Gestión de la seguridad

¿Qué es la gestión de seguridad?

Es el establecimiento de un sistema de funcionamiento donde se controlan las distintas facetas que garantizan la seguridad dentro de nuestra red.

Objetivos de la gestión de seguridad

1. **Diseñar** una política de seguridad efectiva para la empres, clientes, proveedores y empleados.
2. **Asegurar** el cumplimiento de las políticas de seguridad establecidas.
3. **Minimizar** los **riesgos** de seguridad que amenacen la continuidad de los servicios.

Normativa y estándares de referencia

La **Organización Internacional de Normalización (ISO**), establece unos estos estándares normativos en relación a diferentes temas, por ejemplo:

a. **ISO 1000** Unidades SI y recomendaciones para el uso de sus múltiplos y de otras ciertas unidades.

b. **ISO 9000** Sistemas de Gestión de la Calidad - Fundamentos y vocabulario.

c. **ISO/IEC 27000** Sistemas de Gestión de la Seguridad de la Información.

ISO 27000 Sistemas de Gestión de la Seguridad de la Información

a. **ISO 27001: Sistemas de Gestión de la Seguridad de la Información (SGSI).** Cómo se debe abordar la seguridad.

b. **ISO 27002: Buenas prácticas para gestión de la seguridad de la información.** Guión recomendado sobre las buenas prácticas a seguir en seguridad.

NOTA: como recomendaciones que son, no implica obligación ni certificación en sí.

El control 10.6

Este estándar, nos cita en este punto la norma referencial a la gestión de redes, en la cual se fijan los siguientes conceptos:

- Objetivo: **Proteger** la información y la infraestructura de red.
- Gestión: **Administrar** la infraestructura con atención al flujo de datos; teniendo en cuenta la normativa vigente en la LOPD.

10.6.1 Los controles de red

a. Controles: **Implantar procedimientos de seguridad** como por ejemplo controles de salvaguarda, integridad y disponibilidad de datos y servicios.

b. **Establecer responsabilidades** de uso remotamente.

c. **Registro de la actividad** sensible en la seguridad de la red.

d. **Coordinación** con la empresa de este sistema de gestión de seguridad.

10.6.2 La seguridad de los servicios de red

a. En los **contratos** de red se identificarán los requerimientos y niveles de servicios.
b. Se debería **monitorizar** habitualmente y **auditar** la red, descubriendo las anomalías detectadas.
c. Debería utilizarse programas de búsqueda de **vulnerabilidades** (IDS, IPS, firewalls, antivirus, etc.)
d. Debería aplicarse un **control de autenticación**, conexión y codificación, así como la posibilidad de **encriptación** de las comunicaciones de la red.
e. Establecer **restricciones** a servicios o aplicaciones sensibles.

Actividades de la gestión de seguridad

1. **Planificar**: En esta fase se elaboran las políticas de seguridad de la empresa (características del sistema, identificación de amenazas, estimación de la seguridad actual, definición de procedimientos y medidas correctoras).
2. **Implementación**: Establecimiento del plan diseñado previamente.
3. **Evaluación**: Por medio de pruebas y monitorización, se supervisarán los niveles de seguridad analizando tendencias, nuevos riesgos y vulnerabilidades; evitando así ataques mediante exploits.
4. **Mantenimiento**: Mediante comprobaciones y auditorias de seguridad continuas ya que cada cierto tiempo se descubrirán nuevas vulnerabilidades.

Recomendaciones de buenas prácticas

Seguridad Física:

- Controles de acceso físico a los sistemas.
- Condiciones ambientales.
- Redundancia de equipos ante fallos de hardware (ej. RAID).
- Eliminación segura de información.

Seguridad Lógica:

- Controles de acceso lógico.
- Asignación de roles y responsabilidades.
- Copias de seguridad.
- Borrado seguro.
- Uso de certificados.
- Admon. de sistemas y aplicaciones, registro de entradas y salidas.

https://create.kahoot.it/preview/e023e34f-6ec5-42bf-a482-087b05efdece