GUÍA DE IMPLEMENTACIÓN DE UN MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Guía basada en las normas ISO/IEC 27002 y 27799, pensadas para desarrollar las directrices de gestión de seguridad de la información en Instituciones Prestadoras de Salud

Lic. Jorge Armando Guerra
www.managementensalud.com.ar
Diciembre 2021

Guía de implementación de un MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Tabla de contenido

Introducción.

Los objetivos generales de la seguridad de la información son el mantenimiento de la confidencialidad, la disponibilidad y la integridad de la información (incluyendo la autenticidad, la imputabilidad y la posibilidad de ser auditada).

En el cuidado de la salud, la privacidad de los sujetos del cuidado depende de mantener la confidencialidad de la información personal de salud. Para mantener la confidencialidad, también se deben adoptar medidas para mantener la integridad de los datos, aunque más no sea porque existe la posibilidad de corromper la integridad de los datos, de control de acceso, de los rastros de auditoría u otros datos del sistema de manera que permitan que ocurran violaciones a la confidencialidad o que éstas pasen desapercibidas.

Además, la seguridad de los pacientes depende de mantener la integridad de la información personal de salud ya que la falta de ello también puede dar lugar a una enfermedad, una lesión o incluso la muerte. Asimismo, un alto nivel de disponibilidad es un atributo especialmente importante en los sistemas de salud, donde el tratamiento a menudo depende críticamente del tiempo. De hecho, cuando ocurran los desastres que pueden dar lugar a interrupciones en otros sistemas informáticos no relacionados con la salud, es justamente el momento en que la información contenida en sistemas de salud sería necesaria con mayor urgencia.

Además, los ataques de denegación de servicio contra sistemas en red son cada vez más comunes.

Esta guía, basada en la norma internacional ISO/IEC 27.002 y la ISO/IEC 27.799, está diseñada para que las organizaciones la usen como referencia a la hora de seleccionar controles dentro del proceso de implantación de un Sistema de Gestión de la Seguridad de la Información (SGSI).

Para ello es necesario contar con un nivel de madurez institucional en la temática, que facilite la implementación del conjunto de controles que se requieren.

Dicho nivel de madurez se logra contando con una estructura organizativa que permita gestionar la seguridad de la información en toda la institución.

Deben identificarse las responsabilidades para la protección de activos individuales, así como para llevar a cabo procesos de seguridad específicos.

Es muy recomendable que se nombre un **responsable de seguridad de la información** para asumir la responsabilidad general del desarrollo e implantación de la seguridad de la información y para dar soporte a la identificación de los controles.

Sin embargo, la responsabilidad de la provisión e implantación de los controles a menudo permanece en directivos a título individual.

Una práctica común es **nombrar un propietario para cada activo** quien se hace responsable de la protección en el día a día.

Las funciones y áreas de responsabilidad deben segregarse para reducir la posibilidad de que se produzcan modificaciones no autorizadas o no intencionadas o usos indebidos de los activos de la organización.

Se debe cuidar el hecho de que una persona por sí sola no pueda acceder, modificar o utilizar los activos sin autorización o sin que se detecte. El lanzamiento de un evento debe separarse de su autorización.

Las organizaciones deben tener implantados procedimientos que especifiquen cuándo y con qué autoridades se debe contactar.

El mantenimiento de tales contactos puede ser un requisito para dar soporte a la gestión de los incidentes de seguridad de la información o a la continuidad del negocio y a los planes de contingencia.

La participación como miembro en grupos de interés especial o foros debe ser considerado como medio para:

- mejorar el conocimiento sobre las mejores prácticas y mantenerse actualizado sobre información relevante de seguridad;
- recibir avisos tempranos de alertas, asesoramiento y parches correspondientes a los ataques y las vulnerabilidades;
- compartir e intercambiar información sobre nuevas tecnologías, productos, amenazas o vulnerabilidades;

La seguridad de la información debe integrarse en la gestión de proyectos de la organización para asegurar que los riesgos de seguridad de la información se identifiquen y se contemplen en el marco de un proyecto.

Los métodos de gestión de proyectos deben exigir que:

- los objetivos de seguridad de la información estén incluidos en los objetivos del proyecto;
- se realiza una evaluación de riesgos de seguridad de la información en una fase temprana del proyecto para identificar los controles necesarios;

Las organizaciones deben definir una "**política de seguridad de la información"** al máximo nivel que sea aprobada por la dirección y establezca el enfoque de la organización para gestionar sus objetivos de seguridad de la información.

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

a) la definición de la seguridad de la información, de sus objetivos y principios, para orientar todas las actividades concernientes a la seguridad de la información;

a) la asignación de responsabilidades generales y específicas en materia de gestión de la seguridad de la información, para los roles definidos;
b) los procesos para el tratamiento de desviaciones y excepciones.

