MNEMO

Anexo 11

SEGURIDAD FÍSICA Y AMBIENTAL

Dentro de esta área se localizan los siguientes objetivos y principios, controles y posibles mediciones asociadas:

A7.1	Perímetros de seguridad física
Objetivo	Los perímetros de seguridad deberían definirse y utilizarse para proteger las áreas que contienen información y otros activos asociados.
Principios	Impedir el acceso físico no autorizado, los daños y las interferencias en la información de la organización y otros activos asociados. Se deben utilizar perímetros de seguridad para proteger las áreas que contienen información sensible así como los recursos de tratamiento de la información. Los servicios de procesamiento de información sensible deberían ubicarse en áreas seguras y protegidas en un perímetro de seguridad definido por barreras y controles de entrada adecuados. Estas áreas deberían estar protegidas físicamente contra accesos no autorizados, daños e interferencias. La protección suministrada debería estar acorde con los riesgos identificados.
Información	El estándar parece centrarse en el CPD, pero hay muchas otras áreas vulnerables a considerar, p. ej., armarios de cableado, "servidores departamentales" y archivos (recuerde: los estándares se refieren a asegurar la información, no sólo las TI). Examine la entrada y salida de personas a/de su organización. ¿Hasta dónde podría llegar el repartidor de pizza o el mensajero sin ser parado, identificado y acompañado? ¿Qué podrían ver, llevarse o escuchar mientras están dentro? Algunas organizaciones usan tarjetas de identificación de colores para indicar las áreas accesibles por los visitantes (p. ej., azul para la

A7.1	Perímetros de seguridad física
	1ª planta, verde para la 3ª, etc.; ahora, si ve a alguien con una identificación verde en la 4º planta, reténgalo). Asegúrese de retirar todos los pases de empleado y de visita cuando se vayan. Haga que los sistemas de acceso con tarjeta rechacen y alarmen ante intentos de acceso. Use pases de visita que se vuelvan opacos o muestren de alguna manera que ya no son válidos a las x horas de haberse emitido. Debe definirse una Normativa Interna donde se indique que todo visitante debe estar acompañado, dentro de las instalaciones de la organización. Las siguientes directrices deben ser consideradas e implementadas cuando sea apropiado para los perímetros de seguridad física: a) definir los perímetros de seguridad y el emplazamiento y la resistencia de cada uno de los perímetros de acuerdo con los requisitos de seguridad de la información relacionados con los activos dentro del perímetro; b) disponer de perímetros físicamente sólidos para un edificio o emplazamiento que contenga instalaciones de tratamiento de la información (es decir, no debe haber huecos en el perímetro ni zonas en las que pueda producirse fácilmente un robo). Los tejados, paredes, techos y suelos exteriores del recinto deben ser de construcción sólida y todas las puertas exteriores deben estar convenientemente protegidas contra el acceso no autorizado con mecanismos de control (por ejemplo, barras, alarmas, cerraduras). Las puertas y ventanas deberán estar cerradas con llave cuando no estén vigiladas y deberá considerarse la posibilidad de instalar una protección externa en las ventanas, sobre todo a nivel del suelo; también deberán tenerse en cuenta los puntos de ventilación; c) alarma, control y prueba de todas las puertas cortafuegos en un perímetro de seguridad junto con las paredes para establecer el nivel de resistencia requerido de acuerdo con las normas adecuadas. Deben funcionar a prueba de fallos.

A7.1	Perímetros de seguridad física
	La protección física puede lograrse creando una o más barreras físicas alrededor de los locales de la organización y de las instalaciones de procesamiento de la información.
Medición	Informes de inspecciones periódicas de seguridad física de instalaciones, incluyendo actualización regular del estado de medidas correctivas identificadas en inspecciones previas que aún estén pendientes

A7.2	Entrada física
Objetivo	Las áreas seguras deberían estar protegidas por controles de entrada y puntos de acceso adecuados.
Principios	Garantizar que sólo se produce el acceso físico autorizado a la información de la organización y a otros activos asociados. Las áreas seguras deben estar protegidas mediante controles de entrada adecuados, para asegurar que únicamente se permite el acceso al personal autorizado. Deben controlarse los puntos de acceso tales como las áreas de carga y descarga y otros puntos, donde pueda acceder personal no autorizado a las instalaciones, y si es posible, aislar dichos puntos de los recursos de tratamiento de la información para evitar accesos no autorizados. Los servicios de procesamiento de información sensible deberían ubicarse en áreas seguras y protegidas en un perímetro de seguridad definido por barreras y controles de entrada adecuados. Estas áreas deberían estar protegidas físicamente contra accesos no autorizados, daños e interferencias. La protección suministrada debería estar acorde con los riesgos identificados.

