SEGURIDAD FISICA.

INTRODUCCIÓN Y ANTECEDENTES:

Es muy importante ser consciente que por más que nuestra empresa sea la más segura desde el punto de vista de ataques externos, Hackers, virus, etc. (conceptos luego tratados); la seguridad de la misma será nula si no se ha previsto como combatir un incendio.

La seguridad física es uno de los aspectos más olvidados a la hora del diseño de un sistema informático. Si bien algunos de los aspectos tratados a continuación se prevén, otros, como la detección de un atacante interno a la empresa que intenta a acceder físicamente a una sala de operaciones de la misma, no.

Esto puede derivar en que para un atacante sea más fácil lograr tomar y copiar una cinta de la sala, que intentar acceder vía lógica a la misma. No será la primera vez que se mencione en este trabajo, que cada sistema es único y por lo tanto la política de seguridad a implementar no será única. Este concepto vale, también, para el edificio en el que nos encontramos. Es por ello que siempre se recomendarán pautas de aplicación general y no procedimientos específicos.

Las principales amenazas que se prevén en la seguridad física son:

- Desastres naturales, incendios accidentales tormentas e inundaciones.
- Amenazas ocasionadas por el hombre.
- Disturbios, sabotajes internos y externos deliberados.

OBJETIVOS.

La seguridad lógica trata de conseguir los siguientes objetivos:

Impedir accesos no autorizados, daños e interferencia en las sedes e información de la empresa, por lo que se recomienda la implementación de políticas de escritorios y pantallas limpias para reducir estos riesgos, además las instalaciones de procesamiento de información crítica o sensible deben estar en áreas protegidas con un perímetro de seguridad definido por: vallas y controles de acceso apropiados “La protección debe ser proporcional a los riesgos identificados”.

- Identificar las amenazas naturales, humanas y de ubicación a las que están expuestos los recursos informáticos.
- Aplicar barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial.
- Restringir el acceso a los programas y archivos.
- Asegurar que los usuarios puedan trabajar sin supervisión y no puedan modificar los programas ni los archivos que no correspondan.
- Asegurar que se estén utilizados los datos, archivos y programas correctos en y por el procedimiento correcto.
- Verificar que la información transmitida sea recibida sólo por el destinatario al cual ha sido enviada y que la información recibida sea la misma que la transmitida.
- Disponer de pasos alternativos de emergencia para la transmisión de información.

CHECKLIST.

---

1. **Áreas seguras.**
    a. **Perímetro de seguridad física.**

    Un perímetro de seguridad es algo delimitado por una barrera. Por Ejemplo.

    - Una Pared
    - Una puerta con acceso mediante tarjeta
    - Una oficina de recepción atendida por personas
    - Una persona en escritorio
    - El emplazamiento y la fortaleza de cada barrera dependerán de los resultados de una evaluación de riesgos.

    b. **Controles físicos de entrada.**

    - Debe mantenerse una pista protegida que permita auditar todos los accesos
    - Todo el personal debe exhibir alguna identificación visible y se lo debe alentar a cuestionar la presencia de desconocidos no escoltados y a quien no exhiba una identificación
    - Se deben revisar y actualizar periódicamente los derechos de acceso a las áreas protegidas

    c. **Seguridad de oficinas, despachos y recursos.**

    - Obligatoriamente la seguridad física en oficinas, despachos y recursos deben de ser asignadas y a la vez usadas.
    - Se debería tomar en cuenta las regulaciones y estándares de salud y seguridad.
    - Se deben instalar equipos con clave deben para evitar el acceso del público.
    - Los directorios y las guías telefónicas internas identificando locaciones de los recursos de información sensible no deben ser fácilmente accesibles por el público.

    d. **Protección contra las amenazas externas y ambientales.**

    Hace referencia a la protección contra distintos tipo de desastres naturales o humanos que se dan a lo largo de los años como son terremotos,

inundaciones, explosión, la protección contra el fuego, el malestar civil, tsunami, entre otros.