A un nivel inferior, la política de seguridad de la información debe apoyarse en políticas sobre temas específicos que profundicen en la implantación de controles y que, por lo general, estén estructuradas para atender las necesidades de determinados grupos dentro de una organización o para cubrir ciertos temas.

Estas políticas temáticas deben contemplar:

a) control de acceso,
b) clasificación de la información (y su manejo),
c) seguridad física y ambiental,
d) temas orientados al usuario final tales como:
    - uso adecuado de activos,
    - puesto de trabajo despejado y pantalla limpia ,
    - transferencia de información,
    - dispositivos móviles y teletrabajo,
    - restricciones de instalación y uso de software,
e) copias de respaldo,
f) transferencia de información,
g) protección ante el software malicioso (malware),
h) gestión de vulnerabilidades técnicas,
i) controles criptográficos,
j) seguridad de las comunicaciones,
k) relaciones con proveedores.

Estas políticas deben ser comunicadas a los empleados y terceras partes relevantes de una forma que sea apropiada, entendible y accesible al lector al que va dirigida.

Las políticas para la seguridad de la información se pueden incluir en un solo documento de "política de seguridad de la información" o como un conjunto de documentos individuales, pero relacionados entre sí.

Política sobre control de acceso.

Debe limitarse el acceso a los recursos de tratamiento de información y a la información.

- Los propietarios de los activos deben determinar las reglas apropiadas para el control de acceso, los derechos y las restricciones de acceso a sus activos para los diferentes roles de usuarios, con el nivel de detalle y rigor de los controles que refleje los riesgos de seguridad de la información asociados.
- La política debe tener en cuenta lo siguiente:
  - ✓ las políticas para la diseminación y autorización de la información,
  - ✓ la legislación aplicable y cualquier obligación contractual relativa a la limitación de acceso a datos o servicios,
  - ✓ los requisitos para la revisión periódica de los derechos de acceso,
  - ✓ la retirada de los derechos de acceso,
  - ✓ los roles con derechos de acceso privilegiados.
- Las reglas de control de acceso deben estar detalladas en procedimientos formales.
- El control de acceso basado en roles es una aproximación utilizada con éxito por muchas organizaciones para vincular los derechos de acceso con las funciones desempeñadas en el negocio.
- Sólo se debe dar acceso a aquella información necesaria para realizar las tareas. Diferentes tareas/roles recogen diferentes 'necesidades de conocer' y por tanto diferentes perfiles de acceso.
- Respecto al acceso a las redes y a los servicios de red, únicamente se debe proporcionar a los usuarios el acceso a las redes y a los servicios en red para cuyo uso hayan sido específicamente autorizados.

Altas, Bajas y Modificaciones (ABM) de usuarios

Debe implantarse un procedimiento formal para asignar o revocar los derechos de acceso para todos los tipos de usuarios de todos los sistemas y servicios.

- El proceso para la gestión de los identificadores (IDs) de usuario debe contemplar el uso de identificadores (ID) de usuario únicos que le identifiquen y le hagan responsable de sus acciones; tan sólo debe permitirse el uso de identificadores (ID) compartidos cuando fuera necesario por razones del negocio o de operación y debe ser aprobado y quedar documentado
- Adaptar los derechos de acceso de usuarios que han cambiado de rol o de tareas y la eliminación o bloqueo inmediato de los derechos de acceso de los usuarios que han dejado la organización.
- Debe considerarse la inclusión de cláusulas en los contratos del personal y en los contratos de servicios que especifiquen las sanciones en caso de que el personal o los contratistas intenten realizar un acceso no autorizado.

Gestión de privilegios de acceso

La asignación y el uso de privilegios de acceso debe estar restringida y controlada.

- Deben identificarse los derechos de acceso privilegiados asociados a cada sistema o proceso, por ejemplo, sistema operativo, el sistema de gestión de base de datos y cada aplicación, junto con los usuarios a los que hay que asignarlos.
- Debe mantenerse un proceso de autorización y registro de todos los privilegios asignados y deben definirse los requisitos para el vencimiento de los derechos de acceso privilegiados.

- Los derechos de acceso privilegiados deben asignarse a un identificador (ID) de usuario diferente al usado en las actividades normales del negocio. Las actividades normales del negocio no deben ser ejecutadas desde un identificador (ID) privilegiado.

Gestión de la información secreta de autenticación de los usuarios

La asignación de la información secreta de autenticación debe ser controlada a través de un proceso formal de gestión.

- Mantener un registro central de derechos de acceso a sistemas de información y servicios concedidos a un identificador (ID) de usuario;
- Asegurar que los derechos de acceso no se activen (por ejemplo, por los proveedores de servicio) hasta concluir con los procedimientos de autorización.
- Se debe requerir a los usuarios la firma de un compromiso de mantener la confidencialidad de la información secreta para la autenticación personal, proporcionárseles inicialmente una autenticación temporal a cambiar obligatoriamente en el primer uso.
- Adaptar los derechos de acceso de usuarios que han cambiado de rol o de tareas y la eliminación o bloqueo inmediato de los derechos de acceso de los usuarios que han dejado la organización.

