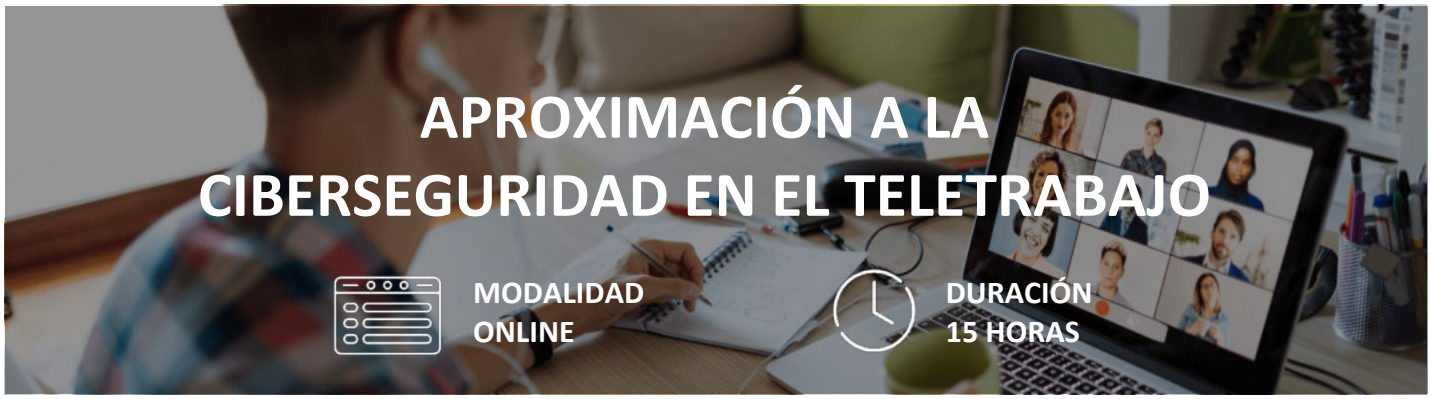
ingertec



COD	IS2722
MATERIA	SEGURIDAD DE LA INFORMACIÓN
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

Al término de este curso, el alumnado sabrá:

- 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 realizar la prevención y dar respuesta a los incidentes ocasionados.
- Conocer prácticas seguras y cultura de la ciberseguridad.

ingertec

TEMARIO

1. Introducción a la Ciberseguridad

1.1. Introducción
1.2. Concepto de Ciberseguridad
1.3. Terminología de la Ciberseguridad
1.4. Amenazas más Frecuentes a los Sistemas de Información
1.5. Gestión de la Seguridad Informática

2. Conceptos Básicos de Ciberseguridad

2.1. Identidad y Autentificación
2.2. Contraseñas seguras y autenticación de dos factores
2.3. Principios de Cifrado y Privacidad de Datos
2.4. Requerimientos de Seguridad en los Sistemas de Información
2.5. Clasificación de las Amenazas
2.6. Principios y Buenas Prácticas de la Seguridad de la Información
2.7. Sistemas de Gestión de la Seguridad de la Información (SGSI)

3. Ciberseguridad en el Lugar de Trabajo

3.1. Política de seguridad en el trabajo
3.2. Seguridad en la red corporativa y en redes Wifi
3.3. Uso seguro del correo electrónico y mensajería
3.4. Gestión Segura de Comunicaciones, Carpetas y Otros Recursos Compartidos
3.5. Introducción a la Elaboración de un Plan de Recuperación ante Desastres (DRP)

4. Protección de Dispositivos

4.1. Seguridad en dispositivos móviles
4.2. Seguridad en PCs de escritorio y portátiles
4.3. Actualización de software y parches

5. Software malicioso (malware) y ataques informáticos

5.1. Tipos de malware (virus, ransomware, spyware)
5.2. Phishing y ataques de ingeniería social
5.3. Ataques de denegación de servicio (DoS) y distribuidos (DDoS)
5.4. Protección, Análisis y Detección: Antivirus, Cortafuegos y Antimalware

6. Prevención y Respuesta a Incidentes

6.1. Monitorización de seguridad y detección de amenazas
6.2. Planificación de respuesta a incidentes
6.3. Recuperación de datos y sistemas después de un ataque
6.4. Introducción al Análisis Forense y Peritaje
6.5. Equipos de Respuesta: Red Team, Blue Team y Purple Team

7. Cumplimiento Legal y Regulatorio

7.1. Leyes y Regulaciones de Ciberseguridad
7.2. Protección de la privacidad de datos

7.3. Conformidad con estándares de seguridad

8. Prácticas Seguras y Cultura de Ciberseguridad

8.1. Educación y concienciación de los empleados
8.2. Buenas prácticas en la gestión de contraseñas
8.3. Formación continua en ciberseguridad

9. Seguridad en Sistemas Windows

9.1. Vulnerabilidades en Sistemas Windows
9.2. Control del Acceso de los Usuarios al Sistema Operativo
9.3. Introducción al Bastionado (Hardening) en Windows

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

900 897 931 formacion@ingertec.com www.ingertec.com