Estándar para la elaboración del manual del sistema de gestión de seguridad de la información

Contenido

Introducción

El Gobierno del Estado de México es el principal impulsor de los servicios que ofrece basados en esquemas de mejora, así como el establecer una relación más próxima y cercana con la sociedad, buscando constantemente la innovación e implementar nuevos modelos de gestión funcionales derivado del acelerado desarrollo de la tecnología y el manejo de grandes volúmenes de información.

Por tal motivo el uso eficiente de las tecnologías de la información y Comunicación (TIC) se vuelve tema primordial para acercar dichos servicios de manera rápida y eficaz a la ciudadanía, materializando en un mejoramiento tangible las condiciones de vida de la ciudadanía y permitiendo el acceso a los mismos con mayor comodidad, logrando mediante el uso de la tecnología el acercamiento del gobierno al ciudadano.

Como parte de las acciones tendentes a buscar esquemas de mejora, se emite el presente estándar, para la Elaboración del Manual para un Sistema de Gestión de Seguridad de la Información que pudiera ser implementado en las Dependencias u organizaciones, el cual está basado en la norma ISO 27001:2013.

Es importante considerar que, en este contexto, el Sistema de Gestión de Seguridad de la Información (SGSI) debe tener una estructura que le permita constituirse como documento básico para:

- Describir la estructura del Sistema de Gestión de Seguridad de la Información de la Dependencia u Organización.
- Precisar cómo se da cumplimiento a los requisitos de la norma;
- Usarlo como guía y referencia para la ejecución de revisión y/o auditorías internas de seguridad.
- Operar el SGSI e identificar puntos de mejora en los procesos de la Dependencia u Organización.

Alcance

Este manual para sistemas de gestión de seguridad de la información será aplicado por los sujetos considerados en la Ley de Gobierno Digital del Estado de México tomando en cuenta las medidas para preservar la información de sus entidades, tanto en los equipos, dispositivos, sistemas informáticos y de comunicaciones, documentos o el personal que tenga acceso a ella de manera documental o en medio electrónico, con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad y confiabilidad de la información, y hacer frente a amenazas internas o externas, deliberadas o accidentales, mediante la aplicación de un proceso de gestión del riesgo.

1. Áreas de aplicación

Todas las dependencias, organismos auxiliares y organismos autónomos del Poder Ejecutivo, ayuntamientos, dependencias y entidades de la Administración Pública Municipal, Poder Legislativo, Poder Judicial y Notarios del Estado de México.

Es responsabilidad de los Titulares de las dependencias y entidades de la Administración Pública Municipal y Estatal, Poder Legislativo, Poder Judicial y Notarios del Estado de México, responsables de las áreas de TIC dentro de dichas instituciones, así como los empleados de las mismas que tengan a su cargo la planeación, contratación y administración de bienes y servicios relacionados con las TIC, el dar el debido cumplimiento al presente manual de seguridad de la información.

2. Referencias normativas

El estándar para la elaboración del manual del sistema de gestión de seguridad de la información está basado en la norma internacional ISO/IEC 27001:2013 que comprende la Gestión de la Seguridad de la Información.

El término “debe” se utiliza claramente en todos los lineamientos para identificar los controles de seguridad informática requeridos en todas las áreas donde sean utilizadas las TIC, de voz, e IP; en una referencia clara de que su cumplimiento es obligatorio.

En forma excepcional, el área laboral puede decidir no aplicar algún(os) control(es) bajo ciertas circunstancias, en ese caso siempre se estará obligado a justificar dicha excepción, en función a una previa evaluación de los riesgos asociados.

Las Dependencias u Organizaciones de manera conjunta con sus áreas tecnológicas, serán las responsables de la seguridad; los Directores Generales o equivalentes serán los encargados de revisar y mantener actualizadas las políticas y lineamientos utilizados al interior de las instituciones, así como publicarlas, difundirlas e implementarlas.

Todas las áreas directivas que responden por el uso de los equipos y de los sistemas de tecnologías de información, comparten esta responsabilidad por los recursos y operaciones bajo su control.

3. Términos y definiciones

- Acción Correctiva: Es la acción tomada para eliminar la causa de una No Conformidad detectada u otra situación potencialmente indeseable. Esta acción se toma para prevenir que algo vuelva a producirse.
- Acción Preventiva: Es la acción para eliminar la causa de una No Conformidad Potencial u otra situación potencialmente indeseable. Esta acción se toma para prevenir que algo suceda.
- Activos de TIC: Son los aplicativos de cómputo, bienes informáticos, soluciones tecnológicas, sus componentes, las bases de datos o archivos electrónicos y la información contenida en éstos.
- Administrador de Seguridad Informática: Es el personal técnico especializado en la seguridad de la información y el soporte de la operación.
- Alta Dirección: Cago o cargos con los niveles más altos dentro del área laboral.
- Aplicativo de Cómputo: Es el software y/o los sistemas informáticos, que se conforman por un conjunto de componentes o programas construidos con herramientas de software que habilitan una funcionalidad o automatizan un proceso, de acuerdo a requerimientos previamente definidos.
- Arquitectura Tecnológica: Es el conjunto de decisiones significativas sobre la organización del software, sus interfaces, su comportamiento y su interacción, así como la selección y composición de los elementos estructurales (infraestructura tecnológica). Es una definición del estilo, motivaciones o fundamentos que determinan por qué un sistema está diseñado de esa forma.
- Borrado Seguro: Es el proceso mediante el cual se elimina de manera permanente y de forma irrecuperable la información contenida en medios de almacenamiento digital; componentes de software reutilizables para la interoperabilidad de aplicativos de cómputo.
- Cortafuego: Sistema diseñado para prevenir el acceso no autorizado o desde una red privada.
- Cualificación: Es el conjunto de competencias profesionales con significación para el empleo que pueden ser adquiridas mediante formación modular u otros tipos de formación, y a través de la experiencia laboral. Una competencia profesional es el conjunto de conocimientos y capacidades que permitan el ejercicio de la actividad profesional, conforme a las exigencias de la producción y el empleo.

- Datos Abiertos: Datos digitales de carácter público accesibles en línea que pueden ser reutilizados y redistribuidos por cualquier interesado y que son accesibles, integrales, gratuitos, no discriminatorios, oportunos, permanentes, primarios, legibles por máquinas, en formatos abiertos y de libre uso, en términos de las disposiciones jurídicas de la materia.
- Dependencia u Organización: Son las unidades administrativas y/o áreas que conforman a los sujetos de la ley o usuarios y para quienes aplica el presente documento.
- Directorio Activo: Es un servicio establecido en uno o varios servidores en donde se crean objetos tales como usuarios, equipos o grupos, con el objetivo de administrar los inicios de sesión en los equipos conectados a la red, así como también la administración de políticas en toda la red.
- Documento electrónico: Soporte escrito con caracteres alfanuméricos, archivo de imagen, video, audio o cualquier otro formato tecnológicamente disponible, que contenga información en lenguaje natural o convencional, intercambiado por medios electrónicos, con el que sea posible dar constancia de un hecho y que esté signado con la firma electrónica avanzada y/o en el que se encuentre plasmado el sello electrónico.
- Encriptación: Proceso para volver ilegible cierta información considerada importante. La información una vez encriptada solo puede leerse aplicándole una clave.
- Expediente digital: Conjunto de documentos electrónicos que se utilicen en la gestión electrónica de trámites, servicios, procesos y procedimientos administrativos y jurisdiccionales.
- Gobierno Digital: Son las políticas, acciones, planeación, organización, aplicación y evaluación de las tecnologías de información para la gestión pública entre los sujetos de la presente Ley, con la finalidad de mejorar los trámites y servicios para facilitar el acceso de las personas a la información, así como hacer más eficiente la gestión gubernamental.
- ID: Identificación única de usuario.
- Identidad electrónica: Conjunto de datos con los cuales los sujetos de la presente Ley, se han identificado con carácter legal como únicos ante la Dirección al inscribirse en el Registro Único de Personas Acreditadas en el Estado de México.
- IDS: Sistema de detección de intrusos.
- Infraestructura de TIC: Es el hardware, software, redes e instalaciones requeridas para desarrollar, probar, proveer, monitorear, controlar y soportar los servicios de TIC.

- IP: Protocolo de Internet, estándar que se emplea para el envío y recepción de información mediante una red que reúne paquetes conmutados.
- IPS: Sistema de prevención de intrusos.
- LAN: Es una red que conecta los ordenadores en un área relativamente pequeña y predeterminada (como una habitación, un edificio, o un conjunto de edificios).
- Lineamientos técnicos: Son los criterios emitidos por el Consejo Estatal de Gobierno Digital orientados a proporcionar las reglas básicas que permitan, la interoperabilidad de las plataformas tecnológicas de los sujetos de la presente Ley, así como determinar los estándares abiertos que deban utilizarse.
- Medios electrónicos: Es la tecnología que permita transmitir o almacenar datos e información, a través de computadoras, líneas telefónicas, microondas o de cualquier otra naturaleza.
- Mensaje de datos: Es la información generada, enviada, recibida o archivada por medios electrónicos o cualquier otra tecnología.
- OLA: Es un contrato que define las relaciones técnicas internas que son necesarias en la empresa proveedora de un servicio para dar soporte a los SLA pactados entre esta y la empresa que recibe el servicio.
- Personas: Son las personas físicas o jurídicas colectivas que decidan utilizar los medios electrónicos antes las autoridades del Estado.
- Planes de Solventación: Documento que establece y describe las acciones tomadas para mitigar las fallas o riesgos detectados durante el uso de la información dentro de la organización, así como a los responsables de su ejecución.
- Programa: Aplicaciones y recursos que permiten desarrollar diferentes tareas en una computadora, teléfono u otros equipos tecnológicos, comúnmente llamado software.
- Proveedores: Empresa o personal contratado para la prestación de algún servicio en particular.
- Responsable del Plan de Solventación: Persona encargada de dar seguimiento y conclusión a una o varias de las acciones descritas hasta su solución.
- Seguridad de la información: Es la capacidad de preservar la confidencialidad, integridad y disponibilidad de la información, así como la autenticidad, confiabilidad, trazabilidad y no repudio de la misma.
- Sistema: Comprende redes de área local, computadoras personales, sistemas administrativos, centros de procesamiento locales de cómputo, de telecomunicaciones y conmutación, proveedores de servicios de Internet (ISP) y proveedores externos de servicios de información.

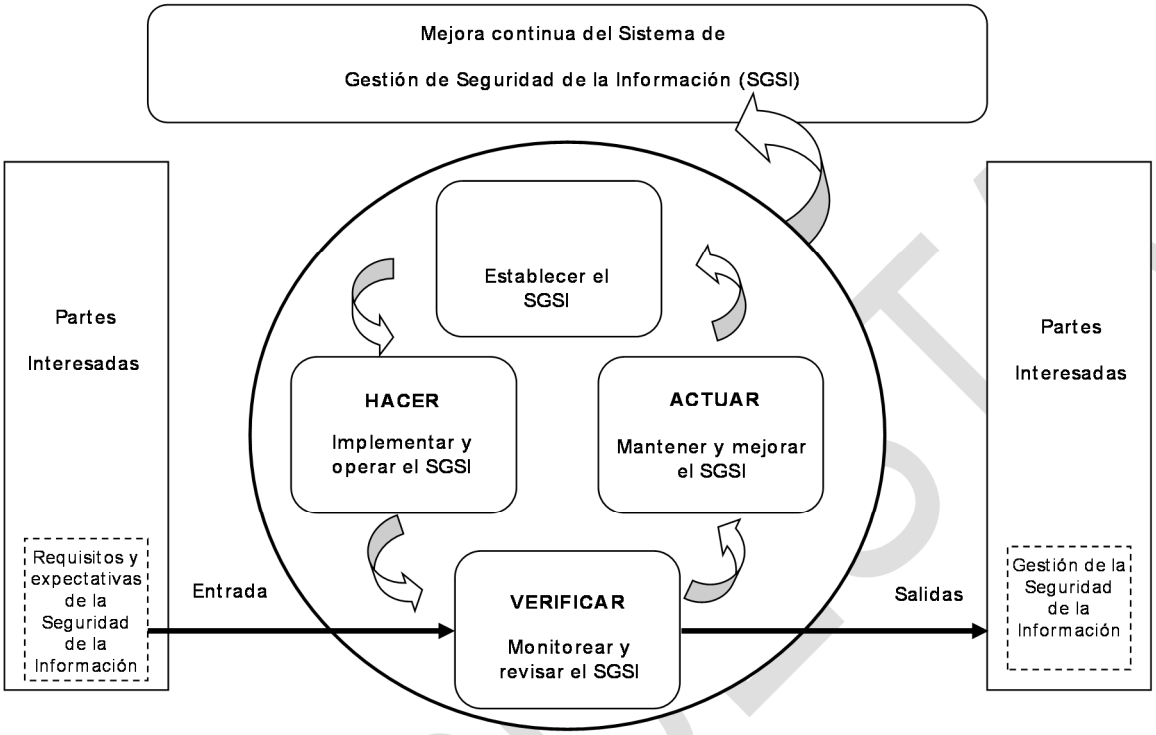
- SLA: Es un contrato escrito entre un proveedor de servicio y su cliente con objeto de fijar el nivel acordado para la calidad de dicho servicio.
- Sujetos de la ley: A los establecidos en la Ley de Gobierno Digital del Estado de México y Municipios.
- Tecnologías de Información: Es el conjunto de elementos y técnicas utilizadas en el tratamiento y transmisión de información vía electrónica, a través del uso de la informática, internet o las telecomunicaciones.
- TIC: Son todas las tecnologías de información y comunicaciones que comprenden el equipo de cómputo, software y dispositivos de impresión que sean utilizados para almacenar, procesar, convertir, proteger, transferir y recuperar información, datos, voz, imágenes y video.
- Usuarios: Es todo el personal dentro de las áreas laborales que tengan funciones administrativas o relacionadas con las TIC respecto de la implementación, ejecución, supervisión, o control de la seguridad de la información.
- Visitante: Toda persona ajena al área de trabajo ya sean usuarios externos, invitados, etc.
- WAN: Red de área amplia, una red de computadoras que abarca un área geográfica relativamente grande. Normalmente, un WAN consiste en dos o más redes de área local.

4 ESTRUCTURA DE LA NORMA

4.1 Conocimiento de la organización y de su contexto

La organización debe determinar el contexto en el cual estará ejerciendo control con el fin de poder dar cumplimiento a los objetivos trazados en materia de seguridad de la información y poder alcanzar los resultados esperados, identificando los servicios críticos dentro de su operación.

Será necesario seguir el siguiente modelo para aplicarlo en el contexto de seguridad de la información dentro de la Dependencia u Organización.



4.2 Comprensión de las necesidades y expectativas de las partes interesadas
Será necesario realizar un análisis de la organización, en el que se considere:

a) Identificación de activos dentro del alcance del SGSI

La Dependencia u Organización debe realizar un inventario de todos los activos para tener un control más riguroso de los mismos, poniendo énfasis en los activos de alta criticidad requeridos para la prestación de los servicios de mayor importancia. Toda la información y activos asociados a los recursos para el tratamiento de la información, deben tener un propietario y pertenecer a una parte designada de los mismos.

La Dependencia u Organización debe realizar un análisis y evaluación de riesgos de manera inicial partiendo del inventario de activos, a través del cual se pueda determinar cuál es la situación real y actual en la que se encuentra en materia de seguridad de la información. Para ello se define la metodología que se utilizará y también se debe realizar un análisis de las amenazas y vulnerabilidades de los activos de TIC asociados, que nos permiten:

- Identificar los riesgos
- Analizar y evaluar los riesgos encontrados
- Definir objetivos de control y controles para el tratamiento de riesgos

- Proponer soluciones para el tratamiento de riesgos

En el apartado de amenazas y vulnerabilidades, se debe:

- Realizar una lista de las amenazas que puedan presentarse en forma accidental o intencional con relación a los activos de información. Diferenciar estas amenazas de las vulnerabilidades de los activos ya que el análisis debe radicar en las amenazas.
- Identificar los riesgos internos de los procesos o procedimientos analizando tanto las actividades que se desarrollan como las amenazas identificadas.
- Identificar los riesgos externos en los procesos que requieran la subcontratación de un servicio, o si existe personal externo laborando dentro de la organización.
- Realizar un análisis del ambiente organizacional, el ambiente tecnológico y los aspectos socioculturales que rodea la Dependencia u Organización para definir las amenazas a las que pueden estar expuestos los activos.

b) Evaluación de seguridad de la información en relación a los recursos humanos

La Dependencia u Organización debe realizar una evaluación a los empleados, contratistas y usuarios de terceras partes, verificando que se entienden sus responsabilidades y están aptos para ejercer las funciones para las cuales fueron considerados, con el fin reducir el riesgo de hurto, fraude o uso inadecuado de la información y de las instalaciones.

4.3 Determinación del alcance del sistema de gestión de seguridad de la información

La Dependencia u Organización define y establece los límites que tendrá el Sistema de gestión de seguridad de la información, considerando los resultados de los puntos anteriores (4.1, 4.2), así como la interferencia y dependencia entre las actividades realizadas por la organización y las que correspondan a otras instituciones, verificando que todo se encuentre alineado con los objetivos de la organización en la seguridad de la información.

4.4 Sistema de gestión de seguridad de la información

La Dependencia u Organización debe identificar los asuntos internos y externos que pueden influir en los resultados esperados en relación con la seguridad de la información, de igual manera identifica a todas las partes interesadas, sus necesidades, y establece los requisitos para el adecuado funcionamiento.

5 LIDERAZGO

5.1 Liderazgo y compromiso

Es compromiso del Director General o equivalente de la Dependencia u Organización el apoyar activamente la cultura del Sistema de Gestión de Seguridad de la Información a través de una dirección clara, asignación explícita y reconocimiento de las responsabilidades según correspondan.

Del mismo modo proveerá todos los recursos necesarios para el adecuado funcionamiento del sistema, apoyará activamente la concientización al personal y mantendrá un compromiso constante para garantizar la seguridad de la información que se maneja en la organización.

El Director General o equivalente asegura el establecimiento y la eficacia del Sistema de Gestión de la Seguridad de la Información verificando que los procesos de comunicación son apropiados dentro de la Dependencia u Organización, que la comunicación es efectiva y es evaluada mediante la ejecución del procedimiento emitido para tal fin.

El Director General o equivalente revisa el Sistema de Gestión de Seguridad de la Información, para asegurarse de su conveniencia, adecuación y eficacia continua, mediante la ejecución y cumplimiento del procedimiento de revisión y evaluación. La revisión incluye la evaluación de las oportunidades de mejora y la necesidad de efectuar cambios en el Sistema de Gestión de Seguridad de la Información, incluyendo la política y objetivos y se establecen mecanismos para el control de los registros derivados de las revisiones realizadas por el Director General o equivalente.

La información requerida para la revisión por el Director General o equivalente incluye:

a) Evaluación de la Política y Objetivos de Seguridad de la Información
b) Resultados de revisiones y/o auditorías;
c) Retroalimentación del usuario;
d) Desempeño de los procesos enfocados a la Seguridad de la Información;
e) Estado de las Acciones Correctivas y Preventivas;
f) Acciones de seguimiento de revisiones anteriores realizadas por la Director General;
g) Gestión de Recursos y
h) Cambios que podrían afectar al Sistema de Gestión de Seguridad de la Información;

5.2 Política

El Director General o equivalente debe establecer la Política de Seguridad de la Información, considerando que ésta debe ser medible y alcanzable, alineada con los objetivos en materia de seguridad que pretende alcanzar la Dependencia u Organización y debe proporcionar un marco de trabajo que incluya los compromisos, requisitos relacionados a la seguridad y la aplicación de la mejora continua.

El Director General o equivalente debe asegurar que la Política de Seguridad de la Información está formalmente documentada, disponible; bien comunicada y difundida para toda la organización y las partes interesadas.

La Política de Seguridad de la Información será revisada de manera periódica por el Director General o equivalente, los directores de áreas y responsables de la seguridad de la información, para verificar su vigencia o, en su caso, realizar las modificaciones pertinentes.

5.3 Roles, responsabilidades y autoridades en la organización

El Director General o equivalente se debe asegurar de que las responsabilidades estén definidas y sean comunicadas dentro de la Dependencia u Organización, establece de manera genérica en base a la estructura organizacional una Matriz de responsabilidades asegurando que se tiene claramente definida la responsabilidad, rol y autoridad del personal, y que dicho personal tiene conocimiento de los procedimientos, instructivos o documentación generados dentro del Sistema de Gestión de Seguridad de la Información, es consiente y está comprometido con el mismo.

6 Planificación

Organización de la seguridad de la información

La Dependencia u Organización debe definir y establecer los objetivos de control y asegurarse que los usuarios de cada área los conocen, que se mantienen las medidas de seguridad adecuadas en su entorno, de tal manera que les permite asegurar que la información cumple con:

- Disponibilidad: Asegura que los usuarios autorizados tienen acceso cuando lo requieran en los tiempos adecuados.
- Integridad: Garantiza con exactitud que la información está completa, así como los métodos de su procesamiento.
- Confidencialidad: Asegura que la información es sólo accesible para aquellos que están autorizados.

6.1 Organización Interna

La Dependencia u Organización debe realizar un ejercicio que le permita evaluar sus necesidades de seguridad en la información y verificar el grado de cumplimiento con los objetivos esenciales de seguridad, mediante listados de verificación basados en los puntos de disponibilidad, integridad y confidencialidad.

Una vez realizado el ejercicio, los resultados mostrarán la situación real que se mantiene en la organización, identificando y definiendo cuáles son los controles que hay que implementar, el nivel de complejidad, los roles, responsabilidades y funciones que surjan, y en general todos los requerimientos que necesita cubrir la organización para alcanzar sus objetivos.

6.1.1 Roles y responsabilidades de la seguridad de información

Para lograr la protección de la información, se requiere contar con el compromiso de cada una de las áreas involucradas y de quienes administran y controlan la seguridad de la información a través de la función o rol de cada usuario, por ejemplo:

- Coordinador de Seguridad de la Información: Responsable de la institución, es quien coordina las actividades de implementación de la seguridad dentro de la Dependencia u Organización, organiza y da respuesta ante incidentes de seguridad, según lo informado por cada Responsable de área.
- Responsable de Seguridad de la Información: Asegura la información de la Dependencia u Organización colaborando con el Coordinador de Seguridad de la Información, controla que se cumplan los requerimientos de seguridad acorde a lo informado por los propietarios de la información, implementa y mantiene las medidas de seguridad definidas dentro de la organización.
- Propietario de la Información: Clasifica y establece el nivel de criticidad, confidencialidad y disposición final de su información, informa y otorga al Responsable de la Seguridad de la Información los permisos pertinentes según sea el caso.
- Administrador de Aplicativos: Aplicar las medidas de seguridad necesarias en los aplicativos, sistemas y software, acorde a la clasificación de la información establecida por el Propietario de la Información.

6.1.2 Segregación de funciones

La Dependencia u Organización y el Coordinador de Seguridad de Información deben garantizar que:

a. En los controles de acceso al sistema se llevan una rigurosa administración, y éstos están separados de otros deberes no compatibles.
b. La operación de sistemas automatizados de información, el soporte técnico y el desarrollo de los mismos incluyen la administración de accesos, y su utilización es sólo para fines laborales.
c. Se documentan todas las solicitudes para crear, cambiar o borrar los derechos de los usuarios de sistemas automatizados de información mediante la ejecución de procedimientos formales y se cuenta con la autorización de la administración de usuarios, los derechos son revisados y validados por periodos no mayores a 6 meses.
d. Que los procedimientos cumplen con los controles adicionales, sobre todo en los casos que representen un alto riesgo, tales como: el mantenimiento del equipo y/o las contraseñas creadas para usarse una sola vez, para la resolución de problemas del sistema automatizados de información en producción.
e. Que los datos de las identidades y contraseñas sean distribuidos a los usuarios de los sistemas automatizados de información, a través de medios seguros.
f. Que los derechos de acceso a sistemas automatizados de información sean revisados con regularidad y cancelados cuando el usuario ya no los requiera.

Los administradores deben asignar un responsable específico para la revisión y mantenimiento de contraseñas.

g. Que los procedimientos administrativos sean supervisados, para asegurar que los controles sean adecuados en relación con el riesgo, y sean operados de forma correcta y pertinente.

El Especialistas en seguridad debe de:

a. Desarrollar, revisar y actualizar las políticas y normas de seguridad conjuntamente con el Director General o equivalente.
b. Proporcionar una dirección funcional en el ámbito de seguridad informática de la Dependencia u Organización
c. Acordar las prioridades de seguridad informática de la Dependencia u Organización
d. Coordinar la implementación de las políticas y normas del Área de Seguridad Informática en la Dependencia u Organización
e. Monitorear e informar sobre el trabajo de seguridad informática a la Dirección General o área equivalente.
f. Dar capacitación al personal sobre seguridad dentro de las instalaciones de la organización.
g. Reportar al jefe inmediato superior las anomalías relacionadas con la seguridad.
h. Asegurar que todo el activo de TIC esté debidamente protegido y seguros.
i. Asegurar que se le dé la prioridad correspondiente al trabajo de seguridad informática, de manera oportuna.

6.1.3 Contacto con autoridades

El Responsable de la Seguridad debe realizar, revisar y actualizar anualmente, o cuando sea necesario, el listado de las autoridades competentes a contactar, el cual debe contener los datos de autoridades regulatorias, organismos de comunicación y denuncia de incidentes de seguridad, servicios públicos relacionados con seguridad física y emergencias y autoridades de supervisión en materia de seguridad.

La Dependencia u Organización debe mantener un procedimiento formal para establecer el contacto con los responsables de las instituciones y gestionar los asuntos relevantes en materia de seguridad, es decir, qué temas no debe perder de vista, y en todo caso, a quién y cómo se debe canalizar dicha información.

6.1.4 Contacto con grupos especiales de interés

El Responsable de la Seguridad debe mantener un listado de las asociaciones empresariales y profesionales, comisiones de trabajo sectoriales, foros de seguridad webs de publicación

de vulnerabilidades, entidades de certificación, fabricantes de HW y SW relevantes, proveedores de servicios o los que la organización considere pertinentes, registrando en el listado: nombre del responsable, teléfono, correo electrónico, especialidad en la que interviene en cuestión de seguridad (información técnica, legislación, emergencias, continuidad de negocio, etc.).

La Dependencia u Organización debe mantener un procedimiento formal para establecer el contacto con los responsables de las instituciones y gestionar los asuntos relevantes en materia de seguridad, es decir, qué temas no debe perder de vista, y en todo caso, a quién y cómo se debe canalizar dicha información.

