CAPITULO 1
Nociones de Seguridad de la Información
Seguridad Física y Seguridad Lógica

Jenny Torres, PhD.

Seguridad Física

Definición

- Aplicación de **barreras físicas** y **procedimientos de control**, como medidas de prevención y contramedidas, que permiten disuadir, detectar, denegar y defenderse de ataques, a fin de evitar o minimizar daños a los recursos e información confidencial.

- Son **controles** y **mecanismos de seguridad** dentro y alrededor del Centro de Cómputo así como los medios de acceso remoto al y desde el mismo; implementados para **proteger el hardware** y m**edios de almacenamiento** de datos.

Seguridad Física

Amenazas

- Algunas amenazas de la seguridad física son:
  - **Humanas**: robo, fraude, espionaje, sabotaje, destrucció ́n, p ́erdida, acceso no autorizado, errores, etc.
  - **Naturales**: incendios, inundaciones, tormentas eléctricas, terremotos, electricidad, temperaturas extremas, etc.

Seguridad Física

Objetivos

- Proteger y conservar los activos de la organización.
- Reducir la probabilidad de perdidas a un mínimo aceptable.
- Asegurar que existan controles adecuados para las condiciones ambientales.
- Controlar el acceso a agentes de riesgo dentro de la organización.

Seguridad Física

Requisitos

- Servicio de guardianía, escoltas, cercas o barreras.
- Llaves y cerraduras.
- Sistemas de monitoreo.
- Utilización de detectores de metales.
- Verificación Automática de Firmas (VAF).
- Sensores de movimiento.
- Sistemas de control de acceso.
- **Sistemas Biométricos.**

Seguridad Lógica

Definición

- Aplicación de barreras y procedimientos que resguarden el acceso a los datos y sólo se permita acceder a ellos a las personas autorizadas para hacerlo.
- La seguridad lógica se enfoca en la autorización a los usuarios para acceder a los servicios de tecnologías de información (TI). Estos recursos pueden incluir: roles, permisos en una base de datos, acceso a correos electrónicos y privilegios de acceso remoto.
- *“Todo lo que no está permitido debe estar prohibido.”*

Seguridad Lógica

Objetivos

- Restringir el acceso a los programas y archivos.
- Asegurar que los usuarios no puedan modificar los programas ni los archivos que no correspondan.
- Asegurar que se estén utilizados los datos, archivos y programas correctos en el procedimiento correcto.
- Que la información transmitida sea recibida solo por el destinatario al cual ha sido enviada y no a otro.
- Que la información recibida sea la misma que ha sido transmitida.
- Que existan sistemas alternativos secundarios de transmisión entre diferentes puntos.
- Que se disponga de pasos alternativos de emergencia para la transmisión de información.

Seguridad Lógica

Requisitos

- **Roles**
  - programador, líder de proyecto, gerente de un área, administrador del sistema, etc.
- **Transacciones**
  - claves
- **Limitaciones a los Servicios**
  - licencias para la utilización simultánea de un software
- **Modalidad de Acceso**
  - lectura/escritura/ejecución/borrado creación/búsqueda

Seguridad Lógica

Requisitos

- **Ubicación y Horario**
  - determinadas horas del día o días de la semana
- **Administración del Personal y Usuarios**
  - verificación de controles para la terminación de contrato y transferencia de personal
- **Identificación y Autentificación**
  - **Sistema de Gestión de Identidades**

Seguridad física y Seguridad lógica

Convergencia

- Conseguir acceso físico a un centro de control, y más concretamente a dispositivos pertenecientes a la red de control, normalmente implica ganar acceso lógico a todo el sistema de procesos.
- Conseguir acceso lógico a los sistemas de la sala de control permitirá probablemente ejercer cambios en las medidas de seguridad y autorizaciones de acceso físico.
- Como se ha visto, la línea que separa la relación entre seguridad lógica y la seguridad física es difusa.
- Por esto, debe prestarse especial atención a las protecciones físicas de nuestros dispositivos lógicos, dentro de las infraestructuras.