Responsabilidades del usuario

Se debe requerir a los usuarios que sigan las prácticas de la organización en el uso de la información secreta de autenticación.

- Los usuarios deben ser advertidos de:
  - ✓ mantener confidencial la información de autenticación, asegurando que no se divulgue a cualquier otra parte, incluyendo personas con autoridad;
  - ✓ evitar guardar (por ejemplo, en papel, en un fichero software o en un dispositivo portátil) la información secreta de autenticación;

- ✓ cambiar la información secreta de autenticación siempre que haya indicios de su posible compromiso;
- ✓ cuando se usen contraseñas como información secreta de autenticación, seleccionar contraseñas de calidad con una longitud mínima suficiente y que contengan letras (mayúsculas y minúsculas), números y caracteres especiales;
- ✓ no compartir la información secreta de autenticación individual del usuario;
- ✓ no usar la misma información secreta de autenticación para propósitos laborales y no laborales.

Control de acceso a sistemas y aplicaciones

Se debe prevenir el acceso no autorizado a los sistemas y aplicaciones.

- Cuando se requiera una autenticación y verificación robusta de la identidad deben usarse métodos de autenticación alternativos a las contraseñas, como, por ejemplo, medios criptográficos, tarjetas inteligentes, dispositivos hardware o medios biométricos.
- Un buen procedimiento de inicio de sesión debe:
  - ✓ no mostrar identificadores del sistema o aplicación hasta que el proceso de inicio de sesión se haya completado con éxito;
  - ✓ mostrar un aviso general de que únicamente deben acceder al ordenador los usuarios autorizados;
  - ✓ no proporcionar mensajes de ayuda durante el proceso de entrada que pudieran ayudar a un usuario no autorizado;
  - ✓ validar la información de inicio de sesión solo cuando se hayan completado todos los datos de entrada. Si ocurre alguna condición de error, el sistema no debe indicar qué parte del dato es correcta o incorrecta;
  - ✓ proteger contra los intentos de fuerza bruta de inicio de sesión;
  - ✓ registrar los intentos con y sin éxito ocurridos;

- ✓ generar un evento de seguridad cuando se detecte un intento potencial o con éxito de violación de los controles de inicio de sesión;
- ✓ no mostrar la contraseña que se está introduciendo;
- ✓ no transmitir por la red contraseñas sin cifrar;
- ✓ terminar las sesiones inactivas tras un periodo definido de inactividad (time out), especialmente en lugares de alto riesgo, como áreas públicas o externas que queden fuera de la gestión de la seguridad de la organización o en dispositivos móviles;
- ✓ restringir los tiempos de conexión para proporcionar una seguridad adicional a las aplicaciones de alto riesgo y reduciendo la ventana de oportunidad de los usuarios no autorizados.

- Controlar qué datos pueden ser accedidos por un usuario determinado.
- Controlar los derechos de acceso de los usuarios, por ejemplo, de lectura, de escritura, de borrado y de ejecución.
- Controlar los derechos de acceso de otras aplicaciones.

Sistema de gestión de contraseñas

Los sistemas para la gestión de contraseñas deben ser interactivos y establecer contraseñas seguras y robustas.

- Un sistema de gestión de contraseñas debe:
  - ✓ permitir a los usuarios escoger y cambiar sus propias;
  - ✓ imponer la selección de contraseñas de calidad;
  - ✓ forzar a los usuarios a cambiar sus contraseñas tras el primer inicio de sesión;
  - ✓ forzar los cambios regulares de contraseñas y bajo petición;
  - ✓ mantener un registro de las contraseñas usadas anteriormente y evitar su reutilización;
  - ✓ no mostrar las contraseñas en la pantalla cuando se estén introduciendo.

Política sobre clasificación de la información.

La información debe ser clasificada en términos de la importancia de su revelación frente a requisitos legales, valor, sensibilidad y criticidad ante revelación o modificación no autorizadas.

- Los propietarios de los activos de información deben ser responsables de su clasificación.
- El **esquema de clasificación** debe incluir normas para la clasificación y los criterios de revisión de la clasificación en el tiempo. El nivel de protección en el esquema debe ser evaluado analizando los requisitos de confidencialidad, integridad y disponibilidad y cualquier otro para la información considerada. El esquema debe estar alineado con la política de control de acceso

  Un ejemplo de esquema de clasificación de confidencialidad de la información podría basarse en cuatro niveles tales como:

  1. la revelación no conlleva daños;
  2. la revelación causa incomodidad menor o molestias operativas menores;
  3. la revelación tiene un impacto significativo a corto plazo sobre operaciones u objetivos tácticos;
  4. la revelación tiene un impacto serio sobre objetivos estratégicos a largo plazo o pone en riesgo la supervivencia de la organización.
- Debe desarrollarse e implantarse un conjunto adecuado de procedimientos para etiquetar la información, de acuerdo con el esquema de clasificación adoptado por la organización.
- Los procedimientos de etiquetado de la información deben contemplar la información y los activos relacionados tanto en soporte físico (etiquetas físicas) como electrónico (metadatos).