6.1.5 Seguridad de la información en la gestión de proyectos

Durante todo el proceso de desarrollo, los responsables del mismo deben atender lo siguiente:

a. El software, la información y la documentación del desarrollo de los sistemas automatizados de información debe ser considerada confidencial.
b) Deben ejercerse la administración de cambios y los controles de acceso apropiados para la información y la documentación del proyecto.
c) Los registros de las revisiones formales del proyecto, deben conservarse por un periodo mínimo de 5 años y un año adicional de reserva, específicamente:

- La aprobación de los resultados de las pruebas al sistema, incluyendo las pruebas de seguridad, por la autoridad competente en la materia dentro de la Dependencia u Organización
- El Certificado de Implementación, que registre la aceptación de la autoridad competente en la materia, y la aceptación del área usuaria de que se ha cumplido con todos los requisitos operacionales.

d) Deben aplicarse procesos documentados de Administración de Configuración y Administración de Cambios durante la transición entre los proyectos de desarrollo y la puesta en marcha en producción.

Sin prejuicio de lo aquí establecido se debe cumplir con las determinaciones del área especializada relacionada a sistemas y la normatividad vigente en la materia.

6.2 Dispositivos móviles y trabajo remoto

La definición de trabajo remoto trae implícito el uso de las tecnologías de la información y las comunicaciones como herramientas esenciales para el logro de los objetivos. En este aspecto se debe considerar que al hablar de tecnología se está hablando de una combinación entre infraestructura, dispositivos, contenidos y aplicaciones, y en consecuencia de su uso y apropiación efectivos para alcanzar las metas organizacionales.

6.2.1 Política para dispositivos móviles

La Dependencia u Organización debe establecer los lineamientos y proveer las condiciones para el uso y manejo de los dispositivos móviles (teléfonos inteligentes y tabletas, entre otros) institucionales y personales de los que se haga uso de la institución, así como los servicios relacionados. Así mismo, debe vigilar que los usuarios o trabajadores hagan un uso responsable de los servicios y equipos proporcionados por la entidad, y en todo caso especificar documentalmente las responsabilidades de ambas partes, en el caso de uso de equipo personal para labores de trabajo.

Las condiciones de uso de los dispositivos deben quedar por escrito y ser del conocimiento de todos los empleados de la organización.

6.2.2 Trabajo remoto

La Dependencia u Organización en coordinación con el área tecnológica responsable de las comunicaciones, debe establecer las condiciones y requisitos para el establecimiento de conexiones remotas a la plataforma tecnológica; así mismo, suministrará las herramientas y controles necesarios para que dichas conexiones se realicen de manera segura estableciendo la política de uso, la cual debe ser difundida y conocida por los implicados.

Será necesario definir las normas adecuadas para el uso de conexiones remotas a la plataforma tecnológica considerando:

- Analizar y aprobar los métodos de conexión remota.
- Implantar los métodos, procedimientos y controles de seguridad para establecer conexiones remotas.
- Restringir las conexiones remotas a los recursos de la plataforma tecnológica; únicamente se deben permitir estos accesos a personal autorizado y por periodos de tiempo establecidos, de acuerdo con las labores desempeñadas.
- Verificar la efectividad de los controles aplicados sobre las conexiones remotas a los recursos de la plataforma tecnológica de manera permanente.
- Realizar auditorías y/o revisiones sobre los controles implantados.
- Contar con las aprobaciones requeridas por el control interno y la Unidad de TI, para establecer conexión con los dispositivos de la plataforma tecnológica y acatar las condiciones de uso establecidas.

7 SOPORTE

Seguridad ligada a los recursos humanos

7.1 Previo al empleo

La Dependencia u Organización debe asegurarse que los empleados y contratistas entienden sus responsabilidades, y que son aptos para los roles y tareas para los que están siendo contratados.

7.1.1 Selección

Los responsables de las unidades de TICs en coordinación con el área de Recursos Humanos de la Dependencia u Organización, deben definir los perfiles de cualificación y establecer claramente las funciones y responsabilidades relacionadas con la seguridad de la información dentro de la organización, adecuar los requisitos del puesto a ocupar y especificar las competencias que deben cubrir las personas que ocupen dicho puesto.

La selección de personal se realizará evaluando los perfiles e informando las obligaciones y responsabilidades del empleado, los términos y condiciones de contratación.

7.1.2 Términos y condiciones de la relación laboral

Los candidatos deben de estar de acuerdo con los términos y condiciones del empleo al firmar, y es obligación de la Dependencia u Organización informarles las políticas en materia de seguridad que están vigentes, capacitarlos e informarle sus responsabilidades en materia de seguridad de la información considerando los términos y las condiciones del empleo, por ejemplo:

- Los candidatos con acceso a la formación sensible, deben firmar acuerdos de confidencialidad y no divulgar la información de la Dependencia u Organización.
- Los candidatos están conscientes de que son responsables de la clasificación y administración de los activos de la Dependencia u Organización.
- Los candidatos son responsables del manejo de toda la información recibida.
- Los candidatos no pueden pactar acuerdos relacionados con la información fuera de la Dependencia u Organización, o fuera de las horas de trabajo y sin contar con la autorización formal de su inmediato superior.
- Los candidatos están conscientes de las acciones que se deben tomar frente al incumplimiento de las políticas de seguridad de la información.
- Los candidatos son conscientes que las responsabilidades adquiridas están contenidas dentro de los términos y condiciones del empleo y que siguen vigentes de manera permanente aun cuando deje de laborar en la Dependencia u Organización.

7.2 Durante el empleo

7.2.1 Responsabilidades de la dirección o equivalente

La Dirección General o equivalente debe vigilar el funcionamiento del Sistema de Gestión de Seguridad de la Información implementado en su Dependencia u Organización y verificar que las áreas técnicas que tienen bajo su responsabilidad la seguridad informática, presenten los resultados de las revisiones, que incluyan toda decisión y acción relacionada con la seguridad informática, la actualización de las Evaluaciones del Riesgos y el Plan de Riesgos, modificación de procedimientos y controles que afectan a la seguridad de la información, necesidades de recursos, mejora de la efectividad y medida de los controles que garantizan su buen desempeño, y vigilar que se cumplan los planes de capacitación en materia de seguridad.

La Delegación Administrativa o su equivalente, tiene bajo su responsabilidad la seguridad física debiendo implementar la custodia mediante personal de vigilancia, controles de acceso, disposición de áreas restringidas, contratación de personal adecuado, proveer los recursos necesarios, etc.

7.2.2 Concientización, educación y formación en seguridad de la información

El Responsable de la Seguridad de la Información debe contar con un plan de trabajo que proporcione a todos los servidores públicos que integran la organización y a los responsables de las TIC la concientización, educación y capacitación adecuada en función de las necesidades, para que estos a su vez lo transmitan hacia los usuarios responsables de los activos de información.

El personal de la Dependencia u Organización debe recibir capacitación periódica (1 vez al año) que lo concientice sobre problemas de seguridad de la información.

Deben existir estrategias de difusión que permitan afianzar la cultura de seguridad en el personal, por ejemplo:

- Correos electrónicos,
- Videos institucionales,
- Pláticas de seguridad de la información,
- Carteles o trípticos en materia de seguridad de la información,
- Otros.

7.2.3 Proceso disciplinario

La Dependencia u Organización debe establecer claramente las responsabilidades para implementar, operar y administrar los controles de seguridad informática en el entendido de que, en caso de una violación a las mismas, la persona que incurra en una falta, será acreedora a la sanción correspondiente.

7.3 Desvinculación y cambio de empleo

La desvinculación es el proceso mediante el cual se procede a finalizar el contrato de trabajo o relación laboral, independientemente de la causa, ya sea con una o más personas que cumplen alguna labor dentro de una organización; por ello la Dependencia u Organización debe verificar que se cumplan con todos los procedimientos establecidos ante la baja de un empleado, tales como eliminación de accesos, devolución de contraseñas, materiales de trabajo e información utilizada o generada durante el ejercicio del empleo, etc.

7.3.1 Responsabilidades en la desvinculación o cambio de empleo

En los casos relacionados con el cese del puesto de trabajo, todos los empleados, contratistas y externos deben devolver todos los activos (componentes software, documentos corporativos y equipos prestados) de la dependencia u Organización que tengan en posesión y estén relacionados con su empleo. Asimismo, se deberán revocar todos los privilegios al usuario cesado en todos los entornos de producción o accesibles desde el exterior de la organización.

En los casos relacionados con el cambio de puesto de trabajo dentro de la misma Dependencia u Organización, el Administrador del Sistemas deberá revocar todos los privilegios extendidos que el usuario tuviera en el puesto actual, respecto al nuevo puesto a desempeñar.

8 OPERACIÓN

Administración de Activos

Se deben identificar los activos de la Dependencia u Organización y definir las responsabilidades de protección pertinentes.

8.1 Administración de activos

La administración de activos de TI consiste en administrar el ciclo de vida de los elementos de TI (hardware y software). Esto incluye detectar los activos, mantener el control de asignaciones (personal responsable de su uso, rastrear el historial sus ubicaciones, disponibilidad de piezas e inventario. Incorporar las funciones de administración de activos de TI simplifica la tarea de administrar el inventario y también es importante para la preparación y planificación de adquisiciones de nuevos activos.

8.1.1 Inventario de activos

El propósito del inventario es recopilar información relevante que describa de manera plena los activos de tal forma que al realizar una consulta esta refleje la condición real del bien, de manera que permita la toma de decisiones pertinentes al caso.

Las premisas de un inventario físico son:

- El inventario de activos fijos no es una actividad menor.
- La logística del inventario debe estar basada en el profundo conocimiento de los procesos de trabajo y servicios prestados por de la organización.
- El levantamiento o inventario se hará describiendo los activos con todo detalle.
- La planeación y diseño de la estructura de la base original de datos del inventario será determinante en el resultado final.

Se debe de considerar el contar con la asesoría de personal especializado al momento de realizar un inventario sobre los elementos de TI, considerando sobre todo aquellos elementos implicados que guardan información sensible o forman parte de un servicio crítico para la Dependencia u Organización.

Las características físicas que describen a uno y otro activo son totalmente de naturaleza distinta. Por supuesto que la regla que dice que "todo activo deberá de describirse con marca, modelo, serie y capacidad", no está demás. Sin embargo, el énfasis debe estar en la especialización del personal que realizará la tarea del inventario para que dé por resultado una codificación inteligente de la información.

El inventario tendrá mejor calidad de información si lo realiza conforme al criterio de la Unidad Mínima Indivisible.

8.1.2 Propiedad de los activos

Generalmente, los activos de la organización se dividen en dos categorías: activos físicos o tangibles, incluidos los edificios, la maquinaria, los activos financieros y la infraestructura, y activos intangibles, que van desde el capital humano y los conocimientos técnicos hasta las ideas, las marcas, los dibujos y modelos, y otros frutos intangibles de la capacidad creadora e innovadora de la organización.

Un punto fundamental sobre la protección por medios legales de la propiedad intelectual es que convierte los activos tangibles e intangibles en derechos de propiedad exclusivos, si bien por un período de tiempo limitado. Gracias a esto, cualquier organización puede reivindicar la titularidad sobre sus activos intangibles y explotarlos al máximo. En resumen, la protección de la propiedad intelectual hace que los activos intangibles sean algo más tangibles, al convertirlos en activos valiosos y exclusivos que a menudo pueden ser objeto de comercio en el mercado.

Un modo fundamental de valerse de activos intangibles es mediante su protección por medios jurídicos y, en caso de que se satisfagan los criterios de protección de la propiedad intelectual, mediante la adquisición y mantenimiento de derechos de propiedad intelectual. Los derechos de propiedad intelectual pueden adquirirse en particular en relación con las categorías siguientes de activos intangibles:

- Productos y procedimientos innovadores (por medio de patentes y modelos de utilidad);
- Obras culturales, artísticas y literarias, entre las que también figuran, en la mayoría de los países, los programas informáticos y las bases de datos (por medio de la protección por derecho de autor y derechos conexos);
- Dibujos y modelos innovadores, incluidos los dibujos y modelos textiles (por medio de los derechos de dibujos o modelos industriales);
- Signos distintivos (principalmente, mediante la protección de marcas, incluidas las marcas colectivas y de certificación, pero también en algunos casos por medio de las indicaciones geográficas; véase más adelante);
- Microchips (por medio de la protección de esquemas de trazado o topografías de circuitos integrados);
- Denominaciones de productos de una calidad o reputación determinadas atribuibles a la procedencia geográfica (mediante la protección de las indicaciones geográficas); y
- Secretos comerciales (mediante la protección de información no divulgada de valor comercial).

8.1.3 Uso aceptable de los activos

Todos los usuarios que usen activos de información que sean propiedad de Organización, son responsables de cumplir y acoger con integridad los siguientes estándares de Política de Uso Aceptable para dar un uso racional y eficiente los recursos asignados:

Uso de los sistemas y equipos de cómputo.

La organización tiene regla de renuncia (disclaimer) que debe utilizarse al inicio de sesión en los equipos de cómputo y si no es posible el usuario debe de tener entender la siguiente leyenda: “Advertencia! Este sistema (hardware, software y periféricos), así como la información en él contenida es propiedad de la organización y su uso está restringido únicamente para propósitos de la misma, reservándose el derecho de monitorearlo en cualquier momento (según sea el caso). Cualquier utilización, modificación o acceso no autorizado a este sistema dará lugar a las acciones disciplinarias y/o legales que correspondan. El ingreso y utilización de este sistema implica su consentimiento con esta política.”

- Correo electrónico.

La Dependencia u Organización debe establecer los mecanismos adecuados para garantizar el uso correcto del correo electrónico y verificar que cumple con las medidas de seguridad necesarias que eviten la vulnerabilidad de la información, asegurar a través de unas políticas de uso que éste se da solo para fines laborales y la información es resguardada y protegida

por el usuario, en caso de detectar que se incurre en faltas, el responsable de la seguridad podrá denegar el acceso a los servicios de correo electrónico, inspeccionar, monitorear y/o cancelar un buzón de correo asignado.

- Navegación en Internet.

El uso de Internet debe estar destinado exclusivamente a la ejecución de las actividades de la organización y deben ser utilizados por el usuario para realizar las funciones establecidas para su cargo, por lo cual la organización definió los siguientes parámetros para su uso:

- El usuario debe abstenerse de descargar programas que realicen conexiones automáticas o visores de sitios clasificados como pornográficos y la utilización de los recursos para distribución o reproducción de este tipo de material, ya sea vía web o medios magnéticos.
- La descarga de música y videos no es una práctica permitida.
- Evitar el uso de servicios de descarga de archivos de cualquier tipo, salvo que se requieran con fines laborales y se cuente con la autorización correspondiente
- Las salas de video-conferencia de la organización deben ser de uso exclusivo para asuntos relacionados con la misma.
- Abstenerse de usar sitios que salten la seguridad del servidor de acceso a Internet y vulneren la seguridad.
- El uso con fines comerciales, políticos, particulares o cualquier otro que no sea el laboral y que dio origen a la habilitación del servicio, no está permitido.
- Evitar coleccionar, almacenar, difundir, transmitir, solicitar, inducir o incitar en cualquier forma actos ilegales, inmorales, engañosos y/o fraudulentos es una responsabilidad de los colaboradores de la organización; así como también amenazas, abusos, difamaciones, injurias, calumnias, escándalos, actos obscenos, pornográficos, profanos, racistas, discriminatorios, actos que invadan la privacidad de los demás u otro tipo de materias, informaciones, mensajes o comunicaciones de carácter ofensivo.
- Los usuarios no deberán coleccionar, almacenar, divulgar, transmitir o solicitar cualquier material, información, mensaje o comunicación que pueda infringir o violar cualquier patente, derechos de autor, marcas, secretos organizacionales o cualquier otro derecho intelectual de otra persona.
- Abstenerse de coleccionar, almacenar, divulgar, transmitir o solicitar cualquier material, información, mensaje o comunicación que viole la ley o de la cual puedan surgir responsabilidades u obligaciones de carácter criminal o civil bajo cualquier ley estatal, local, nacional o internacional.
- Coleccionar, almacenar, divulgar, transmitir o solicitar información personal (incluyendo sin limitación alguna, información biográfica, habitacional, social,

marital, ocupacional, financiera, y de salud) sobre otros usuarios, sin su consentimiento o conocimiento, son prácticas no permitidas por la organización.

- Los usuarios se deben abstener de coleccionar, divulgar, transmitir o solicitar programas de computación dañinos, virus, códigos, expedientes o programas.
- Hacer ofertas fraudulentas de compra o venta, así como también, conducir cualquier tipo de fraude financiero, tales como "cartas en cadena" o "las pirámides", son faltas se constituyen como violaciones a esta Política.
- Hacer o intentar hacer, cualquier cosa que afecte desfavorablemente la habilidad de utilizar el servicio de internet por otros usuarios, incluyendo sin limitación alguna, "negación de servicios", ataques contra otros sistemas o contra el anfitrión de redes u otros usuarios, se constituye como una violación a esta Política.
- Uso de herramientas que comprometen la seguridad.

Hacer o intentar hacer, sin permiso del responsable de la seguridad cualquiera de los siguientes actos:

- Acceder el sistema o red.
- Monitorear datos o tráfico.
- Sondear, copiar, probar firewalls o herramientas de hacking.
- Atentar contra la vulnerabilidad del sistema o redes.
- Violar las medidas de seguridad o las rutinas de autenticación del sistema o de la red.

• Recursos compartidos.

El uso de carpetas compartidas en los equipos de cómputo de los usuarios es una práctica que, aunque puede ser una herramienta útil de trabajo, tiene implícitos algunos riesgos que pueden afectar los principios de confidencialidad, integridad y disponibilidad de la información, por lo tanto, su uso y aplicación debe ser controlado. Con este propósito la organización define los siguientes lineamientos para su uso seguro:

- Se debe evitar el uso de carpetas compartidas en equipos de escritorio.
- Los administradores de la red establecen e implementan, en los casos aprobados, la configuración de acceso a la carpeta, previo requerimiento formal de la misma a través del área competente.
- El usuario que autoriza y dispone el recurso compartido es el responsable por las acciones y los accesos sobre la información contenida en dicha carpeta.
- Se debe definir el tipo de acceso y los roles estrictamente necesarios sobre la carpeta (lectura, escritura, modificación y borrado).

- Debe tenerse claramente especificado el límite de tiempo durante el cual estará publicada la información y compartido el recurso en el equipo.
- Si se trata de información confidencial o crítica para la organización, deben utilizarse las carpetas destinadas para tal fin en el servidor de archivos de usuarios, para que sean incluidos en las copias diarias de respaldo de información o implementar herramientas para el respaldo continuo de información sobre dichos equipos.
- El acceso a carpetas compartidas debe delimitarse a los usuarios que las necesitan y deben ser protegidas con contraseñas.

• Sitios Web para compartir documentos.

El dueño del sitio será el responsable de la seguridad del mismo y del acceso a la información que se encuentra alojada.

- El dueño del sitio será el responsable de otorgar los permisos requeridos.
- El dueño del sitio definirá un delegado que tengan control total sobre el sitio, a manera de contingencia, para la asignación de los permisos requeridos en su ausencia.

• Computación en nube.

Ninguna información de la Dependencia u Organización podrá utilizar tecnologías de computación en nube si no está previamente autorizado por el Responsable de la Seguridad.

- Uso equipos portátiles y dispositivos móviles.

Los usuarios se comprometen a hacer uso adecuado de los dispositivos móviles para el acceso a los servicios de movilidad proporcionados por la organización, tales como escritorios y aplicaciones virtuales, correo, comunicaciones unificadas, redes virtuales privadas (VPN), entre otros, atendiendo las siguientes directrices:

- El dispositivo móvil debe estar configurado para bloqueo automático por un tiempo de inactividad a través de medios disponibles de configuración tales como contraseña, patrón huella dactilar, reconocimiento de voz, entre otras.
- Uso de aplicación de antivirus.
- Uso de canales seguros y cifrados cuando se conecte a redes compartidas de acceso libre, no seguras.

- Acceso de equipos distintos a los asignados.
- Desactivar la opción de autoguardado de contraseñas en los diferentes navegadores web.

- No dejar claves en ningún sistema de almacenamiento de información web.
- Creación de contraseñas seguras, no incluir información personal como nombres, fechas de nacimiento, otros.

8.1.4 Devolución de activos

La unidad encargada de la asignación de los activos, en conjunto con el usuario son los encargados del proceso de terminación de funciones y verificación que todos los activos propios de la organización sean devueltos, los accesos físicos y lógicos sean eliminados, y la información pertinente sea transferida, según sea el caso.

8.2 Clasificación de la información

Los diferentes niveles de seguridad serán establecidos atendiendo a las características propias de la información, tal como lo establece la Ley de Protección de Datos del Estado de México en su Título sexto, Capítulo Primero, y por aquellos lineamientos o políticas que se establezcan dentro de las propias dependencias u organizaciones y por los dueños de la información.

8.2.1 Clasificación de la información

Se debería clasificar la información para indicar la necesidad, prioridades y nivel de protección previsto para su tratamiento.

La información tiene diversos grados de sensibilidad y criticidad. Algunos temas podrían requerir niveles de protección adicionales o de un tratamiento especial. Debería utilizarse un esquema de clasificación de la información para definir el conjunto adecuado de niveles de protección y comunicar la necesidad de medidas especiales para el tratamiento.

Distinguir los requisitos de seguridad básicos (globales) de los avanzados, de acuerdo con el riesgo.

La definición de la clasificación de los activos de información tiene que ser realizada por el responsable de dicho activo. La clasificación tiene que ser revisada cada cierto tiempo para controlar que se encuentra actualizado al nivel de seguridad oportuno.

Se debe tener en consideración el número de categorías de clasificación y los beneficios que se pueden obtener de su utilización. Hay que poner especial cuidado a la hora de interpretar las etiquetas de clasificación en los diferentes documentos de dicha organización, ya que pueden contar con diferentes definiciones para nombrar las etiquetas que son iguales.

8.2.2 Etiquetado de la información

Será necesario que el dueño de la información y el usuario responsable de su uso, de manera conjunta, determinen el nivel de valor y grado de criticidad de la información, con el fin de identificar los controles de seguridad que se requieran para salvaguardarla adecuadamente, así como establecer los controles y autorización de acceso a la misma.

- Los documentos con información del tipo "restringida" deberán ser controlados por medio de copias individuales perfectamente numeradas y registro de las personas que han tenido acceso.
- La copia o transferencia de información "restringida" por cualquier medio (electrónico, magnético, en papel) deberá estar autorizada y controlada.
- Todos los documentos del tipo "Altamente Restringida" se deberán conservar bajo llave y en lugares seguros.
- El envío de documentos con clasificación Confidencial (De Uso Interno, Restringida y Altamente Restringido), se deberá hacer por medio de canales seguros tales como mensajería privada, correo electrónico cifrado o entrega personal. En caso de hacerse por medio de forma física, los paquetes deberán estar debidamente cerrados y que sea imposible observar su contenido.
- Toda recepción de información confidencial deberá solicitar acuse de recibo.
- En caso de ser necesario, se considerará un procedimiento o centro de destrucción de documentos y activos de información que garantice la no reutilización de la información.
- La información Confidencial (De Uso Interno, Restringida y Altamente Restringido) deberá reflejar por medio de una leyenda, la clasificación a la que pertenece, sin importar la forma o medio en la que se encuentre para ello se debe tener en cuenta
- La organización, a través de sus instancias correspondientes, se reserva el derecho de iniciar denuncias, y procesos disciplinarios para sancionar a los funcionarios que divulguen o destruyan ilícitamente la información de la organización.

8.2.3 Manejo de activos

Se identificarán los activos de información de mayor importancia tales como servidores, aplicaciones, procedimientos operativos, etc., asociados a cada sistema de procesamiento de la información en su respectivo proceso, con sus responsables y su ubicación, para luego elaborar un inventario con dicha información.

El Inventario se deberá identificar, documentar y actualizar ante cualquier modificación de la información y los activos asociados con los medios de procesamiento. Este debe ser revisado con la periodicidad que cada área determine.

La responsabilidad de realizar y mantener actualizado el inventario de activos de información es de las áreas responsables de Tecnologías de la Información.

El uso de los activos de información pertenecientes a cada área de TI es responsabilidad del propietario asignado; y es su deber proteger y mantener la confidencialidad, integridad y disponibilidad de los activos de información y de la información contenida en ellos.

8.3 Manejo de los Medios

Dado que la información puede ser almacenada o distribuida por diferentes medios electrónicos o de TI, es de suma importancia que la Dependencia u Organización mantenga especial cuidado en su manejo y se establezcan políticas formales para su uso.

8.3.1 Gestión de los medios removibles

La gestión de los medios removibles comprende la administración y uso seguro de medios de almacenamiento de información, tales como:

Memorias tipo USB, Discos duros, CD-ROM, DVD y Cintas para realizar el respaldo, este procedimiento tiene como uno de sus principales fines evitar la divulgación, modificación, retiro o destrucción de información de manera no autorizada, y la interrupción en las actividades institucionales que puedan derivarse.

Para un adecuado uso de los medios removibles, se tendrán en cuenta los siguientes lineamientos:

- Todos los medios removibles que contengan información sensible o confidencial serán almacenados en un ambiente seguro y vigilado según las especificaciones del fabricante y los niveles de clasificación de la información.
- Todo el contenido de medios reutilizables que contengan información crítica o sensible de la Dependencia u Organización que se van a retirar de las instalaciones. se le deberá realizar un borrado seguro con el fin de evitar recuperación de información. Para el retiro de dichos medios se debe contar con un procedimiento formal y la autorización del responsable o dueño de la misma.
- La información crítica o sensible de la Organización cuya duración es mayor al tiempo de vida del medio en donde se encuentra almacenada, deberá respaldarse de manera segura para evitar la pérdida de información.
- El usuario debe asegurar el resguardo de la información contenida en el medio removible que le fue asignado.
- El funcionario debe dar buen uso a los medios removibles asignados, informando en forma oportuna cualquier deterioro.
- Se debe de garantizar la integridad y disponibilidad de la información almacenada en medios removibles, cambiando de contenedor cuando culmine el tiempo de vida, de éste.

- Es de exclusiva responsabilidad de cada usuario tomar las medidas adecuadas para el almacenamiento y resguardo de los medios removibles. Evitando accesos no autorizados, daños, pérdida de información o extravío del medio.
- En caso de ocurrir pérdida, modificación o daño de la información o del medio, se debe informar al Responsable de seguridad o quien tenga dicha función.

