Madrid Tech School

Tema 1: Fundamentos de Ciberseguridad

Descripción del curso:

Proporciona una **introducción** a los fundamentos de la ciberseguridad, incluyendo **conceptos básicos** de seguridad, riesgos y amenazas, **tipos** de ataques y vulnerabilidades, **políticas** y procedimientos de seguridad, y mejores prácticas de seguridad. También se discutirán los **aspectos legales y éticos** de la ciberseguridad.

Objetivos de aprendizaje:

- **Comprender** los conceptos básicos de la ciberseguridad.
- **Identificar** los riesgos y amenazas comunes en la seguridad cibernética.
- **Comprender** los tipos de ataques y vulnerabilidades comunes en la seguridad.
- **Conocer** las políticas y procedimientos de seguridad utilizados.
- **Conocer** las mejores prácticas de seguridad para proteger los sistemas y datos.
- **Comprender** los aspectos legales y éticos de la ciberseguridad.

Programa:

1. Introducción a la ciberseguridad
2. Amenazas y vulnerabilidades en la seguridad informática
3. Políticas de seguridad y modelos de seguridad
4. Arquitectura de seguridad en la empresa
5. Gestión de riesgos y continuidad de negocio
6. Protección de la información y privacidad
7. Técnicas de análisis y prevención de incidentes de seguridad

Audiencia:

Adecuado para aquellos que tienen un interés en la ciberseguridad y quieren aprender los fundamentos básicos de la seguridad cibernética.

Duración: 20 horas.

Requisitos previos: No se requiere experiencia previa en seguridad cibernética

Madrid Tech School

Tema 2: Seguridad en redes y sistemas

Descripción del curso:

Se centra en la **seguridad** de redes y sistemas, incluyendo la **identificación y gestión de riesgos de seguridad**, la identificación y protección de **vulnerabilidades** en sistemas y redes, y la **configuración** y gestión de políticas de seguridad de redes y sistemas.

Objetivos de aprendizaje:

- **Comprender** los riesgos de seguridad en redes y sistemas.
- **Identificar** y proteger las vulnerabilidades en sistemas y redes.
- **Configurar** y **gestionar** las políticas de seguridad de redes y sistemas.
- **Conocer** las herramientas y técnicas utilizadas en la seguridad de redes y sistemas.

Programa:

1. Introducción a la seguridad en redes y sistemas
2. Amenazas y vulnerabilidades en las redes y sistemas informáticos
3. Seguridad en redes y sistemas operativos
4. Firewall y control de acceso
5. Tecnologías VPN y autenticación de usuarios
6. Monitoreo y análisis de tráfico de red
7. Prácticas recomendadas en la seguridad en redes y sistemas

Audiencia:

Adecuado para aquellos que tienen un **interés** en la seguridad de redes y sistemas, y quieren **aprender a identificar y proteger las vulnerabilidades** en sistemas y redes.

Duración: 30 horas.

Requisitos previos: Se requiere conocimiento básico de redes y sistemas.

Madrid Tech School

Tema 3: Protección de datos y privacidad

Descripción del curso:

Se enseñarán los **fundamentos de protección de datos y privacidad**, incluyendo la regulación de protección de datos en diferentes jurisdicciones y las **mejores prácticas** de seguridad de la información. Se aprenderá a **diseñar e implementar medidas de seguridad** para **garantizar la privacidad** de los datos de los usuarios y protegerlos de amenazas internas y externas.

Objetivos de aprendizaje:

- **Comprender** la regulación de protección de datos en diferentes jurisdicciones.
- **Conocer** las mejores prácticas de seguridad de la información.
- **Diseñar** e **implementar** medidas de seguridad para garantizar la privacidad de los datos de los usuarios.
- **Proteger** los datos de amenazas internas y externas.

