TÍTULO

Especialista en ciberseguridad industrial

2ª edición
(octubre 2022 / julio 2023)
Duración: 33 ECTS (300 h)
Modalidade virtual

Información e inscripción
http://ecsi.uvigo.es

Universidade Vigo

Escola de Enxeñaría Industrial

Escola de Enxeñaría de Telecomunicación

Escola Aberta de Formación Permanente

Información básica

Inicio del curso: octubre de 2022
Fin del curso: julio de 2023
Horario: viernes de 16:00 h a 21:00 h
sábado de 9:00 h a 14:00 h
Duración: 33 ECTS (300 horas)
Lengua de impartición: castellano
Preinscripción y matrícula: ecsi.uvigo.es
Plazas: mínimo 21, máximo 30
Tasas de matrícula: 2.500 €
Descuentos para:
Comunidad Alumni UVigo: 2.250 €
Comunidad UVigo y desempleados: 2.125 €
Modo de pago: el pago se realizará en efectivo, tarjeta u hoja de liquidación mecanizada.
Director académico: Jose Ignacio Armesto Quiroga
armesto@uvigo.es /+34 986 812 244
Coordinación: Miguel Ramón Díaz-Cacho Medina y Adriel Regueira Suárez
Entidad Organizadora: Escuela Abierta de Formación Permanente eafp.uvigo.es
Bonificación: curso bonificable para trabajadores en activo contratados por cuenta ajena, a través de la FUNDAE. Contacta con nosotros si deseas más información.
Destinatarios: orientado a personas tituladas universitarias de primer y segundo ciclo (grado/licenciatura/diplomatura/ingeniería/máster/doctorado) cuya dedicación profesional esté encaminada a la implantación, mantenimiento y gestión de sistemas automatizados en el ámbito industrial.

Deseño: Área de Imaxe. Vicerreitoría de Comunicación e Relacións Institucionais. Fotografías: Adobe Stock e Unsplash

Objetivos

Esta titulación pretende ser una amplia introducción sobre el estado actual de las técnicas de ciberseguridad aplicadas en las plantas industriales (OT). Los conocimientos teóricos impartidos se llevarán a la práctica utilizando herramientas y tecnologías de diversos fabricantes (FORTINET, MICROSOFT, NOZOMI NETWORKS y SIEMENS entre los más destacados).

El objetivo final del título es proporcionar, al profesional de este sector, conocimientos prácticos actualizados y eficaces sobre algunas de las soluciones más modernas del mercado de la ciberseguridad en el ámbito del control, operación y comunicación de procesos industriales.

Justificación académica

La introducción de las nuevas tecnologías en los procesos productivos supuso la necesidad de disponer de profesionales con un mayor nivel de cualificación tecnológica. Por este motivo, el estado amplió su oferta formativa con nuevas titulaciones, tanto en el ámbito de la formación profesional como universitaria, tratando así de adecuarlos a las propias necesidades del mercado.

En el ámbito de la ciberseguridad de sistemas industriales, los avances que se produjeron - y se están produciendo - en los últimos años, exigen sin duda la puesta al día del personal relacionado. La Universidade de Vigo, consciente de la importancia de la formación continua en este sector, ofrece la posibilidad de formarse a través de éste y otros títulos propios.

El profesorado que va a impartir este curso tiene una titulación, conocimientos y experiencia industrial adecuados al contenido que se pretende impartir y, aunque la ciberseguridad industrial es parte de algunas materias, es imposible abordarla en un título de primer o segundo ciclo con la profundidad y extensión con la que se va a hacer aquí.

Justificación social

Esta formación puede ser una buena oportunidad de mantenerse al día y renovar los conocimientos para los profesionales de la industria, muy en especial los del sector de la informática industrial, en el que continuamente se presenta la necesidad de conocer y dominar los nuevos equipamientos de ciberseguridad que se aplican actualmente en una planta industrial en continua evolución.

Destinatarios

Orientado a personas tituladas universitarias de primer y segundo ciclo (grado/licenciatura/diplomatura/ingeniería/máster/doctorado) cuya dedicación profesional esté encaminada a la implantación, mantenimiento y gestión de sistemas automatizados en el ámbito industrial.

Condiciones de acceso

- Estar en posesión de un título universitario dentro del EEES que otorgue el acceso a enseñanzas oficiales de posgrado.
- Estar en posesión de un título extranjero, ajeno al EEES, homologado a un título universitario oficial del EEES.
- Estar en posesión de un título extranjero, ajeno al EEES, no homologado, pero que acredite un nivel equivalente a un título universitario de grado dentro del EEES que faculte, en el país de expedición del título, para el acceso a las enseñanzas de posgrado.