8.4 Eliminación de medios

La información contenida en medios de almacenamiento digital, muchas veces es altamente confidencial y su divulgación no puede ser permitida bajo ninguna circunstancia.

Bajo esta premisa, si se desea eliminar de forma segura la información confidencial, no se debe eliminar la información contenida en los medios de almacenamiento a través de los métodos convencionales, tales como: la eliminación de archivos y el formateo de las unidades. Basados en la experiencia en Informática Forense, se puede asegurar que, aplicando métodos convencionales para la eliminación de información, es posible recuperar la información eliminada, representando un riesgo critico que esta información de carácter confidencial sea recuperada y accedida por personas incorrectas.

Las actividades de eliminación segura de la información corresponden a:

- Desechar: Desechar el medio de almacenamiento, sin consideraciones de limpieza u otros. Esto se realiza normalmente en el reciclaje de papel que no contiene información confidencial, pero también se pueden incluir otros medios de almacenamiento
- Borrado: Es el método para borrar la información de los medios de almacenamiento mediante el uso de software o hardware, los cuales sobrescriben el espacio de almacenamiento con datos no sensibles. Este proceso puede incluir sobrescribir no solo la ubicación de almacenamiento lógico de un archivo(s), sino que también pueden incluir todas las ubicaciones direccionales. El objetivo de la seguridad del proceso de sobrescritura es remplazar los datos escritos con datos alterados
- Limpieza: consiste en la desmagnetización y ejecución del comando de borrado seguro.

8.5 Transferencia física de datos

Los medios deberían ser controlados y físicamente protegidos.

Se deberían establecer los procedimientos operativos adecuados para proteger los documentos, medios informáticos (discos, cintas, etc.), datos de entrada o salida y documentación del sistema contra la divulgación, modificación, retirada o destrucción de activos no autorizadas.

Asegure los soportes y la información en tránsito no solo físico sino electrónico (a través de las redes). Cifre todos los datos sensibles o valiosos antes de ser transportados.

Actividades de control del riego

Gestión de soportes extraíbles: Se deberían establecer procedimientos para la gestión de los medios informáticos removibles acordes con el esquema de clasificación adoptado por la organización.

Eliminación de soportes: Se deberían eliminar los medios de forma segura y sin riesgo cuando ya no sean requeridos, utilizando procedimientos formales.

Soportes físicos en tránsito: Se deberían proteger los medios que contienen información contra acceso no autorizado, mal uso o corrupción durante el transporte fuera de los límites físicos de la organización.

9 Control de acceso

La información es un recurso que, como el resto de los activos, tiene un valor importante para las Dependencias u Organizaciones por consiguiente debe ser debidamente protegida, garantizando la continuidad de los sistemas de información, minimizando los riesgos de daño y contribuyendo de esta manera a una mejor gestión.

9.1 Requisitos para el control de acceso:

El control de acceso determina las actividades permitidas a los usuarios legítimos, supervisando la actividad que realiza el usuario según sea el nivel de sensibilidad de la información que tenga el sistema en el que se encuentre. En algunos sistemas, el acceso se concede completo después de la autenticación exitosa del usuario, pero la mayoría de los sistemas requieren un control más sofisticado y complejo. Además del mecanismo de autenticación (por ejemplo, una contraseña), control de acceso se refiere a cómo se estructuran las autorizaciones. En algunos casos, la autorización podrá reflejar la estructura de la organización, mientras que en otros puede basarse en el nivel de sensibilidad de la información y el nivel de autorización del usuario para acceder a ella, o bien basado en roles que pueden cumplir las normas especificadas por el administrador.

La Dependencia u Organización debe limitar el acceso a información y a las instalaciones de procesamiento de información con los siguientes requisitos:

a. Impedir el acceso no autorizado a los sistemas de información, bases de datos y servicios de información.
b. Implementar seguridad en los accesos de usuarios por medio de técnicas de autenticación y autorización.

c. Controlar la seguridad en la conexión entre la red de la Dependencia u Organización y otras redes públicas o privadas.
d. Registrar y revisar eventos y actividades críticas llevadas a cabo por los usuarios en los sistemas.
e. Concientizar a los usuarios respecto de su responsabilidad frente al uso de contraseñas y equipos.
f. Garantizar la seguridad de la información cuando se utiliza un equipo de cómputo portátil y conexiones remotas.

Los procedimientos deben de contener todas las fases del ciclo de vida del acceso del usuario, desde el registro inicial de los usuarios nuevos, hasta la cancelación final del registro de usuarios que ya no requieren acceso a los servicios y sistemas de información. Se debe poner atención especial, según el caso, a la necesidad de controlar la asignación de derechos de acceso privilegiado que permiten a los usuarios anular los controles del sistema.

9.2 Política de control de acceso:

Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos de la unidad y de seguridad de la información.

Debe existir un procedimiento formal para el registro y cancelación de usuarios con el fin de conceder y revocar el acceso a todos los sistemas y servicios de información.

El procedimiento de control del acceso para el registro y cancelación de usuarios debe incluir:

a. Uso de ID para permitir que los usuarios queden vinculados y sean responsables de sus acciones.
b. El uso de identificadores (ID) de grupo únicamente se debe permitir cuando son necesarios por razones operativas o de la Dependencia u Organización, y deben estar aprobados y documentados.
c. Verificación de que el usuario tenga autorización del dueño del sistema para el uso del sistema o servicio de información, también pueden ser conveniente que la dirección o equivalente apruebe por separado los derechos de acceso.
d. Verificar que el nivel de acceso otorgado sea adecuado para los propósitos de la Dependencia u Organización y sea consistente con la política de seguridad, es decir, no pone en peligro la distribución de funciones.
e. Se dará a los usuarios una declaración escrita de sus derechos de acceso.
f. Los usuarios deberán firmar de conocimiento las declaraciones que indiquen que ellos entienden las condiciones del control de acceso.
g. Asegurar que los proveedores del servicio no otorguen el acceso hasta que se hallan terminado los procedimientos internos de autorización.

h. Retirar o bloquear inmediatamente los derechos de acceso de los usuarios que han cambiado de función, de trabajo o que han dejado la Dependencia o u Organización
i. Verificar, retirar o bloquear periódicamente las identificaciones (ID) y cuentas redundantes de usuarios.
j. Garantizar que las identificaciones (ID) de usuario redundantes no se otorgan a otros usuarios.

Se deberá considerar el establecimiento de roles de acceso de usuario basadas en los requisitos del Dependencia u Organización que incluyan un número de derechos en perfiles típicos de acceso de usuario. Las solicitudes y revisiones de acceso se gestionan más fácilmente en el ámbito de dichas funciones que en el ámbito de derechos particulares.

9.2.1 Accesos a las redes y a los servicios de la red:
Solo se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.

Los sistemas de usuario múltiple que requieren protección contra el acceso no autorizado deben controlar la asignación de privilegios a través de un procedimiento formal de autorización.

a. Se deben identificar los usuarios y sus privilegios de acceso asociados con cada producto del sistema, como sistema operativo, sistema de gestión de bases de datos y aplicaciones.
b. Se deben asignar los privilegios a los usuarios sobre los principios de necesidad de uso, de manera acorde con la política de control de acceso, es decir, el requisito mínimo para su función, sólo cuando sea necesario.
c. Promover el desarrollo y empleo de rutinas del sistema para evitar la necesidad de otorgar privilegios a los usuarios.
d. Promover el desarrollo y empleo de programas que eviten la necesidad de funcionar con privilegios.
e. Los privilegios se deben asignar a un identificador de usuario (ID) diferente a los utilizados para el uso normal de la Dependencia u Organización
f. El administrador de Seguridad Informática definirá controles para garantizar la seguridad de los datos y los servicios conectados en las redes de la Dependencia u Organización, para controlar el acceso no autorizado.
g. El acceso a Internet será utilizado con propósitos autorizados o con el destino por el cual fue provisto. El administrador de Seguridad Informática debe implementar los procedimientos necesarios para solicitar y aprobar accesos a Internet. Los accesos serán autorizados formalmente por el responsable del

área, que es quien tiene a su cargo al personal que lo solicite. Asimismo, se definirán las pautas de utilización de Internet para todos los usuarios.

h. Se incorporarán controles de ruteo, para asegurar que las conexiones informáticas y los flujos de información no violen la Política de Control de Accesos. Estos controles contemplarán mínimamente la verificación positiva de direcciones de origen y destino.
i. Se debe realizar una segmentación a las redes en función de los grupos de servicios, usuarios y sistemas de información.

Según el caso, se debe configurar un cortafuego que permita definir qué tipo de accesos desde y hacia el equipo o equipos que se autorizan o se deniegan, para proteger así su integridad, la información y preservar su correcto funcionamiento.

El uso no apropiado de los privilegios de administración del sistema (cualquier característica o servicio de un sistema que permita al usuario anular los controles del sistema o de la aplicación) puede ser un factor contribuyente importante a las fallas o vulnerabilidades del sistema.

9.3 Gestión de acceso del usuario:

Con el objetivo de impedir el acceso no autorizado a la información la Dependencia u Organización debe implementar procedimientos formales para controlar la asignación de derechos de acceso a los sistemas, datos y servicios de información.

9.3.1 Registro y cancelación del registro de usuarios.

Los Responsables de las áreas de TIC deben implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.

El proceso deberá incluir los siguientes requisitos:

a. Se debe solicitar a los usuarios la firma de una declaración para mantener confidenciales las contraseñas personales y conservar las contraseñas de grupo únicamente entre los miembros de éste.
b. Cuando se solicita a los usuarios mantener sus propias contraseñas, inicialmente se les otorgara una contraseña temporal segura, la cual están forzados a cambiar inmediatamente.
c. Las contraseñas temporales se deben suministrar de forma segura a los usuarios; se recomienda evitar mensajes de correo electrónico de terceras partes o sin protección.
d. Las contraseñas temporales deben ser únicas para un individuo y no ser descifrables.
e. Los usuarios deben confirmar la entrega de las contraseñas.

f. Las contraseñas nunca se deben almacenar en sistemas de equipo de cómputo en un formato no protegido.
g. Las contraseñas predeterminadas por el proveedor se deben cambiar inmediatamente después de la instalación de los sistemas o del software.

Las contraseñas son un medio común de verificación de la identidad de un usuario, antes de darle acceso a un sistema o servicio de información de acuerdo con la autorización del usuario.

Según el caso, se recomienda considerar otras tecnologías disponibles para la identificación y autenticación del usuario tales como biométricos, (verificación de huella digital, verificación de firma) y el uso de tokens de autenticación, (tarjetas inteligentes).

9.3.2 Asignación de acceso de usuario:
La Dependencia u Organización, a través del Coordinador de Seguridad de la Información debe definir e implementar un procedimiento formal de suministro de acceso formal de usuarios para asignar y revocar los derechos de acceso a todo tipo de sistemas base de datos y servicios de información multiusuario.

9.3.3 Gestión de derechos de acceso privilegiado:
El Responsables de la Seguridad debe restringir y controlar la asignación y uso de derechos de acceso privilegiado.

Se limitará y controlara la asignación y uso de privilegios debido a que el uso inadecuado de los privilegios del sistema resulta frecuentemente en el factor más importante que contribuye a la falla de los sistemas a los que se ha accedido ilegalmente. Los sistemas multiusuario que requieren protección contra accesos no autorizados, deben prever una asignación de privilegios controlada mediante un procedimiento de autorización formal.

9.3.4 Gestión de información secreta de autenticación de usuarios:
La asignación de la información secreta se debe controlar por medio de un procedimiento de gestión formal.

El Responsable de la Seguridad debe solicitar a los usuarios el cumplimiento de buenas prácticas de seguridad en la selección y el uso de las contraseñas.

Todos los usuarios deben:

a) Mantener la confidencialidad de las contraseñas.
b) Evitar conservar registros (por ejemplo, en papel, archivos de software o dispositivos manuales) de las contraseñas, a menos que éstas se puedan almacenar de forma segura y el método de almacenamiento esté aprobado.

c) Cambiar las contraseñas siempre que haya indicación de puesta en peligro del sistema o de la contraseña.
d) Seleccionar contraseñas de calidad con longitud mínima suficiente.
e) Cambiar las contraseñas a intervalos regulares o con base en el número de accesos (las contraseñas para cuentas privilegiadas se deberán cambiar con más frecuencia que las contraseñas normales) y evitar la reutilización de contraseñas antiguas.
f) Cambiar las contraseñas temporales en el primer registro de inicio.
g) No incluir contraseñas en ningún proceso de registro automatizado, por ejemplo, almacenadas en un macro o en una clave de función.
h) No compartir las contraseñas de usuario individuales.
i) No utilizar la misma contraseña con fines laborales, de la Dependencia u Organización, y para los que no lo son.

Si los usuarios necesitan acceso a múltiples servicios, sistemas o plataformas y se les solicita conservar múltiples contraseñas separadas, se les debe notificar que pueden usar una sola contraseña de calidad para todos los servicios cuando se les garantiza que se ha establecido un nivel razonable de protección para almacenar la contraseña en cada servicio, sistema o plataforma.

9.3.5 Revisión de los derechos de acceso de usuarios:

Coordinador de Seguridad de la Información de la Dependencia u Organización debe establecer un procedimiento formal de revisión periódica de los derechos de acceso de los usuarios.

a. El derecho de acceso de los usuarios se debe revisar a intervalos regulares, por ejemplo, cada seis meses y después de cada cambio, como por ejemplo promoción, cambio a un cargo en un nivel inferior, o terminación del contrato laboral.
b. Se debe verificar la asignación de privilegios a intervalos regulares para garantizar que no se obtienen privilegios no autorizados.
c. Los cambios en las cuentas privilegiadas se deben registrar para su revisión periódica.

Es necesario revisar con regularidad los derechos de acceso de los usuarios para mantener un control eficaz del acceso a los datos y a los servicios de información.

9.3.6 Retiro o ajuste de los derechos de acceso.

El Responsable de la Seguridad debe verificar que los derechos de acceso de todos los empleados y de usuarios externos a la información, y a las instalaciones de procesamiento de

información se retiren al terminar su empleo, contrato o acuerdo, o se ajusten los derechos cuando se hagan cambios.

9.4 Responsabilidades del usuario.

La Dependencia u Organización debe asegurarse que los usuarios sean responsables y cumplan con la salvaguarda de su información de autenticación.

Así mismo evitar el acceso de usuarios no autorizados, el robo o la puesta en peligro de la información y de los servicios de procesamiento de información.

La cooperación de los usuarios autorizados es esencial para la eficacia de la seguridad.

Se debe concientizar a los usuarios sobre sus responsabilidades por el mantenimiento de controles de acceso eficaces, en particular con relación al uso de contraseñas y a la seguridad del equipo del usuario.

9.4.1 Uso de la información de autenticación secreta.

El Responsable de la Seguridad debe vigilar que los usuarios cumplan los procedimientos establecidos en la organización para el uso de información de autenticación secreta.

a) Uso de Contraseñas: Los usuarios deben seguir buenas prácticas de seguridad en la selección y uso de contraseñas. Las contraseñas constituyen un medio de validación y autenticación de la identidad de un usuario, y consecuentemente un medio para establecer derechos de acceso a las instalaciones o servicios de procesamiento de información.
b) Los usuarios deben cumplir las directivas que se impartan a tal efecto.
c) Equipos a cargo de Usuarios: Los usuarios deberán informar cuando detecten que los equipos no se encuentren debidamente protegidos.
d) El administrador de Seguridad Informática debe coordinar con el Área de Recursos Humanos las tareas de concientización a todos los usuarios y contratistas, acerca de los requerimientos y procedimientos de seguridad, para la protección de equipos.
e) Implementar una política de escritorio y pantalla despejados para reducir el riesgo de acceso no autorizado o daño de reportes, medios y servicios de procesamiento de información.

9.5 Control de acceso a sistemas y aplicaciones:

Los especialistas de TIC deben restringir y controlar estrictamente el uso de programas utilitarios que pueden anular los controles del sistema y de la aplicación. También se deben utilizar restricciones en los tiempos de conexión para brindar seguridad adicional para las aplicaciones de alto riesgo.

9.5.1 Restricción de acceso a la Información.

El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso.

Las restricciones del acceso se deben basar en los requisitos de las aplicaciones individuales de la Dependencia u Organización. La política de control de acceso a la información y sistemas también debe ser congruente con la política de acceso físico en la organización.

a) Proporcionar menús para controlar el acceso a las funciones del sistema de aplicación.
b) Controlar los derechos de acceso de los usuarios, por ejemplo, leer, escribir, eliminar y ejecutar.
c) Controlar los derechos de acceso de otras aplicaciones.
d) Garantizar que los datos de salida de los sistemas de aplicación que manejan información sensible sólo contienen la información pertinente para el uso de la salida y que se envía únicamente a terminales o sitios autorizados; ello debe incluir revisiones periódicas de dichas salidas para garantizar el retiro de la información redundante.

Los sistemas sensibles deben tener un entorno informático dedicado (aislados), considerando que:

a. La sensibilidad de un sistema de aplicación se debe identificar y documentar explícitamente por parte del dueño de la aplicación.
b. Cuando una aplicación se ha de ejecutar en un entorno compartido, los sistemas de aplicación con los cuales compartirá recursos y los riesgos correspondientes deben ser identificados y aceptados por el dueño de la aplicación sensible.

Algunos sistemas de aplicación son lo suficientemente sensibles a la pérdida potencial que requieren manejo especial. La sensibilidad puede indicar que el sistema de aplicación debe:

a. Ejecutarse en un equipo de cómputo dedicado.
b. Únicamente debe compartir recursos con sistemas de aplicación confiables.

El aislamiento se puede lograr utilizando métodos físicos o lógicos

9.5.2 Procedimiento de inicio de sesión seguro.

La Dependencia u Organización deberá controlar mediante un proceso formal de ingreso seguro los controles de acceso, el acceso a sistemas y aplicaciones, y dar complimiento a la política de seguridad de la información.

El acceso a los sistemas operativos se debe controlara mediante un procedimiento de registro de inicio seguro.

El procedimiento de registro en un sistema operativo debe estar diseñado para minimizar la oportunidad de acceso no autorizado. Por lo tanto, el procedimiento de registro de inicio divulgara información mínima sobre el sistema para evitar suministrar asistencia innecesaria a un usuario no autorizado. Un buen procedimiento de registro de inicio debe cumplir los siguientes aspectos:

a. No mostrar identificadores de aplicación, ni de sistema hasta que el proceso de registro de inicio se haya completado exitosamente.
b. Mostrar una advertencia de notificación general indicando que sólo deben tener acceso al equipo de cómputo, los usuarios autorizados.
c. No suministrar mensajes de ayuda durante el procedimiento de registro de inicio, que ayuden a un usuario no autorizado.
d. Validar la información de registro de inicio únicamente al terminar todos los datos de entrada. Si se presenta una condición de error, el sistema no debe indicar qué parte de los datos es correcta o incorrecta.
e. Limitar la cantidad de intentos permitidos de registro de inicio, por ejemplo, tres intentos, y considerar:
    1. Registrar intentos exitosos y fallidos.
    2. Forzar un tiempo de dilación antes de permitir intentos adicionales del registro de inicio o de rechazar los intentos adicionales sin autorización específica.
    3. Desconectar las conexiones de enlaces de datos.
    4. Enviar un mensaje de alarma a la consola del sistema si se alcanza la cantidad máxima de intentos de registro de inicio.
    5. Establecer la cantidad de reintentos de contraseña junto con la longitud mínima de ella y el valor del sistema que se protege.
f. Limitar el tiempo máximo y mínimo permitido para el procedimiento de registro de inicio. Si se excede, el sistema debe finalizar esta operación.
g. Mostrar la siguiente información al terminar un registro de inicio exitoso:
    1. Fecha y hora del registro de inicio exitoso previo.
    2. Detalles intentos fallidos de registro de inicio desde el último registro exitoso.
h. No mostrar la contraseña que se introduce o considerar esconder los caracteres mediante símbolos.
i. No transmitir contraseñas en texto claro en la red.

9.5.3 Sistema de gestión de contraseñas.

Los especialistas de las áreas de TIC deben contar con sistemas de gestión de contraseñas, los cuales serán interactivos y deben asegurar la calidad de las contraseñas.

Los usuarios deben firmar las políticas de manejo adecuado de contraseñas, en las que se considera:

a. Asignación de contraseñas temporales y cambios de la misma al primer acceso.
b. Mantener confirmaciones de recepción de contraseñas por parte de los usuarios.
c. Las contraseñas default de los sistemas de información deben ser cambiadas.
d. Se deberá cumplir con el uso de identificadores de usuario (ID) individual y de contraseñas para conservar la responsabilidad.
e. Aplicar una elección de contraseñas de calidad por parte del usuario.
f. No mostrar contraseñas en la pantalla cuando se hace su ingreso.
g. No compartir sus contraseñas.

Las contraseñas son un mecanismo principal para validar una autoridad del usuario para tener acceso a un servicio del equipo de cómputo.

Algunas aplicaciones requieren la asignación de contraseñas de usuario por parte de una autoridad independiente, en tales casos. En la mayoría de los casos, las contraseñas son seleccionadas y conservadas por los usuarios.

9.5.4 Uso de programas utilitarios privilegiados.

Los especialistas de las áreas de TI deben restringir y controlar estrictamente el uso de programas utilitarios que pudieran tener capacidad de anular el sistema y los controles de las aplicaciones, considerando los siguientes puntos:

a. Uso de procedimientos de identificación, autenticación y autorización para las utilidades del sistema.
b. Separación de las utilidades del sistema del software de aplicaciones.
c. Limitación del uso de las utilidades del sistema a la cantidad mínima viable de usuarios de confianza autorizados.
d. Definición y documentación de los niveles de autorización para las utilidades del sistema.
e. Retiro o inhabilitación de todas las utilidades o el software del sistema basado en software innecesario.

La mayoría de las instalaciones de equipos de cómputo tienen uno o más programas de utilidades del sistema que pueden anular los controles del sistema y de la aplicación.

9.5.5 Control de acceso al código fuente de los programas:

Es responsabilidad de Dependencia u Organización, y de los diseñadores y desarrolladores de sistemas:

1. Mantener los códigos fuente de los programas y artículos asociados en un almacenamiento seguro centralizado y controlado.

2. Mantener el control de acceso y cambiar al código fuente del programa, se debe tener un procedimiento formal de recuperación a un estado anterior, que permita una vuelta a estados anteriores al código fuente.
3. Las modificaciones del código fuente del programa solo deben realizarse bajo aprobación y supervisión de los respectivos líderes de proyecto para el caso de nuevos desarrollos.
4. Es responsabilidad del líder de proyecto mantener el registro de las modificaciones y versiones de los códigos fuente del programa.

10 Criptografía

En la actualidad la información como recurso estratégico está convertida en el activo más importante tanto para las empresas como para el Gobierno del Estado de México, es por eso que el contar con los controles de seguridad criptográficos que garanticen la confidencialidad, autenticidad o integridad de la información con la ayuda de técnicas criptográficas.

Entendemos por criptografía a las técnicas que permiten cifrar mensajes o hacerlos ininteligibles, por medio de algoritmos que permitan garantizar la confidencialidad y la autenticidad de un mensaje.

10.1 Controles criptográficos

La Dependencia u Organización debe garantizar que los controles de cifrado sean diseñados, implementados, operados, administrados y mantenidos con sumo cuidado, para garantizar que el nivel de riesgo sea disminuido de manera efectiva y eficiente.

Para optimizar la eficiencia y capacidad de respuesta operacional de los sistemas, debe implementarse el cifrado de información utilizando métodos que sean independientes de la infraestructura, del sistema de comunicación y de las aplicaciones para garantizar la seguridad de la información.

10.1.1 Política sobre el uso de los controles criptográficos:

La Dependencia u Organización debe desarrollar e implementar una política sobre el uso de controles criptográficos que sea implementada, difundida y conocida por los responsables de la información y los responsables de la seguridad, para garantizar la protección de la información considerando los siguientes puntos:

a) Es necesario renovar las claves frecuentemente ya que una clave queda expuesta cada vez que se usa.
b) Se deben emplear claves diferentes para servicios diferentes (autenticación, transmisión, almacenamiento, etc.) con el fin de minimizar la exposición de las claves.

c) Deben asignarse claves diferentes a cada persona o grupo que acceden a una red, servidor o sistema, de tal manera que sólo las personas autorizadas tengan acceso a determinada información.
d) Las claves que por alguna razón se vuelven no seguras o aquellas que ya no son usadas deben ser eliminadas del sistema para evitar comprometer la información.

Las áreas tecnológicas y de seguridad deben considerar el uso de:

a) Códigos de validación de mensajes y controles de la integridad de los archivos para evitar una modificación no autorizada de la información,
b) Certificados digitales, en los casos en que la incapacidad de comprobar la recepción o el envío de información automatizada de, o hacia contrapartes específicas, expondría a la DGSEI a un riesgo inaceptable,
c) El cifrado de la información automatizada, ya que en el caso de una divulgación no autorizada de información expondría a la Dependencia u Organización a un riesgo inaceptable. Los ejemplos de información confidencial incluyen, sin ser exhaustivos:
    - Información sobre datos personales de los trabajadores u otros individuos que puedan ser identificados.
    - Información sobre controles de seguridad, tales como contraseñas de acceso a los sistemas automatizados de información.

El riesgo de que ocurra una divulgación no autorizada de información se incrementa si se transmite o procesa información confidencial en equipos que no estén bajo el control total de los responsables de la seguridad.

Se debe evitar, en lo posible, la utilización de medios de almacenamiento externos, redes no controladas y la transmisión de información a través de redes de dominio público.

10.1.2 Gestión de claves:

Si la Dependencia u Organización implementa esquemas de cifrado de información debe recurrir, siempre que sea posible, a una administración automatizada de la llave de cifrado, así como a métodos de distribución. Se debe garantizar que:

a) El proceso de cifrado es llevado a cabo en equipos seguros con dispositivos a prueba de modificaciones, de manera que no puedan hacerse visibles los valores de la llave. Debe evitarse hacer uso de procesos de cifrado de software y la clave de cifrado nunca debe estar visible en el código de la máquina,
b) Se almacena la llave en lugar seguro y será transportada con dispositivos de seguridad,
c) Cuando sea necesario recurrir a métodos manuales, las llaves de cifrado de información deben ser generadas, grabadas, almacenadas, manipuladas e ingresadas en los dispositivos de cifrado bajo control dual; de manera que en ningún momento

una sola persona posea las llaves completas, y que toda manipulación manual de los componentes de la llave sea documentada minuciosamente y en detalle,

d) Se cumple con los requisitos de seguridad informática sobre la extensión mínima de la llave de cifrado,
e) Los valores obsoletos de la llave son destruidos de inmediato utilizando métodos seguros,
f) Se implementa el cifrado utilizando los algoritmos y técnicas estándar en los servicios públicos ofrecidos que correspondan. Cuando no se especifiquen estos, la política es utilizar triple algoritmo de seguridad bajo la asesoría del área especializada,
g) Ninguna llave de cifrado puede ser usada para soportar más de un propósito de cifrado, y los valores de la llave deben ser cambiados periódicamente utilizando métodos seguros con la frecuencia que el riesgo amerite,
h) Todas y cada una de las inhabilitaciones temporales o permanentes de los controles de cifrado deben tener la autorización del responsable de la seguridad. Toda inhabilitación temporal debe hacerse bajo supervisión y sus controles deben ser restablecidos tan pronto como sea posible,
i) Se cuenta con los procedimientos para permitir un cambio de llaves en caso de emergencia,
j) Cualquier violación a estos controles se considera como un incidente de seguridad.

