

GUÍA DIDÁCTICA

GESTIÓN DE LA SEGURIDAD INFORMÁTICA EN LA EMPRESA (IFCT050PO)

ESTATAL

Presentación

A través de la realización de este curso, se revisarán diferentes servicios y aplicaciones de Internet con el objeto de entender los principales riesgos (ciber-acoso, sexting, ataques de software malicioso, etc.) a los que se enfrentan los menores en el uso de las TIC (Redes sociales, mensajería instantánea, blogs, weblogs, bitácoras, foros, buscadores, etc.)

Descripción

A nadie se nos escapa la problemática que existe con los contenidos en Internet, con los límites que se suponen en la libertad de expresión y de información. Evidentemente Internet no es un espacio ajurídico y sin ningún tipo de control. Aunque a alguien se le pueda escapar, las respectivas jurisdicciones nacionales protegen esa libertad de expresión y de información que caracteriza a la Red, mediante la protección de los derechos fundamentales y dentro de estos, muy especialmente los derechos fundamentales de los menores.

Características



Modalidad

E-learning.



Duración

100h.

Contacto

GESTIÓN DE LA SEGURIDAD INFORMÁTICA EN LA EMPRESA (IFCT050PO)

Objetivos

Gestionar la seguridad informática en la empresa.

Programa

100 horas	GESTIÓN DE LA SEGURIDAD INFORMÁTICA EN LA EMPRESA (IFCT050PO)	
100 horas	<p>1. Introducción a la seguridad.</p> <p>1.1. Introducción a la seguridad de información. 1.2. Modelo de ciclo de vida de la seguridad de la información. 1.3. Confidencialidad, integridad y disponibilidad. Principios de protección de la seguridad de la información. 1.4. Políticas de seguridad. 1.5. Tácticas de ataque. 1.6. Concepto de hacking. 1.7. Árbol de ataque. 1.8. Lista de amenazas para la seguridad de la información. 1.9. Vulnerabilidades. 1.10. Vulnerabilidades en sistemas Windows. 1.11. Vulnerabilidades en aplicaciones multiplataforma. 1.12. Vulnerabilidades en sistemas Unix y Mac OS. 1.13. Buenas prácticas y salvaguardas para la seguridad de la red. 1.14. Recomendaciones para la seguridad de su red.</p> <p>2. Políticas de seguridad.</p> <p>2.1. Introducción a las políticas de seguridad. 2.2. ¿Por qué son importantes las políticas? 2.3. Qué debe de contener una política de seguridad. 2.4. Lo que no debe contener una política de seguridad. 2.5. Cómo conformar una política de seguridad informática. 2.6. Hacer que se cumplan las decisiones sobre estrategia y políticas.</p> <p>3. Auditoría y normativa de seguridad.</p> <p>3.1. Introducción a la auditoría de seguridad de la información y a los sistemas de gestión de seguridad de la información. 3.2. Ciclo del sistema de gestión de seguridad de la información. 3.3. Seguridad de la información. ã 3.4. Definiciones y clasificación de los activos. 3.5. Seguridad humana, seguridad física y del entorno. 3.6. Gestión de comunicaciones y operaciones. 3.7. Control de accesos. 3.8. Gestión de continuidad del negocio. 3.9. Conformidad y legalidad.</p> <p>4. Estrategias de seguridad.</p> <p>4.1. Menor privilegio. 4.2. Defensa en profundidad. 4.3. Punto de choque. 4.4. El eslabón más débil. 4.5. Postura de fallo seguro. 4.6. Postura de negación establecida: lo que no está prohibido. 4.7. Postura de permiso establecido: lo que no está permitido. 4.8. Participación universal. 4.9. Diversificación de la defensa. 4.10. Simplicidad.</p>	<p>5. Exploración de las redes.</p> <p>5.1. Exploración de la red. 5.2. Inventario de una red. Herramientas del reconocimiento. 5.3. NMAP y SCANLINE. 5.4. Reconocimiento. Limitar y explorar. 5.5. Reconocimiento. Exploración. 5.6. Reconocimiento. Enumerar.</p> <p>6. Ataques remotos y locales.</p> <p>6.1. Clasificación de los ataques. 6.2. Ataques remotos en UNIX. 6.3. Ataques remotos sobre servicios inseguros en UNIX. 6.4. Ataques locales en UNIX. 6.5. ¿Qué hacer si recibimos un ataque?</p> <p>7. Seguridad en redes inalámbricas</p> <p>7.1. Introducción. 7.2. Introducción al estándar inalámbrico 802.11 ã WIFI 7.3. Topologías. 7.4. Seguridad en redes Wireless. Redes abiertas. 7.5. WEP 7.6. WEP Ataques. 7.7. Otros mecanismos de cifrado.</p> <p>8. Criptografía y criptoanálisis.</p> <p>8.1. Criptografía y criptoanálisis: introducción y definición. 8.2. Cifrado y descifrado. 8.3. Ejemplo de cifrado: relleno de una sola vez y criptografía clásica. 8.4. Ejemplo de cifrado: criptografía moderna. 8.5. Comentarios sobre claves públicas y privadas: sesiones.</p> <p>9. Autenticación.</p> <p>9.1. Validación de identificación en redes. 9.2. Validación de identificación en redes: métodos de autenticación. 9.3. Validación de identificación basada en clave secreta compartida: protocolo. 9.4. Establecimiento de una clave compartida: intercambio de claves Diffie-Hellman. 9.5. Validación de identificación usando un centro de distribución de claves. 9.6. Protocolo de autenticación Kerberos. 9.7. Validación de identificación de clave pública. 9.8. Validación de identificación de clave pública: protocolo de interbloqueo.</p>