SEGURIDAD Y ALTA DISPONIBILIDAD

Resultados de aprendizaje y criterios de evaluación:

1. Adopta pautas y prácticas de tratamiento seguro de la información, reconociendo las vulnerabilidades de un sistema informático y la necesidad de asegurarlo.

Criterios de evaluación:

a) Se ha valorado la importancia de asegurar la privacidad, coherencia y disponibilidad de la información en los sistemas informáticos.
b) Se han descrito las diferencias entre seguridad física y lógica.
c) Se han clasificado las principales vulnerabilidades de un sistema informático, según su tipología y origen.
d) Se ha contrastado la incidencia de las técnicas de ingeniería social en los fraudes informáticos.
e) Se han adoptado políticas de contraseñas.
f) Se han valorado las ventajas que supone la utilización de sistemas biométricos.
g) Se han aplicado técnicas criptográficas en el almacenamiento y transmisión de la información.
h) Se ha reconocido la necesidad de establecer un plan integral de protección perimetral, especialmente en sistemas conectados a redes públicas.
i) Se han identificado las fases del análisis forense ante ataques a un sistema.

2. Implanta mecanismos de seguridad activa, seleccionando y ejecutando contramedidas ante amenazas o ataques al sistema.

Criterios de evaluación:

a) Se han clasificado los principales tipos de amenazas lógicas contra un sistema informático.
b) Se ha verificado el origen y la autenticidad de las aplicaciones instaladas en un equipo, así como el estado de actualización del sistema operativo.
c) Se han identificado la anatomía de los ataques más habituales, así como las medidas preventivas y paliativas disponibles.
d) Se han analizado diversos tipos de amenazas, ataques y software malicioso, en entornos de ejecución controlados.
e) Se han implantado aplicaciones específicas para la detección de amenazas y la eliminación de software malicioso.
f) Se han utilizado técnicas de cifrado, firmas y certificados digitales en un entorno de trabajo basado en el uso de redes públicas.
g) Se han evaluado las medidas de seguridad de los protocolos usados en redes inalámbricas.
h) Se ha reconocido la necesidad de inventariar y controlar los servicios de red que se ejecutan en un sistema.
i) Se han descrito los tipos y características de los sistemas de detección de intrusiones.

SEGURIDAD Y ALTA DISPONIBILIDAD

3. Implanta técnicas seguras de acceso remoto a un sistema informático, interpretando y aplicando el plan de seguridad.

Criterios de evaluación:

a) Se han descrito escenarios típicos de sistemas con conexión a redes públicas en los que se precisa fortificar la red interna.
b) Se han clasificado las zonas de riesgo de un sistema, según criterios de seguridad perimetral.
c) Se han identificado los protocolos seguros de comunicación y sus ámbitos de utilización.
d) Se han configurado redes privadas virtuales mediante protocolos seguros a distintos niveles.
e) Se ha implantado un servidor como pasarela de acceso a la red interna desde ubicaciones remotas.
f) Se han identificado y configurado los posibles métodos de autenticación en el acceso de usuarios remotos a través de la pasarela.
g) Se ha instalado, configurado e integrado en la pasarela un servidor remoto de autenticación.

4. Implanta cortafuegos para asegurar un sistema informático, analizando sus prestaciones y controlando el tráfico hacia la red interna.

Criterios de evaluación:

a) Se han descrito las características, tipos y funciones de los cortafuegos.
b) Se han clasificado los niveles en los que se realiza el filtrado de tráfico.
c) Se ha planificado la instalación de cortafuegos para limitar los accesos a determinadas zonas de la red.
d) Se han configurado filtros en un cortafuegos a partir de un listado de reglas de filtrado.
e) Se han revisado los registros de sucesos de cortafuegos, para verificar que las reglas se aplican correctamente.
f) Se han probado distintas opciones para implementar cortafuegos, tanto software como hardware.
g) Se han diagnosticado problemas de conectividad en los clientes provocados por los cortafuegos.
h) Se ha elaborado documentación relativa a la instalación, configuración y uso de cortafuegos.

5. Implanta servidores «proxy», aplicando criterios de configuración que garanticen el funcionamiento seguro del servicio.

Criterios de evaluación:

a) Se han identificado los tipos de «proxy», sus características y funciones principales.
b) Se ha instalado y configurado un servidor «proxy-cache».
c) Se han configurado los métodos de autenticación en el «proxy».
d) Se ha configurado un «proxy» en modo transparente.
e) Se ha utilizado el servidor «proxy» para establecer restricciones de acceso Web.
f) Se han solucionado problemas de acceso de los clientes al «proxy».

g) Se han realizado pruebas de funcionamiento del «proxy», monitorizando su actividad con herramientas gráficas.
h) Se ha configurado un servidor «proxy» en modo inverso.
i) Se ha elaborado documentación relativa a la instalación, configuración y uso de servidores «proxy».

6. Implanta soluciones de alta disponibilidad empleando técnicas de virtualización y configurando los entornos de prueba.

Criterios de evaluación:

a) Se han analizado supuestos y situaciones en las que se hace necesario implementar soluciones de alta disponibilidad.
b) Se han identificado soluciones hardware para asegurar la continuidad en el funcionamiento de un sistema.
c) Se han evaluado las posibilidades de la virtualización de sistemas para implementar soluciones de alta disponibilidad.
d) Se ha implantado un servidor redundante que garantice la continuidad de servicios en casos de caída del servidor principal.
e) Se ha implantado un balanceador de carga a la entrada de la red interna.
f) Se han implantado sistemas de almacenamiento redundante sobre servidores y dispositivos específicos.
g) Se ha evaluado la utilidad de los sistemas de «clusters» para aumentar la fiabilidad y productividad del sistema.
h) Se han analizado soluciones de futuro para un sistema con demanda creciente.
i) Se han esquematizado y documentado soluciones para diferentes supuestos con necesidades de alta disponibilidad.