Ciclo de vida de las Claves:

- Almacenamiento: Ubicación que tendrán todas las claves de la red.
- Distribución: Es la manera en que el emisor envía la clave al receptor de un determinado mensaje para que pueda descifrarlo. Actualmente existen varias formas de hacerlo.
- Borrado: Eliminar las claves que por alguna razón se consideren ya no son seguras o que ya no estén en uso en el sistema, este proceso lo debe realizar el administrador de la red.
- Actualización: La actualización la puede realizar el propio usuario que por alguna razón decida hacerlo, o bien la puede realizar el administrador de la red que con base en las políticas deba actualizar las claves.
- Recuperación: Cuando un usuario se olvida de su contraseña y no existe alguna razón para desecharla, es posible volver a proporcionar la misma clave al usuario para que cumpla con su ciclo de vida, en la política de gestión de claves se debe contemplar este caso y establecer a detalle bajo qué condiciones una clave es recuperada.
- Protección: Es recomendable cifrar las claves antes de ser almacenadas para que en caso de una violación al acceso de dichas claves no represente un riesgo en la

confidencialidad en las mismas, en la política de gestión de claves se debe establecer el algoritmo para cifrarlas, así como las claves utilizadas.

- Aplicación: Se refiere a la utilidad que tendrá cada una de las claves generadas.

Tipos de Claves:

Clave Estructural: A cada nivel de privilegios en la red le es asignada una clave estructural evitando así la comunicación entre entidades con distintos privilegios. La clave estructural es implementada en hardware o en memoria ROM o similar.

Clave Maestra: Es generada aleatoriamente ya sea de forma manual o con un generador automático de claves, puede ser modificada por el usuario (el administrador de seguridad informática) y se usa para cifrar únicamente claves secundarias. Se almacena sin cifrar en un módulo de seguridad.

Un módulo de seguridad es un circuito integrado o bien una tarjeta chip en donde se almacena la clave maestra, el algoritmo de cifrado y descifrado y en ocasiones claves de rango menor a la maestra lo cual resulta poco aconsejable ya que resulta ser muy caro. Este módulo debe ser resguardado en un lugar seguro (físico) de la organización y sólo debe tener acceso a él personal encargado de la seguridad de la información.

Clave Primaria: Clave generada con la clave maestra que puede ser almacenada en una memoria no tan protegida como el módulo de seguridad, generalmente es utilizada para acceder a los sistemas o servicios.

Clave de Generación: Es una clave primaria utilizada para generar claves de sesión o claves de archivos con la finalidad de protegerlas en la transmisión y almacenamiento.

Clave de sesión o de mensaje: Clave creada con una clave de generación, utilizada para iniciar una sesión o bien para cifrar los datos intercambiados entre dos entidades durante su conexión, una vez terminada la sesión la clave se destruye.

Clave de cifrado de archivos: Clave cifrada con una clave de generación, su finalidad es cifrar archivos. Es utilizada únicamente en el cifrado de un archivo y después se destruye.

11 Seguridad física y del ambiente

11.1 Áreas seguras

Prevenir el acceso físico no autorizado, el daño o la interferencia a la información y a las instalaciones de procesamiento de información de la Dependencia u Organización es vital para la organización, por lo que se deben tener resguardados los lugares donde se encuentre localizada la información crítica para la organización, y estarán protegidas por un perímetro de seguridad y por los controles de acceso pertinentes.

11.1.1 Perímetro de seguridad física

La Dependencia u Organización debe definir y usar perímetros de seguridad y proteger las áreas que contengan información sensible o crítica, así como las instalaciones para el manejo de la información, por lo que la información más importante y el equipamiento que la contenga debe estar localizadas en zonas bien delimitadas, perfectamente identificadas y debidamente protegidas con un alto grado de control.

Se debe contar con un procedimiento formal que indique la forma de acceder a estas áreas y que contempla con las autorizaciones correspondientes, indicando las normas de estadía en el lugar, etc. dicho procedimiento se debe revisar y actualizar de manera periódica, y se debe implantar el cumplimiento obligado para todo el personal que acceda a las áreas restringidas.

La organización debe contemplar las sanciones correspondientes en caso de algún incumplimiento al procedimiento por parte de su personal o los visitantes.

11.1.2 Controles de acceso físico

La Dependencias u Organización debe implementar los procedimientos formales que regulen los controles de acceso a sus instalaciones, e impedir que personal no autorizado ingrese, tales como: sistema de vigilancia 24x7, alarmas, accesos biométricos, guardias de seguridad o aquellos que la organización determine.

Para la recepción de todos los visitantes y/o terceros en las instalaciones de la Dependencia u Organización se deben atender los procedimientos establecidos por la organización, dentro de los cuales se observan los siguientes puntos:

a) Concentrar a los visitantes en un área controlada al momento de su llegada,
b) Recibir fuera del perímetro de las áreas restringidas a los visitantes, en caso de requerir acceder a ellas, debe ubicarse una recepción previa que los reciba y registre, antes de que éstos tengan acceso a dichas instalaciones,
c) Confirmar la autorización de acceso y registrar en bitácora los datos de identificación de los visitantes, organización a la que representan, objeto de su visita, así como fechas, horarios de entrada y salida, conservando dichos registros por un periodo de tiempo determinado,
d) Proporcionar a los visitantes gafetes o distintivos, los cuales deben portar durante su visita, y brindarle las instrucciones básicas de seguridad,
e) Garantizar que los visitantes estén bajo observación y son supervisados durante su estancia por personal del área a visitar, en función de los riesgos,
f) Prohibir el acceso de los visitantes a las áreas restringidas, a menos que se cuente con la autorización correspondiente.

Es necesario mantener un control adecuado de los registros de toda persona que entre a la Dependencia u Organización fuera de horas y días laborables, en lo posible deberá existir un oficio interno o indicación oficial que justifique su estancia.

El ingreso de equipo o personal a las instalaciones debe estar autorizado y se debe garantizar que se han tomado las medidas necesarias establecidas en el apartado de seguridad lógica para asegurar y proteger la información de la organización.

El uso de equipo personal estará supeditado a lo establecido en el acuerdo de confidencialidad.

Cualquier incumplimiento en casos específicos debe ser notificado al área responsable del control.

11.1.3 Seguridad de oficinas, salas e instalaciones

La Dependencia u Organización debe definir el uso de salas, laboratorios, auditorios, almacenes, áreas administrativas, cuartos de máquinas y las instalaciones que la organización considere necesarias, para ello debe contar con un procedimiento documentado formalmente que indique como llevar el control particular sobre su uso, mantener registros de ingreso, nombrar un responsable de abrir y cerrar las puertas, vigilar que los visitantes guarden las políticas de acceso dentro de las instalaciones y, en caso contrario generar el reporte correspondiente. De ser necesario generar los Reglamentos de Uso de las áreas y mantenerlos visibles.

Dentro de las oficinas, empleados son responsables de sus equipos de trabajo (computadoras de escritorio, laptop, teléfonos, etc.) y de la información que tiene a su cargo, por lo que deben asegurarse que quedan a buen resguardo cuando ellos no se encuentren de manera física en su lugar de trabajo; lo cual les debe ser informado al ingresar a prestar sus servicios dentro de la organización, por lo que deben considerar:

a) Cumplir con las instrucciones y los procedimientos de seguridad aprobados, y aquellas responsabilidades de seguridad específicas documentadas,
b) Mantener la confidencialidad de las contraseñas personales y evitar que terceros utilicen los derechos de acceso de los usuarios autorizados,
c) Mantener la seguridad de los equipos de cómputo, así como de la información bajo su control directo,
d) Informarle al jefe inmediato superior cualquier sospecha de violaciones de la seguridad y de cualquier debilidad detectada en los controles de la misma, incluyendo sospechas de divulgación de contraseñas y/o información.

11.1.4 Protección contra amenazas externas y del ambiente

La Dependencia u Organización debe prever y mantener el control de los factores ambientales de origen interno y/o externo (en lo posible) para garantizar el correcto funcionamiento de los equipos de procesamiento y minimizar las interrupciones de servicio.

La información almacenada en los sistemas de procesamiento y la documentación contenida en diferentes medios de almacenamiento, son susceptibles de ser vulneradas mientras no están siendo utilizados. Es por ello que el transporte y la disposición final presentan riesgos que deben ser evaluados, especialmente en casos en los que el equipamiento perteneciente a la organización esté físicamente fuera del mismo (housing) o en equipamiento ajeno que albergue sistemas y/o preste servicios de procesamiento de información (hosting/cloud). De ser necesario se verificará, en el contrato de servicio con la empresa, una descripción del control de seguridad de la información utilizado.

En lo posible la Dependencia u Organización debe vigilar que las áreas con información crítica o sensible, como pudiera ser un Centro de Datos deben ser ubicadas y diseñadas de forma tal que se reduzcan los riesgos resultantes de desastres naturales, los inherentes a la zona circundante, y riesgos de otra naturaleza, de ser necesario solicitar el consejo de asesores en construcción, prevención de incendios y seguridad que correspondan, y cumplir con sus recomendaciones, incluyendo también los requerimientos legales y los códigos de prácticas correspondientes.

Dichas instalaciones deben emplazarse y construirse a fin de reducir todo tipo de riesgos:

a) El acceso directo público o el acercamiento directo de vehículos,
b) El riesgo de inundaciones y otros peligros inherentes a la zona circundante y el medio ambiente,
c) La cantidad de vías de acceso a las instalaciones, contando con áreas de entrega, carga y depósito controladas por separado,
d) Los riesgos potenciales en el suministro de energía eléctrica, agua y de servicios de telecomunicaciones.

- Protección contra incendio y explosión

Las medidas de prevención de incendios y explosiones deben incluir:

a) Medidas de prevención de incendios en los planos de las instalaciones tan pronto como comience la construcción de las mismas,
b) Implementación de las recomendaciones correspondientes hechas por los fabricantes de los equipos,
c) Además de los dispositivos manuales esenciales, la instalación de sistemas automáticos de detección y extinción de incendios deben ser supervisados las 24 horas del día, siempre que sea posible,

d) Probar con regularidad los sistemas de advertencia de incendios de acuerdo con la recomendación técnica especializada. Debe hacerse un registro de dichas pruebas,
e) La capacitación adecuada al personal adscrito en el uso de los equipos de extinción de incendios. Todo procedimiento relacionado debe ser documentado, evaluado, publicado y puesto en práctica;
f) La eliminación de material flamable, tales como papeles, artículos de papelería, desechos de los centros de cómputo o equipos de computación, o de otros lugares que representen un peligro potencial de incendio, a menos que se requiera para el trabajo programado.

- Protección contra daños provocados por el agua

Para proteger los equipos contra el agua, se deben utilizar sistemas de alarma, contar con techos y pisos impermeables y un sistema de drenaje adecuado.

- Control ambiental

La temperatura, la humedad y la ventilación dentro de las instalaciones que albergan equipos de computación y de comunicaciones y medios de almacenamiento de información, deben cumplir con las normas técnicas estipuladas por los fabricantes de los equipos. Cuando sea necesario, debe vigilarse la calidad ambiental y tomar las medidas correctivas pertinentes.

- Suministro de energía eléctrica

Los suministros de energía eléctrica deben cumplir con las normas técnicas estipuladas por los fabricantes de los equipos. Cuando sea necesario, debe vigilarse la calidad del suministro de energía eléctrica y tomar las medidas correctivas pertinentes.

Debe proporcionarse a los sistemas críticos una fuente alternativa de energía eléctrica adecuada, como son generadores de reserva, y si fuera necesaria una fuente ininterrumpida de energía eléctrica (UPS). Las fuentes alternativas de energía eléctrica deben probarse periódicamente para verificar su correcto funcionamiento en caso de requerirlas.

Las instalaciones deberán contar con todos los elementos necesarios para atender cualquier contingencia que asegure la integridad de los activos.

11.1.5 Trabajo en áreas seguras

La Dependencia u Organización debe asegurarse que todo el personal, equipamiento e información que se utiliza para la prestación de los servicios cuenta con todas las mayores medidas de seguridad posibles, ya que se han implementado todos los controles apropiados y la protección suministrada es acorde con los riesgos que se han identificado antes y durante la operación del SGSI.

La Dependencia u Organización mantiene las áreas de trabajo seguras, mediante la ejecución de procedimientos formalmente documentados de evaluación, e informes de inspecciones periódicas que se realizan en las instalaciones y en las cuales se consideran los accesos físicos y lógicos de la organización, y de manera regular se realiza la actualización del estado, implementando las medidas preventivas o correctivas necesarias que se han identificado durante las mismas.

11.1.6 Áreas de entrega y carga

La Dependencia u Organización debe mantener vigiladas las áreas de despacho, entrega o carga, así como otros puntos que se consideren vulnerables y a través de los cuales pueden acceder personas no autorizadas a la organización, estas áreas deben estar completamente alejadas de las instalaciones de procesamiento de información y será necesario nombrar a una persona responsable de su control y en lo posible utilizar las herramientas tecnológicas necesarias para su monitoreo.

11.2 Equipamiento

La Dependencia u Organización debe mantener un inventario actualizado de todos los equipos utilizados en la prestación de los servicios; en el caso de los equipos de cómputo se incluirán todos sus componentes identificando el estado en el que se encuentran, los licenciamientos que incluyen, así como sistema operativo, paquetería y antivirus; de igual manera se debe identificar al resguardatario o responsable del bien asignado.

El caso de que el usuario requiera sacar el equipo de las instalaciones, es su responsabilidad el tomar las medidas necesarias para prevenir un daño o robo del propio equipo, así como de la información que en él se transporta.

El inventario debe ser actualizado, al menos, cada 6 meses o en cuanto se realicen cambios en el equipamiento.

11.2.1 Ubicación y protección del equipamiento

La Dependencia u Organización debe mantener dentro del inventario, la ubicación física que se les ha asignado a los equipos, tanto los responsables de la instalación técnica, así como los responsables del equipo deberán vigilar las siguientes recomendaciones para su protección física:

- Instalar el equipo en un lugar limpio ventilado y seco.
- Limpieza periódica (interior y exterior) del equipo de cómputo y los periféricos.
- Utilizar aire comprimido o una aspiradora para la limpieza.
- No consumir alimentos y bebidas cerca del equipo, o en las salas de cómputo.
- Tener limpia el área de la PC.
- Cubrir el equipo cuando no se está utilizando.
- Mantener limpia toda la instalación.

- Verificar que los ventiladores del equipo estén libres de polvo.
- Procurar los lugares libres de polvo.
- Apagar el equipo de manera correcta.
- La corriente eléctrica debe ser confiable.
- Eliminar la estática de las manos cuando se va a dar mantenimiento físico correctivo o preventivo.
- Evitar movimientos bruscos o golpes en el equipo de cómputo.
- La temperatura del ambiente debe ser controlada adecuadamente.
- Prestar atención a los calentamientos y sonidos anormales en la fuente de poder, cables, etc.
- El equipo debe estar sobre un mueble fijo y seguro.
- Verificar todas las conexiones.

Protección lógica:

- Mantener el antivirus actualizado.
- Utilizar contraseñas y no proporcionarlas a nadie.
- No dejar discos dentro de las unidades de lectura.
- No mover el equipo mientras está encendido.
- Corregir o reportar cualquier falla del equipo.
- No utilizar programas sospechosos.
- Conocer correctamente las aplicaciones del equipo.
- Analizar los dispositivos externos en el programa antivirus antes de utilizarlos.
- Evitar las conexiones y bajar programas o aplicaciones de origen dudoso.
- No dejar guardadas las contraseñas en los diversos sistemas que sean utilizados.
- No almacenar las contraseñas en el equipo de cómputo.
- Analizar si conviene el cifrado de disco duro entero.
- Endurecimiento del sistema operativo.
- No proporcionar al usuario acceso mediante cuenta administrador para prevenir ejecuciones de configuración y aplicaciones no permitidas.
- Utilizar la regla del mínimo privilegio.

11.2.2 Elementos de soporte

La Dependencia u Organización debe hacer un análisis detallado de los equipos y dispositivos que se utilizan en la prestación de los servicios, y realizar una prueba inicial con todos como si fuesen a trabajar al mismo tiempo, así se podrá obtener la carga máxima que se pudiera llegar a utilizar dentro de la organización y detectar los riesgos que se asocian en el caso de una situación eventual para tomar las medidas pertinentes.

Se debe considerar que los equipos de cómputo, servidores y cualquier elemento de TI, forman parte de los equipos más sensibles a las variaciones de corriente eléctrica, por lo tanto, es necesario instalar equipos de protección que permitan una correcta protección contra cortes de luz y otras interrupciones provocadas por fallas en los suministros básicos de apoyo.

Se sugiere tener como mínimo los siguientes equipos y medidas de protección:

- Planta eléctrica.
- Sistema de flujo o suministro continúo (UPS).
- Aire Acondicionado
- Polo a tierra física
- Reguladores de voltaje
- Cableado

Referente a la iluminación:

- El sistema de iluminación debe ser apropiado para evitar reflejos en las pantallas, falta de luz en determinados puntos, y se evitará la incidencia directa del sol sobre los equipos.
- La iluminación no debe alimentarse de la misma fuente que la de los equipos de cómputo.
- Del 100% de la iluminación, deberá distribuirse el 25% para la iluminación de emergencia y se conectará al sistema de fuerza continúa.
- En el área de computadoras debe mantenerse un promedio mínimo de 450 lúmenes midiendo a unos 70 cm del suelo.
- Debe evitarse la luz directa para poder observar adecuadamente la pantalla.

En el caso de contar con contratos servicios para soportar la provisión de los mismos, es importante tener presentes los SLAs y OLAs que se hayan generado.

11.2.3 Seguridad en el cableado

El área responsable de TI debe considerar los estándares vigentes de cableado estructurado durante el diseño de nuevas áreas o en el crecimiento de áreas existentes.

De igual forma las unidades administrativas responsables deben asegurar que el cableado eléctrico, de telecomunicaciones, transmisor de datos o de soporte a servicios, esté protegido de daños e interceptación de información, y que es revisado periódicamente para asegurar su correcto funcionamiento, en este caso se debe considerar:

- Utilizar, en lo posible, un piso falso en donde será importante ubicar los cables de forma separada (de alto voltaje, de bajo voltaje, de telecomunicación y los de señales para dispositivos detección de fuego).
- Evitar conectar múltiples dispositivos en el mismo tomacorriente.

- Evitar sobrecargar el cableado con extensiones o equipos de alto consumo.
- Cambiar cables eléctricos que estén perforados o con roturas.

La organización debe tener claro que toda su información, incluyendo aquella que es confidencial, pasa a través de redes públicas o redes telemáticas, internas o externas y suele requerir de controles adicionales de protección en toda la infraestructura de soporte.

La gestión segura de las redes, la cual puede abarcar los límites organizacionales, requiere de la cuidadosa consideración del flujo de datos, implicaciones legales, monitoreo y protección.

Se deben controlar los accesos de usuarios a servicios internos y externos conectados en red y no deben comprometer la seguridad de los servicios si se garantizan:

a) que existen interfaces adecuadas entre la red de la organización y las redes públicas o privadas de otras organizaciones,
b) que los mecanismos de autenticación son adecuados se aplican a los usuarios y equipos,
c) se da cumplimiento al control de los accesos de los usuarios a los servicios de información.

La organización debe mantener el equilibrio entre controles de seguridad perimetrales (LAN/WAN) e internos (LAN/LAN), frente a controles de seguridad en aplicaciones (defensa en profundidad).

Preparar e implantar estándares, directrices y procedimientos de seguridad técnicos para redes y herramientas de seguridad de red como IDS/IPS (detección y prevención de intrusiones), gestión de vulnerabilidades, etc.

Actividades de control del riesgo: se deben administrar y controlar las redes para proteger la información en sistemas y aplicaciones.

Mecanismos de seguridad asociados a servicios en red: se deben identificar e incluir en los acuerdos de servicio (SLA) los mecanismos de seguridad, los niveles de servicio y los requisitos de administración de todos los servicios de red, independientemente de si estos servicios se entregan de manera interna o están externalizados.

Intercambio de información con partes externas.

Los intercambios de información por parte de las organizaciones se deben basar en una política formal de intercambio y en línea con los acuerdos de intercambio, y cumplir con cualquier legislación relevante, para abordar la transferencia segura de información comercial entre la organización y las partes externas.

Se deben establecer políticas, procedimientos y controles formales para proteger la información y los medios físicos que contienen información que viaja a través del uso de todo tipo de instalaciones de comunicación.

Se deben definir canales de comunicaciones alternativos y pre-autorizados, en especial direcciones de e-mail secundarias por si fallan las primarias o el servidor de correo, y comunicaciones offline por si caen las redes.

El verificar canales de comunicación alternativos reducirá el estrés en caso de un incidente real.

En el caso de uso de mensajería electrónica, el remitente debe tomar las medidas pertinentes para asegurar que la información se protege adecuadamente.

11.2.4 Mantenimiento del equipamiento

La Dependencia u Organización debe realizar inspecciones periódicas a los equipos incluyendo actividades como la revisión de rendimiento, capacidad, disponibilidad, integridad, eventos de seguridad y limpieza de los diversos componentes (aplicaciones, almacenamiento, CPU, memoria, red, etc.) de los bienes informáticos, considerados críticos, y mantener un Calendario de Mantenimiento Preventivo-Correctivo debidamente planificado, para garantizar que los equipos se mantienen de forma adecuada para garantizar la prestación de los servicios.

El Calendario de Mantenimiento Preventivo-Correctivo debe elaborarse anualmente y tener un responsable de su ejecución, o verificación y validación en caso de servicios contratados.

El Calendario de Mantenimiento Preventivo-Correctivo debe ser difundido y conocido por el personal de las áreas implicadas y los procesos de mantenimiento siempre deben ser realizados por personal de soporte técnico especializado y los registros se deben mantener por un periodo de tiempo determinado.

11.2.5 Retiro de activos

La Dependencia u Organización debe contar con un procedimiento documentado para el retiro de los equipos, la información o el software y éstos no pueden ser retirados del sitio sin una autorización previa, y para la cual se debe justificar de manera formal el motivo de la salida del bien informático, sea mediante oficio, nota informativa o correo electrónico en el que se especifique lo al menos lo siguiente:

- Número de serie y/o número de inventario del equipo, así como de sus periféricos.
- Motivo de la salida: si es reparación, reasignación, trabajo de campo, etc.
- Estado en el que se encuentra el quipo al salir (bueno, regular, dañado), en caso de contar con alguna avería, se deberá notificar al área responsable.
- Lugar al que se llevará el equipo.

- Responsable de la salida del equipo.
- Fecha de salida.
- Fecha de reingreso.
- Autorización del vigilante o encargado de la seguridad de los bienes.
- Autorización del responsable del área de TI o su equivalente.
- Autorización del Departamento Administrativo o su equivalente.

11.2.6 Seguridad del equipamiento y los activos fuera de las instalaciones

La persona que cuente con la autorización de salida de algún bien informático, es responsable del equipo durante el traslado y su uso fuera de la organización, por lo que deberá aplicar las medidas de seguridad necesarias, considerando los distintos riesgos que puede sufrir el bien, en donde se considere:

a) Proteger todos los equipos que contengan información de la organización y/o usuarios,
b) La seguridad física de ese equipo debe cumplir con las instrucciones de uso y manejo del mismo,
c) El equipo será utilizado sólo para los propósitos autorizados, para el personal designado,
d) Utilizar los controles de seguridad previstos con el equipo, en relación a los riesgos inherentes del bien y funciones del personal que lo tiene asignado,
e) Resguardar de manera segura las unidades de almacenamiento.

En caso de robo o extravió durante el periodo de tiempo que el bien se encuentre fuera de la organización, el resguardatario tendrá la obligación de informar a la Delegación Administrativa o su equivalente, el incidente, así como los realizar los trámites conducentes para su reporte y para la reposición del bien.

Transportación de la información

Las áreas o servidores públicos que por sus actividades requieren realizar la transportación de información, deben implementar los controles apropiados para proteger la información y evitar fallas de seguridad durante la transportación de cualquier unidad de almacenamiento. Estos controles deben incluir los requisitos para:

a) Proteger la integridad del contenido de la información,
b) Autenticar los puntos de origen y recepción,
c) Proteger la confidencialidad de la información en tránsito,
e) Verificar que el equipo cuente con licencias válidas para evitar riesgos,
f) Verificar que no se procese información confidencial en equipos privados no autorizados,

g) Realizar los respaldos adecuados de la información antes de sacarla de las instalaciones, con el objeto de protegerse contra una pérdida de información mientras esté fuera de las instalaciones,
h) Borrar toda la información de la organización del equipo privado incluyendo el vaciado de las papeleras de reciclaje y los archivos cache del navegador, tan pronto como se haya concluido con el trabajo,
i) Registrar los detalles pertinentes en una pista de auditoria.

Se deben modificar los paquetes que muestren su contenido para así proteger las unidades de almacenamiento físico de información; y para la entrega deben utilizarse métodos seguros y proteger la información con controles de cifrado de información con los que se cuente en la organización.

De igual manera, para proteger información confidencial debe considerarse el dividir el envío en varias partes. De ser necesario, debe llevarse a cabo una evaluación de riesgo para identificar y justificar los controles.

Los Responsables de la seguridad deben investigar todos los casos sobre aparentes violaciones de estos controles.

11.2.7 Seguridad en la reutilización o descarte de equipos

La Dependencia u Organización debe contar con un procedimiento formal para la devolución de los activos o equipos que el personal tenga asignado mientras labora en la organización, dichos equipos deben pasar por un proceso interno de asignación y/o rotación de equipos de cómputo, durante su periodo de vida útil. Se debe ejecutar el procedimiento previo de eliminación total de la información, con el fin de que el nuevo usuario del equipo no tenga acceso a información no autorizada, el jefe inmediato superior debe garantizar que cuando algún subalterno deje de laborar en la organización o sea transferido a otra área, la información electrónica de carácter laboral haya quedado previamente respaldada y bajo su resguardo, con el fin de evitar la pérdida o extracción de información.

