Telefono y whatsapp +34 630 06 65 14



# CIBERSEGURIDAD. SECTOR HOSTELERÍA. IFCT151PO

SKU: EVOL-7171-iNO-B | Categorías: INFORMÁTICA Y COMUNICACIONES, Seguridad Informática

## INFORMACIÓN DEL CURSO

**Horas** <u>150</u>

Más información

CONTENIDO ADAPTADO A CERTIFICADO DE

PROFESIONALIDAD

CURSO DE ESPECIALIZACIÓN

## CIBERSEGURIDAD. SECTOR HOSTELERÍA

## **Objetivos**

Este Curso IFCT151PO CIBERSEGURIDAD. SECTOR HOSTELERÍA le ofrece una formación especializada en la materia dentro de la Familia Profesional de Informática y comunicaciones. Con este CURSO IFCT151PO CIBERSEGURIDAD. SECTOR HOSTELERÍA el alumno será capaz de Utilizar el conjunto de herramientas, políticas, conceptos y salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios.

#### **Contenidos**

#### UNIDAD DIDÁCTICA 1. CONCEPTOS BÁSICOS DE CIBERSEGURIDAD

- 1. El valor de la información
- 2. Hackers y ciberdelincuentes
- 3. Seguridad por defecto
- 4. Políticas y procedimientos
- 5. Delitos informáticos
- 6. Código de derecho de ciberseguridad

## UNIDAD DIDÁCTICA 2. AMENAZAS, VULNERABILIDADES Y RIESGOS

- 1. Tipos de Amenazas.
- 2. Tipos de vulnerabilidades.
- 3. Vulnerabilidades de IoT
- 4. Ingeniería Social
- 5. Malware
- 6. Virus







Telefono y whatsapp +34 630 06 65 14

- 7. Troyanos
- 8. Gusanos
- 9. Spyware
- 10. Ransomware
- 11. PUPs
- 12. Key Loggers
- 13. Bots.

## UNIDAD DIDÁCTICA 3. ATAQUES A CREDENCIALES

- 1. Demostración práctica del robo de credenciales de usuario
- 2. Almacenamiento de credenciales
- 3. Passwords en Windows
- 4. Credenciales en caché
- 5. Contramedidas

# UNIDAD DIDÁCTICA 4. DOS/DDOS

- 1. Características
- 2. Motivación
- 3. Víctimas
- 4. Ejemplos
- 5. Contramedidas

## **UNIDAD DIDÁCTICA 5. OTROS RIESGOS**

- 1. Webcam
- 2. Estafas telefónicas
- 3. Dispositivos USB
- 4. Seguridad física

## UNIDAD DIDÁCTICA 6. MEJORAR LA SEGURIDAD. PARTE I

- 1. Password
- 2. Ataques por e-mail (pishing)
- 3. Seguridad en el navegador
- 4. Seguridad Wireless
- 5. VPN
- 6. Seguridad DNS
- 7. Usuarios predeterminados
- 8. Actualizaciones
- 9. Antivirus
- 10. Firewalls (cortafuegos)
- 11. Sentido Común







Telefono y whatsapp +34 630 06 65 14

### UNIDAD DIDÁCTICA 7. MEJORAR LA SEGURIDAD. PARTE II

- 1. Seguridad por defecto y/o por diseño
- 2. Sistemas actualizados
- 3. Control de accesos
- 4. Gestión segura de contraseñas
- 5. Antimalware.
- 6. El correo electrónico
- 7. Navegación Segura
- 8. Aplicaciones de confianza.
- 9. Copias de seguridad
- 10. Destrucción segura
- 11. Necesidades específicas en IoT
- 12. Necesidades específicas en Cloud.
- 13. Sistemas operativos de confianza (TOS)

### UNIDAD DIDÁCTICA 8. REACCIÓN FRENTE UN INCIDENTE

- 1. Detección
- 2. Análisis
- 3. Evaluación
- 4. Clasificación de los incidentes de seguridad
- 5. Priorización
- 6. Reacción

Tal vez te interese este curso: Auditoría y Certificación del RGPD

O quizá este otro: COMPETENCIAS DIGITALES AVANZADAS

Síguenos en: Instagram

