en materia de ciberseguridad, bomberos, protección civil, proveedores de electricidad, telecomunicaciones, climas, alarmas, etc.

10. Elaborar, revisar y/o validar el procedimiento que especifique cuándo y por quién deben ser contactadas las autoridades y cómo identificar los incidentes de seguridad de la información y ser reportados de manera oportuna.

11. Elaborar, revisar y/o validar el método de gestión de proyectos el cual deberá exigir que: los objetivos de seguridad de la información sean incluidos en los objetivos del proyecto; la valoración de los riesgos de seguridad de la información se lleve a cabo en una fase temprana del proyecto para identificar los controles necesarios, y la seguridad de la información sea parte de todas las fases de la metodología del proyecto aplicada.

12. Delegar las funciones de elaboración y revisión.

13. Proponer al Titular todos los documentos en materia de seguridad informática que previamente sean validados para su correspondiente aprobación.

14. Definir el ciclo de vida de los activos de información.

2.7.2.2. Responsable de definir los controles para mitigar riesgos.

Vigila el cumplimiento y validez de políticas y procedimientos, buscando la mejora continua, y debe de cumplir con las siguientes funciones:

1. En cuanto a la normatividad:

    a. Coordinar esfuerzos con la finalidad de definir las directrices institucionales de seguridad de la información.

    b. Definir políticas, procedimientos y controles que permitan minimizar los riesgos con base en su impacto.

    c. Coordinar la implementación de políticas, procedimientos y controles para garantizar y resguardar la confidencialidad, integridad y disponibilidad de la información y activos de información asociados.

    d. Coordinar la capacitación de seguridad de la información.

    e. Desarrollar y aplicar una metodología de administración de riesgos de seguridad, la cual permitirá identificar, valorar y tomar acciones al respecto.

2. En cuanto al cumplimiento:

    a. Coordinar la actualización de forma periódica los análisis de riesgos que coadyuven a identificar nuevos riesgos a la información y los activos de información relacionados.

    b. Vigilar el cumplimiento de políticas, procedimientos y controles existentes, así como su concordancia con las necesidades en materia de seguridad de la información.

    c. Coordinar los esfuerzos para implementar controles en materia de seguridad.

    d. Coordinar revisiones internas así como recibir y atender auditorías internas y externas relacionadas a la seguridad de la información.

    e. Atender las recomendaciones derivadas de las auditorías internas y externas en materia de seguridad de la información.

    f. Supervisar el cumplimiento de las iniciativas establecidas por la Comisión de Infraestructura Tecnológica, en tiempo, costo y alcance.

    g. Coordinar, implantar y alinear cualquier acción que permita sustentar la estrategia de seguridad de la información.

    h. Reforzar los hábitos en materia de seguridad de la información.

    i. Recibir y revisar de manera periódica los reportes de monitoreo de la seguridad, por ejemplo:

        i. Bitácoras de firewall.
        ii. Bitácoras de sistemas operativos.

iii. Bitácoras de aplicaciones de negocio.

j. Recibir y revisar los reportes de la administración de las cuentas (altas, bajas y cambios) de todos los sistemas.

k. Reportar de forma periódica los indicadores de seguridad de la información.

l. Coordinar el seguimiento y cierre de incidentes de seguridad detectados.

2.7.3. Responsabilidades tácticas.

2.7.3.1. Responsable de auditoría interna.

Servidor público independiente a la estructura del área de seguridad, encargada de llevar a cabo la auditoria relacionada a la estructura y cumplimiento de la seguridad de la información, que debe de cumplir con las siguientes funciones:

1. Verificar la concordancia entre las políticas de seguridad y las necesidades de seguridad mínimas requeridas.

2. Verificar que el análisis de riesgos se encuentre actualizado, que refleje las nuevas vulnerabilidades y amenazas de seguridad a las que podría encontrarse expuesta la información y los activos de información relacionados.

3. Verificar que las iniciativas de seguridad de la información se encuentren alineadas a los "planes de mitigación de riesgos" autorizados.

4. Verificar que exista una adecuada segregación de funciones.

5. Notificar los resultados a la Comisión de Infraestructura Tecnológica y en su caso proporcionar las recomendaciones pertinentes.

6. Verificar el cumplimiento y la eficacia del presente Manual.

2.7.4. Responsabilidades operativas.

2.7.4.1. Responsable del monitoreo de la seguridad informática.

Lleva a cabo la explotación de bitácoras que permitan identificar incumplimientos al presente Manual y debe de cumplir las siguientes funciones:

1. Ejecutar el proceso de monitoreo para identificar incidentes de seguridad, como violaciones o debilidades en la seguridad.

2. Realizar el monitoreo de los controles establecidos para el cumplimiento de las Políticas de Seguridad.

3. Iniciar el proceso de respuesta a incidentes de seguridad al detectarse una desviación dentro de la operación.

4. Llevar la administración de vulnerabilidades, analizar las causas por las cuales se presentó e implementar las acciones preventivas y correctivas para adecuar las medidas de seguridad.

5. Identificar acciones y sus responsables (rastreabilidad).

6. Definir el proceso de registro de eventos (bitácoras) de los sistemas de información.

7. Explotar las bitácoras de los sistemas de información con el objetivo de identificar a los responsables de incidentes.

8. Notificar cualquier incidente encontrado.

9. Enviar de manera periódica los reportes de monitoreo, por ejemplo:

    i. Bitácoras de firewall.
    ii. Bitácoras de sistemas operativos.
    iii. Bitácoras de aplicaciones de negocio.

2.7.4.2. Responsable de la administración de cuentas y asignación de privilegios

Custodia o maneja activos de información, y debe cumplir con las siguientes funciones:

1. Asignar privilegios de los perfiles en sistemas operativos, aplicaciones y bases de datos.

2. Llevar la administración de cuentas y grupos.

3. Proveer a los Custodios un resumen de los accesos a los sistemas y aplicaciones.

4. Llevar la administración de la seguridad en usuarios, configurar cuentas y privilegios de usuario, así como, administrar las contraseñas.

5. Enviar de forma periódica los reportes de la administración de las cuentas (altas, bajas y cambios) de todos los activos de información bajo su responsabilidad.

6. Notificar de manera inmediata los incidentes de seguridad.

2.7.4.3. Responsable de la operación de tecnologías de seguridad

Opera y mantiene los recursos informáticos de seguridad, coordina las acciones necesarias para mitigar cualquier tipo de incidente de seguridad y restablecer lo antes posible la operación normal de los servicios, minimizando el impacto negativo sobre las operaciones de los sistemas y asegurándose de mantener el mejor nivel de servicio, calidad y disponibilidad, y debe de cumplir las siguientes funciones:

1. Controlar la ejecución de los procesos operativos de administración de dispositivos de seguridad.
2. Ser responsable de la disponibilidad de las tecnologías de seguridad.
3. Monitorear el desempeño de los dispositivos de seguridad.
4. Identificar virus y código malicioso en los dispositivos de seguridad.
5. Llevar a cabo la supervisión de proveedores.
6. Realizar respaldos de datos y recuperar la información en caso de ser necesario.
7. Llevar a cabo pruebas periódicas de integridad de los respaldos de información.
8. Identificar el mal funcionamiento de hardware (bajo desempeño de equipos, daños de discos, procesador, entre otros) y software (configuraciones erróneas, daños en el código, entre otros).
9. Registrar y evaluar los incidentes de seguridad que se llegarán a presentar.
10. Notificar cualquier incidente en materia de seguridad.
11. Llevar la administración de seguridad en los activos de información, (administrar los accesos de control, configurar las bitácoras de auditoria, etc).
12. Desarrollar procedimientos para la instalación y administración de telecomunicaciones.
13. Desarrollar procedimientos para la instalación y administración de los servidores y equipos de cómputo.
14. Llevar a cabo instalaciones y configuraciones seguras de sistemas operativos, con base a procedimientos y lineamientos específicos.
15. Establecer y mantener estándares de configuración para componentes de red y sistemas operativos.