La Dependencia u Organización debe evitar la fuga de información o la propagación de información sensible, por lo que la reasignación de los bienes informáticos dentro de organización deberá cumplir con las siguientes recomendaciones:

- Respaldar información solo en caso de ser necesario.
- El equipo se deberá ser formateado para eliminar la información del usuario anterior.
- Se debe entregar el equipo actualizado.
- El antivirus y la paquetería correspondiente deben estar activados en el equipo.
- Se debe crear el nuevo usuario y contraseña.
- Se deben actualizar los registros del inventario y el nuevo resguardatario.

Se deben verificar todos los equipos que contengan medios de almacenamiento para garantizar que cualquier tipo de datos sensibles y software con licencia se hayan extraído, o se haya reescrito de manera segura antes de su eliminación o reutilización.

La Dependencia u Organización debe contar con un procedimiento de restauración y resguardo de información para el uso aceptable de los activos de información.

La Dependencia u Organización debe contar con un procedimiento documentado para dar de baja los equipos informáticos que ya son inservibles, si procede solicitar la gestión de opinión técnica de baja mediante oficio justificando la baja, dando seguimiento al procedimiento establecido, y lo mismo aplica en el caso de donaciones de equipo.

11.2.8 Equipo de usuario desatendido

Es responsabilidad del usuario del equipo proteger toda la información que está bajo su responsabilidad, siempre que abandone su escritorio o que tenga que ausentarse de su lugar de trabajo por cualquier motivo, y asegurarse de activar el protector de pantalla con protección de contraseña de su computadora personal, tener un antivirus activado para la protección de la información.

Todos los equipos de cómputo deben contar con la última actualización proporcionada por el proveedor del sistema operativo, así como tener los licenciamientos de la paquetería y equipo de cómputo.

11.2.9 Política de escritorios y pantalla limpios

La Dependencia u Organización debe adoptar una política de escritorio y pantalla limpios para documentación en papel, medios de almacenamiento extraíbles y una política de monitores sin información para las instalaciones de procesamiento de información.

Puesto de trabajo despejado:

- El usuario debe mantener en orden su área de trabajo.
- Evitar dejar información sensible a disposición de personas no autorizadas.
- Guardar bajo llave documentación que a su criterio se importante, confidencial o secreta.
- Evitar dejar en lugares visibles y fácilmente accesibles pendrives, Cds , y otro tipo de almacenamiento de información.
- Si utiliza un computador portátil déjelo en un lugar seguro cuando usted esté ausente.
- No deje durante encima del escritorio documentos que contengan: Nombre de usuario y contraseña; Contratos con información a terceros; Números de Cuentas.
- Evitar el tener alimentos o bebidas.

Bloqueo de Pantalla

- El usuario debe bloquear la pantalla cuando se aleje de su escritorio.
- No dejar medios portátiles como CD y pendrives conectados.
- Apagar la computadora al alejarse por períodos prolongados de tiempo.
- Nunca escribir las contraseñas en notas autoadhesivas ni tratar de esconderlas en la oficina.
- Quitar impresiones antes de dejar el lugar.
- Triturar impresiones con datos sensibles una vez utilizados.
- Borrar archivos de memorias caché e impresoras.

12 Seguridad de las operaciones

12.1 Procedimientos operacionales y responsabilidades

La Dependencia u Organización debe garantizar que cuenta con las operaciones correctas y seguras de las instalaciones de procesamiento de información, mediante la implementación y ejecución de procedimientos de operación formales y apropiados, el establecimiento de responsabilidades y la segregación de tareas, para reducir el riesgo de un mal uso en los sistemas ya sea forma deliberada o por negligencia y vigilar su correcta ejecución.

12.1.1 Procedimientos de operación documentados

El control inadecuado de los cambios en los medios de procesamiento de la información y los sistemas de la organización es una causa común de fallas en el sistema o en la seguridad, por lo que la Dependencia u Organización debe implementar el uso de procedimientos relacionados con la administración y operación de dichos cambios en las plataformas tecnológicas o cualquier elemento de TI, así como identificar toda la documentación relacionada para su ejecución, registro, control y medición.

Las áreas técnicas deben generar los manuales de configuración y operación de los sistemas, firmware, servicios de red, bases de datos y sistemas de información o comunicación que conforman la plataforma tecnológica de la organización, mantenerlos en las áreas de trabajo y ponerlos a disposición de todo el personal que los requiera.

Dentro de ellos se pueden considerar los procedimientos para encender y apagar computadoras, copias de seguridad, mantenimiento del equipo, manejo de medios, salas de cómputo, manejo de correo electrónico y seguridad. Los procedimientos de operación deben especificar las instrucciones para la ejecución detallada de cada trabajo incluyendo:

a) Personal responsable de la ejecución.
b) Procesamiento y manejo de información.
c) Copia de seguridad o respaldo.

d) Requerimientos de programación de horarios, incluyendo las interdependencias con otros sistemas, los tiempos de culminación y horarios de los primeros y últimos trabajos.
e) Instrucciones para el manejo de errores u otras condiciones excepcionales, las cuales podrían surgir durante la ejecución del trabajo, incluyendo las restricciones sobre el uso de las utilidades del sistema.
f) Contactos de soporte en el caso de dificultades operacionales o técnicas inesperadas.
g) Instrucciones para el manejo de output especial y medios, tales como el uso de papelería especial o el manejo de output confidencial incluyendo los procedimientos para la eliminación segura del output de trabajo fallidos.
h) Procedimientos de reinicio y recuperación del sistema para su uso en el evento de una falla en el sistema.
i) Gestión de la información del rastro de auditoría y registros del sistema.

Los procedimientos de operación y los procedimientos documentados para las actividades del sistema deben ser tratados como documentos formales, revisados de manera periódica para asegurar su vigencia y en caso de requerir cambios, éstos deben ser autorizados por la Dirección o equivalente.

Donde sea técnicamente factible, los sistemas de información deben ser manejados consistentemente, utilizando los mismos procedimientos, herramientas y utilidades.

12.1.2 Gestión de cambios

La Dependencia u Organización debe controlar todos los cambios que se realicen en los sistemas de procesamiento de información, infraestructura, instalaciones, procesos de negocio y todos aquellos aspectos en los que se pueda ver afectada la seguridad de la información, para ello debe nombrar a un Responsable de la Administración de Cambios, quien se asegurará de dar cumplimiento al proceso, medirá y verificará el estatus que guarda la administración de cambios dentro del Sistema de Gestión de la Seguridad de la Información, y generará las mejoras necesarias dentro del mismo.

Los sistemas operacionales y el software de aplicación deben estar sujetos a un estricto control de administración de cambios mediante un proceso documentado formal, debidamente implementado dentro de la organización. En particular, se deben considerar los siguientes temas:

a) Identificación y registro de cambios significativos.
b) Planeación y prueba de cambios.
c) Evaluación de los impactos potenciales de los cambios, incluyendo los impactos de seguridad.
d) Aprobación y autorización formal para los cambios propuestos.

e) Comunicación del cambio para todas las personas involucradas.
f) Procedimientos de emergencia y respaldo.
g) Procedimientos y responsabilidades en caso de interrumpir el cambio.
h) Planes de retorno.
i) Eventos inesperados.

Es necesario establecer las responsabilidades en los procedimientos formales, para asegurar un control satisfactorio de que todos los cambios en los elementos de TI se realizan de manera ordenada y planificada y se mantienen los registros necesarios durante su ejecución.

En el caso de que la organización tenga la necesidad de genera un cambio de emergencia, se debe dar prioridad a la atención del mismo, sin embargo, el Responsable de la administración de cambios deberá verificar que es documentado de manera posterior.

Cuando se realizan los cambios, se debe mantener un registro de auditoría conteniendo toda la información relevante.

Los cambios, especialmente cuando se transfiere un sistema de la etapa de desarrollo a la etapa operacional, pueden influir en la confiabilidad de la aplicación. Los cambios en los sistemas de operación sólo se deben realizar cuando existe una razón válida para hacerlo, como un incremento en el riesgo para el sistema.

12.1.3 Gestión de capacidad

Las áreas de TI deben planificar y monitorear los requerimientos de capacidad en los componentes de la infraestructura, a fin de evitar fallas indebidas o una capacidad inadecuada de los sistemas automatizados de información y de comunicaciones, asegurando que siempre existan los niveles adecuados en la capacidad y ésta sea rentable, cubriendo las necesidades presentes y las futuras, para brindar un servicio oportuno.

Para tal efecto, se deben documentar y ejecutar las siguientes actividades:

a) Determinar los requisitos de Capacidad,
b) Generar el Plan de Capacidad,
c) Implementar el Plan de Capacidad,
d) Monitorear y reportar periódicamente la Capacidad de los componentes,
e) Reportar e investigar las excepciones.

La Dependencia u Organización debe designar a una persona responsable de llevar a cabo la administración de la capacidad, quien deberá monitorear constantemente el equipamiento utilizado en la prestación de los servicios, para asegurar que se cuenta con la capacidad necesaria actual o futura, y poder afinar el uso de los recursos. De manera periódica realizará una evaluación a los componentes y de ser necesario realizará las proyecciones necesarias de los requerimientos de capacidad para asegurar el buen desempeño en los servicios.

Para ello es necesario contemplar los siguientes lineamientos de implementación:

a) Identificar los requerimientos de capacidad de cada actividad o servicio nuevo y en proceso.
b) Aplicar la afinación y monitoreo del sistema para asegurar y, cuando sea necesario, mejorar la disponibilidad y eficiencia de los sistemas.
c) Establecer controles para mostrar los problemas en el momento debido.
d) Las proyecciones de requerimientos futuros deberán tomar en cuenta los requerimientos de los negocios y sistemas nuevos, y las tendencias actuales y proyectadas en las capacidades de procesamiento de la información de la organización.
e) Se debe prestar particular atención a cualquier recurso con tiempo de espera largos en el abastecimiento o costos altos; por lo tanto, los administradores deben monitorear la utilización de los recursos claves del sistema, con esto deberán identificar las tendencias de uso, particularmente en relación con las aplicaciones comerciales o las herramientas del sistema de información gerencial.
f) Los gerentes deben utilizar esta información para identificar y evitar cuellos de botella potenciales y depender del personal clave que podría presentar una amenaza a la seguridad o los servicios del sistema, y deben planear la acción apropiada.

12.1.4 Separación de los ambientes de desarrollo, pruebas y operación

La Dependencia u Organización deberá separar los ambientes de desarrollo, prueba y operación en los sistemas de información, para reducir los riesgos de acceso o cambios no autorizados en el ambiente de operación.

Al implementar los controles apropiados, se debe considerar:

a) Definir y documentar las reglas para la transferencia de software del estado de desarrollo al operacional.
b) El software de desarrollo y de operación deben correr en sistemas o procesadores de cómputo y en diferentes dominios o directorios.
c) Los compiladores, editores y otras herramientas de desarrollo o utilidades del sistema no deben tener acceso desde los sistemas operacionales, cuando no se requieran.
d) El ambiente del sistema de prueba debe simular el ambiente del sistema operacional con la mayor realidad posible.
e) Los usuarios deben utilizar perfiles diferentes para los sistemas operacionales y de prueba, y los menús deben mostrar los mensajes de identificación apropiados para reducir el riesgo de error.
f) La data confidencial no debe ser copiada en el ambiente del sistema de prueba.

El personal de desarrollo y prueba que tiene acceso a los sistemas operacionales y su información no pueden introducir códigos no-autorizados o no-probados, o alterar la data de operación y deberán mantener el manejo de ambientes separados en todo momento para evitar cualquier riesgo que ponga en peligro la información de la organización o sus servicios.

12.2 Controles contra códigos maliciosos

La Dependencia u Organización debe estar alerta, ya que todo el software y los medios de procesamiento de la información son vulnerables a la introducción de códigos maliciosos y se requiere tomar las precauciones necesarias para evitar y, de ser posible, detectar la introducción de códigos de programación maliciosos y códigos con capacidad de reproducción y distribución automática no autorizados para la protección de la integridad del software y de la información que sustentan.

El código malicioso es código informático que provoca infracciones de seguridad para dañar un sistema informático. El malware se refiere específicamente a software malicioso, pero el código malicioso incluye además scripts de sitios web (applets de Java, controles de ActiveX, contenido insertado, plug-ins, lenguajes de scripts u otros lenguajes de programación en páginas web y correo electrónico) que pueden aprovechar vulnerabilidades con el fin de descargar un malware.

El Responsable de la Seguridad y las áreas de TI deben estar conscientes de que el software y los recursos de tratamiento de información son vulnerables a la introducción de software malicioso como virus informáticos, gusanos de la red, troyanos y bombas lógicas, por lo que aplicaran las medidas necesarias para proteger la información de todas las posibles amenazas, realizarán monitoreo diario a los componentes de redes y servidores y periódicamente estarán evaluando los nuevos riesgos para tomar las acciones necesarias.

Es necesario para la Dependencia u Organización el contar con controles tecnológicos como es software antivirus, firewall, sistemas de detección de intrusos, etc., así como crear una cultura, educación, concienciación y formación dentro de la organización.

Los empleados son responsables de sus equipos y de la información que reciben, por lo que deben tener cuidado al abrir e-mails de remitentes desconocidos y no descargando ficheros de sitios no confiables y deben estar al tanto de los peligros, como son los códigos maliciosos como el robo y destrucción de la información o daños e inutilización de los sistemas de la organización.

12.2.1 Controles contra códigos maliciosos

Se deben implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.

El Responsable de la Seguridad y las áreas de TI deben contar con procedimientos formales para el manejo de los recursos de TI y de tratamiento de la información que es vulnerable a la introducción de software malicioso como virus informáticos, gusanos de la red, troyanos y bombas lógicas, por lo que aplicaran las medidas necesarias para proteger la información de todas las posibles amenazas, realizarán monitoreo diario a los componentes de redes y servidores y periódicamente estarán evaluando los nuevos riesgos para tomar las acciones necesarias.

Es necesario para la Dependencia u Organización el contar con controles tecnológicos como es software antivirus, firewall, sistemas de detección de intrusos, etc., así como crear una cultura, educación, concienciación y formación dentro de la organización.

Los empleados son responsables de sus equipos y de la información que reciben, por lo que deben tener cuidado al abrir e-mails de remitentes desconocidos y no descargando ficheros de sitios no confiables y deben estar al tanto de los peligros, como son los códigos maliciosos como el robo y destrucción de la información o daños e inutilización de los sistemas de la organización.

Como parte de los lineamientos de implementación, de debe considerar:

a) Establecer una política prohibiendo el uso de software no-autorizado.
b) Establecer una política para proteger contra riesgos asociados con la obtención de archivos, ya sea a través de redes externas o cualquier otro medio, indicando las medidas de protección a tomarse.
c) Realizar revisiones regulares del software y contenido de data de los sistemas que sostienen los procesos comerciales críticos; se debiera investigar formalmente la presencia de cualquier activo no-aprobado o enmiendas no-autorizadas.
d) La instalación y actualización regular de software para la detección o reparación de códigos maliciosos para revisar las computadoras y medios como un control preventivo o una medida rutinaria; los chequeos llevados a cabo deben incluir:
    - Análisis de cualquier archivo en medios electrónico u óptico, y los archivos recibidos a través de la red para detectar códigos maliciosos antes de utilizarlo.
    - Análisis de archivos adjuntos y descargas de los correos electrónicos para detectar códigos maliciosos antes de utilizarlos, este chequeo debiera llevarse a cabo en lugares diferentes; por ejemplo, servidores de correo electrónico, computadoras desktop y cuando se ingresa a la red de la organización.
e) Análisis las páginas Web para detectar códigos maliciosos.
f) Definición, gestión, procedimientos y responsabilidades para lidiar con la protección de códigos maliciosos en los sistemas, capacitación en su uso, reporte y recuperación de ataques de códigos maliciosos.

g) Preparar planes apropiados para la continuidad del negocio para recuperarse de ataques de códigos maliciosos, incluyendo toda la data y respaldo (back-up) de software y procesos de recuperación.
h) Implementar procedimiento para la recolección regular de información, como suscribirse a listas a analizar de correos y web sites que dan información sobre códigos maliciosos nuevos.
i) Implementar procedimientos para verificar la información relacionada con el código malicioso y para asegurar que los boletines de advertencia sean exactos e informativos, los directivos deberán asegurar que se utilicen fuentes calificadas; por ejemplo, periódicos acreditados, sitios de Internet confiables o proveedores que producen software para protegerse de códigos maliciosos; que diferencien entre bromas pesadas y códigos maliciosos reales; todos los usuarios deben estar al tanto del problema de las falsas alarmas y qué hacer cuando se reciben.

Es recomendable el uso de dos o más productos de software para protección de códigos maliciosos de diferentes proveedores, ya puede mejorar la efectividad de la protección contra códigos maliciosos.

Se puede instalar software para protección de código malicioso que contenga actualizaciones automáticas de archivos de definición y motores de lectura para asegurarse dicha protección.

Se debe tener cuidado del uso a proteger contra la introducción de códigos maliciosos durante el mantenimiento y procedimientos de emergencia, los cuales pueden evadir los controles de protección contra códigos maliciosos normales.

12.3 Respaldo

La Dependencia u Organización deben establecer procedimientos rutinarios para conseguir la estrategia aceptada de respaldo, realizar copias de seguridad y probar su puntual recuperación, para ello será necesario designar al Responsable de la generación de los respaldos, quien deberá realizar los respaldos de los sistemas y/o de la información crítica de la organización, manteniendo y ejecutando los procedimientos formales; para cumplir con ello deberá:

- Realizar una evaluación de riesgos para determinar cuáles son los activos de información más importantes o críticos y usar esta información para crear su estrategia de backup y recuperación.
- Decidir y establecer el tipo de almacenamiento, soporte a utilizar, aplicación de backup, frecuencia de copia y prueba de soportes.
- Establecer las técnicas de cifrado a copias de seguridad y archivos que contengan datos sensibles o valiosos.

- Contar con los procedimientos de recuperación que satisfagan no sólo requisitos contractuales, sino también requisitos de la organización.

12.3.1 Respaldo de la información

El responsable de la generación de respaldos debe hacer las copias de respaldo y realizar las pruebas necesarias de la información, del software e imágenes de los sistemas, de manera regular y de acuerdo con una política aprobada en dentro de la organización.

El responsable de la generación de los respaldos deberá documentar la información siguiente:

- Porcentaje de operaciones de backup exitosas.
- Porcentaje de recuperaciones de prueba exitosas.
- Tiempo medio transcurrido desde la recogida de los soportes de backup de su almacenamiento fuera de las instalaciones hasta la recuperación exitosa de los datos en todas ubicaciones principales.
- Porcentaje de backups y archivos con datos sensibles o valiosos que están cifrados.

El objetivo final de un backup es poder restaurarlo en caso de pérdida de los datos. Por lo tanto, es importante tener presente el contar con una herramienta adecuada. Para ello, es importante haber decidido previamente (en la gestión de riesgos) los siguientes puntos:

- RTO (Recovery Time Objective): Es el tiempo máximo en el que se debe alcanzar un nivel de servicio mínimo tras una caída del servicio (por ejemplo, debido a pérdida de datos) para no causar consecuencias inaceptables en el negocio.
- RPO (Recovery Point Objective): Es el periodo de tiempo máximo en el que se pueden perder datos de un servicio. Si el periodo de tiempo es de 6 horas, se deben realizar backups en un tiempo menor y poder recuperar la información antes de agotar el periodo.

El tiempo de restauración de un backup en caso de pérdida de datos forma parte del tiempo en que no hay servicio, entre menos tarde más rápido se restablecerá el proceso de negocio.

El responsable de la generación de los respaldos no puede eliminar ninguna información de los sistemas automatizados de información si no existe la autorización previa del Director o similar, y el dueño de la información.

El responsable de la generación de los respaldos es el encargado de asignar las cuentas de los usuarios, las contraseñas serán concedidas en el momento en que el usuario desee activar su cuenta, mediante una solicitud formal previa.

12.4 Registro y monitoreo

Para las organizaciones en necesario el mantener un registro de los eventos que suceden en todos los componentes de TI para poder tomar las acciones necesarias que les permitan entender las fallas y posteriormente mejorar sus servicios, y también en una forma de generar evidencia para presentarla ante una posible revisión.

12.4.1 Registro de eventos

La Dependencia u Organización debe elaborar, conservar y revisar regularmente los registros acerca de actividades de los usuarios, excepciones, fallas y eventos de seguridad en la información.

Las áreas de TI y el Responsable de la Seguridad deben establecer los procedimientos y responsabilidades en el manejo de los eventos y la detección de debilidades en la seguridad de información de una manera efectiva.

Las áreas de TI y el Responsable de la Seguridad deben aplicar el monitoreo necesario a los equipos y sistemas, evaluar, gestionar y atender en su totalidad los incidentes en la seguridad de información, manteniendo los registros de cada actividad.

Se debe elaborar un informe mensual de los eventos presentados en la seguridad de información y de los procedimientos de escalado.

Todo el personal de las áreas de TI y de Seguridad deberán estar al tanto de los procedimientos para informar los diferentes tipos de eventos y debilidades detectadas, que puedan tener impacto en la seguridad de los activos de la organización, e igualmente las áreas especializadas deberá solicitar que se informe cualquier evento o debilidad en la seguridad de información, lo más rápido posible y el punto de contacto designado.

En caso de contar con una mesa de ayuda de TI, se hará uso de ella para que el personal pueda informar los eventos y problemas de seguridad, si no es el caso, proporcionar un número telefónico y/o extensión.

Se debe tomar en consideración lo siguiente:

a) Asignar responsabilidades y procedimientos: Establecer las responsabilidades y procedimientos de gestión para garantizar una respuesta rápida, eficaz y ordenada a los eventos de seguridad de la información.
b) Notificación de los eventos de seguridad de la información: Los eventos de seguridad de la información se debe informar lo antes posible utilizando los canales de administración adecuados.
c) Notificación de puntos débiles de la seguridad: Requerir anotar e informar sobre cualquier debilidad sospechosa en la seguridad de la información en los sistemas o

servicios tanto a los empleados como a externos que utilizan los sistemas y servicios de información de la organización.

d) Valoración de eventos de seguridad de la información y toma de decisiones: Evaluar los eventos de seguridad de la información y decidir su clasificación como incidentes.
e) Respuesta a los incidentes de seguridad: Responder ante los incidentes de seguridad de la información en atención a los procedimientos documentados.
f) Aprendizaje de los incidentes de seguridad de la información: Utilizar el conocimiento obtenido del análisis y la resolución de incidentes de seguridad de la información para reducir la probabilidad y/o impacto de incidentes en el futuro.
g) Recopilación de evidencias: La organización debe definir y aplicar los procedimientos necesarios para la identificación, recopilación, adquisición y preservación de la información que puede servir de evidencia.

Las revisiones de los eventos y los casos de estudio identifican oportunidades de mejora y conforman por sí mismos un mecanismo eficaz de concienciación en seguridad, los registros de se generan en cualquiera de las etapas de la prestación de los servicios cobran una mayor importancia, porque en el caso de revisiones donde se requieran evidencias, éstas podrán ser recolectadas para asegurar el cumplimiento de los requisitos legales.

12.4.2 Protección de la información de registro

La Dependencia u Organización debe mantener todos los registros relacionados con los controles de seguridad que se tienen implementados en la organización, en áreas seguras y de ser necesario bajo resguardo, con la intención de que permanezcan protegidos, no se puedan extraviar o sean susceptibles de sufrir daños o modificaciones, ya sea de manera intencional o no.

El personal que labora en las diferentes áreas debe estar comprometido y concientizado de la importancia que tiene tanto la generación de los registros como su adecuada conservación, ya que son evidencia relevante en caso de alguna revisión técnica o legal.

12.4.3 Registros del administrador y del operador

La necesidad de implantar procesos de supervisión es más evidente ahora que la medición de la eficacia de los controles se ha convertido en un requisito específico.

Analizar la criticidad e importancia de los datos que se va a monitorizar y cómo esto afecta a los objetivos globales de la organización en relación a la seguridad de la información.

La organización deberá cumplir con todos los requerimientos legales aplicables para el monitoreo y el registro de actividades, y el monitoreo del sistema debe ser utilizado para verificar la efectividad de los controles adoptados y la conformidad del modelo de política de accesos, certificando que se mantiene de manera segura todos los registros generados ya sea de forma manual o automatizada.

El registro de los operadores y el registro de fallas deben ser usados para garantizar la identificación de los problemas del sistema de información.

Los especialistas en seguridad deben llevar el control documentado de la siguiente información:

a) Registro y gestión de eventos de actividad: Se deben producir, mantener y revisar periódicamente los registros relacionados con eventos de actividad del usuario, excepciones, fallas y eventos de seguridad de la información.
b) Protección de los registros de información: Se debe proteger contra posibles alteraciones y accesos no autorizados la información de los registros.
c) Registros de actividad del administrador y operador del sistema: Se deben registrar las actividades del administrador y del operador del sistema y los registros asociados se deben proteger y revisar de manera regular.

12.4.4 Sincronización de relojes

Control: Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deben sincronizar con una única fuente de referencia de tiempo.

La medida del tiempo es una cuestión muy importante en los sistemas de procesamiento de información, pero no se le da importancia debido a que no es ningún problema conseguir que todos los procesos tengan una misma referencia: el reloj compartido; en cambio en los sistemas distribuidos cada ordenador tiene su propio reloj.

Resulta normal tener que saber a qué hora del día han sucedido los distintos eventos que se producen en un ordenador. La precisión requerida en cada caso varía, siendo los sistemas de tiempo real los que posiblemente requieren una mayor precisión. No obstante, incluso en sistemas de propósito general se hace necesario el disponer de una sincronía horaria.

12.5 Control de software de operación

12.5.1 Instalación de software en sistemas operacionales

La Dependencia u Organización debe implementar los procedimientos necesarios para controlar la instalación de software en los sistemas operativos.

Los especialistas de TI deben minimizar los riesgos de alteración de los sistemas de información mediante controles de implementación de cambios, imponiendo el cumplimiento de procedimientos formales que garanticen que se cumple con la seguridad y control, y respetando la división de funciones.

Deben verificar que los cambios son gestionados por el personal autorizado, y atendiendo los términos y condiciones que surjan de la licencia de uso.