Criterios de selección

Para aquellos/as que cumplan las condiciones de acceso, la selección se hará por riguroso orden de abono de las tasas de matriculación hasta completar la oferta de plazas disponible.

Programa

Introducción a la Industria 4.0 (1 ECTS)

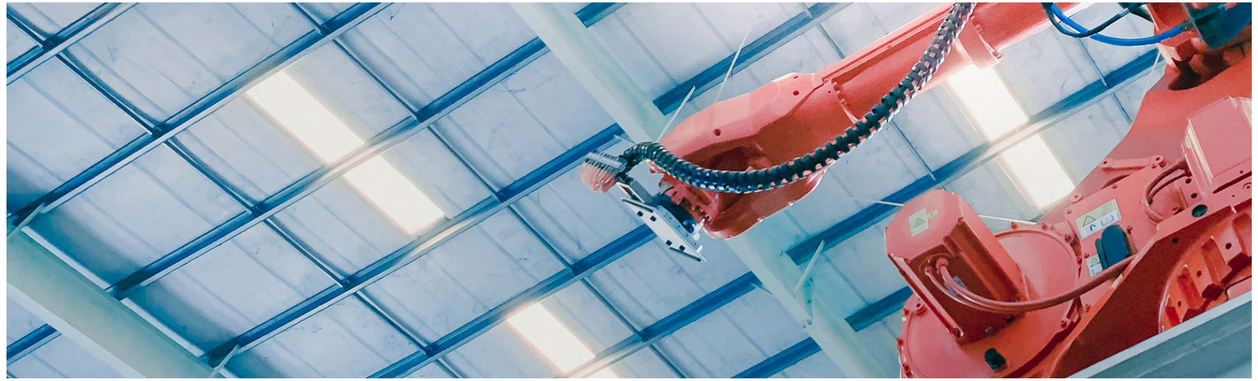
- Antecedentes y visión global de la Industria 4.0
- Tecnologías habilitadoras
- Infraestructuras de comunicaciones industriales en la planta de proceso (OT)
- Ciberseguridad industrial
- Implantación de la industria 4.0 en diferentes sectores industriales. Evolución

Introducción a los sistemas de control (2 ECTS)

- Sistemas de control industrial: sistemas de control distribuído (DCS), autómata programable (PLC), control numérico por computador (CNC), robot industrial, computador industrial
- Sistemas de fabricación flexible. Interfaces hombre-máquina: sistemas HMI y SCADA
- Comunicaciones industriales
- Protocolos de comunicación industrial ethernet: Modbus/TCP, Profinet, Ethernet/IP
- Protección de los sistemas de control industrial

Cumplimiento y gestión de la ciberseguridad industrial (6 ECTS)

- Introducción
- Evaluación de riesgos: inventario de activos, identificación de vulnerabilidades y amenazas
- Normativa aplicable: directivas NIS europeas. Esquema Nacional de Seguridad ENS
- Ley de protección de infraestructuras críticas LPIC, Reales Decretos, Código civil y penal
- Estándares de referencia: ISA/IEC 62443, NIST/ISO 27001
- Tipos de ataques y amenazas
- Gestión de la ciberseguridad: elaboración de un Plan integral de la Ciberseguridad-SGCI: administrativo, operacional y técnico



Redes industriales
Familia Scalance de Siemens (5 ECTS)

- Modelo de referencia ISO de OSI
- Elementos de red: hub, switch, router, proxy, gateway y firewall
- Arquitecturas de referencia en control industrial: centros de procesamiento de datos (CPD) y virtualización
- Dispositivos de comunicaciones industriales SIEMENS Scalance. Gestión de switches: redes VLAN, anillos MRP y HRP
- Protocolo Spanning Tree. Listas ACL. Gestión de routers: tablas de enrutado, protocolo VRRP para redundancia de routers. Gestión de firewalls: redes VPN, políticas de firewall, tablas NAT, acceso remoto
- Gestión centralizada con SINEC NMS: monitorización de dispositivos
- Gestión de copias de seguridad. Gestión de actualizaciones. Gestión de políticas por grupos
- Gestión de accesos remotos con SINEMA RC
- Taller práctico

Virtualización en arquitecturas de control industrial
Familia vSphere de VMware (4 ECTS)

- Introducción
- Conceptos básicos
- Tipos de hipervisores
- Elementos de la plataforma VMware: Hosts esxl, vCenter.
- Características de las ediciones
- Principales funcionalidades
- Instalación de host VMware: descarga de imágenes, versiones originales de VMware, versiones de fabricantes de hardware, configuración básica de red
- Switches virtuales: tipos, configuración de un vSwitch, conexión con redes físicas, tags VLAN
- Almacenamiento: conceptos, tipos de almacenamiento
- Máquinas virtuales: conceptos, máquina virtual vs máquina física, ficheros, snapshots, operaciones básicas
- Hardware virtual: componentes, edición, tipos de discos
- Taller práctico