A7.2	Entrada física
Información	El estándar parece centrarse en el CPD, pero hay muchas otras áreas vulnerables a considerar, p. ej., armarios de cableado, "servidores departamentales" y archivos (recuerde: los estándares se refieren a asegurar la información, no sólo las TI). Examine la entrada y salida de personas a/de su organización. ¿Hasta dónde podría llegar el repartidor de pizza o el mensajero sin ser parado, identificado y acompañado? ¿Qué podrían ver, llevarse o escuchar mientras están dentro? Algunas organizaciones usan tarjetas de identificación de colores para indicar las áreas accesibles por los visitantes (p. ej., azul para la 1ª planta, verde para la 3ª, etc.; ahora, si ve a alguien con una identificación verde en la 4º planta, reténgalo). Asegúrese de retirar todos los pases de empleado y de visita cuando se vayan. Haga que los sistemas de acceso con tarjeta rechacen y alarmen ante intentos de acceso. Use pases de visita que se vuelvan opacos o muestren de alguna manera que ya no son válidos a las x horas de haberse emitido. Debe definirse una Normativa Interna donde se indique que todo visitante debe estar acompañado, dentro de las instalaciones de la organización.
Medición	Informes de inspecciones periódicas de seguridad física de instalaciones, incluyendo actualización regular del estado de medidas correctivas identificadas en inspecciones previas que aún estén pendientes

A7.3	Aseguramiento de oficinas, salas e instalaciones
Objetivo	Se deberían diseñar e implementar seguridad física para oficinas, salas e instalaciones.
Principios	Impedir el acceso físico no autorizado, los daños y las interferencias en la información de la organización y otros activos asociados en oficinas, salas e instalaciones. Para las oficinas, despachos y recursos, se debe diseñar y aplicar la seguridad física. Los servicios de procesamiento de información sensible deberían ubicarse en áreas seguras y protegidas en un perímetro de seguridad definido por barreras y controles de entrada adecuados. Estas áreas deberían estar protegidas físicamente contra accesos no autorizados, daños e interferencias. La protección suministrada debería estar acorde con los riesgos identificados.
Información	El estándar parece centrarse en el CPD, pero hay muchas otras áreas vulnerables a considerar, p. ej., armarios de cableado, "servidores departamentales" y archivos (recuerde: los estándares se refieren a asegurar la información, no sólo las TI). Examine la entrada y salida de personas a/de su organización. ¿Hasta dónde podría llegar el repartidor de pizza o el mensajero sin ser parado, identificado y acompañado? ¿Qué podrían ver, llevarse o escuchar mientras están dentro? Algunas organizaciones usan tarjetas de identificación de colores para indicar las áreas accesibles por los visitantes (p. ej., azul para la 1ª planta, verde para la 3ª, etc.; ahora, si ve a alguien con una identificación verde en la 4° planta, reténgalo). Asegúrese de retirar todos los pases de empleado y de visita cuando se vayan. Haga que los sistemas de acceso con tarjeta rechacen y alarmen ante intentos de acceso. Use pases de visita que se vuelvan opacos o muestren de alguna manera que ya no son válidos a las xxx horas de haberse emitido.

A7.3	Aseguramiento de oficinas, salas e instalaciones
	Debe definirse una Normativa Interna donde se indique que todo visitante debe estar acompañado, dentro de las instalaciones de la organización.
Medición	Informes de inspecciones periódicas de seguridad física de instalaciones, incluyendo actualización regular del estado de medidas correctivas identificadas en inspecciones previas que aún estén pendientes.

A7.5	Protección contra amenazas físicas y ambientales
Objetivo	Se debe diseñar e implementar protección contra amenazas físicas y ambientales, como desastres naturales y otras amenazas físicas intencionales o no
Principios	Prevenir o reducir las consecuencias de los eventos originados por las amenazas físicas y ambientales. Se debe diseñar y aplicar una protección física contra desastres naturales, ataques provocados por el hombre o accidentes. Los servicios de procesamiento de información sensible deberían ubicarse en áreas seguras y protegidas en un perímetro de seguridad definido por barreras y controles de entrada adecuados. Estas áreas deberían estar protegidas físicamente contra accesos no autorizados, daños e interferencias. La protección suministrada debería estar acorde con los riesgos identificados.
Información	El estándar parece centrarse en el CPD, pero hay muchas otras áreas vulnerables a considerar, p. ej., armarios de cableado, "servidores departamentales" y archivos (recuerde: los estándares se refieren a asegurar la información, no sólo las TI). Examine la entrada y salida de personas a/de su organización. ¿Hasta dónde podría llegar el repartidor de pizza o el mensajero sin

