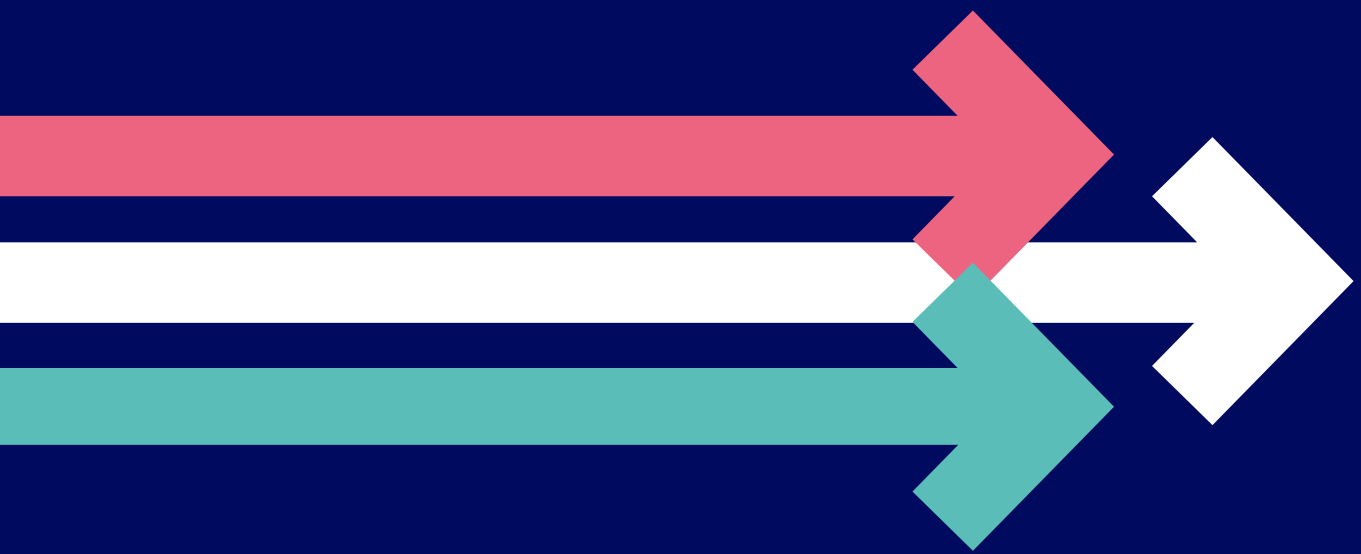
Tokio. School

Curso de

CIBERSEGURIDAD



Módulo 1. Seguridad Informática y Criptografía

Tema 1. Fundamentos de la Ciberseguridad

- Introducción a la ciberseguridad
- Conceptos básicos de internet
- La red: concepto y tipos
- Seguridad informática y seguridad de la información
- Tríada CIA
- Conceptos de seguridad de software

Tema 2. Amenazas y vulnerabilidades

- Conceptos generales de vulnerabilidades, amenazas y riesgos
- Ciberdelincuentes y hackers
- Ciclo de vida de un ataque
- Ataques más comunes

Tema 3. Criptografía

- Introducción a la criptografía
- Diagrama de la criptografía clásica
- Taxonomía del cifrado actual

Tema 4. Cifrado simétrico

- Principales métodos del cifrado simétrico

Tema 5. Cifrado asimétrico

- Criptografía de clave pública
- Elementos básicos
- Tipos de cifrado asimétrico

Tema 6. Firma digital

- Flujo de la firma digital
- Certificados digitales
- Hash

Tema 7. Autenticación y almacenamiento seguro de claves

- Clasificación de protección de almacenamiento
- Protección por software
- Protección por hardware

Resumen Módulo 1: En este módulo aprenderemos los fundamentos esenciales de la ciberseguridad en entornos digitales, abordando amenazas, vulnerabilidades y tipos comunes de ataques. Conoceremos de la criptografía, tanto clásica como moderna, incluyendo métodos de cifrado simétrico y asimétrico. Finalmente, nos centraremos en la autenticación y almacenamiento seguro de claves, evaluando enfoques de protección por software y hardware.

Módulo 2. Arquitecturas de seguridad y técnicas

Tema 1. Arquitectura de seguridad y su aplicación

- Introducción a las arquitecturas de seguridad
- ¿Dónde aplica la seguridad en los departamentos de una compañía?
- ¿Cómo definir una arquitectura de seguridad?

Tema 2. Modelos de arquitectura de seguridad

- Modelos de arquitectura de red más utilizados
- Diseño de arquitecturas de redes

Tema 3. Amenazas inteligentes

- ¿Qué son?
- Los sistemas SIEM
- SOAR
- Seguridad OSINT (Open Source Intelligence)

Tema 4. Despliegue de servidores proxy

- Servidores proxy
- Tipos de proxys
- Arquitectura y componentes
- Configuración

Tema 5. Seguridad en dispositivos móviles y web

- Seguridad en dispositivos móviles
- Android
- iOS
- Seguridad en aplicaciones web

Tema 6. Seguridad en sistemas operativos y software

- Windows
- Linux

Tema 7. Seguridad en la nube

- Azure
- AWS
- Google Cloud

Resumen Módulo 2: Nos adentraremos en la seguridad de redes y web conociendo los diferentes protocolos de seguridad; también estudiaremos las medidas de seguridad en diferentes entornos como son los sistemas operativos y el software, los dispositivos móviles, la web y la nube.