Información de salud a proteger (ISO/IEC 27.799)

En el caso de las instituciones de salud, existen varios tipos de información cuya confidencialidad, integridad y disponibilidad) necesitan ser protegidas:

a) la información personal de salud;
b) los datos seudonimizados obtenidos a partir de la información personal de salud a través de alguna metodología para la identificación de seudónimos;
c) los datos estadísticos y de investigación, incluyendo los datos anónimos obtenidos a partir de la información personal de salud
d) el conocimiento médico y/o clínico que no está relacionado con los sujetos del cuidado específicos, incluyendo los datos de apoyo a la decisión clínica (por ejemplo, los datos sobre los profesionales de la salud, el personal y los voluntarios;
e) la información relacionada con la supervisión de la salud pública;
f) los datos de rastros de auditoría, producidos por los sistemas de información de salud que contienen información personal de salud, datos seudonimizados obtenidos a partir de la información personal de salud, o que contienen datos acerca de las acciones de los usuarios en lo que respecta a información;
g) los datos de seguridad para los sistemas de información de salud, incluyendo datos de control de acceso y otros datos de configuración, relacionados a la seguridad, de los sistemas de información de salud.

<u>Clasificación de la información de salud</u>

- La confidencialidad de la información personal de salud es a menudo más subjetiva que objetiva. Es decir, en última instancia, sólo el titular de los datos (es decir, el sujeto del cuidado) puede hacer una determinación adecuada de la confidencialidad relativa de los

diferentes campos o grupos de datos. Por ejemplo, una persona que huye de una relación de abuso puede considerar su nueva dirección y número de teléfono mucho más confidenciales que los datos clínicos sobre su brazo roto.

- La confidencialidad de la información personal de salud depende del contexto. Por ejemplo, el nombre y dirección de un sujeto del cuidado en una lista de admitidos a la sala de emergencia de un hospital pueden no ser considerados especialmente confidenciales para esa persona; sin embargo, el mismo nombre y la dirección en una lista de admisión a una clínica para tratar la impotencia sexual pueden ser considerados altamente confidenciales por el individuo.
- Debido a que no se puede predecir la sensibilidad de un elemento dado de la información personal de salud a través de todos sus usos y todas las etapas de su ciclo de vida, se recomienda que toda la información personal de salud sea objeto de adecuada atención y protección en todo momento.

Política sobre seguridad física y ambiental.

Amenazas y vulnerabilidades de la seguridad de la información de salud (ISO/IEC 27.799).

Por su naturaleza, las organizaciones de salud operan en un entorno en el que los visitantes y el público en general nunca pueden ser totalmente excluidos.

En las grandes organizaciones de salud, el enorme volumen de personas que se desplazan a través de las zonas operativas es significativo. Estos factores aumentan la vulnerabilidad de los sistemas a las amenazas físicas.

La probabilidad de que esas amenazas se produzcan puede aumentar ante la presencia de pacientes o sus familiares con trastornos emocionales o mentales.

La confidencialidad de la información personal de salud puede cambiar a lo largo del tiempo en la historia clínica de un individuo. Por ejemplo, el cambio en las actitudes de la sociedad en los últimos 20 años ha dado lugar a que muchas personas dejen de considerar su orientación sexual como confidencial. Por el contrario, las actitudes hacia la drogadicción y el alcoholismo han hecho que algunos sujetos del cuidado consideren los datos sobre tratamientos de adicción aún más confidenciales hoy de lo que los habrían considerado hace 20 años.

Perímetro de seguridad física

Se deben utilizar perímetros de seguridad para proteger las áreas que contienen información sensible, así como los recursos de tratamiento de la información.

- Los perímetros de seguridad deben estar claramente definidos, y la situación y fortaleza de cada perímetro debe depender de los requisitos

de seguridad de los activos dentro del perímetro y de los resultados de la evaluación del riesgo;

- Los perímetros de un edificio o instalación que contiene los recursos de tratamiento de la información deben ser físicamente sólidos (por ejemplo, no deben existir huecos en el perímetro o áreas dónde pudieran producirse rupturas fácilmente); los tejados y muros externos y el solado del sitio deben ser de construcción sólida y todas las puertas externas deben estar adecuadamente protegidas contra los accesos no autorizados a través de mecanismos de control, por ejemplo barras, alarmas, cerraduras, etc.; las puertas y ventanas deben estar bloqueadas cuando no estén atendidas y se debe considerar una protección externa para las ventanas, en especial para las que se encuentran a nivel del suelo;
- Debe situarse un área de recepción atendida u otros controles de acceso físico a las instalaciones o al edificio; se deben restringir los accesos a las instalaciones y edificios únicamente al personal autorizado;
- Todas las puertas del perímetro de seguridad que actúen como cortafuegos deben estar dotadas de un sistema de alarma, monitorizadas y probadas conjuntamente con las paredes, para establecer el nivel requerido de resistencia de acuerdo a las normas regionales, nacionales e internacionales.