16. Realizar la administración de parches y actualizaciones (probar con el objetivo de encontrar las consecuencias de su instalación dentro de los sistemas afectados).

17. Proveer al responsable encargado del monitoreo de la seguridad informática los reportes de administración de parches de actualización de seguridad.

2.7.4.4. Responsable de seguridad en el desarrollo y mantenimiento de sistemas de información

Verifica que los sistemas de información cuenten con los lineamientos de seguridad adecuados durante su desarrollo, adquisición e implantación, y debe de cumplir las siguientes funciones:

1. Desarrollar, integrar y mantener los controles de seguridad en los sistemas de información.

2. Desarrollar metodologías de desarrollo que integren elementos de seguridad en el desarrollo de código y en el manejo de fuentes, programas y objetos.

3. Asegurar que se separen los ambientes de desarrollo y producción.

4. Vigilar que dentro del ciclo de desarrollo de sistemas queden considerados los aspectos de seguridad de la información.

5. Notificar cualquier incidente en materia de seguridad.

2.8. Política de Clasificación de Información

La clasificación de información tiene como objetivo que ésta reciba un nivel apropiado de protección, la cual puede ser clasificada de acuerdo con el marco normativo aplicable a la misma y/o el valor que ésta le aporte a las operaciones de la dependencia o entidad, para así asignar los recursos que garanticen su confidencialidad, disponibilidad e integridad.

La información podrá ser clasificada de acuerdo a las siguientes definiciones:

2.8.1. Confidencialidad.

Garantiza que la información sea accesible solo al servidor público o tercero autorizado a tener acceso a la misma, protegiéndola contra divulgación no autorizada.

La información deberá ser clasificada de acuerdo a lo siguiente:

1. Su divulgación no causa ningún daño a la dependencia o entidad.
2. Su divulgación provoca una complicación o inconveniente operacional menor a la dependencia o entidad.

3. Su divulgación tiene un significativo impacto a corto plazo sobre las operaciones o los objetivos de la dependencia o entidad.
4. Su divulgación tiene un grave impacto sobre los objetivos a largo plazo de la dependencia o entidad.

2.8.2. Integridad.

Propiedad de la información orientada a salvaguardar la exactitud y totalidad de la información y los métodos de procesamiento de la misma, con el fin de brindarle la protección adecuada durante su ciclo de vida.

De acuerdo con el nivel de integridad la información se debe clasificar en:

1. **Alta:** esta clasificación aplica a los activos de información que requieren de manera obligatoria la aplicación de controles robustos que aseguren su integridad durante su procesamiento, transferencia o almacenamiento, de no ser así puede ocasionar un impacto negativo en las operaciones o procesamiento de información, impidiendo el cumplimiento de sus objetivos.

2. **Media:** esta clasificación aplica a los activos de información que requieren de la aplicación de controles que aseguren su integridad durante su procesamiento, transferencia o almacenamiento, de no ser así puede ocasionar un impacto medio en las operaciones, dificultando el cumplimiento de sus objetivos.

3. **Baja:** esta clasificación aplica para aquellos activos de información que no requieren de la aplicación de controles que mantengan su integridad durante su procesamiento, transferencia o almacenamiento.

2.8.3. Disponibilidad.

Garantizar que el no acceso a la información provoque una afectación a las operaciones o cumplimiento de los objetivos de la dependencia o entidad.

De acuerdo con el nivel de disponibilidad, la información se clasifica de la siguiente manera:

1. **Disponibilidad Alta:** Información cuya inaccesibilidad hasta por **2 horas** podría ocasionar afectaciones significativas.

2. **Disponibilidad Media:** Información cuya inaccesibilidad a partir de **2 horas y hasta 24 horas** podría ocasionar afectaciones significativas.

3. **Disponibilidad Baja:** Información cuya inaccesibilidad por un periodo **mayor a 24 horas** podría ocasionar afectaciones significativas.

Cada Dependencia o Entidad deberá llevar a cabo un proceso de reclasificación de la información, con base en los puntos estipulados en esta política.

Envío de la información
Se deben definir las acciones necesarias para el envío de información con la finalidad de preservar su propiedad de confidencialidad.

Eliminación de información
Se deben definir las acciones necesarias para la eliminación de información, de acuerdo a su propiedad de confidencialidad y considerando su medio de almacenamiento.

Etiquetado de información

Se deben definir las acciones para etiquetar la información de acuerdo con la Ley de Archivos del Estado de Colima, asegurando su propiedad de confidencialidad.

2.9. Política de Inventario de Activos de Información.

La política de inventario de activos de información tiene como propósito identificar a dichos activos, las instalaciones de procesamiento de información y definir las respectivas responsabilidades, y tiene como finalidad ayudar a garantizar la protección de la información, por lo que dichos inventarios deberán ser exactos, actualizados periódicamente con al menos una frecuencia anual, coherentes y alineados a otros inventarios.

Se recomienda que la entidad o dependencia identifique los activos de información relevantes en el ciclo de vida de la información (creación, procesamiento, almacenamiento, transmisión, eliminación y destrucción) para que los mismos sean inventariados.

Así también se deberán de inventariar las instalaciones de procesamiento de información.

Para elaborar el inventario se deberán de identificar los activos e instalaciones asociadas a la información, así como su ubicación, su respectivo responsable y Custodios, quienes deberán cumplir con las responsabilidades previamente establecidas.

2.10. Política de Uso Adecuado de los Activos de Información.

La política de uso adecuado de los activos de información tiene como propósito definir los lineamientos que contribuyan a salvaguardar la confidencialidad, integridad y disponibilidad de los mismos y de las instalaciones de procesamiento de información mediante su uso adecuado.

2.10.1. Protección de los activos de información

Los servidores públicos son responsables de salvaguardar cada uno de los activos de información que se encuentran bajo su custodia, uso o resguardo. El robo o la colaboración por parte de un servidor público para el mismo fin, así como el préstamo, desecho, venta, mal uso, o cualquier situación no autorizada se consideran acciones de uso indebido y serán ser sancionadas de acuerdo a lo establecido por el marco normativo que les resulte aplicable y las condiciones contractuales.

De igual forma son responsables de la protección de activos de información con copias temporales de información.

2.10.2. Uso indebido de los activos de información

Los activos de información están destinados estrictamente para ser usados en operaciones propias de la dependencia o entidad, por lo tanto está prohibido cualquier otro uso distinto al permitido.

En caso de que se solicite un servicio o se use algún activo de información con fines distintos, esto deberá apegarse a las autorizaciones y condiciones definidas para cada caso específico.

2.10.3. Uso y mantenimiento de instalaciones y equipos.

Las instalaciones y equipos deben ser operados solo por los servidores públicos que tienes asignadas funciones que los involucra, teniendo como responsabilidad mantenerlos en buen estado.

Para el almacenamiento se deben de considerar las especificaciones de uso recomendadas por el fabricante en cuanto a condiciones de humedad, temperatura, alimentación eléctrica, etc.

Se deberán observar las prácticas y calendarios de mantenimiento y aplicar programas de prevención de riesgos para aprovechar al máximo de su vida útil, buscando también no interrumpir la operación de los procesos y reducir al mínimo la ocurrencia de incidentes y fallas.

Como parte de mantenimiento se deben realizar verificaciones periódicas de la situación y estado actual del software instalado en los equipos de cómputo, reportando las desviaciones respecto al software autorizado y su uso.

Toda la información referente a la documentación y licencias del software deben mantenerse actualizadas y disponibles para cualquier verificación interna o externa que sea necesaria.

2.10.4. Uso adecuado de los equipos de cómputo

Los equipos de cómputo son esenciales para la operación diaria. Resulta indispensable que el hardware, software, así como el acceso, procesamiento y almacenamiento de los datos sean adecuadamente resguardados y utilizados exclusivamente para los propósitos debidamente autorizados.

