IFCT151PO Ciberseguridad. Sector hostelería

Descripción:

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.

Nº de horas:
150 horas

Objetivos:

• Estudiar la figura del hacker y del ciberdelincuente.
• Conocer y saber aplicar los principales estándares de la seguridad de la información.
• Estudiar los tipos de amenazas que reciben los sistemas informáticos.
• Profundizar en el conocimiento de los diferentes tipos de malware.
• Conocer qué son las credenciales y qué valor tienen dentro de una empresa u organización.
• Estudiar el almacenamiento de credenciales.
• Explicar qué son las credenciales en caché.
• Saber aplicar las contramedidas adecuadas contra los ataques a credenciales.
• Conocer las características de los ataques DoS y DDoS.
• Explicar las diferentes motivaciones que tienen los ciberdelincuentes para realizar los ataques.
• Conocer los riesgos que conlleva utilizar una webcam y las pautas que se deben seguir para asegurarla.
• Explicar los diferentes tipos de estafas telefónicas.
• Aprender los riesgos asociados al uso de un dispositivo USB.
• Estudiar aspectos relacionados con la seguridad física.
• Entender la importancia de mantener los sistemas actualizados.
• Saber cómo gestionar el control de accesos y la gestión segura de contraseñas.
• Estudiar cómo actúa un antimalware.
• Explicar qué son las aplicaciones de confianza.
• Comprender las necesidades especiales en IoT y en la nube.
• Exponer qué son los sistemas operativos de confianza.
• Estudiar cómo detectar un incidente de seguridad.
• Conocer la manera de realizar un análisis de un incidente.
• Explicar cómo se realiza la priorización de de los incidentes.
• Saber reaccionar frente a un incidente.

Requisitos y conocimientos:

No son necesarios conocimientos previos, sin embargo es aconsejable contar con nociones básicas de matemáticas y tecnologías, así como facilidad de comprensión lectora para seguir y asimilar correctamente los contenidos. También es de gran valor disponer de capacidad de planificación y organización.

Contenido IFCT151PO: Ciberseguridad. Sector hostelería

Unidad didáctica 1. Conceptos básicos de ciberseguridad
1.1 El valor de la información.
1.2. Hackers y ciberdelincuentes.
1.3. Seguridad por defecto.
1.4. Políticas y procedimientos.
1.5. Delitos informáticos.
1.6. Código de derecho de ciberseguridad.

Unidad didáctica 2. Amenazas, vulnerabilidades y riesgos
2.1. Tipos de Amenazas.
2.2. Tipos de vulnerabilidades.
2.3. Vulnerabilidades de IoT.
2.4. Ingeniería Social.
2.5. Malware.

2.6. Virus. Troyanos. Gusanos. Spyware. Ransomware. PUPs. Key Loggers. Bots.

Unidad didáctica 3. Ataques a credenciales
3.1. Demostración práctica del robo de credenciales de usuario.
3.2. Almacenamiento de credenciales.
3.3. Passwords en Windows.
3.4. Credenciales en caché.

Unidad didáctica 4. DoS/DDoS
4.1. Características. Motivación.
4.2. Víctimas.
4.3. Ejemplos.
4.4. Contramedidas.

Unidad didáctica 5. Otros riesgos
5.1. Cámara web (webcam).
5.2. Estafas telefónicas.
5.3. Dispositivos USB.
5.4. Seguridad física.

Unidad didáctica 6. Mejorar la seguridad. Parte I
6.1. Password.
6.2. Ataques por e-mail (phishing).
6.3. Seguridad en el navegador.
6.4. Seguridad Wireless.
6.5. VPN.
6.6. Seguridad DNS.
6.7. Usuarios predeterminados. Actualizaciones.
6.8. Antivirus. Firewalls (cortafuegos).
6.9. Sentido Común.

Unidad didáctica 7. Mejorar la seguridad. Parte II
7.1. Seguridad por defecto y/o por diseño.
7.2. Sistemas actualizados.
7.3. Control de accesos. Gestión segura de contraseñas.
7.4. Antimalware.
7.5. El correo electrónico. Navegación segura.
7.6. Aplicaciones de confianza.
7.7. Copias de seguridad. Destrucción segura.
7.8. Necesidades especiales en IoT.
Necesidades específicas en Cloud.
7.9. Sistemas operativos de confianza (TOS).

Unidad didáctica 8. Reacción frente a un incidente
8.1. Detección.
8.2. Análisis.
8.3. Evaluación.
8.4. Clasificación de los incidentes de seguridad.
8.5. Priorización.
8.6. Reacción.