GUÍA DIDÁCTICA

CB05

CIBERSEGURIDAD PARA USUARIOS

CIBERSEGURIDAD PARA USUARIOS

RELACIÓN DE MÓDULOS DE FORMACIÓN

MÓDULO DE FORMACIÓN CB0501

INTRODUCCIÓN A LA SEGURIDAD EN SISTEMAS DE INFORMACIÓN

DURACIÓN

7,5 horas

PÚBLICO OBJETIVO

Empresas y emprendedores, estudiantes y público en general

OBJETIVO DEL MÓDULO

Clasificar y comprender los diferentes conceptos de seguridad en los sistemas y los requerimientos que estos conllevan para poder aplicarlos de forma avanzada.

CIBERSEGURIDAD PARA USUARIOS

RELACIÓN DE MÓDULOS DE FORMACIÓN

MÓDULO DE FORMACIÓN CB0502

CIBERSEGURIDAD

DURACIÓN

7,5 horas

PÚBLICO OBJETIVO

Empresas y emprendedores, estudiantes y público en general

OBJETIVO DEL MÓDULO

Lograr el entendimiento específico y avanzado de la importancia de la ciberseguridad de cara a lidiar con las diferentes amenazas existentes en la red, así como la gestión de la seguridad informática para aumentar la eficacia a nivel defensivo.

CIBERSEGURIDAD PARA USUARIOS

RELACIÓN DE MÓDULOS DE FORMACIÓN

MÓDULO DE FORMACIÓN CB0503

SOFTWARE DAÑINO

DURACIÓN

7,5 horas

PÚBLICO OBJETIVO

Empresas y emprendedores, estudiantes y público en general

OBJETIVO DEL MÓDULO

Estudiar el concepto y la clasificación de los softwares dañinos y como estos pueden dañar los dispositivos del usuario. Entender la importancia de la ingeniería social y el funcionamiento avanzado de las redes sociales en la época actual.

CIBERSEGURIDAD PARA USUARIOS

RELACIÓN DE MÓDULOS DE FORMACIÓN

MÓDULO DE FORMACIÓN CB0504

SEGURIDAD EN REDES INALÁMBRICAS

DURACIÓN

7,5 horas

PÚBLICO OBJETIVO

Empresas y emprendedores, estudiantes y público en general

OBJETIVO DEL MÓDULO

Comprender los conceptos avanzados relacionados con la seguridad en las redes inalámbricas y su relevancia a nivel de protección del usuario.

CIBERSEGURIDAD PARA USUARIOS

RELACIÓN DE MÓDULOS DE FORMACIÓN

MÓDULO DE FORMACIÓN CB0505

HERRAMIENTAS DE SEGURIDAD

DURACIÓN

7,5 horas

PÚBLICO OBJETIVO

Empresas y emprendedores, estudiantes y público en general

OBJETIVO DEL MÓDULO

Se profundizará en el conocimiento de las diferentes herramientas de seguridad que existen teniendo como principales objetivos la comprensión de las medidas de protección que otorgan, así como la gestión segura de recursos compartidos y el control de acceso de los usuarios al sistema operativo.

CIBERSEGURIDAD PARA USUARIOS

Índice de contenidos

CB 0501

Introducción a la seguridad en sistemas de información

Introducción
1.1 Conceptos de seguridad en los sistemas
1.1.1 Definición de seguridad informática
1.1.2 Importancia de la seguridad en sistemas de información
1.1.3 Objetivos de la seguridad informática
1.2 Clasificación de la seguridad en sistemas de información
1.2.1 Seguridad de la información
1.2.2 Seguridad de sistemas
1.2.3 Seguridad de redes
1.2.4 Seguridad física
1.3 Tipos de ataques informáticos
1.4 Requerimientos de seguridad en los sistemas de información
Resumen