Controles físicos de entrada

Las áreas seguras deben estar protegidas mediante controles de entrada adecuados, para asegurar que únicamente se permite el acceso al personal autorizado.

- Se debe registrar la fecha y la hora de entrada y salida de los visitantes, y todos los visitantes deben ser supervisados a menos que su acceso haya sido previamente aprobado.

- El acceso a las áreas dónde se procesa o se almacena información sensible debe estar controlado y restringido únicamente a personal autorizado; se deben utilizar controles de autenticación para autorizar y validar todos los accesos, por ejemplo, implantando un mecanismo de doble factor de autenticación como tarjetas de control de acceso con número de identificación personal secreto (PIN)-
- Para el personal proveniente de terceros que prestan servicios de apoyo, se debe proporcionar acceso restringido a las áreas seguras o a los recursos de tratamiento de la información sensible únicamente cuando sea requerido; este acceso debe estar autorizado y controlado.

Seguridad de oficinas, despachos y recursos

Para las oficinas, despachos y recursos, se debe diseñar y aplicar la seguridad física.

- Se deben situar las instalaciones claves de manera que se evite el acceso por el público en general.
- Donde sea aplicable, los edificios deben proporcionar de una manera discreta una mínima indicación de su función, con señales no obvias, que identifiquen la existencia de actividades de tratamiento de la información, ya sea fuera o dentro del edificio.
- Las instalaciones deben configurarse para prevenir que las actividades o la información de tipo confidencial sean visibles o audibles desde el exterior.

Protección contra las amenazas externas y ambientales

Se debe diseñar y aplicar una protección física contra desastres naturales, ataques provocados por el hombre o accidentes.

- Se debe recabar asesoramiento especializado sobre cómo evitar daños causados por fuego, inundación, terremoto, explosión, revueltas

sociales y otras formas de desastres naturales o provocados por el hombre.

Seguridad de los equipos

Se debe evitar la pérdida, daño, robo o el compromiso de los activos y la interrupción de las operaciones de la organización

- Los equipos deben situarse de tal manera que se minimicen los accesos innecesarios a las áreas de trabajo.
- Los equipos de tratamiento de información que manejen datos sensibles se deben instalar donde se reduzca el riesgo de que la información sea vista durante su uso por personas no autorizadas.
- Las instalaciones de almacenamiento deben asegurarse para evitar los accesos no autorizados.
- se deben adoptar controles para minimizar el riesgo de posibles amenazas físicas y ambientales como, por ejemplo, robo, fuego, explosivos, humo, agua (o fallo de suministro de agua), polvo, vibración, agentes químicos, interferencias en el suministro eléctrico, interferencias en las comunicaciones, radiaciones electromagnéticas y vandalismo.
- Se deben controlar las condiciones ambientales, tales como la temperatura y la humedad, que puedan afectar negativamente al funcionamiento de los equipos de tratamiento de información.
- Se deben aplicar sistemas de protección contra rayos en todos los edificios y colocar filtros de protección contra rayos en todas las entradas de corriente eléctrica y en todas las líneas de comunicación.

Instalaciones de suministro

Los equipos deben estar protegidos contra fallos de alimentación y otras alteraciones causadas por fallos en las instalaciones de suministro.

- Los suministros de apoyo como, por ejemplo, electricidad, telecomunicaciones, agua, gas, aguas residuales, calefacción/ventilación y aire acondicionado, deben:
  - ✓ ser conformes a las especificaciones del fabricante de los equipos y a los requisitos legales locales;
  - ✓ ser evaluadas regularmente respecto a su capacidad para satisfacer el desarrollo de negocio y respecto a la interacción con otros servicios de apoyo;
  - ✓ ser inspeccionadas regularmente mediante las pruebas apropiadas para asegurar su correcto funcionamiento;
  - ✓ se sugiere, disponer de alarmas para detectar fallos en su funcionamiento;
  - ✓ se sugiere, disponer de múltiples fuentes con canales físicos de alimentación independientes.
- Debe proporcionarse alumbrado y comunicaciones de emergencia. Los interruptores y válvulas de emergencia para cortar el suministro de energía, agua, gas u otros servicios no deben estar ubicados cerca de las salidas de emergencia o de las salas de los equipos.