Sistemas de supervisión.
Soluciones Zabbix (4 ECTS)

- Introducción
- Necesidad
- Tipos de sistemas de supervisión
- Aplicabilidad en entornos industriales
- Aplicabilidad en ciberseguridad industrial
- Monitorización con Zabbix: Arquitectura, requisitos, modelos On-premise, Cloud, SaaS
- Host, ítems y modelos
- Triggers, macros, funciones y tags
- Acciones, notificaciones y ACK. Gestión de usuarios
- Visualización de datos en Zabbix: Históricos y tendencias, Mapas, Dashboards, Informes
- Buenas prácticas de monitorización
- Monitorización de logs: tipos, aplicabilidad en entornos industriales y ciberseguridad, criterios de elección
- Taller práctico

Firewalls de nueva generación.
Familia Fortigate de Fortinet (3 ECTS)

- Introducción a los firewalls de nueva generación (NGFW)
- Tablas y políticas de routing
- Gestión de túneles VPN, IPSEC y SSL
- Tablas NAT en NGFW
- Dominios virtuales
- Inspección en capa de aplicación
- Modo transparente
- Alta disponibilidad (HA). Logging
- Diagnóstico y resolución de problemas
- Taller práctico

Sistemas de detección de intrusiones.
Familia NOZOMI NETWORKS SOLUTIONS de Nozomi Networks (3 ECTS)

- Introducción a los sistemas de detección de intrusiones (IDS)
- Captura y análisis de tráfico con Wireshark
- Tipos de IDS. Tipos de amenazas
- Técnicas para detección de amenazas
- Arquitectura de Nozomi Networks: implementación estándar, integracións de terceros
- Taller práctico

Sistemas de gestión de eventos e información de seguridad.
Soluciones Microsoft Azure Sentinel e Inprotech Guardian(2 ECTS)

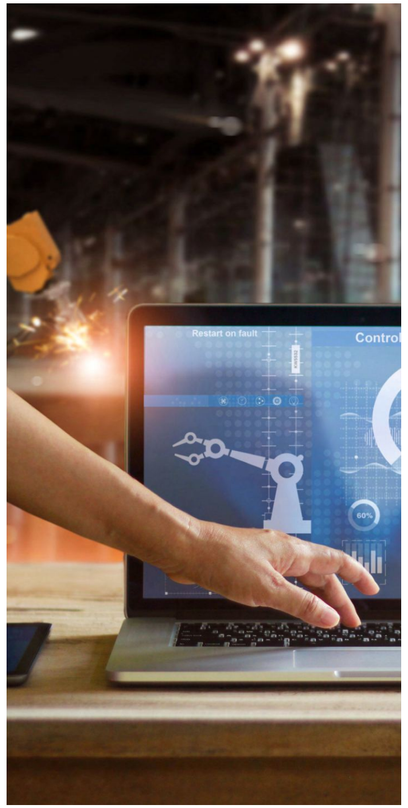
- Introducción a los sistemas de gestión de eventos y información de seguridad (SIEM)
- Funcionamiento, diferencias entre IDS e SIEM. Necesidad
- Casos de uso y elementos de un SIEM
- Taller práctico

Trabajo final de curso (3 ECTS)

Este trabajo tiene como objetivo que el alumnado ponga en práctica los distintos conocimientos adquiridos en un caso real. De este modo, verá como todo lo aprendido se interrelaciona en la realidad y tendrá que afrontar decisiones sobre cómo segurizar una fábrica. El/la estudiante desarrollará y presentará un proyecto relacionado con un componente o sistema de ciberseguridad industrial: Objetivos, Antecedentes y bases de partida, Desarrollo, Conclusiones, Presupuesto.

Software utilizado durante el curso (licencias educacionales)

- Scalance de SIEMENS
- FortiOS 6 y GNS3 de FORTINET
- Nozomi Networks Solutions de Nozomi Networks
- Zabbix
- vSphere de VMWARE
- Wireshark
- Azure Sentinel de MICROSOFT
- Inprotech Guardian de INPROTECH
- KICS de KASPERSKY



Sistema de evaluación

Todas las pruebas y/o entrega de trabajos se realizará de modo virtual mediante las plataformas Campus Remoto y/o Moovi de la Universidade de Vigo. La evaluación de cada materia se basará en la asistencia y participación en las actividades síncronas, realización de trabajos basados en los contenidos y/o pruebas teóricas.