Deben efectuar un análisis de riesgos previo a los cambios, en atención al posible impacto por situaciones adversas.

Deben aplicar los cambios en sistemas de prueba y/o de manera escalonada, empezando por los sistemas menos críticos, además de aplicar medidas de backups y puntos de restauración junto a actividades adicionales que permitan retornar los sistemas al estado de estabilidad inicial con ciertas garantías.

Deben actualizar la documentación para cada cambio implementado, tanto de los manuales de usuario como de la documentación operativa.

Deben informar a las áreas usuarias antes de la implementación de un cambio que pueda afectar sus operaciones y envolver a usuarios finales en pruebas de aceptación del nuevo estado.

12.6 Gestión de las vulnerabilidades técnica

La Dependencia u Organización debe evitar la posible explotación de las vulnerabilidades técnicas que se presenten en la organización.

12.6.1 Gestión de las vulnerabilidades técnicas

Los especialistas en TI y el Responsable de la Seguridad deben obtener de manera previa y oportunamente toda la información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen y evaluar la exposición de la información de la organización ante estas vulnerabilidades, para ejecutar las acciones apropiadas y tratar el riesgo asociado.

Mediante el análisis realizado a los reportes de monitoreo de herramientas, reportes generados por el personal, o los resultados de la ejecución de otros procedimientos, de debe buscar o detectar las vulnerabilidades a que está expuesta la organización, y realizar las acciones conducentes para eliminar o al menos minimizar los riesgos a los que está expuesta la información en ese momento, con el fin de garantizar, que se cumple con la seguridad.

En el caso de los sistemas de información que requieran tratamiento ante vulnerabilidades, se deben aplicar los cambios en sistemas de prueba y/o de manera escalonada empezando por los sistemas menos críticos, además de aplicar medidas de backups y puntos de restauración, junto a actividades adicionales que permitan retornar los sistemas al estado de estabilidad inicial con ciertas garantías.

Se deberá informar a las áreas usuarias antes de la implementación de un cambio que pueda afectar sus operaciones y considerar a usuarios finales en pruebas de aceptación del nuevo estado.

Se deberá actualizar la documentación de cada cambio implementado, tanto de los manuales de usuario, como de la documentación operativa.

Los especialistas en TI y el Responsable de la Seguridad deben realizar pruebas y aplicar parches críticos o tomar otras medidas de protección, tan rápida y extensamente como sea posible, para evitar nuevas vulnerabilidades de seguridad que afecten a los sistemas y que éstos estén siendo explotados afuera de manera activa.

12.6.2 Restricciones sobre la instalación de software

Los especialistas en TI y el Responsable de la Seguridad deben establecer e implementar las reglas para la instalación de software por parte de los usuarios, y en lo posible designar a un responsable para esta actividad y mantener un procedimiento establecido.

Se debe mantener un registro sobre el número de instalaciones de software correctas e incorrectas, realizadas en los sistemas.

Mantener actualizados los registros y el estado de cumplimiento de las instalaciones del software que fueron planificadas aprobadas en los equipos de TI de la organización.

12.7 Controles de auditoría de sistemas de información

La Dependencia u Organización debe minimizar el impacto de las actividades de auditoría sobre los sistemas operacionales, al momento de realizarla.

12.7.1 Controles de auditoría de sistemas de información

Durante las auditorías a los sistemas de información deben existir controles para salvaguardar los sistemas operacionales y a las herramientas propias de la misma auditoría, maximizando la efectividad del proceso y minimizando las intromisiones en su funcionamiento.

Se debe acordar con el/las área/s que corresponda los requerimientos de auditoría, y limitar las verificaciones, por ejemplo: acceso de "sólo lectura" en software y datos de producción, y tomar las medidas necesarias a efectos de aislar y contrarrestar los efectos de modificaciones realizadas al finalizar la auditoría (eliminar archivos transitorios, entidades ficticias y datos incorporados en archivos maestros; revertir transacciones; revocar privilegios otorgados etc.).

De igual manera se deben identificar claramente los recursos TI para llevar a cabo las verificaciones y su disposición para con los auditores al momento de ejecutar la auditoría. Algos de estos recursos son: Sistemas de información, Bases de Datos, hardware, software de auditoría, dispositivos magnéticos, personal y conexiones a red.

En todo momento de deben documentar todos los procedimientos de auditoría, requerimientos y responsabilidades.

Al finalizar la revisión se deben observar las recomendaciones de auditoría, agrupadas y analizadas por su estado (cerradas, abiertas, nuevas, retrasadas) e importancia o nivel de riesgo (alto, medio o bajo).

Indicar el número y porcentaje de hallazgos de auditoría relativos a seguridad de la información que han sido resueltos y cerrados, respecto al total de abiertos en el mismo periodo.

Tiempo medio real de resolución/cierre de recomendaciones, respecto a los plazos acordados con la Dirección o equivalente al final de las auditorías.

13 Seguridad de las comunicaciones

La información es un recurso que, como el resto de los activos, tiene valor para las Direcciones y/o Unidades Informáticas del Gobierno del Estado de México por consiguiente debe ser debidamente protegida, garantizando la continuidad de los sistemas de información, minimizando los riesgos de daño y contribuyendo de esta manera a una mejor gestión de esta.

El control de acceso se refiere a la determinación de las actividades permitidas a los usuarios legítimos y autorizados, supervisando la actividad que realiza el usuario según sea el nivel de sensibilidad o criticidad de la información que tenga el sistema en el que se encuentre. En algunos sistemas, el acceso se concede completo después de la autenticación exitosa del usuario, pero la mayoría de los sistemas requieren un control más sofisticado y complejo. Además del mecanismo de autenticación (por ejemplo, una contraseña), control de acceso se refiere a cómo se estructuran las autorizaciones. En algunos casos, la autorización podrá reflejar la estructura de la organización, mientras que en otros puede basarse en el nivel de sensibilidad de diversos documentos y el nivel de autorización del usuario para acceder a esos documentos.

A medida que los sistemas crecen en tamaño y complejidad, el control de acceso es una preocupación especial para los sistemas que se distribuyen en varios equipos. De tal forma que los desarrolladores pueden utilizar una variedad de mecanismos de control de acceso que deben integrarse para apoyar la política de la organización; por ejemplo, el control de acceso basado en roles que pueden cumplir las normas especificadas por el administrador.

1. Sus propósitos principales son:

a) Configurar y administrar las redes informáticas para garantizar la disponibilidad de los servicios prestados.
b) Establecer los controles para el intercambio de información entre dependencias u organizaciones y con agentes externos, tales como proveedores de servicios.
c) Mediante la creación de un equipo de respuesta a incidentes informáticos se persigue minimizar las consecuencias de ataques a las instituciones públicas y las pérdidas del servicio o de información.
d) Crear el procedimiento técnico de respuesta a los incidentes informáticos.

e) Crear en cada Dependencia u Organización un Plan de Recuperación ante Desastres, el cual contribuirá a la pronta recuperación de los servicios prestados.
f) Crear un Plan de continuidad de Negocio, cuyo objetivo consiste en la puesta en marcha de todas las actividades de la institución en caso de desastre o de ataque a su infraestructura de telecomunicaciones, así como a su operación administrativa.

13.1 Gestión de la seguridad de la red

La Dependencia u Organización debe asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte, en todo momento.

La seguridad de las redes está basada en el establecimiento de recursos de seguridad en el perímetro externo de la red y a diferentes niveles. Esto permite definir niveles de confianza, permitiendo el acceso a determinados usuarios internos o externos, delimitando los servicios y denegando cualquier tipo de acceso a otros.

Los Responsables de la Seguridad de Redes deben implementar soluciones lógicas y físicas que garanticen la protección de la información de la Dependencia u Organización, de posibles ataques internos o externos, bajo las siguientes actividades:

- Rechazar conexiones a servicios comprometidos;
- Permitir sólo ciertos tipos de tráfico (correo electrónico, http, https);
- Proporcionar un único punto de interconexión con el exterior;
- Redirigir el tráfico entrante a la intranet hacia los sistemas indicados;
- Ocultar sistemas o servicios vulnerables que no son fáciles de proteger desde internet;
- Auditar el tráfico entre el exterior y el interior;
- Ocultar información: nombres de sistemas, topología de la red, tipos de dispositivos de red, cuentas de usuarios internos.

13.1.1 Controles de redes

Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones, por lo que:

a. La Área responsable de la seguridad deberá monitorear el rendimiento, evaluar métricas y recopilar datos para soportar las actividades de mejora y administración del servicio.
b. Se deberán tener sistemas de control efectivos tales como:

- Herramientas de monitoreo activo, ya que comprueban los elementos uno a uno para verificar su estado y disponibilidad.
- Herramientas de monitoreo pasivo, detectan y correlacionan alertas operacionales generadas por los propios elementos.

c. Procesos que se recomienda implementar para mantener el control de las redes:
   - Gestión de eventos: mediante la detección y gestión de sucesos que son significativos para la gestión de infraestructura de TI.
   - Gestión de incidentes: es coordinación de recursos (tecnológicos, humanos) para restaurar los servicios de TI a su operación normal lo más pronto posible minimizando el impacto a la operación del negocio.
   - Gestión de problemas: es el manejo del ciclo de vida de los problemas reduciendo el impacto sobre el negocio.
   - Gestión de requerimientos o peticiones: es la atención a los diferentes tipos de solicitudes que son hechas al área de TI por parte de los usuarios.
   - Gestión de accesos: otorga a los usuarios autorizados, el derecho de usar un servicio previniendo accesos no autorizados.

d. Para mantener el control, el área responsable de la seguridad deberá generar informes de:
   - Fallas.
   - Disponibilidad.
   - Tráfico por cada aplicación y protocolos usados.
   - Estado de red (actual e histórico).
   - Estado de los enlaces de respaldo.
   - Utilización de enlaces.
   - Utilización de memoria y procesos de componentes.

Con el fin de poder generar acciones preventivas en relación con la seguridad de la información y la mejor provisión del servicio.

e. El área responsable de la seguridad debe procurar que los informes sean automatizados en la medida de lo posible para hacer la gestión de redes más ágil.

13.1.2 Seguridad de los servicios de red

La Dependencia u Organización debe identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicios de red, ya sea que los servicios se presten internamente o se contraten externamente.

a) El área responsable de la seguridad, especialmente la de telecomunicaciones, será la encargada de generar y cumplir el SLA, los OLA, así como los objetivos de los contratos tanto con los proveedores como con los usuarios.
b) Identificar los diferentes tipos de mecanismos de seguridad, y en caso de no tenerlos implementaros:
   - Mecanismos preventivos. Aquellos cuya finalidad consiste en prevenir la ocurrencia de un ataque informático. Básicamente se concentran en el monitoreo de la

información y de los bienes, a través del registro de las actividades que se realizan en la organización y el control de todos los activos y de quienes acceden a ellos.

- Mecanismos detectores. Tienen como objetivo detectar todo aquello que pueda ser una amenaza para los bienes. Ejemplos de éstos son las personas y equipos de monitoreo que pueden detectar cualquier intruso u anomalía en la organización.
- Mecanismos correctivos. Se encargan de reparar los errores cometidos o daños causados una vez que se ha cometido un ataque; o, en otras palabras, modifican el estado del sistema de modo que vuelva a su estado original y adecuado.
- Mecanismos disuasivos. Se encargan de desalentar a los perpetradores de que cometan su ataque para minimizar los daños que pudieran presentarse.

13.1.3 Separación de las redes

Los Responsables de la seguridad deben realizar un análisis de usuarios y sistemas de información, y separar o segmentar las redes.

a) Todo el personal nuevo de la Institución, deberá ser notificado al responsable de la seguridad para asignarle los derechos correspondientes (Equipo de Cómputo, Creación de Usuario para la Red (Perfil de usuario en el Directorio Activo). En caso de retiro, salida o baja del funcionario, se deben anular y cancelar todos los derechos que le fueron otorgados como usuario.
b) Todos los usuarios de servicios de información, son responsables del acceso y contraseña que se les otorga.
c) Implementar controles en múltiples capas dentro de la arquitectura de red.
d) Aplicar la regla de menos privilegiado.
e) Acceso a la información por segmentos sobre la base de sus requisitos de seguridad.

13.2 Transferencia de información

Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa, por lo que la información institucional proporcionada por un usuario, no puede ser divulgada a terceros o fuera del ámbito laboral, sin la autorización correspondiente del propietario de la información y mediante solicitud formal.

13.2.1 Políticas y procedimientos de transferencia de información

La Dependencia u Organización debe contar con políticas, procedimientos y controles de transferencia de información formales para proteger toda la información al momento de su uso, en cualquier tipo de instalaciones o medio de comunicación.

a) El área responsable de la seguridad debe delimitar el acceso de los usuarios a las redes y servicios en red, para no comprometer la seguridad de los servicios, por ello debe garantizar:

- Que existen interfaces adecuadas entre la red de la Dependencia u Organización y las redes públicas o privadas de otras organizaciones.
- Que los mecanismos de autenticación son adecuados y se aplican a los usuarios y equipos.
- Se da total cumplimiento de los controles de acceso, a los usuarios y a los servicios de información.

b) El área encargada de seguridad debe mantener el equilibrio entre controles de seguridad perimetrales (LAN/WAN) e internos (LAN/LAN), frente a controles de seguridad en aplicaciones (defensa en profundidad).

c) Preparar e implantar estándares, directrices y procedimientos de seguridad técnicos para redes y herramientas de seguridad de red como IDS/IPS (detección y prevención de intrusiones), gestión de vulnerabilidades, etc.

13.2.2 Acuerdos sobre transferencia de información

En caso de que se requiera la transferencia de la información, ésta debe realizarse bajo estrictos controles de seguridad previamente acordados, en los que se garantice la transferencia segura de información entre la organización y las partes externas, se debe prever que toda solicitud de procesamiento de información debe realizarse a través de una solicitud formal, siendo el usuario responsable de la validación de la información y debe mantener el respaldo de la misma, de igual manera se tomara en cuenta que:

a) El área responsable de la seguridad debe proteger la información mediante canales y protocolos seguros.

b) El área responsable de la seguridad debe proteger la información en aquellos lugares, sucursales, sitios web, correos electrónicos, etc. en donde los usuarios deban ingresar información crítica, para garantizar su confidencialidad.

c) El área responsable de la seguridad debe procurar que al igual que en los sitios web de ingreso de información estratégica, tales como pagos en línea, registro de antecedentes, entre otros, la información es protegida a través de dos protocolos de seguridad:
   - Encriptación de Datos
   - Uso de Claves de Seguridad

13.2.3 Mensajería electrónica

La Dependencia u Organización debe proteger adecuadamente la información incluida en la mensajería electrónica.

a) Se deben llevar a cabo campañas de seguridad dirigidas a todo el personal de la Dependencia u Organización, por Responsable de la seguridad.

b) Se debe implantar en la Dependencia u Organización mecanismos que permitan prevenir la fuga de información y que los archivos adjuntos no contengan metadatos.

c) Se debe concientizar al personal de las unidades administrativas que no puede compartir su dirección de correo electrónico.
d) Se debe concientizar al personal de tener cuidado al abrir archivos adjuntos y descargar archivos o aceptar correos electrónicos de desconocidos y que el uso del correo electrónico oficial, es con fines laborales.
e) Se deben inculcar buenas prácticas y crear contraseñas seguras, robustas y poco usuales para los diversos accesos autorizados y personales, y deben ser cambiadas con periodicidad.

13.2.4 Acuerdos de confidencialidad o de no divulgación

La Dirección General de la Dependencia u Organización deberá revisar y documentar regularmente los requisitos para generar los Acuerdos de Confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información, establecer su firma por el personal que labora en la organización, e ir incluyendo al personal de nuevo ingreso, indicando las necesidades de la organización para la protección de datos. Es necesario revisar periódicamente su vigencia y en caso de incumplimiento establecer las medidas disciplinarias necesarias considerando que:

a) La Dirección General o equivalente debe definir cuál es la información confidencial, a fin de que ambas partes comprendan el ámbito del convenio.
b) Describir la razón por la cual la información confidencial no debe ser compartida, en el caso contrario, definir un procedimiento formal que establezca cómo puede ser utilizada.

El área responsable de la seguridad, al momento de requerir y establecer contacto técnico brindado por agentes externos, se asegurará de que se establezca un convenio de confidencialidad asegurado que la información no será divulgada durante la duración del contrato, o posterior a éste.

14 Adquisición, desarrollo y mantenimiento de sistemas

Hoy en día el uso de sistemas de información ha venido a beneficiar a la sociedad en general debido a que los procesos se realizan de una manera más ágil y segura. Lo que se traduce en reducción de tiempo y dinero.

La mayoría de las organizaciones tanto de sector público como privado, consideran necesario contar con un área especializada en el control y manejo de TIC esto debido a su gran crecimiento, pero sobre todo por los beneficios que el uso adecuado de las TIC les genera, lo que deriva en la necesidad de estandarizar los procesos de adquisición, mantenimiento y desarrollo de sistemas de información.

14.1.1 Requisitos de seguridad de los sistemas de información

La Dependencia u Organización debe vigilar que la seguridad de los sistemas de información sea considerada en cada una de las fases durante el ciclo de vida de un sistema.

Durante la Fase de Análisis y Diseño:

- Asegurar la confidencialidad y resguardo de la información proporcionada por parte del usuario a través de minutas de reunión, tanto información digital como en cualquier otro medio donde se comprometa el resguardo y seguridad de la misma.

Durante la Fase de Desarrollo:

- Verificar que no se desarrolle el sistema en equipos privados no autorizados.
- Verificar que el equipo de desarrollo cuente con licencias válidas para evitar riesgos.

Durante la Fase de Pruebas:

- Asegurar que el ambiente de pruebas no haga uso de información sensible que pueda comprometer la operación del sistema, y esté separado del ambiente de producción.

Durante la Fase de Liberación:

- Asegurar que el ambiente de producción cuente con la infraestructura necesaria para mantener segura la información tanto de la base de datos como de la aplicación

14.1.2 Análisis y especificación de requisitos de seguridad de la información

Se debe realizar una revisión sobre los sistemas existentes y evaluar la vulnerabilidad de la información, y a partir de dicha evaluación valorar si es conveniente afianzar la seguridad de la información en el ambiente de producción del sistema tanto en la base de datos como en la aplicación.

Dicha revisión se debe realizar a partir de un análisis al código fuente identificando todas las peticiones que se realizan a la base de datos, por lo que es necesario contar con un procedimiento formal para la revisión, y en su ejecución de deben mantener todos los registros generados.

14.1.3 Aseguramiento de servicios de aplicación en redes públicas

Inicialmente se deben identificar aquellas aplicaciones que requieran operar a través de una red pública, una vez identificadas, por cada aplicación se deberá realizar:

- Identificar el perfil del usuario final
- Llevar una bitácora de los accesos a la aplicación
- Delimitar el acceso por zona o región geográfica a través de la IP
- Robustecer la infraestructura para evitar actividades fraudulentas tanto en la base de datos como en la aplicación

- Valorar la necesidad de que la aplicación opere sobre una red pública y en tal caso restringirla a una red privada

14.1.4 Protección de las transacciones de servicios de aplicación

Se debe realizar un análisis sobre el tipo de transacciones que realiza la aplicación.

Clasificar las transacciones críticas y no críticas dependiendo la información que se maneje.

Para las transacciones críticas se debe hacer uso de un certificado digital (Protocolo seguro de transferencia de hipertexto), para asegurar que la información en tránsito no sea interceptada ni utilizada por terceros.

14.2 Seguridad en procesos de desarrollo y soporte

La Dependencia u Organización debe asegurar a través de los desarrolladores de sistemas, que la seguridad de la información está considerada en el diseño y es implementada dentro del ciclo de desarrollo de los sistemas de información. En todos los casos será necesario conocer y validar con el usuario todas las necesidades que se han de cubrir dentro del desarrollo en el ámbito de seguridad.

14.2.1 Política de desarrollo seguro

La fase de desarrollo en el ciclo de vida de un sistema de información es una fase indispensable para asegurar una confiable implementación y liberación de un sistema, por lo que se deben considerar políticas de desarrollo seguro:

- Hacer uso de un ambiente de desarrollo totalmente independiente al ambiente de pruebas y de producción
- Desarrollar el sistema con un lenguaje de programación confiable y seguro (java, .net o php), y asegurar su interoperabilidad con otros desarrollos, plataformas, servicios, etc.
- Definir un servidor de base de datos independiente al servidor de aplicación
- Definir un manejador de base de datos seguro (oracle, sql server, mysql, MariaDB, Postgres)

14.2.2 Procedimientos de control de cambios en sistemas

El control de cambios en los sistemas de información permite llevar un control ordenado y documentado sobre las diferentes versiones que se manejan en un sistema de información, por lo que se debe contar con un procedimiento documentado y formal dentro de la Dependencia u Organización.

Cada vez que se realice una nueva versión, esta debe estar perfectamente bien documentada a través de un formato de control de cambios en donde se definan los cambios o mejoras con las que cuenta la nueva versión.

Así mismo se deberá llevar un control sobre las versiones anteriores con un respaldo del código fuente por si en algún momento se tiene la necesidad de regresar a una versión anterior, que el cambio se realice de manera inmediata, de igual manera contar con un plan de retorno.

14.2.3 Revisión técnica de las aplicaciones después de cambios en la plataforma de operación

Los procesos de revisión se deberán realizar en un ambiente independiente al de producción, se realizarán todas las pruebas pertinentes y necesarias para asegurar su perfecto funcionamiento, una vez probado se migrará a producción nuevamente.

Se deberá llevar una bitácora de todos los cambios que haya sufrido la plataforma de operación especificando el motivo y el impacto de dicho cambio, llevar todo el registro necesario, así como nombre del responsable de su ejecución.

14.2.4 Restricciones en los cambios a los paquetes de software

Entiéndase paquete de software a todo el software de uso de oficina.

Los paquetes de software deben ser monitoreados a través de un responsable que se encargue de mantener actualizado el software e implementar los candados necesarios a cada equipo de cómputo para que no puedan ser modificados.

La Dependencia u Organización debe asignar un área especializada para concentrar la administración de todo el software que sea utilizado dentro de la organización, la cual debe mantener todos los registros actualizados del mismos, así como su versionamiento, y asegurar que el mismo se encuentra en el lugar físico adecuado y debidamente protegido.

14.2.5 Principios de ingeniería de sistemas seguros

Un Sistema seguro es un sistema íntegro confidencial y disponible, cuando cumple con:

- La disponibilidad, se refiere a que debe ser accesible en todo momento evitando interrupciones en el servicio.
- La confidencialidad, se refiere a que salvaguarda la información de una manera segura.
- La integridad, se refiere a que los procesamientos de información se realicen de una manera certera.

Todo proceso de desarrollo de sistemas debe tener presente estos tres aspectos en todo momento

14.2.6 Entorno de desarrollo seguro

El ambiente de desarrollo debe ser totalmente independiente al ambiente de pruebas y de producción. Así mismo el desarrollador del sistema debe asegurarse que cuenta con un

equipo de cómputo con las características necesarias para poder desarrollar, independientemente del leguaje que esté utilizando.

Durante la fase de desarrollo se hará uso de una base de datos en un ambiente de pruebas con información que no comprometa la operación del sistema.

El ambiente de desarrollo debe soportar cualquier cambio o modificación de código que requiera el desarrollador e interpretarlo de manera inmediata.

14.2.7 Desarrollo tercerizado

Para el caso de desarrollo de sistemas que se adquieren a través de terceros es importante tener en cuenta lo siguiente:

- El proveedor esté debidamente identificado y cumpla con todos los requisitos para poder desarrollar un sistema a cualquier dependencia u Organización
- Validar si el sistema requerido no existe en ninguna otra dependencia u Organización, que lo pudiera proporcionar.
- Llevar un monitoreo minucioso sobre la entrega de avances del proveedor.
- Definir claramente el soporte, garantía y manejo de información una vez que se haya liberado el sistema.

14.2.8 Pruebas de seguridad del sistema

La fase de pruebas en el ciclo de vida de un sistema de información es de vital importancia, ya que es el puente para liberar un sistema a un ambiente de producción.

El ambiente de pruebas debe ser similar al ambiente de producción, el propósito es que todas las pruebas asemejen situaciones reales que podrían afectar al sistema.

Es necesario documentar las pruebas que se realizan, considerando pruebas en el sistema:

- Por tipo de dato: Realizar pruebas en los campos de captura por longitud y tipo de dato para asegurar que el procesamiento de cualquier tipo de dato se realiza correctamente y no pone en riesgo la confiabilidad del resto de la información.
- Pruebas de estrés: Contemplar pruebas de estrés donde se simulen cantidades de acceso concurrentes.
- Ataques: Realizar pruebas de hackeo al servidor de base de datos.

14.2.9 Prueba de aprobación de sistemas

Una vez concluida la fase de pruebas, se deben documentar las pruebas realizadas, así como la aceptación, de manera documentada y formal, del sistema por parte del usuario final.

Se realizará la migración del sistema del ambiente de pruebas al ambiente de producción y se confirmará la puesta en marcha.

Se debe asegurar la entrega de cuentas de usuario al usuario final ya en la base de datos de producción, y deslindar al desarrollador de dichas cuentas, por lo que será necesario ejecutar el procedimiento formal establecido en la organización y mantener los registros generados.

14.3.1 Protección de datos de prueba

Los datos utilizados durante la fase de prueba de un sistema deben ser una muestra que abarque los diferentes escenarios con los que se va a enfrentar el sistema en el ambiente de producción, permitiendo generar pruebas contundentes para asegurar la confiabilidad de la información.

Así mismo se debe asegurar que las pruebas no ponen en riesgo la seguridad de la información existente, ni la operación de la aplicación.

15 Relaciones con el proveedor

15.1 Seguridad de la información en relación con los proveedores

La Dependencia u Organización debe asegurar la protección de los activos de la organización que sean accesibles para los proveedores.

15.1.1 Política de seguridad de la información para las relaciones con el proveedor.

Los riesgos asociados a la externalización, deben ser tratados, documentados y gestionados por los responsables designados para tal fin, a través de la imposición de mecanismos adecuados, que comprendan una combinación de controles administrativos, legales, físicos, lógicos, de procedimiento, y de gestión que regulen las condiciones en las que el proveedor deberá desarrollar su actividad y sean de apoyo para la supervisión de las actividades a realizar por el mismo, con la finalidad de preservar durante el tiempo de la prestación del servicio, la confidencialidad, integridad y disponibilidad de todos los activos de información a los que tendrá acceso, ya sean físicos o electrónicos dentro de la organización.