Módulo 3. Mecanismos de defensa y ataque

Tema 1. Mecanismo de defensa

- Introducción a la defensa
- Escenarios de conflictos

Tema 2. Mecanismos de ataque

- Introducción al ataque
- Principales tipologías de auditoría técnica
- Diferentes metodologías de Pentesting según la auditoria
- Diferentes enfoques de auditorias
- Herramientas de cada tipo de auditorias

Tema 3: Introducción al análisis forense informático

- ¿En que consiste?
- Tipos de análisis forense
- Fases
- Principios durante la recolección de evidencias
- Orden de volatilidad
- Acciones que deben evitarse
- Consideraciones adicionales

Tema 4: Procedimiento del análisis forense informático

- Procedimiento
- Herramientas necesarias
- Proceso de recolección
- Información volátil
- Información no volátil
- Herramientas forenses
- Diferenciar los tipos de entorno de análisis

Tema 5: Laboratorio forense

Resumen Módulo 3: Nos centraremos en las estrategias de seguridad y tácticas ofensivas en entornos digitales. Conoceremos el funcionamiento de un análisis forense informático y de las auditorías de seguridad adentrándonos en el hacking ético.

Exploraremos mecanismos de defensa, abordando escenarios de conflicto, y mecanismos de ataque, que incluyen tipologías de auditoría técnica, metodologías de Pentesting, enfoques de auditoría y herramientas correspondientes.

Módulo 4. Montando entornos de ataque con Docker

Tema 1: ¿Qué son los contenedores?

- Conceptos básicos
- Arquitectura
- Instalación de Docker
- Imagen Docker
- Contenedor Docker

Tema 2: Despliegues de contenedores

- Almacenamiento
- Redes
- Creación de imágenes
- Docker Compose
- Docker Hub

Tema 3: Ciberseguridad en dockers

- Recomendaciones de seguridad

Tema 4: Otro tipo de contenedores

- Rocket
- LXC (Linux Containiners)
- LXD (Canonical)
- Linux – Server
- OpenVZ/Virtuozzo 7

- Otros en Windows

Tema 5: Caso Práctico. Laboratorio con Dockers

- Práctica 1: MobSF
- Práctica 2: Levantar entorno de base de datos

Resumen Módulo 4: Aprenderemos los tipos de contenedores, despliegues de contenedores y la ciberseguridad en Docker. Abordaremos la creación de ambientes de ataque mediante contenedores y además conoceremos otros tipos de contenedores como Rocket, LXC, LXD.

El módulo culmina con un laboratorio práctico de Docker, con ejercicios para desarrollar un entorno de base de datos y una práctica con MobSF.

Módulo 5. Normativa y marco legal

Tema 1: Introducción al Cumplimiento Normativo

- Esquema Nacional de Seguridad
- ISO/IEC 27001
- Ley de protección de infraestructura crítica
- Directiva NIS
- Protección de datos personales

Tema 2: Sistemas de Gestión

- Liderazgo
- Planificación
- Soporte
- Operación
- Evaluación del desempeño
- Mejora

Tema 3: ISO 27001: Sistemas de Gestión de Seguridad de la información

- Liderazgo
- Planificación
- Soporte
- Operación
- Evaluación del desempeño

Tema 4: ISO 27002: Marco de Controles de Seguridad

- Dominios
- Objetivos de control y controles

Tema 5: Gestión de Riesgos

- Definiciones previas
- Gestión de riesgos
- Tratamiento del riesgo
- Herramienta PILAR

Tema 6: Esquema Nacional de Seguridad

- Medidas de seguridad ENS
- Adecuación al ENS
- Política de seguridad
- Roles y responsabilidades
- Conformidad ENS
- Entorno de validación ENS (EVENS)
- Herramientas del CCN

Tema 7: Plan de continuidad de Negocio

- Contexto de la organización
- Liderazgo
- Planificación
- Soporte
- Operación
- Evaluación del desempeño

Tema 8: Protección de Datos Personales: RGPD y LOPD-GDD

- Política de privacidad
- Registro de actividades de tratamiento – RAT
- Análisis de la necesidad de evaluaciones de impacto (EIPD)
- Gestión de riesgos
- Análisis EIPD
- Privacidad por diseño y defecto
- Delegado/a de protección de datos
- Brechas de seguridad
- Evaluación del desempeño
- Sanciones
- Autoridades de protección de datos
- Sistema de gestión de protección de datos

Resumen Módulo 5: Conoceremos los sistemas de gestión y las normas ISO que los componen (ISO27001/27002). También veremos la gestión de riesgos, así como el Esquema Nacional de Seguridad y el Plan de continuidad de Negocio. Finalmente se tratarán las leyes entorno la Protección de Datos Personales.

Proyecto final


Tokio.
School