Cada uno de los servidores públicos tiene la responsabilidad individual de:

1. Asegurar los sistemas de cómputo.
2. Conocer y entender las políticas específicas y los lineamientos que rigen el uso de las redes, los sistemas y la información que se gestiona.
3. Dar buen uso a los equipos de cómputo, entendiéndose como buen uso, su utilización estrictamente para las funciones que les han sido encomendadas.
4. Abstenerse de almacenar programas computacionales e información que no estén relacionados con sus actividades.
5. Abstenerse de realizar copias o apropiación de software de manera indebida.
6. Utilizar el software, así como el correo electrónico para los propósitos establecidos.

Además de lo anterior se deben atender las siguientes reglas generales:

1. No deberán instalar en sus computadoras programas no institucionales, o de los cuales no cuente con los permisos y licencias correspondientes.
2. No deberá hacerse ninguna modificación al software contratado, salvo los casos donde se permita en los convenios y licencias respectivos y bajo la supervisión del área correspondiente.
3. El desarrollo interno de programas, equipos y sistemas de computación, destinado para la planeación y ejecución de las actividades específicas donde se desarrolla.

2.10.5. Documentación de los procedimientos operativos

Se deberán documentar y mantener actualizados los procedimientos operativos identificados en esta Política y sus cambios deberán ser autorizados.

Los procedimientos especificarán instrucciones para la ejecución detallada de cada tarea, incluyendo:

1. Identificador del activo de información en el inventario.

2. Interdependencias con otros sistemas o equipos de cómputo.
3. Instrucciones para el manejo de errores u otras condiciones que puedan surgir durante la ejecución de tareas, incluyendo matrices de escalamiento para soporte.
4. Restricciones en el uso de utilitarios del sistema.
5. Instrucciones especiales para el manejo de "salidas" del activo de información fuera las instalaciones, como el uso de papelería especial (Solicitudes, autorizaciones, etc).
6. Reinicio del sistema y procedimientos de recuperación en caso de producirse fallas en el sistema.
7. Instalación y mantenimiento.
8. Monitoreo del procesamiento y las comunicaciones.
9. Inicio y finalización de la ejecución de los sistemas.
10. Programación y ejecución de procesos.
11. Gestión de servicios.
12. Resguardo de información.
13. Gestión de incidentes de seguridad en el ambiente de procesamiento y comunicaciones.
14. Gestión de cambios en el ambiente de procesamiento y comunicaciones.
15. Uso del correo electrónico.

2.11. Política de Seguridad en el Capital Humano

La presente política tiene como propósito de definir y establecer los lineamientos regulatorios necesarios para garantizar el nivel de seguridad deseado en los servidores públicos, por tal motivo es necesario fijar lineamientos para la selección, contratación y terminación de la relación laboral.

2.11.1. Previo al empleo, cargo o comisión

Se recomienda que la dependencia o entidad previo al empleo de un candidato a servidor público lleve a cabo la verificación de su currículum o antecedentes de acuerdo a lo estipulado en el marco normativo aplicable a la misma, debiendo ser proporcional a las

funciones, roles, y clasificación de la información a la que se accederá, así como los riesgos percibidos y se asegure de que los candidatos comprendan las responsabilidades y roles a desempeñar.

Cuando el empleo implique que el servidor público tenga acceso a las instalaciones de procesamiento de información, es recomendable que el candidato tenga competencia necesaria para desempeñar funciones de seguridad informática y que se pueda confiar en que asumirá el rol con responsabilidad.

2.11.2. Términos y condiciones

Los candidatos a servidores públicos deberán ser informados sobre sus términos y condiciones laborales referentes a la seguridad informática, debiéndose especificar:

1. Que se le concederá acceso a información confidencial, reservada y/o privilegiada.
2. Que adquirirá responsabilidades en materia de seguridad informática dentro de la dependencia o entidad así como fuera de la misma.
3. Que firmará un acuerdo de confidencialidad y no divulgación antes de que se le conceda el tratamiento de información.
4. Que será sujeto de responsabilidades administrativas, y sujeto a la aplicación de las leyes en materia de derechos de autor y protección de datos personales.
5. Que continuará siendo responsable después de concluido el empleo, cargo o comisión, o concluida la vigencia del contrato en su caso.

2.11.3. Durante el empleo

Durante el empleo se debe asegurar que los servidores públicos estén conscientes y cumplan con sus responsabilidades de seguridad informática.

Los servidores públicos tienen la obligación de cumplir con el reglamento interno, manual de organización, manual de procedimientos, código de ética, código de conducta, los lineamientos definidos en el presente manual y cualquier normatividad que se establezca en materia de seguridad informática.

2.11.4. Responsabilidades de la dependencia o entidad

Las dependencias y entidades tienen las siguientes responsabilidades con los servidores públicos de su adscripción:

1. Dar a conocer a todo servidor público de nuevo ingreso dentro de su programa de inducción una presentación que contenga las políticas y marco normativo aplicable en materia de seguridad informática, así como el procedimiento para el uso adecuado de cuentas, contraseñas y activos de información.

2. Comunicar claramente las responsabilidades relacionadas con la seguridad informática antes de darles acceso a información confidencial, reservada y/o privilegiada.

3. Motivarlos constantemente para cumplir cabalmente con las políticas de este Manual.

4. Proporcionarles un canal de denuncia anónima para reportar posibles violaciones en materia de seguridad informática.

5. Concientizar y capacitar en materia de seguridad informática con la finalidad de que los servidores públicos estén conscientes de sus responsabilidades y conozcan las políticas definidas.

   Se recomienda que el programa de capacitación sea periódico y cubra aspectos como:

   1. El propósito de la seguridad informática así como el impacto positivo o negativo.
   2. Afirmar el compromiso de la entidad o dependencia en materia de seguridad informática.
   3. La necesidad de conocer y cumplir las políticas aquí establecidas, así como el marco normativo aplicable.
   4. La rendición de cuentas por acciones u omisiones.
   5. Los procedimientos básicos de seguridad informáticas tal como el de notificación de incidentes.
   6. Contactos y recursos para obtener mayor información y asesoramiento.

6. Implementar métodos que permitan afianzar la cultura de seguridad informática, tales como:

   1. Correos electrónicos.
   2. Promover videos institucionales.
   3. Promover carteles, trípticos o fondos de pantallas.
   4. Realizar acciones de difusión el 17 de mayo de cada año.

2.11.5. Proceso disciplinario

La entidad o dependencia deberá elaborar y comunicar un proceso disciplinario formal para la toma de acciones respecto de los servidores públicos que hayan cometido una posible violación a la seguridad informática.

Se recomienda verificar previamente la posible violación a la seguridad informática antes de iniciar un proceso disciplinario.

Que el proceso disciplinario garantice un trato justo para los servidores públicos, que proporcione una respuesta gradual en relación con los factores de gravedad de la violación y su impacto, independientemente si es o no la primera infracción o repetición, y si el servidor público fue o no capacitado adecuadamente.

Será necesario aplicar el marco normativo, contratos, acuerdos o cartas de confidencialidad, manuales, lineamientos, procesos, otros que al efecto se hayan emitidos por la dependencia o entidad o les sean aplicables.

2.11.6. Responsabilidades en la terminación del empleo, cargo o comisión

Para efectos del presente Manual y los documentos que del mismo deriven en materia de seguridad informática, los cambios del puesto deben ser considerados como una terminación del empleo, cargo o comisión.
La dependencia o entidad deberá al momento de la terminación del empleo, cargo o comisión:

1. Solicitar al servidor público que devuelva la información confidencial, reservada o privilegiada a la que haya tenido acceso, se encuentre bajo su resguardo o custodia, así como las claves, usuarios y contraseñas.

2. Comunicar al servidor público la vigencia del acuerdo de confidencialidad firmado, vigente aún después de la finalización de la relación laboral.

3. Solicitar la baja del total de los activos de información asignados.

4. Coordinar la baja de todos y cada uno de los privilegios inherentes al puesto anterior en conjunto con el visto bueno del jefe inmediato.

5. Actualizar el expediente del servidor público de forma inmediata.

6. Coordinar el alta, los nuevos privilegios y activos de información del nuevo puesto, cargo o comisión con las áreas correspondientes.

2.11.7. Devolución de activos de información

Los servidores públicos deben devolver todos los activos de información que tengan bajo su responsabilidad o custodia a la terminación de su empleo, cargo o comisión.

