SEGURIDAD FÍSICA Y AMBIENTAL

Áreas seguras
Se busca prevenir el acceso físico no autorizado, daños e interferencia a la información y a los recursos de procesamiento de la información de la organización.

Perímetro de seguridad física
Se deberían definir y usar perímetros de seguridad para proteger áreas que contienen información sensible o crítica y recursos de procesamiento de la información.

Deberían considerarse e implementarse las siguientes recomendaciones sobre los perímetros de seguridad física, según corresponda:

a) los perímetros de seguridad deberían ser definidos, y la ubicación y la fortaleza de cada uno de los perímetros debería depender de los requisitos de la seguridad de los activos dentro del perímetro y de los resultados de una evaluación de riesgos;

b) los perímetros de un edificio o un lugar que contenga instalaciones de procesamiento de información, debería tener solidez física (por ejemplo no debería haber espacios en el perímetro y no tener zonas que puedan derribarse fácilmente); los techos exteriores, los muros, paredes y pisos del lugar deberían ser sólidos y todas las puertas exteriores deberían estar convenientemente protegidas contra accesos no autorizados mediante mecanismos de control, (por ejemplo, barras, alarmas y cerraduras); puertas y ventanas deberían estar bajo llave cuando se encuentran desatendidas y debería considerarse protección externa para las ventanas particularmente a nivel de suelo;

c) debería existir un área de recepción atendida u otros medios para controlar el acceso físico al sitio o edificio; dicho acceso debería ser restringido sólo a personal autorizado;

d) donde sea aplicable, deberían construirse barreras físicas para evitar el acceso físico no autorizado y la contaminación del entorno;

e) todas las puertas contra incendios del perímetro de seguridad deberían tener alarma, ser supervisadas y probadas conjuntamente con las paredes para establecer el nivel requerido de resistencia de acuerdo a las normas regionales, nacionales, e internacionales apropiadas; deberían funcionar de acuerdo con las disposiciones locales de protección contra el fuego de tal modo que garanticen la seguridad;

f) Deberían instalarse sistemas de detección de intrusos adecuados según las normas nacionales, regionales o internacionales y probarlos regularmente para que abarquen todas las puertas externas y ventanas accesibles; las áreas desocupadas deberían tener alarmas en todo momento; también debería abarcar protección para otras áreas, por ejemplo, sala de computadoras o de comunicaciones;

g) las instalaciones de procesamiento de información gestionadas por la organización deberían separarse físicamente de aquellas gestionadas por partes externas.

La protección física puede ser alcanzada creando una o más barreras físicas alrededor de las instalaciones de la organización y de los recursos de procesamiento de la información. El uso de múltiples barreras brinda protección adicional, donde el fallo de una sola barrera no significa que la seguridad se vea comprometida inmediatamente.

Un área segura puede ser una oficina bajo llave, o varias habitaciones rodeadas por una barrera interna continua de seguridad física. Las barreras adicionales y los perímetros para controlar el acceso físico pueden ser necesarios entre áreas con diferentes requisitos de seguridad dentro del perímetro de seguridad. Deberían tenerse consideraciones especiales de seguridad de acceso físico en los edificios donde existen activos de múltiples organizaciones.

La aplicación de controles físicos, especialmente para las áreas seguras, debería adaptarse a las circunstancias técnicas y económicas de la organización, según se establece en la evaluación de riesgos.

Controles de entrada física
Las áreas seguras deberían ser protegidas por medio de controles de entrada apropiados para asegurarse de que el acceso sea permitido solamente a personal autorizado.

Deberían considerarse las siguientes recomendaciones:

a) la fecha y hora de entrada y salida de visitantes debería ser registrada, y todos los visitantes deberían supervisarse a menos que su acceso se haya aprobado previamente; el acceso debería concederse sólo para propósitos especificados y autorizados, proporcionándoles instrucciones sobre los requisitos de seguridad del área y los procedimientos de emergencia. La identidad de los visitantes debería ser autenticada por un medio adecuado;

b) el acceso a las áreas donde se procesa o se almacena la información confidencial debería ser restringido solo a las personas autorizadas mediante la implementación de controles de acceso apropiados, por ejemplo, mediante la implementación de un mecanismo de autenticación de dos factores, tales como tarjetas de acceso o tarjetas con número de identificación personal (PIN);

