

TÍTULO: CIBERSEGURIDAD AVANZADA EN ENTORNOS DE LAS TECNOLOGÍAS DE LA OPERACIÓN.

HORAS: 120

OBJETIVOS:

- Adquirir los conocimientos de ciberseguridad y la concienciación necesaria para dotar las redes industriales de los modelos de segmentación y securización de máquinas y dispositivos conectados, así como realizar ciberejercicios de ciberseguridad industrial.
- Conocer los principios básicos de ciberseguridad, incluidos los aspectos técnicos, regulatorios y organizativos de la misma, incluyendo una aproximación al *hacking* ético para entender las principales amenazas y ataques y cómo defenderse de ellos.
- Adquirir los conocimientos básicos de la industria y la transformación digital, incluida la terminología y los dispositivos utilizados en campo, los niveles ISA95, lo relacionado con la llamada industria 4.0, así como la capacitación práctica para adquirir las habilidades necesarias para programar un PLC.
- Introducción a los aspectos específicos relacionados con la ciberseguridad en el entorno industrial, como sistemas ICS-SCADA, redes industriales, amenazas y estándares, para comprender todos los componentes que pueden comprometer la ciberseguridad industrial y la relación entre ellos.
- Evaluar y reforzar los conocimientos de ciberseguridad industrial mediante la ejecución de seis escenarios de ataque y defensa, definidos en la plataforma *Cybertix-Cybring* para redes industriales, para profundizar en los conocimientos de forma práctica.

CONTENIDOS:

MF1. Introducción a la ciberseguridad

Unidad 1. Introducción a la ciberseguridad: fundamentos y gestión de riesgos

Introducción

Conocimiento de los fundamentos de ciberseguridad

Modelos organizativos

Conceptos básicos y tecnológicos

CID: confidencialidad, integridad y disponibilidad

Autenticación y autorización

Criptografía

- Firewalls* y sistemas de detección y prevención de intrusos (IDS/IPS)
- Roles de las personas
- Identificación de amenazas, ataques y vulnerabilidades de los sistemas
- Tipos de amenaza y actores relevantes en el cibercrimen
 - Tipos de amenaza
 - Actores relevantes en el cibercrimen
- Realización de una evaluación de seguridad y gestión de riesgos
- Metodología de gestión de riesgos
- Alcance, activos críticos, identificación y valoración de los riesgos de negocio
 - Activos críticos
 - Identificación y valoración de los riesgos de negocio
- Amenazas y salvaguardas
- Continuidad del negocio
- Ciclo de gestión de riesgos
- Modelos de gobernanza y clasificación de la información
 - Modelos de gobernanza
 - Clasificación de la información
- Estándares y regulación
 - Information security management*: ISO 2700, 27001, 27002, 27005
 - Risk management*: ISO 31000, 31010, COBIT 5, NIST 800-39
 - Risk assessment*: NIST 800-30
 - Security controls*: NIST 800-53
 - Specific*: GDPR (*data protection*), OWASP (*web application security*), PCI-DSS (*payment cards*), etc.
 - Risk framework*: NIST framework
 - Threats of ICS*: NIST 800-82
 - IACS standards*: ISA/IEC-62443
- Gestión de incidentes

Unidad 2. Introducción a la ciberseguridad: seguridad de los sistemas

- Introducción
- Conocimientos de la seguridad de los sistemas
- Hardening*: *software*, *hardware* y redes
 - Sistemas operativos
 - Aplicaciones
 - Servidores, puestos de trabajo, dispositivos móviles
 - Bases de datos
 - Dispositivos de red y sistemas industriales
- Aproximación a los componentes de la seguridad en redes
- Niveles OSI (*open system interconnection model*)
- Modelo TCP/IP: protocolos DNS, FTP, IMAP, TCP, IPv4, IPv6, HTTP
- Encapsulado
- Componentes de seguridad en redes: *firewall*, IDS/IPS, WIDPS, UTM
- Conocimientos y utilización de medidas de seguridad y defensa en

- profundidad
- Tipologías de seguridad
- Seguridad física: riesgos y medidas
- Seguridad lógica: defensa en profundidad
 - Control de accesos: identidad, autenticación
 - Protección: *firewall*, protección de dispositivos, inteligencia y monitorización
 - Perímetro: pasiva/activa
 - Interna: pasiva/activa
 - Cadena de suministro
- Implementación de herramientas de *hacking* ético
- Introducción al *hacking*

MF2. Introducción a los fundamentos industriales de las tecnologías de la operación

Unidad 1. Introducción a los fundamentos industriales de las tecnologías de la operación en el control de procesos industriales