Seguridad del cableado

El cableado eléctrico y de telecomunicaciones que transmite datos o que sirve de soporte a los servicios de información deben estar protegido frente a interceptaciones, interferencias o daños.

- Se deben separar los cables de energía de los de comunicaciones para evitar interferencias;
- Se deben considerar medidas adicionales para sistemas sensibles o críticos, como:
  - ✓ instalación de conductos blindados y cajas o salas cerradas en los puntos de inspección y terminación,
  - ✓ uso de apantallamiento electromagnético para proteger los cables,

- ✓ implantación de barreras técnicas e inspecciones físicas para detectar la conexión al cableado de dispositivos no autorizados,
- ✓ accesos controlados a los paneles de parcheo y a las salas de cableado.

Mantenimiento de los equipos

Los equipos deben recibir un mantenimiento correcto que asegure su disponibilidad y su integridad continuas.

- los equipos deben mantenerse de acuerdo a las recomendaciones de intervalos de servicio y especificaciones del proveedor;
- sólo el personal de mantenimiento debidamente autorizado debe realizar la reparación y el servicio de los equipos;
- se deben mantener registros de todos los fallos, reales o sospechados, así como de todo el mantenimiento preventivo y correctivo;

Retirada de materiales propiedad de la empresa

Sin autorización previa, los equipos, la información o el software no deben retirarse de las instalaciones.

- los empleados y usuarios de terceras partes con permiso para sacar los activos fuera de las instalaciones deben estar claramente identificados;
- se deben establecer limitaciones al tiempo que el equipo puede estar fuera de las instalaciones y verificar a su retorno que se ha cumplido con dichas limitaciones;
- dónde sea necesario y adecuado, se debe registrar la salida de equipos fuera de los locales de la organización, así como su retorno;

Seguridad de los equipos fuera de las instalaciones

Deben aplicarse medidas de seguridad a los equipos situados fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos que conlleva trabajar fuera de dichas instalaciones.

- Cuando el equipo fuera de las instalaciones se transfiere entre diferentes individuos o entidades externas, se debe mantener un registro que defina la cadena de custodia de los equipos incluyendo, al menos, los nombres y las organizaciones de aquellos responsables de los equipos.
- La política de dispositivos móviles debe considerar:
  - ✓ el registro de dispositivos móviles;
  - ✓ los requisitos para la protección física;
  - ✓ las restricciones de instalación de software;
  - ✓ los controles de acceso;
  - ✓ la protección ante el software malicioso (malware);
  - ✓ la inhabilitación, el borrado y bloqueo remotos;
  - ✓ las copias de respaldo.

Reutilización o eliminación segura de equipos

Todos los soportes de almacenamiento deben ser comprobados para confirmar que todo dato sensible y software bajo licencia se ha eliminado de manera segura, antes de deshacerse de ellos.

- Debe comprobarse si los equipos contienen medios de almacenamiento o no antes de su retirada o reutilización.
- Los soportes que contengan información sensible o con derechos de autor deben ser destruidos físicamente o bien la información debe ser destruida, borrada o sobrescrita mediante técnicas que hagan imposible la recuperación de la información original, en lugar de utilizar un borrado o un formateado normal.

Política de puesto de trabajo despejado y pantalla limpia

Debe adoptarse una política de puesto de trabajo despejado de papeles y medios de almacenamiento desmontables y una política de pantalla limpia para los recursos de tratamiento de la información.

- la información de negocio sensible o crítica, por ejemplo, en papel o en soportes de almacenamiento electrónico, debe estar guardada (idealmente en una caja fuerte, armario u otro tipo de mueble de seguridad), cuando no se necesite, especialmente cuando la oficina esté vacía;
- los ordenadores y terminales deben quedarse apagados o protegidos mediante un mecanismo de bloqueo de pantalla y teclado controlado mediante una contraseña, dispositivo hardware o mecanismo similar de autenticación de usuario cuando estén desatendidos y deben estar protegidos mediante claves de bloqueo, contraseñas u otros controles cuando no están en uso;
- debe prevenirse el uso por usuarios no autorizados de fotocopias y otros dispositivos de reproducción (por ejemplo, escáneres, cámaras digitales);
- los soportes que contengan información sensible o clasificada deben retirarse de manera inmediata de las impresoras.

Políticas sobre Copias de seguridad de la información.

Se deben realizar copias de seguridad de la información, del software y del sistema y se deben verificar periódicamente de acuerdo a la política de copias de seguridad acordada.

