### **Seguridad Física y del Entorno**

Dentro de la Seguridad Informática, la Seguridad física hace referencia a las barreras físicas y mecanismos de control en el entorno de un sistema informático, para proteger el hardware de amenazas físicas. La seguridad física contrasta con la seguridad lógica.

**Áreas seguras**:

El objetivo de las áreas seguras evita a los accesos no autorizados como también daños e interferencias contra la Información de la organización.

**Perímetro de seguridad física**:

Se debe de dar la seguridad a las áreas que contengan información única y a los recursos de procesamiento de información.

La seguridad física identifica las amenazas, vulnerabilidades y las medidas que pueden ser utilizadas para proteger físicamente los recursos y la información de la organización. Los recursos incluyen el personal, el sitio donde ellos laboran, los datos, equipos y los medios con los cuales los empleados interactúan, en general los activos asociados al mantenimiento y procesamiento de la información, como por ejemplo activos de información, activos de software y activos físicos.

Se entiende por área donde se procesa la información los siguientes:

Ø Centros de Procesamiento normales o de emergencia.

Ø Áreas con servidores, ya sean de procesamiento o dispositivos de comunicación.

Ø Áreas donde se encuentren concentrados dispositivos de información.

Ø Áreas donde se almacenen y guarden elementos de respaldo datos (CD, Discos Duros, Cintas etc.)

**Controles físicos de entrada**:

Las áreas de seguridad deberían estar protegidas por controles de entrada que aseguren el permiso de acceso sólo a las personas que están autorizadas.

Las visitas a las áreas seguras se deberían supervisar, a menos que el acceso haya sido aprobado previamente, y se debe registrar la fecha y momento de entrada y salida.

Se debería controlar y restringir sólo al personal autorizado el acceso a la información sensible y a los recursos de su tratamiento. Se deberían usar controles de autenticación, por ejemplo, tarjetas con número de identificación personal (PIN), para autorizar y validar el acceso. Se debería mantener un rastro auditable de todos los accesos, con las debidas medidas de seguridad.

Se debe garantizar el acceso restringido al personal de apoyo de terceros, hacia áreas de seguridad o a los recursos de procesamiento de información sensibles, solo cuando este sea requerido. Este acceso debe ser autorizado y monitoreado.

**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 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.

**Protección contra 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.

Por lo cual lo más adecuado para tratar de evitar estos incidentes seria:

Los materiales inflamables como el combustible o materiales peligrosos deberían ser almacenadas en un lugar alejado de las áreas seguras.

Los equipos contra incendios deben ser ubicados en lugares adecuados.

Los equipos y medio de respaldo deben estar en un área segura ubicados adecuadamente para evitar que se dañen en un eventual desastre.

**El trabajo en las 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.