15.1.2 Abordar la seguridad dentro de los acuerdos del proveedor

Para llevar la protección de los activos, entre ellos la información. Se establecerán como mínimo los siguientes contratos y acuerdos con el proveedor:

- Contrato de Confidencialidad

Durante la provisión del servicio se genera conocimiento que es de gran valor tanto para quien realiza la provisión del servicio como para quien lo recibe. Dentro de este conocimiento se incluye información relativa a la resolución de incidencias, problemas, oportunidades de mejora, optimización del rendimiento, etc. por norma general, es el proveedor del servicio quien tiene acceso directo a esta información y, por lo tanto, si externalizamos la prestación del servicio dicho conocimiento se vuelve vulnerable. Si bien este acceso es necesario para desempeñar el servicio, también lleva asociado el riesgo de que dicha información se difunda,

tanto por accidente como intencionadamente, por lo que es vital que exista un compromiso por escrito por parte del proveedor de que considere:

1) No revelará a terceros la información a la que tenga acceso durante la prestación del servicio.
2) Establecerá las medidas de seguridad necesarias para protegerla. Por ejemplo, restringir el acceso a nuestra información exclusivamente a los empleados involucrados, implantar medidas técnicas frente a potenciales atacantes, seguir las pautas legales obligatorias, etc.

Para formalizar dicho compromiso, que protege la información sensible frente a fugas o robos, se debe firmar un contrato de confidencialidad. Este contrato también se conoce como NDA, por las siglas en inglés de Non-Disclosure Agreement. También es posible añadir cláusulas específicas a un contrato de servicios.

Por norma general será necesario firmar dos copias en todas las hojas por ambas partes. Debemos guardar una copia del contrato de confidencialidad firmado por el proveedor. Este contrato garantiza que éste, y por extensión todos los trabajadores implicados en el servicio, guardarán secreto con respecto de la información a la que puedan acceder durante la prestación.

Los puntos que debe contemplar un contrato de confidencialidad son:

- El nombre y datos del proveedor. Es decir, definir quién accederá a información confidencial.
- Definir en el contrato qué se considera confidencial y qué información se encuentra protegida por el acuerdo.

  Pueden existir excepciones, como la información que el proveedor conociera de antemano, o aquella que sea pública o que haya obtenido de fuentes distintas al propio cliente.

- Duración de la relación de confidencialidad. Se debe establecer durante qué período de tiempo debe mantenerse la confidencialidad, que en general será superior al tiempo de prestación del servicio. También deben fijarse las medidas que el proveedor debe llevar a cabo cuando finalice la prestación del servicio: destruir adecuadamente la información a la que ha accedido mientras ha durado el servicio, la obligación de devolverla o devolver toda aquella que surge de dicho trabajo.
- Este acuerdo también se utiliza para establecer restricciones al uso de la información por el proveedor, e indicar las medidas de seguridad que el proveedor deberá aplicar a la información, siempre de manera proporcional al objeto del contrato.

- Por último, en caso de ser necesario, el contrato debe indicar la jurisdicción legal a la que se acoge cada una de las partes, para su resolución en caso de problemas durante o después de la prestación.

El contrato de confidencialidad entre proveedor y cliente es obligatorio por la ley siempre que en la información accedida por el proveedor haya datos de carácter personal, aspecto que se trata en el siguiente punto. Sin embargo, es muy recomendable que se establezca, en cualquier caso, sin olvidar que no sustituye a otras medidas de seguridad que es necesario aplicar.

En los casos de proveedores que acceden a información de la organización sin acceso a datos personales, es importante que la empresa implemente las medidas técnicas necesarias para que así sea, y aun así deberá quedar recogido en el contrato de confidencialidad, la prohibición expresa de acceder a estos datos, y la obligación de secreto respecto a aquellos datos que, en cualquier caso, hubiera podido conocer con motivo de la prestación del servicio.

- Contrato de acceso a datos personales

Para garantizar la seguridad y confidencialidad de nuestra información, debemos firmar un acuerdo de confidencialidad con el proveedor. En él se establecerá la obligación del proveedor a respetar el secreto y la confidencialidad de la información a la que van a tener acceso, y a usarla sólo para el fin que se acuerde. Los datos personales son información de una naturaleza muy específica, cuya manipulación se encuentra regulada por la Ley de Protección de Datos Personales del Estado de México, por tanto, cuando la prestación del servicio vaya a requerir que el proveedor acceda a datos personales, el Titulo Quinto, Capitulo Primero en el apartado de Tratamiento De Datos a cargo de Encargados Externos. El artículo 51 de Ley de Protección de Datos Personales del Estado de México LPDEM dicta lo siguiente:

En caso de que el tratamiento de datos personales lo realice un encargado externo, el sujeto obligado deberá suscribir un convenio o contrato en el que se establezca que los datos personales serán tratados únicamente conforme a las indicaciones del responsable, que no serán utilizados para una finalidad distinta a la estipulada en el contrato, y su destino final. Asimismo, dicho contrato deberá establecer, por lo menos, cláusulas específicas sobre:

I. La obligación del encargado de guardar confidencialidad de los datos;
II. Las responsabilidades y penalizaciones que correspondan por el uso inadecuado de los datos;
III. El nivel de protección requerido para los datos de acuerdo con su naturaleza; y
IV. La obligación de permitir verificaciones a las medidas de seguridad adoptadas mediante la inspección de las instalaciones, los procedimientos y el personal.

Este contrato tiene una finalidad similar al contrato de confidencialidad, pero es obligatorio y está restringido a los datos personales, su contenido básico está establecido por ley.

El contrato de acceso a datos debe contener:

- Las instrucciones bajo las cuales la gestoría debe tratar los datos
- La finalidad con el que se lleva a cabo dicho tratamiento.
- Las medidas de seguridad que el proveedor está obligado a cumplir para acceder a los datos. Por ejemplo, realizar copias de seguridad para evitar pérdidas de información o cifrar las comunicaciones entre ambos.

Estas medidas serán técnicas y organizativas, con el objetivo de evitar que sean accedidos sin autorización o perdidos. Es tan importante que la información no se difunda ni se pierda.

Es importante destacar que legalmente somos responsables en el caso de que se produzca una pérdida o difusión de los datos personales, por lo que debemos velar por la aplicación de las medidas de seguridad.

A la finalización de la prestación del servicio, el proveedor está legalmente obligado a devolvernos los documentos y soportes que contengan datos de carácter personal, o bien destruirlos adecuadamente (tanto copias en papel como en soportes digitales).

Por tanto, la firma de este documento no sólo es obligatorio, y también es necesario que vigilemos que el proveedor aplique las medidas de seguridad necesarias para proteger los datos que le confiemos.

Evidentemente, la adaptación del proveedor a la Ley de Protección de Datos Personales del Estado de México LPDEM o cualquier otra legislación vigente, debe ser un aspecto imprescindible a considerar en

- Acuerdos de Nivel de Servicio

Al contratar servicios, la Dependencia u Organización debe tener en cuenta aquellos riesgos relacionados con la prestación del servicio, ya sean de seguridad o no: el servicio contratado debe cumplir las condiciones pactadas y hacerlo de la manera acordada, para evitar retrasos en las entregas, errores, calidad por debajo de la esperada, etc.

Por este motivo, al establecer una relación comercial con un proveedor que va a prestar un determinado servicio, puede ser necesario o recomendable fijar unos acuerdos de nivel de servicio o SLA.

Con estos acuerdos se establece cuál debe ser la calidad del servicio, es decir, bajo qué parámetros debe prestarse el mismo, y entre otros, se puede establecer:

- Disponibilidad horaria.

- Tiempo de respuesta.
- Tiempo de resolución.
- Personal asignado al servicio.
- Disponibilidad de los sistemas, si aplica.
- Vías de comunicación, entre otros.

Además de definir las necesidades, los acuerdos controlan las expectativas que se esperan del servicio, ya que se detalla qué puede ofrecer el servicio acordado y sirve para establecer un marco entre el cliente y el proveedor en caso de conflicto.

En el SLA se establece cómo notificar las peticiones de servicio, en qué tiempo límite deben ser atendidas y resueltas, o cuál debe ser el perfil del personal que debe atenderlas.

También se especificará el tiempo máximo de interrupción del servicio, en caso de incidente o parada programada, cuándo y en que horario se realizará el servicio y si implica parar la actividad, tiempo de resolución de una falla, etc.

Hemos de tener en cuenta que:

- Las dos partes implicadas en la negociación de los acuerdos de nivel de servicio deben participar activamente en su definición, ya que lo que se acuerde fijará lo que el proveedor debe cumplir y lo que como cliente tenemos derecho a exigir.
- En algunos casos, es posible incluir penalizaciones en caso de incumplimiento de los SLA.
- Los cambios importantes en nuestra infraestructura y funcionamiento pueden afectar a los SLA establecidos, por lo que se deben revisar periódicamente.
- Establecer un SLA no sirve de nada si no se realiza una revisión periódica de su cumplimiento para identificar desviaciones. Esto puede servir para reclamar indemnizaciones si así está establecido, prevenir que el servicio se deteriore más de lo necesario y reconducir el problema, o directamente cambiar de proveedor.
- Esta revisión de cumplimiento se realiza desde nuestro punto de vista: el del cliente, que es quien debe ver cubiertas sus
- En algunos casos el SLA de un proveedor no será negociable. Por ejemplo, una gran compañía de telecomunicaciones puede dar un tiempo límite de 24 horas para la resolución de un problema de conexión a Internet, y hay poco margen para reducir ese tiempo.

La firma de una SLA nos garantiza una definición explicita y con claridad de las actividades, o servicios a realizar por parte de un proveedor.

15.1.3 Cadena de suministros de tecnología de la información y comunicaciones

Las organizaciones requieren en la actualidad la adaptación rápida a la velocidad con que se intercambia la información y mantener usuarios que perciban el valor agregado de los servicios que ellas ofrecen, de ahí la importancia de considerar la relación entre las organizaciones y proveedores con el fin de eficientar dichos servicios, lo que obliga a dar una mayor relevancia a las cadenas logísticas que se encargan de proveer insumos y soportar a los servicios, para adecuarse a ese contexto competitivo, sin perder de vista la seguridad de la información.

Dentro de la compleja red de intereses y relaciones entre las compañías que forman parte de una cadena de suministro, es necesario realinear las estrategias particulares, de manera que la cadena entera esté dirigida a satisfacer las necesidades de servicios de alto nivel en la Dependencia u Organización, en las que el proveedor está comprometido con la seguridad. Esto será viable en la medida que los factores claves del proceso de la organización consideren el torno y la integración de sus cadenas de suministro, al realizar el análisis las cadenas de suministro, suelen aparecer las ineficiencias que impiden conseguir mejoras y todas las acciones que se llevan a cabo en ellas, tienen con fin eliminar ineficiencias, elevación de costos, pérdida de tiempo, información y recursos, o falta de cumplimiento en los contratos.

En el caso de las TIC, el internet es factor importante en la cadena de suministro por muchos motivos: es una red abierta, de bajo costo, puede ser utilizada para tener una noción global del negocio y ayuda a solucionar más rápidamente los cambios en los servicios y la disponibilidad de recursos para la producción.

La Dependencia u Organización debe considerar tres factores clave en las tecnologías, para ayudar a una mejor gestión de la cadena de suministro:

- Relaciones Cliente – Proveedor
- Gestión de Recursos
- Información de Gestión

15.2 15.2 Gestión de entrega del servicio del proveedor

Mantener un nivel acordado de seguridad de la información y entrega del servicio, en línea con los acuerdos del proveedor.

Es necesario distinguir cuando se trata de un servicio que se presta de manera remota o en las propias instalaciones de nuestra empresa, modelo denominado in-house y offshore. En el primer caso, nuestro control sobre las medidas de seguridad es menor y es recomendable solicitar información al proveedor sobre dichas medidas. En el segundo caso, podemos tener más control, pero el personal que trabaje en nuestras instalaciones dispondrá de un mayor

acceso a la información corporativa, no sólo digital sino también conversaciones, información impresa, comentarios, etc.

De manera específica, si el empleado del proveedor va a trabajar en nuestras instalaciones, es conveniente requerir que éstos lleven sus propios equipos de trabajo. En este caso, debemos establecer los requisitos de seguridad necesarios que deben de cumplir dichos equipos y auditarlos convenientemente antes de conectarlos a la red, revisando que dispone de las necesarias medidas de seguridad establecidas. Es importante establecer correctamente los permisos de aquellas carpetas compartidas que contengan información sensible, asegurando que únicamente acceden los usuarios que necesitan esa información.

Es importante revisar y eliminar los metadatos de los documentos que se intercambien con el proveedor.

Si se va a intercambiar información confidencial, es importante cifrarla. Esto aplica a la información compartida por correo electrónico, a la que se almacene en la nube y a la que salga de la empresa en un portátil o en un dispositivo extraíble, en la que se debe emplear herramientas de borrado seguro cuando se desee eliminar información sensible, o cuando se van a intercambiar soportes con el proveedor.

La información confidencial debe intercambiarse utilizando redes seguras únicamente, nunca en entornos no confiables. No se deben utilizar conexiones inalámbricas públicas para intercambiar información de la organización.

Por tanto, en todas las comunicaciones que se establezcan con el proveedor deben utilizarse redes seguras, debe cifrarse la información sensible y limitarse el acceso a aquellas personas que lo necesiten.

Con la prestación del servicio ya iniciada debemos llevar un seguimiento del servicio que estamos recibiendo. Es el momento de comprobar que los acuerdos y contratos firmados se cumplen, y si es necesario, hacer uso de las penalizaciones acordadas.

Estas recomendaciones de seguridad deben ser válidas durante todo el tiempo en que se produzca el intercambio de información durante la prestación del servicio.

15.2.1 Seguimiento y revisión de los servicios del proveedor

Para la supervisión y verificación del cumplimiento de las obligaciones de los contratos, la Dependencia u Organización debe designar a un responsable que coadyuve con el área requirente, el área técnica y administrador del contrato para corroborar que el proveedor de cada contrato, cumpla con las obligaciones estipuladas en el mismo y con los niveles de servicio acordados.

1. El responsable de este proceso deberá realizar las siguientes actividades:
   - Apoyar en la revisión del cumplimiento de las obligaciones contractuales del proveedor, principalmente para la aceptación de los bienes o servicios objeto de la contratación.
   - Confirmar, cuando proceda, que los accesos a los activos o servicios de TIC proporcionados al proveedor, para el cumplimiento del contrato, han sido retirados al darse por finiquitado el mismo.
   - Actualizar el reporte de avance sobre el cumplimiento de obligaciones con la información final, y comunicar cualquier incidente o desviación que se detecte al administrador de proyecto y, en su caso, a la unidad administrativa solicitante o a los responsables de los procesos involucrados, así como a la unidad administrativa facultada en la organización para efecto de dar por concluidas las obligaciones contractuales, en términos de las disposiciones aplicables.
2. Elaborar, de conformidad con el contrato de que se trate, una lista de apoyo para la verificación y seguimiento de las obligaciones contractuales, la cual deberá contener al menos, lo siguiente:
   - La totalidad de las obligaciones asumidas por el proveedor y la Institución.
   - Los supuestos en que se aplicarán penalizaciones al proveedor.
   - Las fechas de entrega de los bienes o de prestación de los servicios contratados y en su caso, el calendario de entrega de los productos o entregables.
   - Los datos del enlace o de los enlaces o responsables, designados por el proveedor.
3. En los casos en que participen diversos proveedores en un contrato, será necesario identificar qué obligaciones corresponden a cada uno.

15.2.2 Gestión de cambios a los servicios del proveedor

Los cambios en la prestación de servicios por parte de los proveedores, incluyendo el mantenimiento y la mejora de las actuales políticas de seguridad de información, procedimientos y controles, se gestionarán, teniendo en cuenta la criticidad de la información, sistemas y procesos que intervienen y re-evaluación de los riesgos.

Una vez establecidos los contratos y acuerdos mencionados, puede ser necesario que se produzca un intercambio de información para que el proveedor tenga acceso a la información que necesite para el servicio.

La prestación del servicio puede finalizar porque acabe el período establecido en el contrato o por cláusulas especificadas en el mismo (incumplimiento de plazos, cambios en el servicio o en las necesidades del cliente, etc.), sea cual sea el motivo de esta finalización, es

importante que se produzca de forma adecuada para garantizar la seguridad de la información de nuestra organización.

Los principales puntos a considerar son:

- El contrato de confidencialidad previamente firmado puede establecer las acciones a llevar a cabo cuando finalice la prestación. Éstas pueden implicar la devolución de toda la documentación compartida. Además, debemos recordar que la duración de este acuerdo de confidencialidad suele ser superior a la del servicio por lo que, aunque la relación contractual haya terminado, el proveedor no podrá difundir ni utilizar la información que ha obtenido durante la misma.
- En caso de que la prestación haya implicado acceso a datos de carácter personal, la Ley LPDPEM obliga al proveedor a destruir toda la información a la que haya accedido (tanto digital como en papel) o bien devolverla.
- Debemos asegurarnos de retirar los accesos físicos y telemáticos que se hayan proporcionado al proveedor para la prestación del servicio. O si en el momento del inicio del contrato se conoce la fecha de finalización, se puede establecer en los sistemas informáticos una duración de los accesos limitándolos a los horarios y fechas estipulados. También se deben desactivar los usuarios que les hubieran dado en nuestros sistemas, cambiar las claves de aquellos usuarios que deban seguir existiendo y el proveedor haya utilizado y restringir los permisos de información compartida en la nube. Es decir, los permisos y accesos a nuestra infraestructura deben quedar como estaban antes de la contratación del servicio.

Por último, conviene recordar que las comunicaciones que se mantengan con cualquier proveedor deben realizarse de manera segura según las recomendaciones anteriormente mencionadas, aunque no tengan lugar en el marco de una prestación concreta de un servicio.

16 Gestión de incidentes de seguridad de la información

16.1 Gestión de incidentes y mejoras en la seguridad de la información

La Dependencia u Organización debe contar con un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades, considerando que un incidente de seguridad es una falla en la confidencialidad, integridad o disponibilidad de la información que ha causado, o es probable que cause, algún daño material, financiero, de imagen o de cualquier otro tipo.

16.1.1 Responsabilidad y procedimientos

Es necesario que la Dependencia u Organización establezca las responsabilidades y procedimientos de gestión necesarios para asegurar una respuesta rápida, eficaz y ordenada en los incidentes de seguridad de la información que se presenten.

a) El área responsable de la seguridad debe definir la clasificación y niveles de incidencias para que una vez integrada toda la información, se aplique la política correspondiente.
b) La Dirección General o equivalente de manera conjunta con el área responsable de la seguridad establecerán el CERT (Computer Emergency Response Team, Equipo de Respuesta a Incidentes informáticos) con integrante(s) procedente de la unidad de Tecnologías de la Información o especialistas en el tema, para proteger la infraestructura crítica de la organización.
c) Se debe designar a un Responsable de Seguridad de la Información, quién deberá velar por la observancia de los procedimientos y normas en la materia, éste conveniente que provenga del CERT o de alguna unidad administrativa relacionada con la implantación de normas y políticas en la dependencia u Organización. La Dirección General o equivalente de manera conjunta con el área responsable de la seguridad deben determinar el BCP (Business Continuity Plan) mediante la integración de la información brindada por las unidades administrativas, de tal manera que se asegure y administre la habilidad de la organización para continuar proporcionando el nivel de servicio acordado y apoyar con los requerimientos después de una interrupción, o como consecuencia de una situación de contingencia, previniendo de este modo, que los servicios y las instalaciones de TIC pueden ser ofrecidos.
d) Los integrantes del CERT deben revisar periódicamente los procedimientos para mejora continua a fin de garantizar la disponibilidad, integridad y confidencialidad de la información.

16.1.2 Informe de eventos de seguridad de la información

Todos los eventos de seguridad de la información se deben informar, a través de los canales de gestión apropiados, tan pronto como sea posible.

a) El personal de la Dependencia u Organización, es responsable de notificar al área de seguridad la presencia de cualquier evento que pueda afectar el funcionamiento de los diversos sistemas de información e infraestructura.
b) Los antecedentes, tratamiento, clasificación, escalamiento y resolución de los eventos de seguridad deberán ser registrados por el Responsable de seguridad, en un formato estandarizado.
c) De deben mantener las características de seguridad (disponibilidad, integridad, confidencialidad, mismidad y autenticidad) de cada una de las evidencias digitales recaudadas después de los incidentes de seguridad.

16.1.3 Informe de las debilidades de seguridad de la información

Es responsabilidad de los directivos de la Dependencia u Organización, requerir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización,

que observen e informen cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.

a) El área responsable de la seguridad debe establecer y dar a conocer una línea telefónica y/o extensión para que el personal de las unidades administrativas pueda informar sobre incidentes, eventos y problemas de seguridad.
b) El área responsable de la seguridad debe contar con estadísticas y análisis sobre el número y tipos de llamadas relativas a seguridad de la información (p. ej., cambios de contraseña; porcentaje de preguntas acerca de riesgos y controles de seguridad de la información respecto al total de preguntas).
c) A partir de las estadísticas, tomar las medidas necesarias que aseguren la concientización del personal y las acciones que mejoren los servicios, en relación con la seguridad de la información.

16.1.4 Evaluación y decisiones sobre los eventos de seguridad de la información

La Dependencia u Organización debe establecer los criterios necesarios para evaluar todos los eventos de seguridad de la información, y en base a ello, decidir si se clasifican como incidentes de seguridad de la información.

a) El área responsable de la seguridad debe, con base en la información recabada en la documentación pertinente, evaluar la reclasificación del incidente si fuera necesario.
b) El área responsable de la seguridad debe contar con un el canal de comunicación adecuado, y de ser necesario notificar la incidencia a organismos externos de acuerdo al nivel y clasificación.
c) El área responsable de la seguridad que cuente con contratos de servicio para asegurar la información, y que de acuerdo a la clasificación establecida en la organización detecte un incidente, lo deberá evaluar para calificar el servicio y de ser necesario, la solicitud de término anticipado de contrato, sanción u otra política aplicable.

16.1.5 Respuesta ante incidentes de seguridad de la información

La Dependencia u Organización deben asegurar que todos los incidentes de seguridad son resueltos y los servicios son restaurados lo más rápido posible de acuerdo a su DRP (Disaster Recovery Plan) y respetando los tiempos acordados en sus Acuerdos de Nivel de Servicio.

La administración adecuada de un incidente debe considerar:

a) La identificación y registro;
b) La categorización;
c) La asignación de prioridad;
d) El diagnóstico inicial;
e) El escalado (si se requiere);
f) La investigación y diagnóstico;

g) La solución del incidente y recuperación del servicio;
h) El cierre;
i) El monitoreo y seguimiento.

Se debe dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados, observando lo siguiente:

a) El área responsable de la seguridad debe generar un Plan de Respuesta a incidentes informáticos.
b) Se debe incrementar el monitoreo, vigilancia de los incidentes y documentar las acciones tomadas para su solución, después de ocurrido el incidente.
c) Se debe generar el procedimiento formal y los controles aplicables e indicadores que permitan la adecuada medición de los incidentes, para establecer mejorar en los servicios.

En caso de que se produzca un incidente mayor en la seguridad informática, las áreas de seguridad especializadas deben:

a) Registrar y documentar todos los hechos pertinentes respecto a la falla de manera tal que puedan ser aceptados como evidencia legal;
b) Documentar en detalle todas las medidas de emergencia y recuperación del curso normal de las operaciones que hayan sido adoptadas;
c) Revisar y fortalecer a la brevedad los controles de seguridad informática a fin de evitar la recurrencia de la falla;
d) Asegurar los registros correspondientes en caso de auditoria, así como la documentación requerida para el análisis de los problemas internos, la compensación de negociaciones con terceros externos, o la evidencia para procedimientos legales.

16.1.6 Aprendizaje de los incidentes de seguridad de la información

Es necesario que el área especializada en la seguridad documente todo el conocimiento adquirido al analizar y resolver incidentes de seguridad de la información, y usarla para reducir la posibilidad o el impacto de incidentes futuros, para ello es necesario que:

a) Se revisen y actualicen las políticas y procedimientos, así como el control documental como forma de prevención.
b) Realizar análisis exhaustivos de lecciones aprendidas, para prevenir que el incidente ocurra nuevamente.
c) Con la información obtenida el CERT debe analizar las causas del incidente para generar nuevas estrategias de respuesta.
d) El CERT debe realizar los Informes de Incidentes de Seguridad, que servirán para aprendizajes futuros.
e) El área responsable de la seguridad en conjunto con el CERT deben cuantificar el costo de los incidentes de seguridad para medir las pérdidas en costo y tiempo.

16.1.7 Recolección de evidencia

La Dependencia u Organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.

a) La recolección de evidencia es trabajo del Responsable de seguridad, para el caso de los medios impresos éstos deben ser asegurados para no ser alterados.
b) El Responsable de seguridad debe crear una copia o imagen del disco para preservar el medio original y ser guardado de manera segura e incluso utilizar mecanismos de protección.
c) Clasificar la evidencia digital de acuerdo a:
   - Si fue un registro generado en el equipo.
   - Registro no generado sino simplemente almacenado.
   - Registro híbrido que contiene generados y no generados.
d) El área responsable de la seguridad debe definir los criterios de admisibilidad de la evidencia, que contemplen:
   - Autenticidad.
   - Confiabilidad.

17 Aspectos de seguridad de la información de la gestión de continuidad de negocio

17.1 Continuidad de seguridad de la información

La Dependencia u Organización debe garantiza la continuidad de seguridad de la información e incluirla en los sistemas de gestión de la continuidad de negocio de la organización para asegurar y administrar la habilidad de la organización y continuar proporcionando el nivel de servicio acordado, apoyar los requerimientos del negocio después de una interrupción o como consecuencia de una situación de contingencia, asegurando que los servicios y las instalaciones de TIC pueden ser ofrecidos.

17.1.1 Planificación de la continuidad de la seguridad de la información

Las áreas de TI deben ejecutar medidas de reducción de riesgos y opciones de recuperación que incluyan a las instalaciones de respaldo. La capacidad de recuperación de los servicios dentro de la Dependencia u Organización esencial para continuar siendo efectivo y para cumplir con ello se deben determinar los requisitos para la seguridad de la información y la continuidad del servicio en situaciones adversas, por ejemplo: el mantenimiento al equipo que soporta la prestación de los servicios es vital y requiere ser continuo, realizar evaluaciones continuas de los riesgos, elaborar Planes de Recuperación ante Desastres.

