UT1: Introducción a la seguridad informática

(<https://www.osi.es/es>) (https://www.incibe.es/) página de seguridad

1. Conceptos de S.I:
   * + Asegurar recursos de un sistema de información de una organización o empresa

organificación de la seguridad que utilizan personas.

* + - Objetos: detectar problemas y amenazas:
    - Gestionar riesgos
    - Garantizar recursos y aplicaciones
    - Limitar pérdidas del sistema
    - Cumplir con el marco legal (ley de protección de datos)
    - La seguridad supone gran coste:
    - Es necesario valorar los costes: tener en cuenta en interrupción de trabajo, tiempo que pierde el personal, la imagen de la empresa.
    - No existe seguridad 100%
    - Que proteger: equipos, aplicaciones, datos, comunicaciones (ACTIVOS)

1. Planificación de la seguridad:
   * + Activos: recursos a proteger (información, software, personal y físicos)
     + Amenazas: Atentar contra un recurso y pueden ser pasivas (escuchas, monitorización) y activas (cambios ni autorizados usurpación de identidad)
     + Riesgos: cuando una amenaza se hace tangible aprovechando un agujero de seguridad. Las empresas realizan análisis de riesgos y los riesgos pueden alto, bajo o medio.
     + Vulnerabilidad: son agujeros de seguridad asociados a fallos en aplicaciones y fallos en sistema operativo.
     + Impacto: Alcance o daño producido.
     + Ataques: Aprovechan la vulnerabilidad para provocar un impacto y las fases son: reconocimiento (coger información) exploración (cogen información ip, hosts) acceso (una vez que obtiene la información implanta herramientas y por último borra las huellas).
2. Servicios y mecanismos de S.I: CIDAN

* Confidencialidad: garantizar que la información solo será disponible para ciertas disponibles para ciertas personas autorizadas para esa información.
* Integridad: No ha sido modificado o manipulado desde que se crea o se modifica en algún momento.
* Disponibilidad: de datos al usuario.
* Autenticación: La identificación del emisor y para ello se utiliza usuario y contraseña.
* No repudio: garantiza la participación de las partes en la comunicación.

🡪Para conseguir estos objetivos se utilizan mecanismos:

* Autenticación, Autorización, Auditoria, Encriptación, Copias de seguridad, Antivirus, Cortafuegos, Proxys, Firmas electrónica, .

1. Clasificación S.I:

* Según activo a proteger:
* Seguridad física: hardware frente a que amenazas (incendios e inundaciones ………etc.)
* Seguridad lógica: complementa a la física y protege el software frente amenazas. (robos, pérdida de información ……..etc.)
* Según el momento:

🡪Activa: es la que previene ante daños en el sistema.

⮚ técnicas (ACLS (listas de control de acceso), encriptación, firmas digitales, cuotas de discos etc.)

🡪Pasiva: Es correctiva y consideran medidas o acciones posteriores.

* Discos redundantes, SAI, copias de seguridad.

1. Modelos de seguridad: Se refiere a la seguridad de los sistemas informáticos, detalla las normas y protocolos.

🡪para elaborar las políticas de s.i:

🡪Se elaboran reglas para servicios críticos.

🡪Se definen las acciones

🡪Se sensibiliza al personal

🡪aspectos a tener en cuenta:

🡪identifica a los activos

🡪se forma a los trabajadores

🡪Se evalúan los riesgos

* Plan de actuación
* Políticas de seguridad
* Planes de contingencia