1. Por lo cual lo más adecuado para tratar de evitar estos incidentes seria:
2. Los materiales inflamables como el combustible o materiales peligrosos deberían ser almacenadas en un lugar alejado de las áreas seguras.
3. Los equipos contra incendios deben ser ubicados en lugares adecuados.
4. Los equipos y medio de respaldo deben estar en un área segura ubicados adecuadamente para evitar que se dañen en un eventual desastre.

e. El trabajo en áreas seguras.

- Se requiere mucho de esta información.
- Se debe diseñar pautas y guía de protección física para poder trabajar en áreas seguras.
- El personal solo debe conocer la existencia de una sola área segura.
- Se debe evitar el trabajo no autorizado para evitar posibles actividades maliciosas.

f. Áreas de acceso público, carga y descarga.

Es importante controlar estas áreas con el fin de evitar accesos no autorizados.

Por lo que debemos seguir:

- Las puertas externas del área deberías estar cerradas cuando las puertas internas del área estén abiertas.
- Los materiales entrantes deberían ser registrados en concordancia con los procedimientos de gestión de activos.
- El material entrante y saliente deben ser físicamente separados donde sea posible.

- Se deberían controlar puntos de acceso a la organización como las áreas de entrega y carga/descarga para evitar el ingreso de personas no autorizadas a las dependencias aislando estos puntos, en la medida de lo posible, de las instalaciones de procesamiento de información.

2. Seguridad de los equipos.

- Las instalaciones se deben ubicar en un lugar de fácil supervisión
- Minimizar el acceso innecesario a las áreas de trabajo
- Establecer políticas dentro de las instalaciones de los sistemas de información.
- Controles para minimizar el riesgo de amenazas potenciales
- Los ítems que requieren protección especial deben ser aislados
- Monitorear las condiciones Ambientales

a. Emplazamiento y protección de equipos.

- Protección especial para los instrumentos ubicados en áreas industriales.
- Considerar el impacto de un eventual desastre que tenga lugar en zonas próximas a la sede de la organización.
- Reducir los riesgos ocasionados por amenazas y peligros ambientales, y oportunidades de acceso no autorizado

b. Instalaciones de suministro.

- Suministros de energía
- El equipo debe estar protegido contra posibles fallas eléctricas y debe contar con un adecuado suministro de energía de acuerdo a las especificaciones del proveedor o fabricante.

A. Múltiples bocas de suministro para evitar un único punto de falla en el suministro de energía.
B. Suministro de energía interrumpible (UPS).
C. Generador de respaldo.

c. Seguridad del cableado.

- El cableado de energía eléctrica
- y de comunicaciones

- que transporta
- datos o brinda apoyo
- a los servicios de información
- debe ser protegido contra interceptación o daño.
- Las líneas de energía eléctrica y telecomunicaciones que se conectan con las instalaciones de procesamiento de información deben ser subterráneas, siempre que sea posible, o sujetas a una adecuada protección alternativa.
- El cableado de red debe estar protegido contra interceptación no autorizada o daño.
- Los cables de energía deben estar separados de los cables de comunicaciones para evitar interferencias.

d. Mantenimiento de los equipos.

- Debe ser en forma adecuada para asegurar su disponibilidad e integridad.
- Debe ser autorizado por el nivel gerencial.
- Deben de ser controlados para asegurar que han sido eliminados o sobrescritos antes de su baja.

e. Salida de activos fuera de las dependencias de la empresa.

- Equipamiento
- Información
- Software
- No deben ser retirados de la organización sin autorización.

Quien interviene:

A. Jefes o encargados de las dependencias o unidades productivas.
B. Personal del departamento de Contabilidad.
C. Personal del departamento de Auditoría Interna.

f. Seguridad de los equipos y activos fuera de las instalaciones.

- Para efectos del inventario de activo fijo, todas las dependencias, secciones o departamentos serán incluidos en su totalidad, para que dicha gestión sea incluyente, responsable y en especial que sea fiable.

