SAD - U1 Introducción a la seguridad informática

Descargar estas actividades

Índice

Actividades

- **Actividad 1.** ¿En qué se diferencian la seguridad activa y la seguridad pasiva?
- **Actividad 2.** Indica algunas razones por las que a alguien le puede interesar realizar un ataque a la seguridad informática de
  una empresa.
- **Actividad 3.** Enumera posibles activos asociados a una organización.
- **Actividad 4.** ¿Cuáles son los posibles puntos débiles en los sistemas informáticos de una organización?
- **Actividad 5.** ¿Qué recomendaciones harías para evitar el acceso no autorizado a la información en una organización?
- **Actividad 6.** Enumera posibles vulnerabilidades asociadas a las estaciones de trabajo en una organización.
- **Actividad 7.** Indica, para los siguientes supuestos, qué principios de la seguridad se están violando:
  a) Destrucción de un elemento hardware.
  b) Robo de un portátil con información de interés de la empresa.
  c) Robos de direcciones IP.
  d) Escuchas electrónicas.
  e) Modificación de los mensajes entre programas para variar su comportamiento.
  f) Deshabilitar los sistemas de administración de archivos.
  g) Alterar la información que se transmite desde una base de datos.
  h) Robos de sesiones.
- **Actividad 8.** Pon un ejemplo de ataque por ingeniería social. ¿Cómo crees que se puede proteger una organización ante los
  ataques de ingeniería social?
- **Actividad 9.** Analiza el grado del impacto que pueda ocasionar la acción de una amenaza meteorológica como pueda ser un huracán para una organización.
- **Actividad 10.** Realiza un diagrama en el que relaciones los elementos de seguridad (activos, vulnerabilidad, amenazas, ataques, riesgos, impacto, desastres).
  ¿Qué relación tienen unos términos con otros? En las líneas que los relacionen, indica dicha relación.
  Por ejemplo, Activo <-> Vulnerabilidad estarían relacionados con "es una debilidad" indicando que una vulnerabilidad es una debilidad de un activo.
- **Actividad 11.** ¿En qué consisten y qué aspectos deben cubrir las políticas de seguridad?
- **Actividad 12.** ¿Por qué crees que es importante que una organización tenga un plan de contingencia? ¿Qué consecuencias podría haber si no tuviese un plan de contingencia establecido?
- **Actividad 13.** ¿En qué consiste el análisis de riesgos? ¿Para qué sirve realizar un análisis de riesgos?
- **Actividad 14.** ¿Qué utilidad tienen para las organizaciones los planes de contingencia?

Casos prácticos

- **Caso 1.** Suponemos que el hospital X está ubicado cerca de un cauce de río que prácticamente no lleva agua. El hospital tiene su centro de cálculo situado en el sótano. Se han anunciado lluvias fuertes y por tanto existe una alta posibilidad de desbordamiento del río que pasa cerca de la zona debido a la falta de limpieza de su cauce.
  Identifica los activos, las amenazas y las vulnerabilidades del sistema.
- **Caso 2.** ¿Qué tipo de aplicaciones se pueden utilizar para comprometer la confidencialidad del sistema?
- **Caso 3.** Una empresa se ha visto atacada de forma que su página web ha sido modificada sin previa autorización. ¿Qué tipo de ataque se ha producido? ¿Qué principios de la seguridad se han visto violados?
- **Caso 4.** ¿Qué soluciones se podrían aplicar para que el sistema informático de una entidad bancaria no se viera afectado por un desastre que afectara a sus clientes?

Caso práctico: Instalación y uso de una herramienta de análisis y gestión de riesgos

Instala en tu equipo la herramienta **PILAR**, desarrollada por el `Centro Criptológico Nacional (CCN)`, que implementa la metodología MAGERIT de análisis y gestión de riesgos y que es de amplia utilización en la Administración Pública española.

Documentación del caso

Proporciona capturas de pantalla de los elementos analizados y de los resultados obtenidos.

Abre el proyecto de ejemplo que incluye, analízalo y contesta a las siguientes cuestiones:

- a) ¿Qué tipo de empresa se estudia en el ejemplo?
- b) ¿Qué clasificación de activos tiene? ¿Cuáles se encuentran dentro de los de la sección Equipamiento? ¿Qué aplicación utilizan?
- c) ¿Qué vulnerabilidades técnicas presenta el servidor? ¿Con qué amenazas se relacionan?
- d) Identifica las categorías de amenazas registradas. ¿En qué categoría entran las siguientes amenazas?
  - Manipulación de la configuración.
  - Fuego.
  - Errores de configuración.
  - Divulgación de la información.
  - Corte de suministro eléctrico.
  - Errores de los usuarios.
  - Extorsión.
- e) Proporciona alguna amenaza más por cada categoría.
- f) Teniendo en cuenta que los valores del 100% indican que la amenaza está totalmente cubierta
  ¿Qué valoración de las amenazas se da para los activos clasificados como Equipos? ¿Y para la LAN?
  ¿Qué subcomponente de la LAN es el más crítico?