- La política de respaldo debe definir los requisitos de conservación y protección.
- Deben proporcionarse los recursos adecuados para las copias de respaldo para asegurar que toda la información y software esenciales pueden ser recuperados después de un desastre o fallo de los soportes.
- Se deben producir registros precisos y completos de las copias de respaldo, así como de los procedimientos de recuperación documentados.
- La extensión (por ejemplo, copias totales o diferenciales) y frecuencia de las copias de respaldo deben reflejar los requisitos del negocio de la organización, los requisitos de seguridad de la información implicada y la criticidad de la información para el funcionamiento continuo de la organización.
- Las copias de respaldo deben ser almacenadas en un emplazamiento alejado, a una distancia suficiente para salvarse de cualquier daño proveniente de un desastre en el emplazamiento principal.
- La información de las copias de respaldo debe tener un nivel adecuado de protección tanto física como ambiental.
- Los soportes de las copias de respaldo deben ser comprobados periódicamente para asegurarse de que pueden responder en caso de uso de emergencia cuando sea necesario.
- En las situaciones donde es importante la confidencialidad, las copias de respaldo deben ser protegidas mediante cifrado.
- Los procedimientos operacionales deben supervisar la ejecución de copias de respaldo e identificar los fallos de realización de copias de

respaldo programadas para garantizar la integridad de las copias de respaldo, de acuerdo con la política de respaldo.

- Debe determinarse el periodo de conservación para la información esencial del negocio, teniendo en cuenta cualquier requisito para las copias de archivo que hayan de ser conservadas de manera permanente.

Políticas sobre transferencia de información.

Deben establecerse políticas, procedimientos y controles formales que protejan el intercambio de información mediante el uso de todo tipo de recursos de comunicación.

- Se deben diseñar procedimientos para:
  - ✓ proteger la información transferida de interceptación, copia, modificación, errores de enrutamiento y destrucción;
  - ✓ la detección y la protección contra el malware que podría ser transmitido a través del uso de comunicaciones electrónicas;
  - ✓ proteger información electrónica sensible que tiene la forma de adjuntos;
- Se deben utilizar técnicas criptográficas, por ejemplo, para proteger la confidencialidad, integridad y autenticidad de la información.
- Se deben implementar los controles y las restricciones asociadas con el uso de los recursos de comunicación, por ejemplo, reenvío automático del correo electrónico a las direcciones de correo externas.
- Debe recordarse al personal que no debe tener conversaciones confidenciales en lugares públicos o usando canales de comunicación inseguros, oficinas abiertas y lugares de reunión.
- Deben establecerse acuerdos para el intercambio seguro de información del negocio y software entre la organización y terceros.
- La información que sea objeto de mensajería electrónica debe estar adecuadamente protegida.
- Deben identificarse, documentarse y revisarse regularmente los requisitos de los acuerdos de confidencialidad o no revelación.

Políticas sobre protección ante el software malicioso (malware).

Se debe asegurar que los recursos de tratamiento de información y la información están protegidos contra el malware. Se deben implementar los controles de detección, prevención y recuperación que sirvan como protección contra el código malicioso, así como procedimientos adecuados de concienciación al usuario.

- Se debe prohibir el uso de software no autorizado.
- Se deben implementar controles para prevenir o detectar el uso de sitios web de los que se conoce o sospecha su carácter malicioso.
- Se debe instalar y actualizar software de detección y reparación de código malicioso para escanear los ordenadores y los dispositivos, como control preventivo o rutinario.
- Se deben preparar planes adecuados de continuidad de negocio para la recuperación de los ataques de código malicioso, incluyendo todos los datos y software de respaldo y disposiciones de recuperación necesarios.

Políticas sobre gestión de vulnerabilidades técnicas.

Se deben reducir los riesgos resultantes de la explotación de las vulnerabilidades técnicas.

- Se debe obtener información oportuna acerca de las vulnerabilidades técnicas de los sistemas de información utilizados, evaluar la exposición de la organización a dichas vulnerabilidades y adoptar las medidas adecuadas para afrontar el riesgo asociado.
- Deben adoptarse medidas adecuadas y oportunas en respuesta a la identificación de posibles vulnerabilidades técnicas.
- Identificada la vulnerabilidad técnica, la organización debe identificar los riesgos asociados y las medidas que deben adoptarse, las cuales podrían incluir el parcheo de sistemas vulnerables o la aplicación de otros controles.
- Los parches deben ser probados y evaluados antes de su instalación para garantizar que son efectivos y que no tienen efectos secundarios que no puedan ser aceptados.
- Se deben desactivar los servicios o capacidades relacionadas con la vulnerabilidad.
- Se deben adaptar o incluir los controles de acceso, como por ejemplo, cortafuegos, en los límites de la red.
- Definir un procedimiento para considerar la situación donde una vulnerabilidad ha sido identificada pero no es posible adoptar una contramedida. En esta situación, la organización debe evaluar los riesgos relativos a la vulnerabilidad conocida y definir acciones de detección y corrección adecuadas.

Políticas sobre controles criptográficos.

Se debe garantizar un uso adecuado y eficaz de la criptografía para proteger la confidencialidad, autenticidad y/o integridad de la información.