A7.5	Protección contra amenazas físicas y ambientales
	ser parado, identificado y acompañado? ¿Qué podrían ver, llevarse o escuchar mientras están dentro? Algunas organizaciones usan tarjetas de identificación de colores para indicar las áreas accesibles por los visitantes (p. ej., azul para la 1ª planta, verde para la 3ª, etc.; ahora, si ve a alguien con una identificación verde en la 4° planta, reténgalo). Asegúrese de retirar todos los pases de empleado y de visita cuando se vayan. Haga que los sistemas de acceso con tarjeta rechacen y alarmen ante intentos de acceso. Use pases de visita que se vuelvan opacos o muestren de alguna manera que ya no son válidos a las x horas de haberse emitido. Debe definirse una Normativa Interna donde se indique que todo visitante debe estar acompañado, dentro de las instalaciones de la organización. Las cajas fuertes u otras formas de instalaciones de almacenamiento seguro pueden proteger la información almacenada en ellas contra catástrofes como un incendio, un terremoto, una inundación o una explosión. Las organizaciones pueden tener en cuenta los conceptos de prevención de la delincuencia a través del diseño ambiental a la hora de diseñar los controles para asegurar su entorno y reducir las amenazas urbanas. Por ejemplo, en lugar de utilizar bolardos, las estatuas o los elementos de agua pueden servir tanto de elemento como de barrera física.
Medición	Informes de inspecciones periódicas de seguridad física de instalaciones, incluyendo actualización regular del estado de medidas correctivas identificadas en inspecciones previas que aún estén pendientes.

A.7.1, A.7.2, A.7.3, A.7.5, A.7.6	Áreas seguras
Objetivo	Evitar el acceso físico no autorizado, daños o intromisiones en las instalaciones y a la información de la organización.
Principios	Los servicios de procesamiento de información sensible deberían ubicarse en áreas seguras y protegidas en un perímetro de seguridad definido por barreras y controles de entrada adecuados. Estas áreas deberían estar protegidas físicamente contra accesos no autorizados, daños e interferencias. La protección suministrada debería estar acorde con los riesgos identificados.
Información	El estándar parece centrarse en el CPD pero hay muchas otras áreas vulnerables a considerar, p. Ej., armarios de cableado, "servidores departamentales" y archivos (recuerde: los estándares se refieren a asegurar la información, no sólo las tic). Examine la entrada y salida de personas a/de su organización. ¿hasta dónde podría llegar el repartidor de pizza o el mensajero sin ser parado, identificado y acompañado? ¿qué podrían ver, llevarse o escuchar mientras están dentro? Algunas organizaciones usan tarjetas de identificación de colores para indicar las áreas accesibles por los visitantes (p. Ej., azul para la 1ª planta, verde para la 3ª, etc.; ahora, si ve a alguien con una identificación verde en la 4º planta, reténgalo). Siempre será la mejor opción que el visitante esté todo el tiempo acompañado dentro de las instalaciones.

A.7.1, A.7.2, A.7.3, A.7.5, A.7.6	Áreas seguras
	Asegúrese de retirar todos los pases de empleado y de visita cuando se vayan. Haga que los sistemas de acceso con tarjeta rechacen y alarmen ante intentos de acceso. Use pases de visita que se vuelvan opacos o muestren de alguna manera que ya no son válidos a las x horas de haberse emitido.
Medición	Informes de inspecciones periódicas de seguridad física de instalaciones, incluyendo actualización regular del estado de medidas correctivas identificadas en inspecciones previas que aún estén pendientes.

A11.2	Seguridad de los equipos
Objetivo	Evitar la pérdida, daño, robo o puesta en peligro de los activos e interrupción de las actividades de la organización.
Principios	Deberían protegerse los equipos contra las amenazas físicas y ambientales. La protección del equipo es necesaria para reducir el riesgo de acceso no autorizado a la información y su protección contra pérdida o robo. Así mismo, se debería considerar la ubicación y eliminación de los equipos. Se podrían requerir controles especiales para la protección contra amenazas físicas y para salvaguardar servicios de apoyo como energía eléctrica e infraestructura del cableado.

A11.2	Seguridad de los equipos
Información	Haga que los vigilantes de seguridad impidan a cualquiera (empleados, visitas, personas de soporte TI, mensajeros, personal de mudanzas, etc.), sacar equipos informáticos de las instalaciones sin autorización escrita. Conviértalo en un elemento disuasorio visible mediante chequeos aleatorios (o, incluso, arcos de detección de metales). Esté especialmente atento a puertas traseras, rampas de carga, salidas para fumadores, etc. Tome en consideración el uso de códigos de barras para hacer los chequeos más eficientes. Asimismo, debería considerar la utilización de un sistema de RFID
Medición	De chequeos (a personas a la salida y a existencias en stock) realizados en el último mes y porcentaje de chequeos que evidenciaron movimientos no autorizados de equipos o soportes informáticos u otras cuestiones de seguridad.