- En ese sentido es conveniente que cada empresa establezca un sistema de captación y control de activo fijo. Dentro de los objetivos principales del sistema tenemos:
- Inventariar de forma periódica los bienes de la propiedad planta y equipo.
  1. Codificar o etiquetar los activos fijos.
  2. Controlar las entradas y salidas del activo fijo
  3. Preservar en forma directa el mantenimiento de algunos bienes muebles e inmuebles.

g. Reutilización o retirada segura de dispositivos de almacenamiento.

- Se deberían 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 hayan sobrescrito de manera segura antes de su eliminación o reutilización.

h. Equipo informático de usuario desatendido.

- Los usuarios se deberían asegurar de que los equipos no supervisados cuentan con la protección adecuada.

i. Política de puesto de trabajo despejado y bloqueo de pantalla.

- Se debería adoptar una política de puesto de trabajo despejado para documentación en papel y para medios de almacenamiento extraíbles y una política de monitores sin información para las instalaciones de procesamiento de información.

PUNTOS DE APLICACIÓN.

Detección y prevención de riesgos

Como consecuencia la disminución de la sensación de seguridad en los seres humanos, se plantearon mecanismos para la detección y prevención de situaciones de riesgos en espacios físicos.

Para la detección y prevención de riesgo se toman en cuentan variables fundamentales entre las que se encuentran:

- Estudio del entorno en riesgo
- Probabilidad de ocurrencia de riesgos de acuerdo al tipo
- Características del recinto a proteger

Planificación de la seguridad física.

Una vez que se ha detectado una posible situación de riesgo, se planifican las acciones de seguridad física. La planificación suele depender de:

- Expectativa de seguridad
- Tecnología a emplear
- Presupuesto para la inversión en seguridad

Entre los elementos típicos que se incluyen en un plan de seguridad física están:

- Protección para accesos (puertas, ventanas y otros)
- Sistemas de vigilancia monitorizados (cámaras)
- Sistemas de seguridad privada
- lineamientos de seguridad para usuarios (cómo mantener el nivel de seguridad con acciones cotidianas)

Evaluar y controlar permanentemente la seguridad física del edificio es la base para o comenzar a integrar la seguridad como una función primordial dentro de cualquier organismo.

Tener controlado el ambiente y acceso físico permite:

- disminuir siniestros
- trabajar mejor manteniendo la sensación de seguridad
- descartar falsas hipótesis si se produjeran incidentes
- tener los medios para luchar contra accidentes

Las distintas alternativas estudiadas son suficientes para conocer en todo momento el estado del medio en el que nos desempeñamos; y así tomar decisiones sobre la base de la información brindada por los medios de control adecuados.

Estas decisiones pueden variar desde el conocimiento de la áreas que recorren ciertas personas hasta la extremo de evacuar el edificio en caso de accidentes.

Avance tecnológico en la seguridad de recintos

La automatización de procesos en una vivienda, conocida como domótica, es parte del avance tecnológico de la seguridad física en búsqueda de mejorar la sensación de seguridad del ser humano en sociedad. La tecnología de fabricación de piezas de cerrajería también ha evolucionado de acuerdo a las nuevas necesidades de protección. Actualmente las cerraduras inteligentes y los sistemas reforzados de apertura y cierre de puertas proveen un nuevo nivel de seguridad para recintos, tanto comerciales como residenciales.

INFORMACIÓN Y ELEMENTOS ADICIONAL.

- https://sites.google.com/a/istpargentina.edu.pe/exposicion-areas-seguras/seguridad-fisica-y-del-entorno
- NFPA 75 es el estándar de la National Fire Protection Association para la protección de equipos TI: construcción de edificios, protección anti-incendios, sistemas de extinción, sistemas eléctricos, refrigeración, etc. Versiones en inglés y en español.
- Larga lista de estándares relacionados con la seguridad contra el fuego de la National Fire Protection Association. Versiones en inglés y en español.
- Federal Data Center Consolidation Initiative (FDCCI) Data Center Closings 2010- 2012, http://explore.data.gov/Federal-Government-Finances-and-Employment/ Federal-Data-Center-Consolidation-Initiative-FDCCI/d5wm-4c37