7. Reconoce la legislación y normativa sobre seguridad y protección de datos valorando su importancia.

Criterios de evaluación:

a) Se ha descrito la legislación sobre protección de datos de carácter personal.
b) Se ha determinado la necesidad de controlar el acceso a la información personal almacenada.
c) Se han identificado las figuras legales que intervienen en el tratamiento y mantenimiento de los ficheros de datos.
d) Se ha contrastado el deber de poner a disposición de las personas los datos personales que les conciernen.
e) Se ha descrito la legislación actual sobre los servicios de la sociedad de la información y comercio electrónico.
f) Se han contrastado las normas sobre gestión de seguridad de la información.
g) Se ha comprendido la necesidad de conocer y respetar la normativa legal aplicable.

SEGURIDAD Y ALTA DISPONIBILIDAD

Contenidos mínimos:

· Adopción de pautas de seguridad informática:
- Fiabilidad, confidencialidad, integridad y disponibilidad.
- Elementos vulnerables en el sistema informático: hardware, software y datos.
- Análisis de las principales vulnerabilidades de un sistema informático.
- Políticas de seguridad y planes de contingencia.
- Amenazas. Tipos:
    - o Amenazas físicas.
    - o Amenazas lógicas.
- Seguridad física y ambiental:

o Ubicación y protección física de los equipos y servidores.
o Sistemas de alimentación ininterrumpida.
- Seguridad lógica:
o Criptografía. Técnicas criptográficas.
o Listas de control de acceso.
o Establecimiento de políticas de contraseñas.
o Utilización de sistemas biométricos de identificación.
o Políticas de almacenamiento.
o Copias de seguridad e imágenes de respaldo.
o Medios de almacenamiento.
o Recuperación de datos.
o Realización de Auditorias de seguridad.
Implantación de mecanismos de seguridad activa:
- Ataques y contramedidas en sistemas personales:
o Clasificación y Anatomía de los ataques: Identificación de Sistemas. Análisis de Vulnerabilidades.
Denegación de Servicio. Intercepción de contraseñas. Otros.
o Análisis de software malicioso. Tipos. Software antivirus, antiSpam. Prevención, detección y reacción ante malware.
o Herramientas preventivas. Instalación y configuración.
o Herramientas paliativas. Instalación y configuración.
o Fortalecimiento de sistemas. Configuración segura. Administración Segura (local y remota).

o Actualización de sistemas y aplicaciones.
o Seguridad en la conexión con redes públicas.
o Identificación digital. Firma electrónica, entidades certificadoras y certificado digital.
o Pautas y prácticas seguras.
- Seguridad en la red corporativa:
o Monitorización del tráfico en redes. Aplicaciones para la captura y análisis del tráfico; para la monitorización de redes y equipos.
o Seguridad en los protocolos para comunicaciones inalámbricas. Tipos de ataques. Tipos de seguridad. Autenticación de acceso.
o Riesgos potenciales de los servicios de red.
o Intentos de penetración. Craqueado de contraseñas. Forzado de recursos. Puertas traseras.
o Control de acceso a red.
o Sistemas Detección y Prevención de Intrusos.

Implantación de técnicas de acceso remoto. Seguridad perimetral:
- Elementos básicos de la seguridad perimetral.

SEGURIDAD Y ALTA DISPONIBILIDAD

o Router fronterizo.
o Cortafuegos.
o Redes privadas virtuales.
- Perímetros de red. Zonas desmilitarizadas.
- Arquitectura débil de subred protegida.
- Arquitectura fuerte de subred protegida.
- Redes privadas virtuales. VPN.
o Beneficios y desventajas con respecto a las líneas dedicadas.
o Técnicas de cifrado. Clave pública y clave privada:
o VPN a nivel de red. SSL, IPSec.
o VPN a nivel de aplicación. SSH.
- Servidores de acceso remoto:
o Protocolos de autenticación.
o Configuración de parámetros de acceso.
o Servidores de autenticación.

Instalación y configuración de cortafuegos:
- Utilización de cortafuegos.
- Filtrado de paquetes de datos.
- Tipos de cortafuegos. Características. Funciones principales.
- Instalación de cortafuegos. Ubicación.
- Reglas de filtrado de cortafuegos.
- Pruebas de funcionamiento. Sondeo.
- Registros de sucesos de un cortafuegos.

Instalación y configuración de servidores «proxy»:
- Tipos de «proxy». Características y funciones.
- Instalación de servidores «proxy».
- Configuración del almacenamiento en la caché de un «proxy».
- Configuración de filtros.
- Métodos de autenticación en un «proxy».

Implantación de soluciones de alta disponibilidad:
- Definición y objetivos.
- Análisis de configuraciones de alta disponibilidad.
o Funcionamiento ininterrumpido.
o Integridad de datos y recuperación de servicio.
o Servidores redundantes.
o Sistemas de «clusters».
o Balanceadores de carga.
o Almacenamiento compartido.

- Instalación y configuración de soluciones de alta disponibilidad.
- Virtualización de sistemas.
o Servidores.
o Aplicaciones.
o Escritorio.
- Herramientas para la virtualización.
o Entornos personales.
o Entornos empresariales.

SEGURIDAD Y ALTA DISPONIBILIDAD

- Configuración y utilización de máquinas virtuales.
- Alta disponibilidad y virtualización.
- Simulación de servicios con virtualización.
o Continuidad de servicio
o Análisis del rendimiento del sistema virtualizado.

Legislación y normas sobre seguridad:
- Legislación sobre protección de datos.