Seguridad física y Seguridad lógica

Apoyo normativo

- Todas las normativas y guías de buenas prácticas de seguridad recogen, de alguna manera, los requerimientos de seguridad física. Las más representativas son:
  - El estándar internacional IEC 62443-2-1 '*Industrial communication networks – Network and system security – Part 2-1: Establishing an industrial automation and control system security program*'. Punto 4.3.3.
  - NERC CIP-005-5 '*Cyber Security - Electronic Security Perimeter(s)*'.
  - NERC CIP-014-2 '*Physical Security*'.

- Otra que no es específica del entorno industrial, pero que podría considerarse referente a la hora de implementar controles de seguridad tanto a nivel físico como lógico es:

  - ISO/IEC 27001:2013 '*Information technology -- Security techniques -- Information security management systems – Requirements*'. Puntos A.11.1, A.11.2, A.11.4.

Seguridad física y Seguridad lógica

Apoyo normativo

- Por otra parte, la guía de buenas prácticas del NIST 800-82 '*Guide to Industrial Control Systems (ICS) Security*', recoge los atributos que deben considerarse a la hora de realizar una defensa en profundidad aplicada a la seguridad física:

  - **Protección de las ubicaciones físicas:** Se refiere a las consideraciones clásicas de seguridad física, estableciendo perímetros de seguridad segmentados, con medidas de seguridad específicos aplicados por capas.

  - **Control de acceso:** Controles de seguridad que deben garantizar que solo las personas autorizadas tengan acceso a los espacios controlados. Un sistema debe poder verificar que las personas a las que se les concede acceso, son quienes dicen que son (habitualmente usando algo que la persona tiene, como una tarjeta o clave de acceso; algo que conocen, como un número de identificación personal (PIN); o algo que demuestre quien son, un lector biométrico).

Seguridad física y Seguridad lógica

Apoyo normativo

- **Sistemas de monitorización de accesos:** Se incluyen aquí cámaras fijas y de video, sensores o sistemas de identificación. Estos sistemas no previenen un acceso no autorizado, sino que los almacenan y registran.
- **Sistemas de limitación de acceso:** Dentro de este atributo entrarían vallas, cerraduras, o personal de seguridad, por ejemplo.
- **Sistemas que permitan el seguimiento de personas o activos:** Tecnologías que permitan rastrear los movimientos de personas o vehículos para asegurar que permanecen en las áreas autorizadas.
- **Sistemas de gestión de factores ambientales:** Entornos limpios, libres de electricidad estática, vibraciones, campos magnéticos, etc.

Seguridad física y Seguridad lógica

Apoyo normativo

- **Sistemas de control de condiciones ambientales:** Sistemas denominados en inglés (HVAC), control de humedad, ventilación y aire acondicionado.
- **Sistemas de protección de corriente:** Sistemas de protección y alimentación ininterrumpida, conocidos como UPS por sus siglas en inglés.
- **Sistemas de protección adicionales para centro de control:** Adicionalmente a los anteriores, las salas de control pueden tener necesidades más específicas de seguridad física como pueden ser: centros de control a prueba de explosiones, o incluso tener redundando el espacio físico del centro de control fuera de las instalaciones, para poder seguir controlándola si fuera necesario.

Seguridad física y Seguridad lógica

Apoyo normativo

- **Sistemas de control de los dispositivos de configuración portables:** Sistemas que impidan la movilidad de ciertos equipos de configuración, considerados críticos.
- **Sistemas de protección de cableado:** Este atributo es muy importante ya que el diseño e implementación del cableado para la red de control debe abordarse en el plan de ciberseguridad.

Referencias

- INEN (2012) Descripción General y Vocabulario. Norma Técnica Ecuatoriana NTE INEN-ISO/IEC 27000:2012.

- Stallings, W. (2011) Network Security Essentials 4th edition, New York, US; ISBN:13: 978-1587052460: Prentice-Hall.