Se recomienda que en los procesos de terminación se formalice la devolución con intervención de la Contraloría General del Estado.

Se deben llevar a cabo los siguientes puntos cuando los servidores públicos causen baja:

1. Solicitar y recibir del jefe inmediato del servidor público que causa baja el formato de baja de custodia de activos de información.

2. Para el caso de equipos de cómputo y software, se debe solicitar el apoyo al personal técnico para que revise los activos de información a devolver y verifique que estén completos y en buenas condiciones.

3. Cancelar la aceptación de responsable de activos de información.

4. Para el caso de abandono de trabajo o defunción, el jefe inmediato del personal que abandonó el empleo deberá dar aviso inmediatamente al personal de Capital Humanos o Administrativo para que se realicen las acciones necesarias.

En los casos donde el servidor público utilice equipo propio, es necesario que la información sea transferida a la entidad o dependencia de adscripción, y después eliminarla de forma segura de dicho equipo siguiendo el protocolo de borrado seguro establecido por la propia entidad o dependencia.

2.11.8. Eliminación de privilegios de acceso

Se debe notificar de forma inmediata al área correspondiente cada una de las bajas de los servidores públicos, con la finalidad de eliminar todos y cada uno de los privilegios de acceso inherentes al puesto, encargo o comisión.

2.12. Política de seguridad física y ambiental

El propósito de la presente política consiste en establecer los lineamientos necesarios que deberán seguir los servidores públicos o tercero autorizado para el acceso físico a las instalaciones.

Se debe delimitar el perímetro de seguridad física dentro de las instalaciones y los controles de acceso a implementar, deben permitir la entrada únicamente a servidores públicos y terceros autorizados.

El perímetro de seguridad física a establecer debe estar basado en la protección de la información y los activos de información que representan un valor para la dependencia o entidad.

2.12.1. Medidas de seguridad físicas

De manera enunciativa más no limitativa, se deberán considerar las siguientes actividades:

Prevenir el acceso no autorizado al perímetro del centro de datos, sus instalaciones físicas, áreas críticas, recursos e información;

Prevenir el daño o interferencia a las instalaciones físicas, áreas críticas, recursos e información;

Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico que pueda salir de la organización o ente; y

Proveer a los equipos que contienen o almacenan información de un mantenimiento eficaz, que asegure su disponibilidad e integridad.

2.12.2. Áreas definidas como seguras

Son consideradas áreas seguras todas aquellas que requieren un nivel de seguridad alto debido a que manejan información privilegiada, sin ser restrictivo o limitativo a los demás tipos de información.

Se deberán diseñar y aplicar procedimientos para trabajar en áreas seguras, considerando las siguientes directrices:

Supervisar el trabajo en el área segura

Revisar periódicamente las áreas seguras desocupadas

Autorizar equipo de audio, video o fotográfico

Registro de acceso y salida

Se recomienda asegurar físicamente los perímetros de un edificio o un sitio que contenga instalaciones de procesamiento de información; así como que el techo exterior, las paredes y el piso del sitio sea de construcción sólida y todas las puertas exteriores estén adecuadamente protegidas contra el acceso no autorizado con mecanismos de control (barras, alarmas, cerraduras, etc.), es recomendable que las puertas y ventanas estén aseguradas.

2.12.3. Centro de cómputo y/o centro de datos

El acceso al centro de cómputo y/o centro de datos debe ser controlado y permitido únicamente a los servidores públicos y/o terceros autorizados, debe tener controles de acceso robustos y que sean auditables (tarjetas de proximidad, controles biométricos, arcos magnéticos, etc.) que permitan autorizar y validar los mismos, así como, generar pistas de auditoría y/o rastreabilidad, las cuales deben ser almacenadas de forma segura. Las listas de accesos deben ser revisadas y actualizadas periódicamente para revocar accesos no vigentes (Ver política de control de acceso).

Se deberá implementar:

Un área de recepción y otros medios para el control de acceso físico al sitio o al edificio.
Monitorear o contar con alarmas contra incendios dentro del perímetro de seguridad.

Instalar sistemas adecuados de detección de intrusos al perímetro de seguridad.

2.12.4. Oficinas

El acceso a las áreas seguras que procesan, manejan o almacenan información privilegiada debe ser controlado y permitido únicamente a servidores públicos y terceros autorizados, estas áreas, sin excepción, deben contar con controles de acceso (puertas con llave, bitácora de entradas y salidas, aislamiento de otras áreas, controles de acceso electromecánicos, etc.), las listas de accesos deben ser revisadas y actualizadas periódicamente para revocar accesos no vigentes. (Ver Política de control de acceso)

2.12.5. Control de acceso físico a las instalaciones que procesan información

Para los servidores públicos:

Sin excepción, todo servidor público que ingrese a las instalaciones que procesan información o comprometan la misma, deberá portar su gafete de identificación, no obstruyendo o distorsionando la información del mismo con micas, cintas adheribles o cualquier otro elemento que no permita identificar claramente al portador del mismo.

Los servidores públicos que pierdan u olviden su gafete, deben utilizar un gafete provisional para poder ingresar a sus áreas de trabajo en tanto no se les renueve el gafete que los acredite como tal.

En caso de pérdida o robo de un gafete de identificación o tarjeta de acceso, éste debe ser reportado inmediatamente.

Queda estrictamente prohibido que el servidor público autorizado introduzca cualquier tipo de dispositivos de audio, video, telefonía o medios de almacenamiento masivo (Memorias USB u otro dispositivo) a los Centros de Datos y áreas designadas como seguras, sin previa autorización.

Para los visitantes:

Antes de permitir el acceso de visitantes a las instalaciones, se debe registrar su entrada.
Los datos a registrar en la bitácora de la recepción son:
Fecha
Hora de entrada y salida
Nombre y firma del visitante.

Motivo de su visita.
Registro de equipos de cómputo (en caso de que aplique).
Persona a quien visita o responsable de su visita.
Áreas a las que tendrá acceso como visitante (definidas por el responsable de su visita).

Posterior a su registro se le debe solicitar al visitante una identificación oficial con fotografía para verificar que es la persona quien dijo ser, que le será devuelta al término de su estancia, a cambio de esta se le entregará un gafete de visitante, el cual deberá portar en un lugar visible durante toda su estancia en las instalaciones.

Todo visitante al que se le haya proporcionado acceso a las instalaciones, debe ser acompañado en todo momento por la persona responsable de su visita.

Cualquier servidor público que identifique algún visitante sin compañía de un servidor público o que no porte su gafete de visitante debe ser reportado inmediatamente al área correspondiente.

Queda estrictamente prohibido que el visitante introduzca cualquier tipo de dispositivos de audio, video, telefonía o medios de almacenamiento masivo (Memorias USB u otro dispositivo) a los Centros de Datos y áreas designadas como seguras, sin previa autorización del área correspondiente.

2.12.6. Protección contra amenazas externas

Para la protección contra amenazas externas, se debe aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.

Se deberá tener asesoramiento especializado sobre cómo evitar daños derivados de incendios, inundación, terremoto, explosión, disturbios civiles y otras formas de desastre natural o causadas por el hombre.

Se deberán implementar sistemas de detección/supresión de incendios, acondicionamiento de la energía eléctrica, aire acondicionado, controles de humedad y otros sistemas de protección para las instalaciones, los centros de cómputo o centros de datos para asegurar el servicio continuo de los mismos. Los extractores de aire deben ubicarse donde no estorben o sean bloqueados fácilmente.

2.12.7. Protección a los centros de datos

Con el fin de mantener la confidencialidad e integridad de la información así como la continuidad del servicio, los centros de datos deben contar con:

Alumbrado de emergencia.
Pararrayos ubicados en las instalaciones.
Contar con al menos una fuente de energía alterna (Planta de emergencia).
Controles de supresión de picos.

Una fuente de energía ininterrumpida (UPS, por sus siglas en inglés).
Para el caso de los centros de cómputo, los muros que rodean dichas instalaciones deben ser no combustibles y resistentes a incendios.
Se debe considerar el uso de pisos falsos para una mejor operación y protección de los centros de cómputo.