c) debería mantenerse y supervisarse de manera segura una bitácora de registro físico o una pista de auditoría electrónica;

d) todos los empleados, contratistas y partes externas deberían ser obligados a utilizar algún tipo de identificación visible y deberían notificar inmediatamente al personal de seguridad si encuentran a visitantes no acompañados y a cualquier persona que no lleve la identificación visible;

e) debería concederse el acceso de manera restringida al personal de soporte de partes externas a las áreas seguras o a las instalaciones sensibles de procesamiento de la información sólo cuando sea requerido; este acceso debería ser autorizado y supervisado;

f) los derechos de acceso a las áreas seguras deberían ser regularmente revisados y actualizados, y revocados cuando sea necesario.

Aseguramiento de oficinas, salas e instalaciones
La seguridad física para oficinas, salas e instalaciones debería ser diseñada y aplicada.

Deberían considerarse las siguientes recomendaciones para asegurar oficinas, salas, e instalaciones:

a) las instalaciones claves deberían situarse de manera tal que se evite el acceso al público;

b) cuando corresponda, los edificios deberían ser discretos y dar el mínimo indicio de su propósito, cuando sea posible, sin dar muestras obvias, fuera o dentro del edificio, que identifiquen la presencia de las actividades de procesamiento de la información;

c) las instalaciones deberían estar configuradas para prevenir que la información confidencial o las actividades sean visibles y audibles desde el exterior. Cuando corresponda, también debería considerarse el blindaje electromagnético adecuado;

d) las guías telefónicas y las listas de teléfonos internos que identifican ubicaciones de instalaciones de procesamiento de información confidencial, no deberían ser fácilmente accesibles por personas no autorizadas.

Protección contra amenazas externas y ambientales
La protección física contra desastres naturales, ataques maliciosos o accidentes debería ser diseñada y aplicada.

Debería obtenerse asesoramiento especializado sobre cómo evitar los daños causados por incendios, inundaciones, terremotos, explosiones, disturbios civiles y otras formas de desastres naturales o causados por personas.

Trabajando en áreas seguras
Se deberían diseñar y aplicar procedimientos para trabajar en áreas seguras.

Deberían considerarse las siguientes recomendaciones:

a) el personal sólo debería conocer la existencia de un área segura, o de sus actividades, sobre la base de la necesidad de saber;

b) el trabajo sin supervisión en las áreas seguras, debería evitarse por motivos de seguridad y para prevenir las oportunidades de actividades maliciosas;

c) las áreas seguras desocupadas, deberían estar físicamente cerradas y periódicamente revisadas;

d) no debería permitirse la presencia de equipos de fotografía, video, audio y otros equipos de grabación, tales como, cámaras en dispositivos móviles, salvo autorización expresa.

Los acuerdos para trabajar en áreas seguras incluyen controles para los empleados y los usuarios de partes externas y cubren todas las actividades que tienen lugar en esas áreas.

Áreas de entrega y carga
Se deberían controlar los puntos de acceso tales como áreas de entrega y carga y otros puntos por donde podrían entrar personas no autorizadas a las instalaciones y si es posible, aislarlos de los recursos de procesamiento de la información para evitar accesos no autorizados.

Deberían considerarse las siguientes recomendaciones:

a) el acceso al área de entrega y carga desde fuera del edificio debería ser limitado al personal identificado y autorizado;

b) el área de entrega y carga debería diseñarse para que los suministros puedan cargarse y descargarse sin que el personal de entrega tenga acceso a otras zonas del edificio;

c) las puertas externas del área de entrega y carga deberían ser aseguradas cuando las puertas internas estén abiertas;

d) el material entrante debería inspeccionarse y examinarse en busca de explosivos, químicos u otros materiales peligrosos, antes de que se lleve al área de entrega y carga;

e) el material entrante debería registrarse de acuerdo con el procedimiento de gestión de activos al entrar en el lugar;

f) cuando sea posible, los envíos entrantes y salientes deberían segregarse físicamente;

g) el material entrante debería inspeccionarse para saber si hay pruebas de manipulación en ruta. Si se descubre tal manipulación, se le debería notificar inmediatamente al personal de seguridad.