Programa:

1. Introducción a la protección de datos y privacidad
2. Principios y normativas en protección de datos
3. Gestión de la privacidad y confidencialidad de la información
4. Cifrado y técnicas de anonimización
5. Auditorías de seguridad y cumplimiento de regulaciones
6. Protección de datos en entornos móviles y en la nube
7. Consideraciones éticas en la protección de datos y privacidad

Audiencia:

Dirigido a **profesionales de tecnología de la información, abogados y cualquier persona** interesada en la protección de datos y privacidad.

Duración: 20 horas.

Requisitos previos: No se requieren conocimientos previos de protección de datos o privacidad, aunque se recomienda tener experiencia en tecnología de la información.

Madrid Tech School

Tema 4: Seguridad en la nube

Descripción del curso:

Se enseñará a comprender los **conceptos y herramientas necesarias** para garantizar la seguridad en la nube. Aprenderán los **principios fundamentales** de la seguridad en la nube, incluyendo la **autenticación, autorización y cifrado de datos**, y cómo aplicar estos principios en diferentes entornos de la nube. También se explorarán las **mejores prácticas** para la protección de datos y la privacidad en la nube.

Objetivos de aprendizaje:

- **Comprender** los principios fundamentales de seguridad en la nube
- **Conocer** los principales desafíos de seguridad en la nube y cómo abordarlos.
- **Aprender** sobre las herramientas y tecnologías de seguridad en la nube, incluyendo la autenticación, autorización y cifrado de datos.
- **Comprender** las mejores prácticas para la protección de datos y la privacidad.
- **Aprender** a implementar soluciones de seguridad en la nube.

Programa:

1. Introducción a la seguridad en la nube
2. Modelos de servicio y arquitecturas en la nube
3. Amenazas y vulnerabilidades en la nube
4. Seguridad en la infraestructura y servicios en la nube
5. Seguridad en la gestión de identidades y accesos
6. Monitorización y análisis de actividad en la nube
7. Buenas prácticas en la seguridad en la nube

Audiencia:

Está dirigido a profesionales de **TI, desarrolladores, administradores de sistemas y cualquier persona** interesada en la seguridad en la nube.

Duración: Entre 20-30 horas.

Requisitos previos: conocimientos básicos de informática y redes, conceptos básicos de la nube y sus modelos de servicio y seguridad de la información.

Madrid Tech School

Tema 5: Ethical Hacking y pentesting

Descripción del curso:

Está diseñado para enseñar a cómo **identificar vulnerabilidades** en los sistemas informáticos y aplicaciones web y cómo realizar **pruebas de penetración éticas** para mejorar la seguridad de los mismos. A través de una combinación de conferencias, demostraciones y prácticas, se aprenderá los **fundamentos del hacking ético** y las **técnicas** de pruebas de penetración.

Objetivos de aprendizaje:

- **Comprender** los conceptos básicos de la seguridad informática y el hacking ético.
- **Identificar** las vulnerabilidades comunes en los sistemas informáticos.
- **Realizar** pruebas de penetración éticas para **mejorar** la seguridad de los sistemas.
- **Utilizar** herramientas de hacking ético y pentesting para **identificar** vulnerabilidades y explotarlas.
- **Comprender** la importancia de la ética en la realización de pruebas de penetración.

Programa:

1. Introducción a la seguridad ofensiva
2. Reconocimiento y recopilación de información
3. Escaneo y enumeración de vulnerabilidades
4. Explotación de vulnerabilidades
5. Pruebas de penetración web y aplicaciones móviles
6. Técnicas de evasión y ocultación de actividades
7. Reporte y gestión de resultados en pruebas de penetración

Audiencia:

Dirigido a **estudiantes** y **profesionales** interesados en aprender sobre seguridad informática, hacking ético y pruebas de penetración.

Duración: 40 horas.

Requisitos previos: conocimientos básicos de informática y redes, así como experiencia en programación. Además, es recomendable que tengan conocimientos previos sobre seguridad informática y hacking ético.

Madrid Tech School

Tema 6: Análisis de vulnerabilidades y riesgos

Descripción del curso:

Diseñado para proporcionar una comprensión detallada de las **técnicas y herramientas** utilizadas para identificar y **analizar vulnerabilidades** en sistemas informáticos y **evaluar los riesgos** asociados. Se aprenderá sobre los principales **tipos** de vulnerabilidades, técnicas de explotación, evaluación de riesgos y mitigación de riesgos.