Prevención y detección de incendios:
Las instalaciones deben cumplir con los requisitos de las regulaciones de protección civil aplicables.

Dependiendo de la ubicación y considerando los diferentes tipos de incendios, los sistemas de detección deberán instalarse de modo que tengan calidad, alta confiabilidad y tengan sensores para detectar humo, fuego y altas temperaturas. El equipo y los sensores de detección de incendios deben incluir procedimientos de mantenimiento preventivo y/o correctivo según sea el caso.

Se recomienda que el sistema de detección de fuego incluya un panel de alarma que indique con claridad dónde se identificó el incidente. El equipo deberá ser capaz de alertar a todo el personal en caso de incendio e incluir una señal de alarma de evacuación para garantizar la evacuación oportuna.

Por seguridad del personal y para minimizar en lo posible los daños de incendio en las instalaciones, se deben desarrollar y mantener planes de evacuación. Los simulacros de evacuación de las instalaciones se deben realizar en intervalos regulares y en días hábiles con una operación normal.

De acuerdo al entorno y la ubicación de las instalaciones, se debe considerar:

El uso de materiales a prueba de fuego en las áreas seguras.

En caso de incendio se deben tomar medidas para ventilar el humo y calor e impedir la distribución de humo.

Se debe considerar el uso de luces de emergencia, dichas luces deberán estar activas en forma inmediata y automática en caso de incendio.

Se deben señalar las salidas de emergencia e indicar las rutas más cercanas de salida y todas las que estén disponibles.

Los puntos de reunión deben estar definidos dentro de las instalaciones.

2.12.8. Gestión de medios extraíbles

Todos los medios se deben de almacenar en un entorno seguro de acuerdo con las especificaciones del fabricante.

Si la confidencialidad o la integridad de la información es considerada importante, es recomendable utilizar técnicas criptográficas para protegerla de los medios extraíbles.

Para mitigar el riesgo de la degradación de los medios mientras la información almacenada aún se necesite, es recomendable que la información sea transferida a un nuevo medio antes de que sea ilegible.

Se recomienda que las copias múltiples de la información importante sean almacenadas en medios separados para reducir el riesgo de daño o pérdida de información.

Es recomendable considerar el registro de los medios extraíbles para limitar la posibilidad de pérdida de información.

Se recomienda que las unidades de medios extraíbles sólo se habiliten si hay autorización por el responsable.

Es recomendable se monitoreen los medios extraíbles cuando exista la necesidad de usarlos para el tratamiento o transferencia de información.

Cuando ya no sea necesario, el contenido de cualquier medio reutilizable que sea retirado de la dependencia o entidad es recomendable se hagan irrecuperables.

Debe exigirse la autorización para los medios fuera de la organización y mantener un registro de estos retiros con el fin de conservar una evidencia de auditoría.

2.12.9. Disposición de medios

Se debe disponer de manera segura de los medios cuando ya no se requieran.

Se deberá establecer el procedimiento y registro formal para la eliminación segura de los medios con la finalidad de minimizar el riesgo de fuga de información a personas no autorizadas con el fin de mantener una evidencia de auditoría.

Los medios dañados requieren de una valoración de riesgos para determinar si físicamente deben ser destruidos en lugar de repararse o tirarse.

2.12.10. Protección a los medios de almacenamiento de información durante su traslado fuera de las instalaciones.

Se debe establecer un procedimiento que asegure que el traslado de los medios de almacenamiento se lleve a cabo de manera segura desde el lugar de donde serán extraídos hasta el lugar en donde se resguardarán.

Para el traslado seguro de los medios de almacenamiento se debe:

1. Definir y autorizar al servidor público y personal para trasladarlos, entregarlos y/o recibirlos.

2. Solicitar la identificación del servidor público o personal autorizado para el traslado, entrega y/o recepción.

3. Contar con un registro en el que se identifique el contenido de los medios, la protección aplicada, tiempos de traslados desde su envío hasta su recepción.

4. Establecer el calendario de traslados de manera periódica, estos calendarios deben ser cambiados de forma continua para evitar ser predecibles y minimizar el riesgo de robo o colusión.

5. Definir el medio de traslado más conveniente y confiable de acuerdo a sus necesidades y recursos disponibles.

6. Deberá contar con un empaquetado que sea suficiente para proteger el contenido de cualquier daño que pueda producirse durante el traslado, considerando las especificaciones del fabricante (protección contra factores ambientales como el calor, la humedad o campos electromagnéticos).

7. Cuando la información no se encuentre cifrada, se deberá implementar protección física adicional a los medios de almacenamiento.

8. Se deberá llenar un formato para autorizar la salida y el traslado de las instalaciones al lugar de almacenamiento.

9. Posterior a la entrega, se deberá contar con el soporte de su recepción por parte de quien resguarda y custodia los medios y la información.

10. La dependencia o entidad deberá contar con el soporte de la salida que resguarda y custodia la información.

11. Deben ser sellados de forma externa, para identificar si han sido violados durante su traslado.

12. Deben ser trasladados de manera discreta para evitar que cualquier persona se percate de su contenido.

13. Cada vez que se entreguen para su resguardo y custodia, se deberá solicitar un comprobante de recibido, el cual avale su recepción.

14. En caso de robo, se deben levantar las actas pertinentes y dar aviso al área correspondiente para decidir las acciones a tomar.

15. Debe existir un contrato o convenio del resguardo y/o custodia que garanticen la confidencialidad, integridad y disponibilidad de los mismos.

2.12.11. Escritorio limpio

Cuando el servidor público se ausente de su lugar de trabajo, por ningún motivo se deben dejar documentos con información clasificada como confidencial o privilegiada en los escritorios y/o a la vista del personal, proveedores o visitantes.

Los documentos con información privilegiada o confidencial deben estar resguardados en lugares seguros y bajo llave.

Todos los equipos portátiles deberán contar con dispositivos que eviten el movimiento físico no autorizado.

Está prohibido que los servidores públicos y visitantes fumen, coman o ingieran bebidas en el centro de cómputo, centro de datos o espacios donde se encuentren activos de información, ya que se corre el riesgo de daños a los dispositivos de almacenamiento.

2.13. Política de control de acceso a sistemas y aplicaciones

El propósito de la presente política consiste en establecer los lineamientos que contribuyan a evitar el acceso no autorizado a sistemas y aplicaciones.

2.13.1. Registro de usuarios

Deben existir procedimientos formales establecidos para el registro de usuarios en el cual se otorguen y revoquen accesos a sistemas y aplicaciones.

Los controles de acceso para registro deben incluir:

El identificador de usuario (user-ID, por sus siglas en inglés) debe ser única para cada usuario que solicite acceso a sistemas y aplicaciones. Todos los usuarios deben acceder a los sistemas y aplicaciones a través de la cuenta de usuario asignada.

Todo servidor público deberá ser responsable de los derechos de acceso de su personal y proveedores externos bajo su control.

Bajas o cambios requeridos con relación a derechos de acceso debido a bajas, transferencias y cambios de funciones o de actividades, deben ser formalmente comunicados a las áreas correspondientes en las siguientes 24 horas a su aprobación.

Mantener un registro formal de todas las personas a las cuales se les haya otorgado algún derecho o facultad de acceso.

Se debe validar que los derechos o facultades de acceso del usuario sean debidamente autorizadas, documentadas y archivadas.

Se debe asegurar que a los usuarios les sean dados solo aquellos privilegios y facultades necesarias para ejecutar su función.

Proporcionar al usuario una copia firmada de sus derechos de acceso indicando un apartado donde se especifique que entienden las condiciones de acceso al cual esta sujeto y que son responsables de las actividades realizadas a través de la cuenta asignada.

Asegurar que a proveedores y terceros en general no se les otorgue acceso a las plataformas tecnológicas hasta que no hayan sido debidamente autorizados.

