ingertec

COD	CIBSEG
MATERIA	CIBERSEGURIDAD
TIPO	ESPECIALIZACION
BONIFICABLE	100%

* Gastos de gestión de Bonificación. 10% del valor del importe a bonificar.

¿A QUIÉN ESTÁ DIRIGIDO?

Este curso está dirigido a profesionales de cualquier sector que busquen adentrarse en el mundo de la ciberseguridad para desarrollar planes de seguridad informática, así como a profesionales del sector de las tecnologías que quieran formarse más profundamente en cuestiones relacionadas con el tema.

OBJETIVOS

Gracias a este curso, el alumno obtendrá una formación que le permitirá:

- Conocer la importancia de la ciberseguridad y las buenas prácticas en la gestión de sistemas informáticos.
- Identificar las principales amenazas a los sistemas de seguridad, independientemente del tipo de redes de las que formen parte o el sistema operativo que utilicen.
- Ser capaz de desarrollar un plan de ciberseguridad y/o proyectos relacionados con la seguridad informática.

ingertec

TEMARIO

1. Introducción a la seguridad en los sistemas de información

1.1. Conceptos de seguridad en los sistemas de información
1.2. Clasificación de las medidas de seguridad
1.3. Ejemplos de medidas de seguridad
1.4. Requerimientos de seguridad en los sistemas de información
1.5. Clasificación de las amenazas
1.6. Principios y buenas prácticas de la seguridad de la información
1.7. Normativas, regulaciones y legislación
1.8. Sistemas de gestión de la seguridad de la información
1.9. Introducción a la elaboración de un Plan de Recuperación ante Desastres (DRP)

2. Introducción a la ciberseguridad

2.1. Introducción
2.2. Concepto de ciberseguridad
2.3. Terminología de la ciberseguridad
2.4. Amenazas más frecuentes a los sistemas de información
2.5. Gestión de la seguridad informática
2.6. Introducción al análisis forense y peritaje
2.7. Equipos de respuesta: Red Team, Blue Team y Purple Team

3. Software malicioso (malware)

3.1. Introducción
3.2. Conceptos sobre software dañino
3.3. Clasificación del software dañino
3.4. Amenazas persistentes y avanzadas
3.5. Ingeniería social y redes sociales
3.6. Protección, análisis y detección: Antivirus, cortafuegos, antimalware
3.7. Ransomware

4. Seguridad en la web

4.1. Introducción
4.2. Protocolo HTTP y tecnologías Web
4.3. Vulnerabilidades del lado de cliente
4.4. Guía de buenas prácticas. Autenticación en dos pasos

5. Seguridad en redes inalámbricas (WLAN)

5.1. Introducción
5.2. Introducción a los estándar inalámbricos 802.11
5.3. Autenticación
5.4. Distinción entre dispositivos corporativos y clientes externos
5.5. Tipos de redes inalámbricas y protocolos de seguridad (WEP, WPA)
5.6. Configuración recomendada para una red inalámbrica

6. Seguridad en redes corporativas

6.1. Introducción

6.2. Protocolos seguros en la LAN
6.3. Reconocimiento de red
6.4. Vulnerabilidades y ataques en red
6.5. Gestión segura de comunicaciones, carpetas y otros recursos compartidos
6.6. Gestión de carpetas compartidas en la red
6.7. Seguridad en sistemas Windows

7. Vulnerabilidades en sistemas Windows

7.1. Control de acceso de los usuarios al sistema operativo
7.2. Introducción al bastionado (hardening) en Windows

8. Seguridad en sistemas Linux

8.1. Introducción
8.2. Medidas básicas de seguridad en equipos de escritorio y servidores con Linux
8.3. Introducción al bastionado (hardening) en Linux

VENTAJAS

- Servicio de Tutorización
- Dinamización y Atención al Alumnado
- Libertad horaria para realizar el curso
- Autoevaluaciones tipo test en Bloques de preguntas
- Materiales disponibles 24/7 en tu Plataforma de Teleformación
- Mensajería directa con el Tutor para la resolución de dudas
- Foros de consulta para debates relacionados con la materia
- Salas de Chat y Videoconferencia a disposición del alumno
- Examen final de aptitud online sin requisitos presenciales
- Soporte Técnico Informático sobre el Campus incluido