SEGURIDAD DE LOS EQUIPOS

Se busca prevenir la pérdida, daño, robo o compromiso de los equipos y la interrupción de las operaciones de la organización.

Colocación y protección del equipo
El equipo debería ser colocado y protegido para reducir los riesgos de amenazas ambientales y peligros, así como oportunidades de acceso no autorizado.

Deberían considerarse las siguientes recomendaciones para proteger el equipo:

a) el equipo debería colocarse para minimizar el acceso innecesario a las áreas de trabajo;

b) los recursos de procesamiento de la información que manejan datos sensibles deberían colocarse cuidadosamente para reducir el riesgo de que la información sea vista por personas no autorizadas durante su uso;

c) las instalaciones de almacenamiento deberían asegurarse para evitar el acceso no autorizado;

d) los elementos que requieran protección especial deberían salvaguardarse para reducir el nivel general de protección requerida;

e) deberían adoptarse controles para minimizar el riesgo de potenciales amenazas físicas y ambientales, tales como: hurto, fuego, explosivos, humo, agua (o falla en el suministro de agua), polvo, vibraciones, efectos químicos, interferencias en el suministro eléctrico, interferencia de las comunicaciones, radiación electromagnética, y vandalismo;

f) deberían emitirse directrices que regulen comer, beber y fumar en proximidad de las instalaciones de procesamiento de la información;

g) las condiciones ambientales, tales como temperatura y humedad, deberían supervisarse para verificar que no afecten negativamente el funcionamiento de los recursos de procesamiento de información;

h) debería instalarse protección contra rayos en todos los edificios y aplicar los filtros de protección contra rayos a todas las líneas entrantes de energía y de comunicaciones;

i) el uso de métodos de protección especial, tales como cubiertas para teclados, debería considerarse para el equipo ubicado en ambientes industriales;

j) debería protegerse el equipo que procese información confidencial para minimizar el riesgo de fuga de información debido a la emanación electromagnética.

Servicios de soporte
El equipo debería ser protegido contra fallas de energía u otras interrupciones causadas por fallas en los servicios de soporte

Los servicios de soporte (por ejemplo, la electricidad, las telecomunicaciones, el agua potable, el gas, el alcantarillado, la ventilación y el aire acondicionado) deberían:

a) cumplir con las especificaciones del fabricante de los equipos y con los requisitos legales locales;

b) ser evaluados regularmente en su capacidad para cumplir con el crecimiento del negocio y las interacciones con otros servicios de soporte;

c) ser inspeccionados y probados regularmente para asegurar su buen funcionamiento;

d) si es necesario, contar con alarmas para detectar fallos de funcionamiento;

e) si es necesario, tener múltiples fuentes de suministro con diversos enrutamientos físicos.

Deberían proporcionarse alumbrado y comunicaciones de emergencia. Los interruptores y las válvulas de emergencia para cortar la energía, el agua, el gas u otros servicios básicos deberían ubicarse cerca de las salidas de emergencia o de las salas de máquinas.

Se puede obtener redundancia adicional para la conectividad de redes mediante múltiples rutas de más de un proveedor de servicios básicos.

Seguridad en el cableado
El cableado de energía y de telecomunicaciones que transporta datos o soporta servicios de información, debería estar protegido de interceptación, interferencia o daño.

Deberían considerarse las siguientes guías para la seguridad en el cableado:

a) las líneas de energía y telecomunicaciones en instalaciones de procesamiento de la información deberían ser subterráneas, donde sea posible, o estar sujetas a una protección alternativa adecuada;

b) los cables de energía deberían separarse de los cables de comunicaciones para prevenir interferencias;

c) entre los controles adicionales a considerar para los sistemas sensibles o críticos se incluyen:

    1) instalación de conductos blindados y cuartos o gabinetes con cerradura en los puntos de inspección o terminación;

    2) uso de blindaje electromagnético para proteger los cables;

    3) iniciar barridos técnicos e inspecciones físicas contra dispositivos no autorizados conectados a los cables;

    4) acceso controlado a los paneles de conexión y a los cuartos de cableado.

Mantenimiento del equipo
El equipo debería tener un mantenimiento correcto para asegurarse de su continua disponibilidad e integridad.