CIBERSEGURIDAD PARA USUARIOS

Índice de contenidos

CB 0502

Ciberseguridad

Introducción
2.1 Concepto de ciberseguridad
2.1.1 Definición y alcance de la ciberseguridad
2.1.2 Evolución de la ciberseguridad
2.2 Amenazas más frecuentes en los sistemas de información
2.2.1 Malware
2.2.2 Phishing
2.2.3 Ingeniería social
2.2.4 Ataques de denegación de servicio (ddos)
2.2.5 Ransomware
2.3 Tecnologías de seguridad más habituales en ciberseguridad
2.3.1 Firewall
2.3.2 Antivirus
2.3.3 Criptografía
2.3.4 Ids/ips (sistemas de detección y prevención de intrusiones)
2.3.5 VPN(redes privadas virtuales)
2.3.6 Otros
2.4 Gestión de la seguridad informática en el ámbito de la ciberseguridad
2.4.1 Planificación de la seguridad
2.4.2 Implementación de políticas de seguridad
2.4.3 Monitoreo y detección de amenazas
2.4.4 Respuesta a incidentes de seguridad
2.4.5 Auditoría y evaluación de la seguridad
Resumen

CIBERSEGURIDAD PARA USUARIOS

Índice de contenidos

CB 0503

Software dañino e inteligencia artificial

Introducción
3.1 Software dañino e inteligencia artificial
3.1.1 Uso de IA en el desarrollo de malware
3.1.2 Amenazas específicas de seguridad asociadas con IA
3.1.3 Desafíos y oportunidades para la seguridad cibernética y la IA
3.2 Amenazas persistentes y avanzadas en el software dañino
3.2.1 APT (amenazas persistentes avanzadas)
3.2.2 Botnets
3.2.3 Rootkits
3.3 Técnicas y estrategias de defensa basadas en IA
3.3.1 Uso de herramientas de seguridad basadas en IA
3.3.2 Educación y concienciación de usuarios
3.4 Ingeniería social y redes sociales
3.4.1 Ingeniería social e IA
3.4.2 Redes sociales e IA
Resumen

Índice de contenidos

CB 0504

Seguridad en redes inalámbricas

Introducción
4.1 Fundamentos de seguridad en redes inalámbricas
4.1.1 Tipos de redes inalámbricas
4.1.2 Vulnerabilidades comunes en redes inalámbricas
4.2 Protocolos de seguridad para redes inalámbricas
4.2.1 Wep (wired equivalent privacy)
4.2.2 Wpa (wi-fi protected access)
4.2.3 Wpa2 y wpa3
4.3 Amenazas y vulnerabilidades en redes inalámbricas
4.3.1 Acceso no autorizado
4.3.2 Intercepción de tráfico
4.3.3 Ataques de suplantación de identidad (spoofing)
4.4 Medidas de protección y mitigación de riesgos en redes inalámbricas
4.4.1 Seguridad física de los dispositivos
4.4.2 Configuración adecuada de la red
4.4.3 Uso de protocolos de seguridad robustos
Resumen

Índice de contenidos

CB 0505

hHerramientas de seguridad

Introducción
5.1 Medidas de protección
5.1.1 Copias de seguridad
5.1.2 Encriptación de datos
5.1.3 Actualización de software y parches de seguridad
5.2 Control de acceso de los usuarios al sistema operativo
5.2.1 Autenticación de usuarios
5.2.2 Autorización de accesos
5.3 Gestión segura de comunicaciones, carpetas compartidas y otros recursos de red
5.3.1 VPN (redes privadas virtuales)
5.3.2 Cortafuegos (firewalls)
5.3.3 Seguridad en la transferencia de archivos y comunicaciones
5.4 Herramientas y técnicas para la protección frente a códigos maliciosos y amenazas externas
5.4.1 Antivirus y antimalware
5.4.2 Análisis de vulnerabilidades
5.4.3 Sandbox y virtualización para la ejecución segura de programas
Resumen