2.13.2. Administración de privilegios

Para todo el servidor público y terceros:

El Titular deberá tener documentados todos los privilegios y facultades de accesos asignados, asociados a las diferentes plataformas tecnológicas (Sistema Operativo, Sistema Manejador de Base de Datos, aplicaciones, etc.).

Los privilegios o facultades asignadas a los servidores públicos deben ser restringidas o limitadas específicamente a lo que les compete saber, basado en el principio de mínimo privilegio (lo estrictamente necesario). El área que haga uso de información, debe especificar claramente por escrito, la asignación de responsables de la misma con el propósito de ser autorizada, tales declaraciones deben indicar a los individuos que se les ha concedido autoridad para dar tratamiento a información específica.

2.13.3. Administración de contraseñas de usuarios

Los sistemas de administración de contraseñas deben ser interactivos y deben asegurar contraseñas de calidad.

Para todo el servidor público y terceros:

Una vez autorizado el acceso a los sistemas o aplicaciones se les debe proporcionar una contraseña temporal con la cual podrán firmarse por primera vez al sistema o aplicación. Se recomienda que inmediatamente después los sistemas fuercen al usuario a cambiar ésta, respetando los estándares de contraseñas establecidos en esta política.

Debe existir un procedimiento para verificar la identidad de los usuarios antes de suministrar la nueva contraseña que remplazará a la anterior.

Se recomienda que las contraseñas temporales sean otorgadas a los usuarios de manera segura; evitando el uso de mensajes de correo electrónico oficiales para el envío de éstas.

Las contraseñas no deberán ser almacenadas en formatos no protegidos, es decir, sin el uso de elementos criptográficos.

Las contraseñas referentes a las cuentas por default incluidas en los sistemas o aplicaciones adquiridas deben ser desactivadas, de no ser posible su desactivación las contraseñas deben ser cambiadas posterior a la instalación del producto.

2.13.4. Revisión de derechos de acceso

Los derechos de acceso deben ser revisados a intervalos regulares.

Los derechos de acceso deben ser actualizados si en la revisión son detectadas incongruencias en los privilegios asignados.

Los derechos de acceso de cuentas privilegiadas deben ser revisados a intervalos más cortos y cuando existan cambios significativos en éstas.

2.13.5. Estándares de contraseñas

Las contraseñas no deben ser reveladas ni compartidas, salvo en casos de emergencia, en los cuales se debe contar con la autorización del Titular o en su defecto por el titular del área a la que pertenece el usuario; una vez resuelta la situación de emergencia, se debe cambiar la contraseña de inmediato por parte del responsable directo de la misma.

En caso de sospecha de revelación de contraseñas a servidores públicos o terceros no autorizados, estas contraseñas deben ser cambiadas inmediatamente.

Las contraseñas no deben ser escritas u olvidadas en un lugar en donde puedan ser del conocimiento de otro servidor público o tercero no autorizados.

Si el usuario está utilizando información sensible clasificada como confidencial, privilegiada o reservada no podrá abandonar su PC, terminal o estación de trabajo sin antes salir o bloquear el sistema o aplicación pertinente.

2.13.6. Estándar de contraseñas para usuarios finales

Las contraseñas para el acceso a los sistemas de información o aplicaciones deben cumplir con las siguientes características:

Deben tener una longitud mínima de 8 caracteres.

Deben combinar caracteres alfanuméricos (al menos un número).

Deben cambiarse cada 90 días naturales como mínimo.

Los recursos de procesamiento de información no deben permitir la repetición de contraseñas por al menos las últimas 5 iteraciones.

Las contraseñas deben ser almacenadas en forma cifrada de tal forma que no puedan ser comprometidas con técnicas de análisis criptográfico.

Se debe considerar la opción de que las contraseñas sean almacenadas en archivos electrónicos distintos en los que se almacenan datos de la aplicación y sistemas de información.

Las contraseñas deben viajar cifradas una vez que han sido introducidas en el recurso de procesamiento de información.

Si no es posible seguir con el estándar mencionado en los puntos anteriores porque la tecnología no lo permite, se deben tomar medidas alternas.

2.13.7. Identificación y autenticación

Todas las plataformas tecnológicas autenticarán la identidad de los usuarios antes de iniciar una sesión o transacción, a menos que se tenga acceso a información pública.

Todos los usuarios serán identificados en las plataformas tecnológicas por un:

Único ID usuario.

Método de autenticación asegurando la identificación única de los usuarios, mediante contraseñas estáticas o dinámicas, llave publica, biométrico u otro mecanismo.

Las cuentas de los usuarios deben ser auditables para todas actividades asociadas con su ID de usuario y password.

Las claves de usuario asociadas con passwords estáticos tienen que ser deshabilitadas después de los tres intentos de accesos fallidos.

Se debe asegurar que las claves de usuario son deshabilitadas después de un periodo definido de inactividad. Estos periodos serán definidos dependiendo del nivel de criticidad de los sistemas de información. Las áreas podrían no aplicar los requerimientos de cambio de passwords estáticos y deshabilitación de claves de usuario para acceso a los sistemas de información siempre y cuando las áreas se aseguren que periódicamente les recuerden a sus usuarios que cambien manualmente sus contraseñas.

Se debe considerar el uso de canales y técnicas de autenticación y cifrado para toda aquella información clasificada como confidencial, reservada o privilegiada, los cuales deben ser controlados y asignados por quien se encargará de administrar las identidades y privilegios de seguridad.

Se deben diseñar y establecer esquemas de autenticación para acceso a los sistemas o aplicaciones, de acuerdo al nivel de confidencialidad de la información que se requiera acceder.

Si no ha habido actividad durante un lapso de tiempo de 5 minutos, el sistema deberá suspender la sesión y se deberá reestablecer cuando el usuario introduzca la contraseña adecuada (si la aplicación no lo permite, se debe tener habilitado el protector de pantalla al pasar los 5 minutos antes mencionados).

Se deben utilizar herramientas tecnológicas para dar el acceso a los sistemas o aplicaciones a través de un inicio seguro de sesión en el cual se limite el tiempo máximo y mínimo para el inicio de sesión. Si se excede el tiempo indicado, el sistema finalizará el proceso de inicio de sesión.

2.13.8. Factores de autenticación.

Los usuarios deben ser autenticados con base en algo que ellos conozcan, tengan o sea parte, como son:

Algo que el usuario sabe – Contraseña o *PIN*
Algo que el usuario tiene – *Token* o certificados.
Algo que es parte del usuario – Huella Digital (biométricos).

La autenticación debe ser de uno o dos factores de acuerdo al tipo de sistemas o aplicaciones al que se acceda.

Cuando se trate de un factor de autenticación, el usuario debe proporcionar solo una prueba de identidad.

Cuando se trate de dos factores de autenticación, el usuario debe proporcionar dos tipos de pruebas de identidad.

2.13.9. Estándar de tipos de cuentas

Los tipos de cuentas de usuario para acceder a los recursos de procesamiento de información deben ser:

1. **Cuentas de usuario final.** Cuentas con privilegios normales, asignados de forma individual; con fines de uso y análisis de la información con base en el principio de mínimo privilegio.

2. **Cuenta de default en sistemas o aplicaciones adquiridas.** Cuenta asociada al funcionamiento de una aplicación y/o servicio; con fines de administración de elementos de procesamiento de información, y restringida a las áreas de tecnología de información. Se debe considerar la desactivación de dichas cuentas o de no ser posible las contraseñas de éstas deben ser cambiadas.

3. **Cuentas privilegiadas**. Cuenta asociada a la administración u operación de un elemento de procesamiento de información.

4. **Cuentas grupales**. Cuenta compuesta de cuentas de usuario final, asignadas de forma grupal; con fines de uso y análisis de la información con base en el principio

de mínimo privilegio. Este tipo de cuentas no deben ser utilizadas a menos que sean autorizadas por el Custodio.

2.13.10. Restricciones de acceso a la información

Los sistemas y aplicaciones deben contener menús para controlar el acceso a las diferentes funciones de los mismos.