Las actividades relevantes en el proceso de Administración de Continuidad de Servicios de TI son:

- Requerimientos y estrategias. - Abarca el análisis de impacto, evaluación de riesgo y estrategia, estrategia de continuidad;
- Implementación. - Esta fase requiere la organización, planificación e implementación de medidas de contención, planes de recuperación, las medidas de riesgo, desarrollo de procedimientos, pruebas iniciales, publicación de planes y capacitación del personal designado;
- Operación continua. - Es la operación normal diaria dentro de la cual la administración de riesgos debe asegurar los servicios sobre todo aquellos que pueden tener un impacto grave ante una falla, y asegurarse que todo el personal permanezca informado de los planes de recuperación, incluyendo personal de nuevo ingreso, revisar las solicitudes de cambio, evaluar el impacto sobre los planes y asegurar que los planes permanezcan alineados a los planes de continuidad del negocio;
- Invocación. - Son los lineamientos y actividades que deben seguir en el momento en que el plan de continuidad de los servicios sea requerido, esto involucra a un equipo de administración de crisis. El plan debe aclarar todos los detalles de cómo se llevará a cabo todas las actividades incluyendo notificar a todo el personal requerido, obtener los respaldos para el sitio de recuperación, así como la documentación fundamental;
- Revisión. - Después de todas las pruebas y de cualquier invocación, las áreas técnicas deben llevar a cabo una revisión y los resultados deben ser retroalimentados dentro del proceso de planeación.

17.1.2 Implementación de la continuidad de la seguridad de la información

Las áreas especializadas en TI y el Responsable de la seguridad deben poner en ejecución los procedimientos generados, mantener los controles y registros correspondientes, realizar las pruebas necesarias, dar la capacitación, concientización y formación que requiera el personal involucrado, dar seguimiento al calendario de mantenimiento, y todas las acciones que se generaron durante la planeación, para asegurar el nivel de continuidad de la seguridad de la información, de igual manera:

a) El CERT debe ejecutar pruebas sobre papel para evaluar diferentes escenarios.
b) El CERT y el área responsable de la seguridad deberán ejecutar simulacros completos, así como la recuperación técnica, en un lugar alternativo que cuente con todos los recursos necesarios y los servicios de proveedor.

17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información

Las áreas especializadas en TI y el Responsable de la seguridad deben verificar de manera periódica los controles establecidos para asegurar que las actividades y trabajos siguen vigentes y son eficaces durante situaciones adversas a la continuidad de la seguridad de la información, y en caso de ser necesario se realizan los cambios convenientes.

17.2 Redundancias

Las áreas especializadas en TI y el Responsable de la seguridad deben asegurar la disponibilidad de instalaciones de procesamiento de información, por ello es necesario considerar el uso de tecnología y equipos que permitan repetir aquellos datos o hardware de carácter crítico que se quiere asegurar ante los posibles fallos que puedan surgir, ya que su uso es continuo; de tal manera que los sistemas se encarguen de realizar el mismo proceso en más de una estación, ya que si por algún motivo alguna dejara de funcionar o colapsara, inmediatamente otro tendría que ocupar su lugar y realizar las tareas del anterior.

17.2.1 Disponibilidad de instalaciones de procesamiento de información

Las áreas especializadas en TI y el Responsable de la seguridad deben asegurar que las instalaciones de procesamiento de información se implementan con la redundancia suficiente para cumplir los requisitos de disponibilidad.

a) El área responsable de la seguridad debe encargarse de que la infraestructura de telecomunicaciones se implemente con el nivel más cercano a Tier II.
b) El área responsable de la seguridad debe emitir un SLA que defina cuánto tiempo y en qué horarios debe estar en línea el servicio.
c) El área responsable de la seguridad debe verificar de acuerdo al nivel elegido, la métrica que permita evaluar la disponibilidad anual.

18 Cumplimiento

La política de la Dependencia u Organización debe estipular que se cumpla con la legislación vigente y las regulaciones que afectan las operaciones de la organización en materia de TIC, incluyendo:

a) Protección de la privacidad y la información;
b) Uso indebido de los equipos y delitos informáticos;
c) Copyright del software;
d) Registros de operaciones e informes regulatorios;
e) Transferencias de información;
f) Normas técnicas y administrativas requeridas por las entidades reguladoras.

18.1 Cumplimiento de los requisitos legales y contractuales

El diseño, operación, uso y gestión de los sistemas de información pueden ser objeto de requisitos estatutarios, reguladores y de seguridad contractuales.

Los requisitos legales específicos deben ser considerados por los asesores legales de la Dependencia u Organización, o por profesionales adecuadamente cualificados, en caso de la contratación de servicios o compra de equipamiento o software, especialmente si la organización opera o tiene múltiples jurisdicciones.

Los requisitos que marca la legislación cambian y pueden variar para la información que se genera y se transfiere entre organizaciones distintas, incluso entre un país y otro, por lo que es obligatorio que la Dependencia u Organización preste especial atención a este punto.

18.1.1 Identificación de la legislación vigente y los requisitos contractuales

Se deben identificar, documentar y mantener al día de manera explícita para cada sistema de información y para la organización todos los requisitos estatutarios, normativos y contractuales legislativos junto al enfoque de la organización para cumplir con estos requisitos.

18.1.2 Derechos de propiedad intelectual

La Dependencia u Organización deben garantizar el cumplimiento con los requisitos legislativos, normativos y contractuales relacionados con los derechos de propiedad intelectual y utilizar productos software original.

Derecho de autor y derechos con él relacionados.

El software está sujeto a la Ley del Derecho de Propiedad Intelectual, Diseños y Patentes, por lo general, para los fines de la ley del derecho de propiedad intelectual el software es considerado como obra literaria, con las obligaciones de titularidad y propiedad intelectual respectivas.

No se debe copiar, modificar o utilizar el software en contravención de las condiciones de la licencia.

En el caso del Gobierno del Estado de México, es titular de todo el software y los programas diseñados por los servidores públicos en el desempeño de sus funciones, debiendo incluirse en el código de dichos programas las declaraciones correspondientes referidas al derecho de propiedad intelectual, y de ser necesario efectuar las gestiones correspondientes para su registro

Todos los titulares de los programas, así como las etiquetas de los medios de almacenamiento que contengan software elaborado por la Dependencia u Organización deben llevar una leyenda que los identifique y se especifique la propiedad Este software debe ser utilizado sólo para los fines para los que fue provisto.

Ninguna de sus partes debe ser reproducida, desarmada, transmitida, almacenada en un sistema de recuperación, ni traducida a ningún lenguaje humano o informático en modo alguno o para cualquier fin distinto sin el consentimiento escrito por la autoridad competente.

Copyright de la documentación

Toda la documentación derivada de la creación de un sistema dentro del Gobierno del Estado de México debe incluir la declaración de copyright

Todo software utilizado dentro de la organización elaborado o adquirido debe contar con una autorización de uso y en cumplimiento de las licencias vigentes, cuando se requiera:

a) Los usuarios no pueden ingresar, bajar o usar ningún software a menos que esto haya sido autorizado y aprobado por su jefe inmediato superior;
b) Se prohíbe el uso del software que no esté directamente relacionado con las funciones que desempeña dentro de su área laboral, así como el uso de software ilegal;
c) Todo uso y administración del software adquirido debe ser acorde con los contratos de licencia y copyright respectivos;
d) Deben resguardarse las copias maestras del software y sus licencias en lugar seguro y tenerlas disponibles para su inspección si fuera necesario;
e) Debe protegerse el software contra accesos o modificaciones no autorizadas mediante la utilización de controles automatizados de procedimientos que abarquen la administración de cambios y problemas y las nuevas versiones de software;
g) La administración debe garantizar que el software haya sido probado adecuadamente antes de confiarle el procesamiento de las operaciones de la organización;
h) Deben aplicarse las actualizaciones de seguridad más recientes con las que el proveedor del software cuente.

Las licencias y paquetería de software propiedad del Gobierno del Estado de México deben ser resguardadas.

El software que se instale en los equipos de cómputo registrados en la Dependencia u Organización, debe contar con licencia, la cual será respetada por el usuario en los términos establecidos por el fabricante.

La instalación o reinstalación de cualquier tipo de software será realizada estrictamente por el personal autorizado por el área tecnológica responsable, siempre y cuando el solicitante lo requiera para ejecutar sus funciones, previa autorización del jefe de área, instalándose solamente si se cuenta con la licencia respectiva.

18.1.3 Protección de registros

Los registros se deben proteger contra pérdidas, destrucción, falsificación, accesos y publicación no autorizados de acuerdo con los requisitos legislativos, normativos, contractuales y comerciales.

Cualquier registro derivado de las actividades y tareas realizadas dentro de la Dependencia u Organizaciones importante, por ello se deben generar los procedimientos formales para su resguardo y protección tanto de manera física para evitar su deterioro, así como en su contenido para evitar alteraciones, dichos procedimientos serán difundidos a todo el personal, para asegurarse que los conocen y los siguen.

18.1.4 Privacidad y protección de la información de identificación personal
Se debe garantizar la privacidad y la protección de la información personal identificable según requiere la legislación y las normativas pertinentes aplicables que correspondan.

En el caso de datos personales la Dependencia u Organización debe cumplir con lo que establece la Ley de Protección de Datos Personales de la entidad y la legislación aplicable.

Pueden utilizarse los siguientes principios como una indicación general de los requisitos típicos de protección de la información:

a) Debe procesarse la información personal con imparcialidad y legalidad, y conforme a los derechos del individuo;
b) Solamente se debe obtener información personal para fines específicos y legales, y no se podrá hacer uso de la misma de manera posterior para un fin distinto al inicial;
c) La información personal debe ser válida, pertinente y concisa en relación con el fin o fines para los cuales sea elaborada;
d) La información personal debe ser precisa y actual de conformidad al fin;
e) No debe conservarse la información personal elaborada para cualquier fin, por más tiempo del que sea necesario para el mismo;
f) Deben tomarse las medidas técnicas y de organización adecuadas contra el procesamiento no autorizado o ilegal de la información personal y contra la pérdida o destrucción accidentales o daños causados a la misma.

La información reunida para establecer el perfil de utilización de internet de un usuario pudiera estar sujeta a requerimientos legales de protección de la información, contenida en las leyes locales e internacionales.

Cuando se requiera conservar un registro formal de información relacionada con las operaciones de la Dependencia u Organizaciones, en formato electrónico, éste debe ser almacenado de manera tal que se evite que sea borrado o que se le hagan cambios adicionales. Si esto no fuera posible, deben conservarse los registros o pistas de auditoría de todos los cambios autorizados, de igual manera deben conservarse copias de los mensajes de e-mail en cumplimiento a la política de conservación de registros.

18.1.5 Regulación de los controles criptográficos

La Dependencia u Organización debe utilizar controles de cifrado de la información en cumplimiento con todos los acuerdos, la legislación y las normativas pertinentes, de igual manera debe mantener un control y registros sobre la criptografía utilizada que considere:

a) Identificación de la instrucción general de seguridad criptográfica
b) Fecha de la instrucción
c) Identificación del autorizador de la instrucción
d) Ámbito de aplicación de la instrucción general
e) Identificación de los servicios o información basada en seguridad criptográfica
f) Algoritmos criptográficos aprobados
g) Requisitos de protección de claves y material criptográfico
h) Métodos de protección de seguridad en tránsito y en el lugar de operación
i) Desarrollo de la instrucción general
j) Separación del uso de claves
k) Plazos de duración de las claves
l) Procedimientos de gestión de las claves
m) Estándares de implementación de tecnología criptográfica
n) Cumplimiento normativo
o) Roles y Responsabilidades en relación con la criptografía

EVALUACIÓN DE DESEMPEÑO

18.2 Revisiones de seguridad de la información

Se deben realizar revisiones regulares a la seguridad de los sistemas de información.

Las revisiones se deben realizar según las políticas de seguridad apropiadas, los procedimientos formales establecidos en la Dependencia u Organización, en los que las plataformas técnicas y sistemas de información deben ser revisados o auditados para verificar su grado de cumplimiento, la adecuada de implantación de la seguridad y que prevalezcan controles de seguridad documentados.

Las áreas responsables de la seguridad deben alinear los procesos de autoevaluación de los controles de seguridad con las autoevaluaciones definidas por la Dirección General o equivalente, las cuales permitan verificar el cumplimiento legal y regulatorio en seguridad de la información y su buen funcionamiento.

Las áreas responsables de la seguridad deben mantener los controles necesarios para proteger los sistemas en activo y las herramientas de auditoría durante el desarrollo de las mismas en los sistemas de información.

Las áreas de TI deben conservar las pistas de auditoria de todos los eventos importantes, generadas en los sistemas y herramientas de monitoreo automatizadas o aquellas identificadas en función de una evaluación de riesgo. Las pistas de auditoria deben:

a) Incluir, según corresponda, las identidades de los usuarios, fechas, horarios, códigos del motivo para ingresar al sistema e información importante;
b) Ser protegidas contra accesos y manipulaciones no autorizadas;
c) Ser conservadas por períodos mínimos determinados en función de los riesgos, tomando en cuenta los requisitos de control de las entidades reguladoras, los requisitos contractuales o cualquier otro requisito de control externo;
d) Ser controladas de manera planificada a través de una evaluación de riesgos, para detectar amenazas potenciales, incluyendo transacciones excepcionales.

De igual manera deben monitorear las pistas de auditoría del acceso a sistemas, para identificar cualquier evidencia de deficiencias potenciales de seguridad. La frecuencia del monitoreo de las pistas de auditoría de control de acceso deben revisarse al menos 1 vez al día.

Cuando se realicen revisiones o auditorías, éstas deben ser bien planeadas y llevarse a cabo con fin de detectar si las actividades o acciones y los resultados relativos con la seguridad cumplen con lo establecido en el Sistema de Gestión de Seguridad de la Información y verificar la efectividad del mismo; una vez concluida la revisión o auditoría, la Dependencia u Organización debe asegurar que se mantienen los resultados y los registros generados.

Las revisiones o auditorias se planifican tomando en consideración el estado y la importancia de los servicios, procesos y las áreas a auditar, así como los resultados de revisiones o auditorias previas. Asimismo, se definen los criterios de la revisión o auditoria, el alcance de la misma, su frecuencia y metodología. La selección del grupo de revisores o auditores, y su realización está orientada a asegurar la objetividad e imparcialidad del proceso de revisión o auditoria. Los revisores o auditores no auditan su propio trabajo.

El área responsable del proceso que esté siendo revisada o auditada se asegura que se toman acciones sin demora injustificada para eliminar las vulnerabilidades, fallas o riesgos detectados y sus causas. Las actividades de seguimiento incluyen con la verificación de que las acciones tomadas han sido efectivas y el informe de los resultados de la verificación.

18.2.1 Revisión independiente de la seguridad de la información

La Dependencia u Organización debe revisar a intervalos planificados o cuando tengan lugar cambios significativos en la organización y que el Sistema de Gestión de Seguridad de la Información es efectivo, que el enfoque de la organización para la implementación (los objetivos de control, los controles, las políticas, los procesos y procedimientos para la seguridad de la información) se está cumpliendo asegurando su eficacia e idoneidad.

Dicha revisión debe ser realizada por personas independientes del área sometida a revisión, por ejemplo, por la función de auditoría interna, un director independiente o una organización de tercera parte especializada en tales revisiones. Los individuos que llevan a cabo estas revisiones deberán tener la experiencia y las habilidades adecuadas y se recomienda que los resultados de la revisión independiente se registren y se reporten a la Dirección General o equivalente que ha iniciado la revisión. Estos registros se deben conservar. La revisión debería incluir la evaluación de las oportunidades de mejora y la necesidad de cambios en el enfoque de la seguridad, incluyendo la política y los objetivos de control.

Dichas revisiones se deben realizar por un área independiente a las áreas responsables de la seguridad de la información o por un organismo o consultor externo. La revisión o auditoría debe realizarse al menos una vez al año o cada vez que ocurra un cambio sustancial en la infraestructura o activos de información de la organización. La auditoría requerida seguirá los lineamientos de la norma ISO 27001.

Durante la revisión o auditoria se utilizarán Listas de verificación para auditar los procesos de planificación de la continuidad, desarrollo y adquisición de TI, seguridad de la información, dirección y gestión del SGSI, operación de TI, supervisión de proveedores, de ser necesario el propio proceso de auditorías.

18.2.2 Cumplimiento con las políticas y normas de seguridad

Todo el personal usuario de la Dependencia u Organización debe dar cumplimiento las políticas, procesos, procesamiento y procedimientos establecidos en el Sistema de Gestión de Seguridad de la Información para garantizar su seguridad dentro del área bajo su responsabilidad, los directivos y responsables de la seguridad de la información deben revisar regularmente que estas medidas se cumplan

Los terceros interesados en obtener información de la Dependencia u Organización solamente los podrán hacer a través de los procesos legales, considerando la normatividad vigente y con el consentimiento del dueño de la información.

18.2.3 Verificación del cumplimiento técnico

La Dependencia u Organización debe de cumplir con los criterios de seguridad de la información en todos los componentes de TI asegurando que los controles y medidas en el hardware y software han sido implementados correctamente, al igual que en los sistemas operativos de la organización, y que los sistemas de información con los que se interactúa cumplen con las normas y políticas de seguridad establecidas

Las actividades realizadas por los directivos o proveedores externos en donde se utilicen activos de información, deben acogerse a la política de seguridad y el cumplimiento técnico que les aplique.

Los sistemas de información se deben revisar regularmente y de manera planificada para verificar su cumplimiento, estas revisiones se deben llevar a cabo frente a políticas de seguridad adecuadas, en ellas se deben auditar las plataformas tecnológicas y los sistemas de información para determinar su cumplimiento con las normas aplicables sobre los controles de seguridad documentados.

Es importante asegurar que los sistemas operativos y las herramientas de auditoría están debidamente protegidos antes, durante y después de su ejecución, para maximizar la eficacia de los procesos de auditoría dentro de los sistemas de información y minimizar su interferencia

Este tipo de revisiones las deben realizar y supervisar personal competente y autorizado.

19 MEJORA

La Dependencia u Organización debe asegurar que se establezcan, implementen y se mantengan las medidas necesarias para eliminar las causas de las fallas o los posibles riesgos en la seguridad de la información, a través de Planes de Solventación una vez que son detectadas, y éstas pueden ser descubiertas durante las revisiones o auditorías realizadas al interior de la organización, o bien a través de las quejas de los dueños o usuarios de la información; las no conformidades actuales o potenciales detectadas deben ayudar a prevenir y corregir la ocurrencia o recurrencia de las fallas o riesgos; de igual manera sucede con la aplicación de las acciones preventivas.

La finalidad de realizar dichas acciones es integrar elementos de mejora continua que nos permita garantizar que la información utilizada dentro de la organización, cumple con los principios de continuidad, disponibilidad e integridad requeridos.

Para elaborar los Planes de Solventación será necesario integrar un equipo de personal especializado en el que se involucre a los directivos de alto nivel, para realizar un análisis detallado y encontrar las posibles causas de las fallas o riesgos; una vez detectadas, se elabora dicho plan asignando las actividades, responsables de su ejecución, fecha compromiso para la conclusión de las mismas y líder del grupo de trabajo, quien dará seguimiento al plan hasta su conclusión.

Posteriormente se deberá llevar a cabo una validación para verificar que efectivamente las acciones tomadas han mitigado la falla o disminuido los riesgos, de lo contrario será necesario volver a reunirse, hacer un otro análisis y generar nuevas acciones

Las acciones preventivas-correctivas son detectadas a través de:

a) Auditorías internas
b) Auditorías externas

c) Revisión y Evaluación por la Dirección General o equivalente de la Dependencia u Organización
d) Satisfacción del usuario, incluye las quejas de los usuarios
e) Proceso de Mejora Continua

Los aspectos que pueden ser evaluados, entre otros:

- Registros de monitoreo
- Controles estadísticos
- Manuales de operación
- Instructivos de Trabajo
- Mecanismos de control de los procesos o procedimientos
- Indicadores
- Resultados sobre la satisfacción del usuario
- Cumplimiento de la Política de Seguridad de la Información

Bibliografía

Blaustein L. (2016). Cómo mejorar la seguridad con una adecuada segmentación de redes. junio 14, 2016, de TECHTARGET Sitio web: http://searchdatacenter.techtarget.com/es/cronica/Como-mejorar-la-seguridad-con-una-adecuada-segmentacion-de-redes

Cárdenas G. L. (2008). Evaluación del Centro de Datos. junio 16, 2016, de UNAM Sitio web: http://www.enterate.unam.mx/artic/2008/mayo/art3.html

CIS UNL. (2016). Transferencia Segura de Información. junio 15, 2016, de CIS UNL Sitio web: https://sistemas2009unl.wordpress.com/transferencia-segura-de-informacion/

Delitosinformaticos.com. (2012). ENTORNO SEGURO PARA LA TRANSFERENCIA DE INFORMACIÓN. junio 15, 2016, de Delitosinformaticos.com Sitio web: http://www.delitosinformaticos.com/especial/seguridad/transferencia.shtml

Gutiérrez A.C. (2014). Importancia de la gestión de incidentes para la seguridad de la información. junio 15, 2016, de ESET Sitio web: http://www.welivesecurity.com/la-es/2013/01/07/importancia-gestion-incidentes-seguridad-informacion/

http://dgsei.edomex.gob.mx/sites/dgsei.edomex.gob.mx/files/files/POL_INF_SEG.pdf

http://qmtltda.com/phocadownload/G.Administrativa/doc%201.%20politica%20de%20inventarios.pdf

http://webcache.googleusercontent.com/search?q=cache:r9_KpvntsMIJ:www.mininterior.gov.co/sites/default/files/documentos/OIP-2014-PSI-Especificas 2%2520Activos%2520de%2520Inf.doc+&cd=2&hl=es-419&ct=clnk&gl=mx

http://www.ey.com/Publication/vwLUAssets/Adecuada_gestion_Activos_Fijos/$FILE/Adecuada_gestion_activos_fijos.pdf

http://www.intendenciaatacama.gov.cl/filesapp/Clasificacion_y_etiquetado_de_activos_de_informacion.pdf

http://www.iso27000.es/iso27002_8.html

http://www.logisticamx.enfasis.com/notas/15627-la-tecnologia-como-soporte-la-actividad-logistica

https://es.scribd.com/doc/13266513/Seguridad-de-Los-

IDG Latin America. (2016). Los 10 datos esenciales para proteger su correo electrónico y sistema de mensajería instantánea. junio 15, 2016, de IDG Latin America Sitio web: http://www.pcworldenespanol.com/2006/12/18/los-10-datos-esenciales-para-proteger-su-correo-electronico-y-sistema-de-mensajeria-instantanea/

INTENALCO. (2016). Manual de políticas y estándares en seguridad informática. junio 14, 2016, de INTENALCO Sitio web: http://www.intenalco.edu.co/MP_V01.pdf

ISACA. (2009). Soportando y Auditando la Gestión de la Continuidad del Negocio (BCM). junio 18, 2016, de ISACA Sitio web: http://www.isaca.org/chapters7/Monterrey/Events/Documents/20090224%20Audit%20BCM%20ISO27000.pdf

iso27000.es. (2016). 13. Seguridad en las Telecomunicaciones. junio 15, 2016, de iso27000.es Sitio web: http://www.iso27000.es/iso27002_13.html

iso27002. (2016). Comunicación de eventos y debilidades en la seguridad de la información. junio 17, 2016, de iso27002 Sitio web: https://iso27002.wiki.zoho.com/13-1-Comunicaci%C3%B3n-de-eventos-y-debilidades-en-la-seguridad-de-la-informaci%C3%B3n.html

iso27002.es. (2016). 10. 8. 4. Mensajería electrónica. junio 15, 2016, de iso27002.es Sitio web: https://iso27002.wiki.zoho.com/10-8-4-Mensajer%C3%ADa-electr%C3%B3nica.html

LawInfo.com. (2016). Acuerdos de confidencialidad y no divulgación. junio 15, 2016, de LawInfo.com Sitio web: http://abogados.lawinfo.com/recursos/ley-del-trabajo/acuerdos-de-confidencialidad-y-no-divulgaci-n.html

Ley de Gobierno Digital del Estado de México. http://legislacion.edomex.gob.mx/sites/legislacion.edomex.gob.mx/files/files/pdf/ley/vig/leyvig228.pdf

Ley de Protección de Datos Personales del Estado de México http://inicio.ifai.org.mx/LeyesEstados/LPDEM.pdf

Manual de políticas de seguridad de la información UTO colombiano de crédito educativo y estudios técnicos en el exterior

McAfee. (2016). Consejos de seguridad de McAfee: 13 formas de proteger su sistema. junio 15, 2016, de McAfee Sitio web: http://www.mcafee.com/mx/threat-center/resources/security-tips-13-ways-to-protect-system.aspx

QUINTÍN Martín (1995). "La informática como elemento dinamizador de las nuevas tecnologías en la empresa", en Esic Market. Núm. 88. Abril-junio. Madrid. ISSN: 0212-1867. Recuros-Humanos

Toro B.D. (2014). RECOLECCIÓN Y ADMINISTRACIÓN DE EVIDENCIA. junio 16, 2016, de Consejo Profesional Nacional de Ingeniería Sitio web: https://copnia.gov.co/uploads/filebrowser/DCALIDAD/Sistematizacion/SI-pr-10%20Recolecci%C3%B3n%20y%20administraci%C3%B3n%20de%20evidencia.pdf

UNAM CERT. (2015). Evitando errores comunes en el manejo de incidentes de seguridad. junio 15, 2016, de UNAM CERT Sitio web: http://www.seguridad.unam.mx/descarga.dsc?arch=319

UNAM. (2014). Buenas prácticas para la gestión de redes. junio 08, 2016, de UNAM Sitio web: http://www.revista.unam.mx/vol.15/num9/art71/

UNAM. (2014). Mecanismos de Seguridad. junio 08, 2016, de UNAM Sitio web: http://redyseguridad.fi-p.unam.mx/proyectos/buenaspracticas/mecanismos%20de%20seguridad.html

Unidad de Control de Gestión y Presupuesto. (2014). APRUEBA PROCEDIMIENTOS DE SEGURIDAD DE LA INFORMACIÓN ESPECÍFICOS. junio 15, 2016, de Gobierno de Chile Sitio web: http://web.minsal.cl/sites/default/files/files/REXEX%20780%2014_10_2014%20Procedimiento%20gesti%C3%B3n%20de%20incidentes.pdf

www.isaca.org.uy

Zuccardi G.& Gutiérrez J.. (2006). Informática forense. junio 17, 2016, de Pontificia universidad Javeriana Bogotá Sitio web:

http://pegasus.javeriana.edu.co/~edigital/Docs/Informatica%20Forense/Informatica%20Forense%20v0.6.pdf