Objetivos de aprendizaje:

- **Identificar** y **evaluar** vulnerabilidades en sistemas informáticos.
- **Utilizar** herramientas y técnicas para **realizar** análisis de vulnerabilidades y riesgos.
- **Evaluar** el impacto y la probabilidad de la explotación de vulnerabilidades.
- **Realizar** evaluaciones de riesgos y **desarrollar** planes de mitigación.

Programa:

1. Introducción a la seguridad de la información
2. Evaluación de vulnerabilidades y riesgos
3. Identificación y clasificación de vulnerabilidades
4. Análisis y evaluación de riesgos
5. Herramientas de análisis de vulnerabilidades
6. Pruebas de penetración y simulaciones de ataques

Audiencia:

Dirigido a **profesionales** de la **seguridad informática, administradores de sistemas, ingenieros de red y cualquier persona interesada** en aprender sobre la evaluación de vulnerabilidades y riesgos en sistemas informáticos.

Duración: Mínimo 30 horas.

Requisitos previos: Conocimientos básicos de seguridad informática y sistemas informáticos, incluyendo redes y sistemas operativos. Además, se recomienda tener experiencia práctica en la administración de sistemas informáticos y el uso de herramientas de seguridad.

Madrid Tech School

Tema 7: Seguridad en aplicaciones web

Descripción del curso:

Diseñado para enseñar a cómo **identificar y prevenir vulnerabilidades** de seguridad en aplicaciones web. Se aprenderá **técnicas de hacking ético** y cómo aplicar estas **técnicas** para proteger aplicaciones web. Cubrirá temas como la **configuración segura** de aplicaciones web, la identificación de vulnerabilidades comunes, la **inyección de SQL**, la **vulnerabilidad de Cross-site Scripting**, la gestión de sesiones seguras y la protección de aplicaciones móviles.

Objetivos de aprendizaje:

- **Identificar** las vulnerabilidades más comunes en aplicaciones web y móviles.
- **Aplicar** técnicas de hacking ético para **evaluar** la seguridad de una aplicación web.
- **Comprender** los conceptos de inyección de SQL, Cross-site Scripting y gestión de sesiones seguras.
- **Configurar** aplicaciones web de forma segura y **mitigar** vulnerabilidades.
- **Proteger** aplicaciones móviles contra ataques de seguridad.

Programa:

1. Conceptos básicos de seguridad en aplicaciones web
2. Amenazas comunes en aplicaciones web
3. Inyección de código y SQL
4. Cross-Site Scripting (XSS)
5. Manejo de sesiones y autenticación
6. Seguridad en APIs y servicios web

Audiencia:

Dirigido a **desarrolladores web, administradores de sistemas, auditores de seguridad y cualquier persona interesada** en aprender sobre la seguridad en aplicaciones web.

Duración: 20-30 horas.

Requisitos previos: conocimientos básicos de programación web y experiencia en la administración de sistemas. Se recomienda que los estudiantes tengan conocimientos previos en hacking ético, aunque no es un requisito previo obligatorio.

Madrid Tech School

Tema 8: Criptografía y seguridad de la información

Descripción del curso:

Tiene como objetivo introducir a los fundamentos de la criptografía y la seguridad de la información. Cubrirá los **conceptos básicos** de la criptografía, incluyendo cifrado, descifrado, clave simétrica y asimétrica, **protocolos** de seguridad y **algoritmos** de criptografía. Además, se explorarán las **amenazas** a la seguridad de la información y las **técnicas** de defensa, como el control de acceso y la autenticación.

Objetivos de aprendizaje:

- **Comprender** los conceptos básicos de la criptografía, incluyendo cifrado, descifrado, clave simétrica y asimétrica, protocolos de seguridad y algoritmos de criptografía.
- **Identificar** las amenazas a la seguridad de la información y las técnicas de defensa, como el control de acceso y la autenticación.
- **Evaluar** los diferentes métodos de seguridad de la información.
- **Aprender** a diseñar e implementar sistemas seguros.