Se deben considerar restricciones en las facultades o privilegios de acceso que consideren otorgar el mínimo privilegio para la realización de sus funciones:

Privilegios de sólo lectura
Privilegios de escritura
Privilegios de borrado

Asegurar que la información de salida del sistema que contenga información privilegiada, reservada o confidencial únicamente sea la relevante (la información redundante o no necesaria debe ser eliminada) y sea proporcionada únicamente al personal autorizado.

2.13.11. Eliminación de privilegios de acceso

Se deben notificar de inmediato las bajas de los servidores públicos a las áreas correspondientes, para inhabilitar y/o dar de baja las cuentas de usuario.

Las cuentas de usuario deben ser borradas por el grupo encargado de administrar las identidades y privilegios, cuando alguna de las siguientes situaciones se presente:

Terminación de la relación laboral.
Terminación de la función operativa para la cual fue creada la cuenta del usuario.
Inactividad de la cuenta de usuario en un periodo mayor a 30 días.

2.14. Política de uso de servicios de la red

La presente política tiene como propósito definir los mecanismos para la protección de las redes internas de datos, incluyendo accesos externos.

2.14.1. Seguridad en Redes Internas

Los usuarios de los servicios de red, son responsables del uso de la misma y debe ser sólo para efectos de la operación interna.

2.141.2. Configuración, administración y actualización de la red

Los servidores, estaciones de trabajo, equipos portátiles, impresoras y todos los equipos que sean conectados a la red interna, deben estar configurados con base en los lineamientos establecidos por el área encargada de la administración de la red, donde se determinarán los lineamientos mínimos de configuración.

Los componentes de la red deben contar con las configuraciones adecuadas de seguridad y con la actualización de parches y versiones indicadas por el proveedor.

Se deben tomar las medidas necesarias cuando se lleve a cabo cualquier expansión, reducción y cambios de la red, para asegurar la protección de la misma y de la información almacenada, procesada y transmitida vía red.

La red interna debe estar segmentada por medio de componentes de red. Se debe contar con segmentos de red seguros para los equipos críticos.

Se debe contar con cableado estructurado en la red, que cumpla con especificaciones mínimas de seguridad.

2.14.3. Responsabilidades de la administración de la red

Se debe contar con un inventario de todos los componentes de red y todos los sistemas, aplicaciones y activos de información que estén asociados con la red interna.

Se deben llevar a cabo planeaciones de la capacidad de la red y sus componentes para asegurarse de contar con la disponibilidad y desempeño adecuados.

2.14.4. Monitoreo de la red

Se debe contar con un monitoreo constante para detectar cualquier incidente de seguridad en los servicios de red.

Se debe llevar a cabo un estricto bloqueo de sitios Web que no son necesarios para la operación del Gobierno del Estado, ya que consumen recursos de la red a excepción de los usuarios especiales o del personal que por sus funciones requieran habilitaciones especiales.

Se debe establecer y llevar a cabo un programa de mantenimiento periódico de los componentes de red con base en las recomendaciones del fabricante.

2.14.5. Servicios de red

La información clasificada como confidencial, reservada o privilegiada que se transmita por medio de la red interna debe hacerse de manera segura, considerando el uso de

tecnologías de cifrado de información para proporcionar integridad y confidencialidad en la misma.

El servicio de conectividad a la red debe emplear un mecanismo de administración de nodos para evitar puntos de acceso no controlados. Para llevar a cabo la entrada a los servicios de la red interna se debe contar con un mecanismo de administración de identidades que proporcione el acceso a dichos servicios.

Se debe considerar dentro de la seguridad de la red interna controles para el correo electrónico en donde se revisen como mínimo los siguientes puntos:

Mensajes que puedan provocar denegación de servicio de la red.

Implicaciones de acceso a información privilegiada, reservada o confidencial.

Uso de cuentas de correo no oficiales por parte de los usuarios.

Medios para controlar el acceso de usuarios remotos a las cuentas de correo electrónico.

Alternativas para envíos de información privilegiada, reservada o confidencial.

Información recibida de usuarios desconocidos.

Bloqueo de correo externo cuando el destinatario se encuentre con copia oculta (cuando sea apropiado).

2.14.6. Autenticación de equipos en la red

Se deberá asegurar que los componentes de la red interna, tengan asignada una dirección de red autorizada.

El direccionamiento de red debe ser asignado con base en los procedimientos de instalación y configuración de componentes de red.

2.15. Política para el reporte de incidentes y vulnerabilidades de seguridad de la información

La presente política tiene como propósito establecer los lineamientos para garantizar que los incidentes y vulnerabilidades de seguridad asociados a la información sean comunicados y tratados de acuerdo a su criticidad, además de tomarse las acciones necesarias para su tratamiento.

Un incidente de seguridad es un evento adverso que compromete la confidencialidad, integridad o disponibilidad, la legalidad y confiabilidad de la información. Puede ser causado mediante la explotación de alguna vulnerabilidad o un intento o amenaza de romper los controles de seguridad existentes.

Se considerarán como vulneraciones a la seguridad en cualquier fase del tratamiento de información al menos las siguientes:

a) La pérdida o destrucción no autorizada;
b) El robo, extravío o copia no autorizada;
c) El uso, acceso o tratamiento no autorizado; y
d) El daño, la alteración o modificación no autorizada.

Se debe garantizar que los incidentes de seguridad y las vulnerabilidades asociadas a la seguridad de la información sean comunicados de manera oportuna para tomar las acciones correspondientes.

Todos los servidores públicos y terceros deben conocer los procedimientos para el reporte de los incidentes de seguridad y vulnerabilidades que podrían causar un impacto negativo a la dependencia o entidad, por lo que todo incidente o vulnerabilidad debe ser reportado de manera rápida y oportuna al servidor público correspondiente.

2.15.1. Reportes de incidentes de seguridad

Todos los servidores públicos tienen la obligación de reportar al área correspondiente cualquier incidente de seguridad en los siguientes casos:

1. Pérdida de servicios del área de tecnología.
2. Sustracción, robo o pérdida de equipos de cómputo.
3. Incumplimiento a las políticas de seguridad de la información.
4. Brechas en los controles de seguridad existentes.
5. Accesos no autorizados a las instalaciones de procesamiento de información o asociadas a la información.
6. Accesos no autorizados a los centros de cómputo.
7. Accesos no autorizados a sistemas, aplicativos y/o servicios del área de tecnología.
8. Virus informático (detección o sospecha).
9. Desastres.
10. Fallas de suministro eléctrico.
11. Spam.
12. Otros que consideren vulneran o incidan en la seguridad de la información.

Deben existir procedimientos de respuesta a incidentes de seguridad considerando:

El área encargada de la administración y respuesta a incidentes de seguridad de la información debe elaborar un procedimiento para dar respuesta a incidentes de seguridad.

1. El área encargada de la administración y respuesta a incidentes de seguridad de la información tiene la responsabilidad de coordinar las acciones para solucionar los incidentes que afecten los servicios de información para la operación, con la corresponsabilidad de las áreas involucradas.

2. Todos los usuarios tienen la responsabilidad de reportar los incidentes de seguridad de información que sean de su conocimiento al encargado de la administración de respuesta a incidentes de seguridad en apego a la categoría y tiempo de atención del incidente, por medio de los procedimientos establecidos.

3. Los procedimientos para la notificación de incidentes deben estar fácilmente disponibles para todos los usuarios.

4. Dentro de los procedimientos de respuesta a incidentes, se deben proporcionar criterios para la categorización y atención de los mismos, considerando el grado potencial del incidente para afectar la operación de la Entidad o Dependencia.

5. Todos los incidentes de seguridad se deben registrar y la información utilizada o documentada se debe de resguardar.

6. Toda la información y/o documentación de los incidentes de seguridad registrados deben ser custodiados por el titular del área encargada de la administración y respuesta a incidentes de seguridad de la información.

7. Los procedimientos para la respuesta a incidentes de seguridad deben permitir el seguimiento continuo del estado del incidente.

8. La investigación de los incidentes de seguridad se debe de llevar a cabo con base en los procedimientos de respuesta a incidentes de seguridad.