El trabajo fin de curso es la última materia a evaluar una vez que el alumnado supere todas las restantes materias. El trabajo se presentará en sesión pública ante un tribunal formado por al menos 3 profesores del curso. El tribunal valorará el trabajo realizado, su extensión y el grado de dificultad, el contenido y calidad de la memoria, así como la calidad de la presentación del mismo.

Calendario docente y de evaluación:

- Docencia síncrona: **Octubre 2022 a Junio 2023**
- Primera oportunidad:
  Entrega de trabajos: **Mayo/Junio 2023**
  Pruebas teóricas: **Julio 2023**
  Trabajos fin de curso: **Julio 2023**
- Segunda oportunidad:
  Entrega de trabajos: **Junio/Julio 2023**
  Pruebas teóricas: **Julio 2023**
  Trabajos fin de curso: **Julio 2023**

Titulación

La superación del curso completo dará derecho a la obtención del título de "Especialista universitario en ciberseguridad industrial por la Universidade de Vigo", para lo que deberán dirigirse al Servicio de Gestión de Estudios de Posgrado para la solicitud y pago de las tasas correspondientes (61,55€), no incluidas en el precio de la matrícula del curso:

Edificio Filomena Dato, 2ª Planta

Campus Universitario de Vigo

Telf: +34 986 819 950

negociado.formacionpermanente@uvigo.es

posgrao@uvigo.es

Profesorado

Víctor Manuel Aguilar Gutiérrez
Director regional de Nozomi Networks en Iberia y Turquía
NOZOMI NETWORKS

Ignacio Álvarez Vargas
Director of Automation and Industrial Digitalization & Product and Solutions Security Officer
SIEMENS

José Ignacio Armesto Quiroga
Profesor titular de universidad
UNIVERSIDADE DE VIGO

Manuel Caeiro Rodríguez
Profesor contratado doctor
UNIVERSIDADE DE VIGO

Víctor J. Calvo Querol
CEO
MUUTECH

Enrique Costa Montenegro
Profesor contratado doutor
UNIVERSIDADE DE VIGO

Juan de la Peña Gayo
Account Technology Strategist
MICROSOFT

Miguel Ramón Díaz-Cacho Medina
Profesor contratado doctor
UNIVERSIDADE DE VIGO

Manuel Fernández Veiga
Profesor titular de universidad
UNIVERSIDADE DE VIGO

Ana Fernández Vilas
Profesora titular de universidad
UNIVERSIDADE DE VIGO

Fernando Fernández-Valdés Pedrosa
CTO & Technical Director
MUUTECH

Juan Manuel Ferrer Miralles
Ingeniero técnico industrial. Líder del grupo de trabajo Industria Conectada 4.0
ISA Sección Española

Iago Fortes Caramés
Socio Consultor
INPROSEC

Sergio García Irigoyen
Security and technology consultant - Cybersecurity services
PROFESIONAL INDEPENDIENTE

Javier Larrea Arias
Administrador de sistemas
GADISA

Agustín Valencia
OT security Business Development
FORTINET

David Marco Freire
Iberia OT/ICS/IOT/IIOT (Industrial Cybersecurity) and Industry X Security Lead
ACCENTURE

Juan Jesús Pardo Expósito
Director técnico y director de negocio
TECDESOFT AUTOMATION

Belén Pérez Rodríguez
CISO
GRUPO NUEVA PESCANOVA

Juan Carlos Pozas Bustos
Responsable de produto, sistemas de comunicacións e ciberseguridade Industrial
SIEMENS

Adriel Regueira Suárez
Head of IT & Cybersecurity
TECDESOFT AUTOMATION

Javier Bravo
Responsable de producto comunicaciones industriales y conectividad digital
SIEMENS

Javier Viana
Industrial Communications and OT Cybersecurity Product Manager
SIEMENS

Conferenciantes invitados

José Luis Laguna Merino
Director Systems Engineering
FORTINET

Luis Fernández-Checa
Professional Services Consultant
VMware

Pedro Jorge Viana
Pre-sales Manager Iberia
KASPERSKY

Alberto Ruiz-Zorrila
Professional Services Consultant
VMware

David Alonso Domínguez
Sr. Customer Success Account Manager
Security Advisor
MICROSOFT

Pablo Gámez
Technical Account Manager
VMware

Coordinación: UniversidadeVigo, tecdesoft

Endidades colaboradoras: accenture, kaspersky, SIEMENS, FORTINET, Microsoft, tecdesoft, InprOTech by Inprosec, muutech monitoring solutions, VMUG VMWARE USER GROUP, ISA Sección Española, NOZOMI NETWORKS, vmware