SEGURIDAD DE LOS EQUIPOS

Deberían considerarse las siguientes guías para el mantenimiento del equipo:

a) al equipo se le debería dar mantenimiento de acuerdo con los intervalos y especificaciones de servicio recomendados por el proveedor.

b) sólo el personal de mantenimiento debidamente autorizado debería realizar reparaciones y realizar el mantenimiento a los equipos;

c) deberían mantenerse registros de todos los fallos, reales o sospechados, así como de todo el mantenimiento preventivo y correctivo;

d) se deberían implementar controles apropiados cuando el equipo esté calendarizado para mantenimiento, considerando si este mantenimiento es realizado por personal interno o externo a la organización; donde sea necesario la información confidencial debería borrarse de los equipos o el personal de mantenimiento debería ser suficientemente confiable;

e) debería cumplirse con todos los requisitos de mantenimiento impuestos por las pólizas de seguro.

f) antes de poner el equipo nuevamente en funcionamiento después de su mantenimiento, debería ser inspeccionado para asegurarse de que el equipo no haya sido manipulado y no tenga un mal funcionamiento.

Remoción de activos
El equipo, la información o el software no deberían ser llevados fuera del sitio sin autorización previa.

Deberían considerarse las siguientes guías:

a) deberían identificarse aquellos empleados y usuarios de partes externas que tengan autoridad para permitir el retiro de activos fuera de los locales de la organización;

b) deberían fijarse los límites de tiempo para el retiro del activo y verificar el cumplimiento del retorno;

c) cuando sea necesario y procedente, debería registrarse tanto la salida de los activos del local, como el retorno de éstos;

d) deberían documentarse la identidad, la función y la afiliación de cualquier persona que gestiona o utiliza activos, y esta documentación debería devolverse junto con el equipo, la información o el software.

Las instancias de inspección, establecidas para detectar el retiro no autorizado de activos, también se pueden utilizar para detectar dispositivos no autorizados tales como; equipos de grabación, armas, entre otros y para prevenir su ingreso y salida del sitio. Tales instancias de inspección deberían realizarse de acuerdo con la legislación y las regulaciones pertinentes. Las personas deberían estar en conocimiento de que estas instancias de inspección, serán llevadas a cabo, y las verificaciones deberían realizarse solamente con la autorización apropiada según los requisitos legales y reglamentarios.

SEGURIDAD DE LOS EQUIPOS

Seguridad del equipo y los activos fuera de las instalaciones
Se debería aplicar seguridad a los activos que salen de las instalaciones tomando en cuenta los diferentes riesgos de trabajar fuera de las instalaciones de la organización.

El uso de cualquier equipo que almacene o procese información fuera de las instalaciones de la organización, debería ser autorizado por la dirección. Esto se aplica a los equipos propiedad de la organización y al equipo de propiedad privada utilizado en nombre de la organización.

Deberían considerarse las siguientes guías para la protección de los equipos fuera de las instalaciones de la organización:

a) los equipos y medios que sean llevados fuera de las instalaciones no deberían dejarse desatendidos en sitios públicos;

b) deberían observarse siempre las instrucciones del fabricante para proteger los equipos, por ejemplo, contra exposiciones a campos electromagnéticos intensos;

c) los controles para las ubicaciones fuera de las instalaciones, tales como el trabajo en el domicilio, el teletrabajo y los sitios temporales deberían ser determinados por una evaluación del riesgo y aplicar cuando sea apropiado los controles convenientes, por ejemplo, gabinetes con cerradura para archivar, una política de escritorios limpios, controles de acceso a las computadoras y comunicaciones seguras con la oficina;

d) cuando el equipo ubicado fuera de las instalaciones es transferido entre diferentes personas o partes externas, debería mantenerse un registro que defina la cadena de custodia para el equipo, incluyendo como mínimo, los nombres y las organizaciones de aquellos que son responsables del equipo.

Los riesgos, por ejemplo, de daño, hurto o espionaje, pueden variar considerablemente entre las ubicaciones y éstos deberían tomarse en cuenta para determinar los controles más adecuados.

El equipo de almacenamiento y procesamiento de la información comprende todo tipo de computadoras personales, organizadores, teléfonos móviles, tarjetas inteligentes, documentos u otros, que se lleven para trabajar en el hogar o fuera del lugar habitual de trabajo.

Puede ser apropiado evitar el riesgo desalentando a ciertos empleados a trabajar fuera de las instalaciones o restringiendo el uso del equipo de TI portátil.