- Se recomienda consultar con un especialista al seleccionar los controles criptográficos que sean apropiados para cumplir con los objetivos de la política de seguridad de la información.
- Tomando como base la evaluación de los riesgos, debe identificarse el nivel de protección necesario, teniendo en cuenta el tipo, la fortaleza y la calidad del algoritmo de cifrado requerido.
- Debe tenerse en cuenta el enfoque de la gestión de las claves, incluyendo los métodos para ocuparse de la protección de las claves criptográficas y la recuperación de la información cifrada en caso de pérdida, vulneración o daño de las claves
- Se debe tener en cuenta revocar claves, incluyendo cómo deben retirarse o desactivarse las claves, por ejemplo, cuando éstas han sido comprometidas o cuando un usuario deja una organización (en cuyo caso, las claves también deben archivarse).
- Se debe registrar y auditar las actividades relacionadas con la gestión de las claves.

(La Norma ISO/IEC 11770 ofrece más información acerca de la gestión de claves)

Políticas sobre relaciones con proveedores.

Se debe asegurar la protección de los activos de la organización que sean accesibles a los proveedores.

- La organización debe identificar y encargar los controles de seguridad de información para abordar específicamente el acceso de los proveedores a la información de la organización.
- Se deben definir los tipos de acceso a la información que se permitirá a los diferentes tipos de proveedores, con su supervisión y su control del acceso.
- Se deben realizar sesiones de concienciación para el personal de la organización que participa en compras con respecto a las políticas, procesos y procedimientos aplicables.
- Se debe concientizar el personal de la organización que interactúa con el personal de los proveedores con respecto a las reglas apropiadas referentes al acuerdo y a las actuaciones según el tipo de proveedor y el nivel de acceso de proveedores a los sistemas y la información de la organización.
- Se deben fijar las condiciones bajo las que los requisitos y controles de seguridad de la información se documentarán en un acuerdo firmado por ambas partes.
- Todos los requisitos relacionados con la seguridad de la información deben establecerse y acordarse con cada proveedor que puede acceder, tratar, almacenar, comunicar, o proporcionar componentes de la infraestructura "Tecnología de la Información".
- Los acuerdos con proveedores deben incluir requisitos para hacer frente a los riesgos de seguridad de la información relacionados con las tecnologías de la información y las comunicaciones y con la cadena de suministro de productos.

Políticas sobre Gestión de incidentes de seguridad de la información y mejoras.

Se debe asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación de eventos de seguridad y debilidades

- Se deben establecer las responsabilidades y procedimientos de gestión para garantizar una respuesta rápida, efectiva y adecuada a los incidentes de seguridad de la información.
- Se deben establecerse responsabilidades a nivel de gestión para asegurar que los siguientes procedimientos se desarrollan y comunican adecuadamente dentro de la organización:
  1. procedimientos para la planificación y preparación de la respuesta a incidentes,
  2. procedimientos para monitorizar, detectar, analizar y comunicar eventos e incidentes de seguridad de la información,
  3. procedimientos para registrar las actividades de gestión de incidentes,
  4. procedimientos para el manejo de pruebas forenses,
  5. procedimientos para evaluar y tomar decisiones sobre eventos de seguridad y evaluar puntos débiles de la seguridad de la información,
  6. procedimientos de respuesta incluyendo aquellos relativos al escalado, recuperación controlada a partir de un incidente, y comunicación a personas internas y externas o a terceras organizaciones.
- Se deben establecer procedimientos que aseguren que:
  1. personal competente maneja los asuntos relacionados con los incidentes de seguridad de la información dentro de la organización,

2. se implante un punto de contacto para la detección y comunicación de incidentes de seguridad,
3. se mantienen contactos apropiados con las autoridades, grupos de interés externos o foros que tratan asuntos relacionados con los incidentes de seguridad de la información.

- Los procedimientos de comunicación deben incluir:
  1. la preparación de formularios de comunicación de eventos de seguridad de la información para apoyar la acción de comunicación y para ayudar a la persona que los comunique a recordar todas las acciones necesarias en caso de un evento de seguridad de la información,
  2. el comportamiento adecuado que debe tomarse en caso de un evento de seguridad de la información; por ejemplo, anotar inmediatamente todos los detalles importantes (como el tipo de incumplimiento, fallo de funcionamiento, mensajes en la pantalla...), informar inmediatamente al punto de contacto, y adoptar sólo acciones coordinadas,
  3. la referencia a un proceso disciplinario formal establecido para tratar a los trabajadores, contratistas o terceros que hayan cometido el quebrantamiento de la seguridad,
  4. procesos de retroalimentación adecuados para garantizar que aquellas personas que comuniquen eventos de seguridad de la información son informadas de los resultados después de que se haya tratado y cerrado el problema.

(Una guía detallada sobre la gestión de incidentes de seguridad de la información está disponible en la Norma ISO/IEC 27035)

FUENTE:

- ISO/IEC 27002
- ISO/IEC 27799