Programa:

1. Introducción a la criptografía
2. Cifrado y descifrado de mensajes
3. Criptografía de clave pública y privada
4. Funciones hash y firmas digitales
5. Seguridad en el almacenamiento y transmisión de datos

Audiencia:

Dirigido a **estudiantes de informática, ingenieros de software y profesionales de seguridad de la información** que deseen aprender los conceptos fundamentales de la criptografía y la seguridad de la información.

Duración: 40 horas.

Requisitos previos: deben tener una comprensión básica de la informática y las redes. Además, se recomienda tener conocimientos previos sobre programación y algoritmos.

Madrid Tech School

Tema 9: Ciberseguridad para el Internet de las cosas (IoT)

Descripción del curso:

Diseñado para brindar a los participantes una **comprensión sólida** de la seguridad en el mundo IoT. Cubrirá **conceptos fundamentales** de IoT, sus **riesgos** y **desafíos** de seguridad, y las **estrategias** y mejores **prácticas** para garantizar la seguridad y protección de los dispositivos IoT.

Objetivos de aprendizaje:

- **Comprender** los conceptos básicos de IoT y los protocolos de comunicación utilizados en IoT
- **Conocer** los desafíos de seguridad que enfrentan los dispositivos IoT y las redes IoT.
- **Identificar** y **evaluar** los riesgos de seguridad para los dispositivos y las redes IoT.
- **Desarrollar** estrategias y **aplicar** mejores prácticas para garantizar la seguridad y protección de los dispositivos IoT.
- **Conocer** las normas y regulaciones relacionadas con la seguridad de IoT.

Programa:

1. Introducción a la seguridad de IoT
2. Amenazas en dispositivos IoT
3. Protocolos de seguridad en IoT
4. Vulnerabilidades en dispositivos IoT
5. Seguridad en sistemas de control y automatización
6. Monitoreo y prevención de ataques en dispositivos IoT

Audiencia:

Dirigido a **profesionales de seguridad de la información, ingenieros de redes, desarrolladores de software, consultores de tecnología y cualquier persona interesada** en la seguridad de IoT.

Duración: 20 horas.

Requisitos previos: Conocimientos básicos de redes y seguridad de la información y conocimientos básicos de programación y experiencia en el uso de dispositivos IoT.

Madrid Tech School

Tema 10: Gestión de incidentes y respuesta a amenazas

Descripción del curso:

Diseñado para proporcionar una **comprensión de los procesos** y las mejores **prácticas** para manejar los incidentes de seguridad de la información y responder a las **amenazas** de manera efectiva. Se aprenderá a **identificar**, evaluar y responder a los **incidentes** de seguridad de la información, y se enseñará cómo establecer **planes de contingencia** y respuesta para reducir el riesgo de futuros incidentes.

Objetivos de aprendizaje:

- **Comprender** los conceptos y la terminología clave en la gestión de incidentes y la respuesta a amenazas.
- **Identificar** y **evaluar** los diferentes tipos de incidentes de seguridad de la información.
- **Aprender** las mejores prácticas para la preparación y la respuesta a incidentes de seguridad de la información.
- **Establecer** un plan de contingencia y respuesta para futuros incidentes.

Programa:

1. Planificación de la respuesta a incidentes
2. Identificación y clasificación de amenazas
3. Investigación y análisis de incidentes
4. Contención y eliminación de amenazas
5. Recuperación y restauración de sistemas
6. Evaluación de incidentes y lecciones aprendidas

Audiencia:

Dirigido a **profesionales de seguridad de la información, administradores de sistemas y red, y cualquier persona interesada** en aprender sobre la gestión de incidentes y la respuesta a amenazas.

Duración: 20 horas.

Requisitos previos: Conocimientos básicos de seguridad de la información, conocimientos básicos de redes y sistemas,y familiaridad con herramientas y tecnologías de seguridad de la información.