Seguridad en la eliminación o reutilización del equipo
Todas las partes del equipo que contienen medios de almacenamiento deberían ser verificadas para asegurarse de que cualquier dato sensible o software licenciado haya sido removido o sobrescrito de manera segura antes de la eliminación o reutilización.

Los equipos deberían verificarse para asegurarse de que contengan o no medios de almacenamiento antes de su eliminación o reutilización.

SEGURIDAD DE LOS EQUIPOS

Los dispositivos de almacenamiento con información confidencial o sujeta a derechos de autor deberían destruirse físicamente o la información debería destruirse, borrarse o sobrescribirse usando técnicas para hacer que la información original no sea recuperable, en lugar de utilizar las funciones de borrado o formateado estándar.

Los equipos dañados que contengan medios de almacenamiento, pueden requerir una evaluación de riesgo para determinar si estos deberían destruirse físicamente en lugar de ser enviados a reparar o ser desechados. La información puede verse comprometida si la reutilización o eliminación de los equipos se realiza de manera descuidada.

Además del borrado seguro del disco, cifrar todo el disco reduce el riesgo de divulgación de información confidencial, cuando los equipos son eliminados o reutilizados, siempre que:

a) el proceso de cifrado sea lo suficientemente fuerte y cubra todo el disco (incluyendo el espacio libre, los archivos de intercambio, entre otros);

b) las llaves del cifrado sean lo suficientemente largas como para resistir ataques de fuerza bruta;

c) las llaves del cifrado se mantengan confidenciales (por ejemplo, nunca almacenadas en el mismo disco).

Las técnicas para una sobrescritura segura de los medios de almacenamiento difieren de acuerdo con la tecnología de tales medios. Las herramientas de sobrescritura deberían revisarse para garantizar que sean aplicables a la tecnología de los medios de almacenamiento.

Equipo desatendido por el usuario
Los usuarios deberían asegurarse de que el equipo desatendido tenga la protección adecuada.

Todos los usuarios deberían ser advertidos de los requisitos y procedimientos de seguridad para proteger equipo desatendido, así como de su responsabilidad de implementar tal protección. Debería advertirse a los usuarios sobre:

a) terminar sesiones activas cuando finalice, salvo que se les pueda asegurar por un mecanismo de bloqueo apropiado, por ejemplo, un protector de pantalla protegido con contraseña;
b) cuando ya no sea necesario desconectarse de aplicaciones o de servicios de red;
c) proteger de uso no autorizado las computadoras o dispositivos móviles mediante una clave de bloqueo o un control equivalente, por ejemplo, contraseña de acceso, cuando no se encuentran en uso.

Política de pantalla y escritorio limpios
Se debería adoptar una política de escritorio limpio de papeles y medios de almacenamiento removibles y una política de pantalla limpia para los recursos de procesamiento de la información.

Una política de pantalla y escritorio limpios debería tomar en cuenta la clasificación de la información, requisitos legales y contractuales, y los correspondientes aspectos culturales y de riesgo de la organización. Deberían considerarse las siguientes guías:

a) cuando no se requiere la información sensible o crítica del negocio, contenida, por ejemplo, en medios de almacenamiento electrónicos o en papel, debería asegurarse bajo llave (idealmente una caja de seguridad, un gabinete u otro mueble de seguridad), especialmente cuando la oficina está desocupada;

b) cuando están desatendidas las computadoras y terminales deberían cerrarse las sesiones o protegerlas con un mecanismo de bloqueo de pantalla y teclado controlado por contraseña, hardware de autenticación, o mecanismo similar de autenticación de usuario, y debería protegerse por llaves de bloqueo, o contraseñas u otros controles cuando no están en uso;

c) debería prevenirse el uso no autorizado de fotocopiadoras y otras tecnologías de reproducción (por ejemplo, escáneres, cámaras digitales);

d) los medios que contienen información sensible o clasificada deberían retirarse de las impresoras inmediatamente.

Una política de escritorio y pantalla limpios, reduce los riesgos de acceso no autorizado, pérdida o daño a la información durante y fuera de las horas normales de trabajo. Las cajas de seguridad u otras formas de almacenamiento seguro pueden también proteger información almacenada dentro de ellas contra desastres tales como incendios, terremotos, inundaciones o explosiones.

Considerar el uso de impresoras con una función de código de número de identificación personal (PIN), de modo que quienes generaron los documentos sean los únicos que puedan obtener las impresiones y solamente estando junto a la impresora.