9. Se debe llevar a cabo un informe detallado de los resultados de la investigación de los incidentes de seguridad, antes de que el incidente sea cerrado y se guardarán por un período no menor a tres años.

10. Los informes sobre los incidentes de seguridad, deben ser del conocimiento de los usuarios que levantaron el reporte, siempre y cuando la información que contenga el reporte no esté clasificada como confidencial, reservada o privilegiada.

2.15.2. Respuesta a Incidentes de Seguridad

1. Los procedimientos para la respuesta a incidentes de seguridad deben ser elaborados tomando en consideración la reducción al mínimo del daño potencial a los activos de información.

2. Los procedimientos de respuesta a incidentes de seguridad deben ser revisados periódicamente por el área de respuesta a incidentes y los resultados de dichos ejercicios deben evaluarse para tomar las acciones necesarias con un enfoque de mejora continua.

3. El área encargada de la administración y respuesta a incidentes de seguridad de la información y sistemas debe estar capacitada para el uso de las herramientas que se utilicen para la investigación y la respuesta a incidentes.

4. Se deben llevar a cabo sesiones de lecciones aprendidas con los responsables y los involucrados en los incidentes de seguridad presentados.

2.15.3. Reporte de vulnerabilidades de seguridad

Las vulnerabilidades deben ser tratadas de la misma manera que los incidentes de seguridad. Todos los servidores públicos tienen la obligación de reportar vulnerabilidades de seguridad a efecto de evitar que puedan convertirse en incidentes de seguridad.

De manera periódica (mínimo de forma anual) se deben ejecutar análisis de vulnerabilidades y pruebas de penetración a la plataforma tecnológica a fin de detectar vulnerabilidades de seguridad.

Se debe llevar a cabo el monitoreo de seguridad a los sistemas, aplicaciones y servicios del responsable de la información para identificar cualquier vulnerabilidad de seguridad para su debida atención y seguimiento.

Se debe comunicar a todos los servidores públicos los casos y el medio para reportar vulnerabilidades de seguridad.

Se deben implementar los procedimientos para la atención de vulnerabilidades de seguridad.

2.15.4. Acciones a realizarse en caso de vulneración a la seguridad

En caso de que ocurra una vulneración a la seguridad, se deberá analizar las causas por las cuales se presentó e implementará las acciones preventivas y correctivas para adecuar las medidas de seguridad si fuese el caso, a efecto de evitar que la vulneración se repita.

Se deberá informar sin dilación alguna al Titular, las vulneraciones que afecten de forma significativa los derechos patrimoniales o morales, en cuanto se confirme que ocurrió la vulneración y que el responsable haya empezado a tomar las acciones encaminadas a detonar un proceso de revisión exhaustiva de la magnitud de la afectación, a fin de que los titulares afectados puedan tomar las medidas correspondientes para la defensa de sus derechos.

2.15.5. Bitácora de las vulneraciones a la seguridad

El responsable deberá llevar una bitácora de las vulneraciones a la seguridad en la que se describan los datos siguientes:

1. La fecha en la que ocurrió.
2. El motivo de ésta.
3. Las acciones correctivas implementadas de forma inmediata.
4. Nombre del responsable o responsables.
5. Encargado, cuando la vulneración de seguridad devenga de un tratamiento de información efectuado por el responsable.
6. Origen de las vulneraciones.
7. Número de vulneración o recurrencia de éstas.
8. Los demás que se establezcan.

2.16. Política de dispositivos móviles y trabajo a distancia o remoto.

Con la finalidad de mantener la seguridad de la información en el uso de equipos móviles y trabajo remoto o a distancia se recomienda:

1. Que las computadoras portátiles y comunicaciones móviles cuenten con restricciones de acceso al entorno de la red del Estado.

2. Retirar los accesos y permisos concedidos a los equipos de cómputo y comunicaciones móviles una vez que dejen de ser utilizados para los fines que fueron otorgados.

3. Adoptar medidas de seguridad de soporte para gestionar los riesgos introducidos por el uso de dispositivos móviles.

4. Tener cuidado al usar dispositivos móviles en lugares públicos, salas de reuniones y otras áreas no protegidas, y asegurarse de que la información no se vea comprometida.

5. Se deberán de implementar protecciones para evitar el acceso no autorizado o la divulgación de la información almacenada y procesada.

6. Que los dispositivos móviles estén físicamente protegidos contra robo.

7. Establecer un procedimiento específico que tome en cuenta requisitos legales, el seguro y otros requisitos de seguridad para caso de robo o pérdida.

8. No desatender los dispositivos que lleven información privilegiada, confidencial o reservada, cuando sea posible deben estar físicamente bloqueados o con mecanismos de bloqueo especiales que sean utilizados para asegurar los dispositivos.

9. Evitar conectarse a redes inalámbricas abiertas. En caso de ser necesario preferentemente deberá acceder a una red con seguridad WPA o WPA2, ya que las redes abiertas o con seguridad WEP son inseguras.

10. Deberá deshabilitar los procesos de sincronización de su equipo si va a usar una red pública.

11. Mantener el equipo actualizado, con antivirus instalado correctamente y si es posible, hacer uso de un cortafuegos o firewall.

12. Tener precaución al navegar por páginas cuyos datos no viajan cifrados (la URL no empieza por HTTPS).

13. No deberá iniciar sesión donde deba digitar usuario y contraseña cuando esté conectado en una red pública.

14. Evitar realizar transacciones bancarias y compras online o intercambio de datos privados desde redes wifi-públicas.

15. Eliminar los datos de la red memorizados por el equipo tras una conexión a una red pública.

16. Cuando se usen dispositivos móviles propios o privados para el tratamiento de información reservada, confidencial o privilegiada se deberá firmar una carta en la que renuncia a la propiedad de la información, permitiendo el borrado remoto de la información en caso de robo, pérdida o cuando ya no esté autorizado.

17. Proporcionar acceso a la información solo después de que los usuarios han firmado un acuerdo de confidencialidad y han reconocido sus obligaciones, renuncia a la propiedad de dicha información permitiendo el borrado remoto en caso de robo o pérdida del dispositivo o cuando ya no esté autorizado a utilizar el servicio.

En el supuesto de contar con trabajo remoto se deberá tener en cuenta la seguridad física existente en el sitio de trabajo.

Se deberán establecer requisitos de seguridad para las comunicaciones, teniendo en cuenta la necesidad de acceso remoto a los sistemas internos de la entidad o dependencia, la sensibilidad de la información a la que se pueda acceder y pasar sobre el enlace de comunicación y la sensibilidad del sistema interno.

Proporcionar el acceso desde el escritorio virtual que prevenga el procesamiento y almacenamiento de información sobre el equipo de propiedad privada.

Políticas y procedimientos para prevenir las controversias para relativas a derechos de propiedad intelectual desarrollada en equipos de propiedad privada.

Requisitos de protección de antivirus y firewall.

Se recomienda que los lineamientos y disposiciones considerados incluyan:

1. El suministro de quipo adecuado y dispositivos de almacenamiento para las actividades, donde el uso de los equipos de propiedad privada que no están bajo el control de la dependencia o entidad no esté permitido.

2. Definición del trabajo permitido, horas de trabajo, clasificación de la información que pueda llevarse a cabo y los sistemas internos y servicios que el trabajador o servidor público esté autorizado a acceder.

3. Suministro adecuado de equipo de comunicación, incluyendo métodos para asegurar el acceso remoto.

4. Seguridad física.

5. Normas y lineamientos sobre el acceso al grupo, al equipo visitante y a la información.

6. Suministro y mantenimiento de hardware y software.

7. Provisión de seguros.

8. Procedimientos de respaldos y continuidad de la actividad diaria.

9. Auditoría y supervisión de la seguridad.

10. Revocación de los derechos de acceso y devolución de equipo cuando se terminan las actividades.

Se expide en la ciudad de Colima, Colima, el quince de junio de dos mil veintiuno.

3. SECCIÓN DE CAMBIOS

No. de versión	Fecha de actualización	Descripción del cambio
0	21/06/2021	Inicia su uso
1	30/04/2024	Cambio de formato y modificaciones en el Marco Normativo