TEMARIO

TECNICO EN SEGURIDAD INFORMATICA

Introducción a la Seguridad Informática

Conceptos básicos de seguridad informática: Definición de seguridad informática. Historia de la seguridad informática. Principios de la seguridad informática. Tipos de amenazas de seguridad informática: Ataques físicos. Ataques de redes. Ataques de aplicaciones. Ataques de datos. Ataques de la nube. Ciclo de vida de la seguridad informática: Identificación de riesgos. Evaluación de riesgos. Mitigación de riesgos. Ética de la seguridad informática: Ética en el uso de la tecnología. Ética en la seguridad de la información. Ética en la respuesta a incidentes de seguridad.

Seguridad de la Información

Seguridad física: Controles de acceso físico. Seguridad de los sistemas de archivos. Protección contra incendios. Seguridad de redes: Firewalls. Encriptación. IPS y IDS. Seguridad de aplicaciones: Desarrollo seguro de software. Análisis de vulnerabilidades. Pruebas de penetración. Seguridad de datos: Gestión de contraseñas. Criptografía. Protección contra pérdida de datos. Seguridad de la nube: Seguridad de la infraestructura en la nube. Seguridad de los datos en la nube. Seguridad de las aplicaciones en la nube. Gestión de riesgos de seguridad: Identificación de riesgos. Evaluación de riesgos. Mitigación de riesgos. Ética de la seguridad: Impacto de la seguridad de la información en la sociedad. Responsabilidad social de la seguridad de la información.

Gestión de Incidentes de Seguridad

Introducción a la gestión de incidentes de seguridad: Definición de incidente de seguridad. Ciclo de vida de un incidente de seguridad. Roles y responsabilidades en la gestión de incidentes de seguridad. Etapas de la gestión de incidentes de seguridad: Detección de incidentes. Investigación de incidentes. Contención de incidentes. Recuperación de incidentes. Aprendizaje de incidentes. Herramientas y técnicas de gestión de incidentes de seguridad: Sistemas de detección de incidentes. Sistemas de respuesta a incidentes. Herramientas forenses. Gestión de riesgos de incidentes de seguridad: Identificación de riesgos de incidentes. Evaluación de riesgos de incidentes. Mitigación de riesgos de incidentes. Ética de la gestión de incidentes de seguridad: Protección de la confidencialidad de la información. Responsabilidades legales.

Análisis forense digital

Introducción al análisis forense digital: Definición de análisis forense digital. Historia del análisis forense digital. Principios del análisis forense digital. Evidencia digital: Tipos de evidencia digital. Adquisición de evidencia digital. Preservación de evidencia digital. Técnicas de análisis forense digital: Análisis de archivos. Análisis de redes. Análisis de hardware. Análisis de software. Herramientas de análisis forense digital: Herramientas de adquisición de evidencia digital. Herramientas de análisis de archivos. Herramientas de análisis de redes. Herramientas de análisis de hardware. Herramientas de análisis de software. Legislación en materia de análisis forense digital: Leyes y regulaciones aplicables al análisis forense digital. Ética en el análisis forense digital.

Criptografía

Introducción a la criptografía: Definición de criptografía. Historia de la criptografía. Principios de la criptografía. Tipos de criptografía: Criptografía simétrica. Criptografía asimétrica. Criptografía de clave pública. Criptografía de clave privada. Algoritmos criptográficos: Algoritmos de cifrado simétrico. Algoritmos de cifrado asimétrico. Algoritmos de firma digital. Aplicaciones de la criptografía: Seguridad de la información. Firma digital. Comercio electrónico. Seguridad de las comunicaciones: Seguridad de las redes. Seguridad de las aplicaciones. Técnicas de ataque a la criptografía: Ataques a la criptografía simétrica. Ataques a la criptografía asimétrica. Ataques a la firma digital.