Ciberseguridad practica: proteccion de equipos y navegacion segura en red

Modalidad: curso e-Learning Duración: 4 horas

Categorías: Ofimática, informática y comunicaciones

OBJETIVOS

- Explicar por que la proteccion en red es necesaria y reconocer el impacto de un incidente (datos, tiempo y reputacion)
- Identificar riesgos y vectores de ataque habituales (correo, navegacion web, USB, descargas y Wi-Fi)
- Diferenciar malware de "

CONTENIDOS

Ciberseguridad practica: proteccion de equipos y navegacion segura en red

UNIDAD.- La necesidad de protegerse en la red

- Panorama actual de amenazas y por que afecta a cualquier usuario
- Principios basicos de ciberseguridad aplicados al puesto de trabajo
- Confidencialidad, integridad y disponibilidad (triada CIA)
- Riesgos mas comunes en redes domesticas y corporativas
- Vectores de ataque habituales: correo, web, USB, descargas y Wi-Fi
- El factor humano: habitos, errores frecuentes y buenas practicas
- Ingenieria social: como se explota la confianza del usuario
- Seguridad por capas: concepto y ejemplos en un equipo real
- Coste e impacto de un incidente: perdida de datos, tiempo y reputacion
- Normas basicas de higiene digital: contrasegnas, bloqueos y copias

UNIDAD.- Los peligros posibles: los virus informaticos

- Concepto de malware y diferencias con ?virus? (termino general)
- Tipos de amenazas: virus, gusanos, troyanos, spyware y adware
- Ransomware: funcionamiento, segnales y consecuencias
- Rootkits y amenazas persistentes: ocultacion y privilegios
- Botnets y equipos zombis: uso del equipo sin consentimiento
- Keyloggers y robo de credenciales: tecnicas comunes
- Metodos de propagacion: adjuntos, macros, exploits y redes compartidas
- Indicadores de compromiso (IoC) en un equipo: sintomas tipicos
- Buenas practicas ante sospecha de infeccion: contencion y reporte
- Recuperacion basica tras incidente: limpieza, reinstalacion y restauracion

UNIDAD.- Las soluciones: el antivirus

- Que es un antivirus/antimalware y que problemas resuelve
- Como detecta amenazas: firmas, heuristica y comportamiento
- Proteccion en tiempo real vs analisis bajo demanda
- Actualizaciones de firmas y motores: importancia y frecuencia
- Tipos de analisis: rapido, completo, personalizado y programado
- Cuarentena: que es y como gestionarla con seguridad
- Exclusiones y falsos positivos: criterios y riesgos
- Proteccion web y del correo: filtros, descargas y enlaces
- Antivirus en entornos corporativos: consola centralizada y politicas
- Buenas practicas: configuracion minima recomendada y mantenimiento

NIDAD.- Otros conceptos sobre seguridad informatica

- Firewall
- Que es y para que sirve (entrante/saliente)
- Reglas, perfiles (publico/privado) y puertos habituales
- Buenas practicas de configuracion y revision
- Spam
- Tipos de spam y riesgos asociados
- Filtros antispam y segnales de correo sospechoso
- Buenas practicas de gestion del correo
- Phising
- Que es y variantes: smishing, vishing, spear phishing
- Segnales de alerta: dominio, urgencia, adjuntos, enlaces
- Que hacer ante un intento: verificacion y reporte
- Contrasegnas seguras y gestores de contrasegnas
- Autenticacion multifactor (MFA): tipos y escenarios recomendados
- Principio de minimo privilegio: usuarios, permisos y UAC
- Cifrado basico: disco, archivos y comunicaciones (HTTPS/VPN)
- Copias de seguridad: estrategia 3-2-1 y pruebas de restauracion
- Navegacion segura y descargas: fuentes confiables y control de extensiones
- Seguridad en Wi-Fi: WPA2/WPA3, claves, red de invitados y router
- Control de dispositivos extraibles (USB): riesgos y politicas
- Monitorizacion y registros: eventos, alertas y respuesta inicial

UNIDAD.- Actualizaciones del software

- Que es un parche y por que corrige vulnerabilidades explotables
- Tipos de actualizacion: sistema operativo, aplicaciones, navegador y plugins
- Firmware y drivers: riesgos de desactualizacion y criterios de actualizacion
- Actualizaciones automaticas vs manuales: ventajas e inconvenientes
- Ventanas de mantenimiento y reinicios: planificacion y buenas practicas
- Verificacion de version y estado de parcheo del equipo
- Gestion de actualizaciones en entorno corporativo (politicas y control)
- Pruebas basicas tras actualizar: compatibilidad y estabilidad
- Rollback y restauracion: que hacer si una actualizacion falla
- Fin de soporte (EOL): riesgos y alternativas (migracion/actualizacion)