- Introducción
- Introducción a los aspectos esenciales de la industria
- Fabricación industrial: sistemas comunes
- Las revoluciones industriales
- Industria 4.0: digitalización
- Industria inteligente y conectada
- Reconocimiento de los fundamentos del control de procesos industriales
- Tipos de procesos industriales
- Fundamentos y tipos de sistemas de control
- ICS: sistemas de control industrial
 - PID
 - RTU
 - HMI
 - PLC
 - SCADA
 - DCS
- Implementación de instrumentación industrial
- Sensores
- Conversores

Unidad 2. Introducción a los fundamentos industriales de las tecnologías de la operación en sistemas industriales de comunicación y producción

- Introducción
- EtherCAT
 - Características principales de EtherCAT
 - Aplicaciones de EtherCAT en la industria

- Ventajas de EtherCAT
- Sistemas de producción integrados
- Automatización industrial
- Gestión de materiales y sistemas de identificación
 - Códigos de barra
 - RFID
- Robotización industrial
- RFID y otros protocolos de identificación
- Implementación de sistemas avanzados de fabricación
- Clasificación de maquinaria industrial
- Sistemas MES de fabricación asistida
 - Tecnología colaborativa
 - Funcionamiento de los sistemas MES
 - Beneficios de los sistemas MES
 - Aplicaciones de los sistemas MES
- Operaciones industriales digitalizadas: herramientas, evolución e implementación
- Aproximación a la industria X.0
- Introducción a la industria 4.0 y siguientes versiones
- Los niveles ISA-95 y la transición de la industria 4.0 a la industria X.0

MF3. Introducción a la ciberseguridad industrial avanzada

Unidad 1. Introducción a la ciberseguridad industrial avanzada. Redes y protocolos industriales

- Introducción
- Identificación de los componentes ICS/SCADA
- Diferencias entre la ciberseguridad IT y OT
- Componentes ICS
- Normas de seguridad y salud laboral
 - Protocolo de instalación segura en sistemas ICS
 - Prevención de riesgos laborales en sistemas ICS
- Descripción de redes y protocolos industriales
- Características de las redes de comunicación industrial
- Tipos de redes de comunicación industrial
- Arquitecturas y protocolos ICS
 - Arquitectura de árbol
 - Arquitectura en estrella
 - Arquitectura en anillo
 - Arquitectura doble anillo
 - Arquitectura malla
 - Arquitectura en bus
 - Arquitectura mixta
 - Tipos de protocolos industriales

Amenazas de redes industriales
Impulsar el compromiso con la seguridad de la información y las tecnologías industriales

Unidad 2. Introducción a la ciberseguridad industrial avanzada. Amenazas y vulnerabilidades industriales

Introducción

Reconocimiento de las amenazas y las vulnerabilidades industriales

ISA 95: modelo Purdue de clasificación

- Niveles jerárquicos del modelo Purdue

- Niveles de la arquitectura y sus funciones

- Puntos de control y superficies de ataque en cada nivel

Escenario de riesgos industriales

Introducción a Shodan

Protocolos y superficie de ataque

- Historia de los ataques a redes industriales: modelos

Hacking industrial

Definición de los estándares y conocimiento de las mejores prácticas de ciberseguridad industrial

NIST SP 800-82 securización de sistemas de control industriales

NIST SP 800-53 estrategia de gestión de riesgos

IEC 62443 procesos, personas y tecnología

NERC CIP: infraestructuras críticas de energía (USA)

- Seguridad de redes

- Seguridad activos/dispositivos

- Seguridad de datos y aplicaciones

MF4. Ciberejercicios básicos y avanzados de ciberseguridad industrial

Unidad 1. Ciberejercicios básicos y avanzados de ciberseguridad industrial. Simulación de ataques en la plataforma *Cybertrix-Cybring*

Introducción

Identificación de las vulnerabilidades ICS

Detección y prevención de las mismas

Simulación de ataques en redes industriales OT a través de *cyber range*

- Plataforma KYPO *cyber range*

- Tipos de máquinas virtuales

- Funcionamiento y uso de las máquinas virtuales

- Instalación de *VirtualBox*

- Plataforma de rango cibernético KYPO

Identificación e implementación de ataques DDOS

Origen

Detección

Unidad 2. Ciberejercicios básicos y avanzados de ciberseguridad industrial. Securitización de redes industriales

Introducción

Evaluación escenarios de *ransomware* OT/IT

- Comprendiendo el *ransomware* en entornos industriales

- Visión *red team* / *blue team* en la ciberseguridad industrial

 - Red team*: modelos de ataque y ofensiva en ciberseguridad

 - Blue team*: estrategias de protección y defensa

 - Juago de roles en la seguridad digital

- Herramientas para la detección temprana de *ransomware*

- Estrategias de mitigación y respuesta ante *ransomware*

- Simulación de ataques *ransomware* en entornos OT

- Implementación de planes de respuesta ante incidentes

Diseño seguro de redes industriales con gemelo digital

Aplicación de herramientas de securización de redes industriales