# TÍTULO

## *Especialista en ciberseguridade industrial*

**Del 13 de enero de 2022 al 2 de septiembre de 2022**
Duración: 300 h (33 ECTS)
Modalidad virtual

Información, Preinscrición e matrícula
http://ecsi.uvigo.es/

Universidade Vigo

Escola Aberta de Formación Permanente

Escola Aberta
de Formación Permanente
Universidade Vigo

# MEMORIA DEL TÍTULO DE ESPECIALISTA EN CIBERSEGURIDAD INDUSTRIAL

## Especialista en Ciberseguridad Industrial

| |
|---|
| CURSO ACADÉMICO: **2021/2022** |


| |
|---|
| Promotor del título (Profesor/a, Departamento, Facultad, Escuela, …):<br>**José Ignacio Armesto Quiroga, Ingeniería de Sistemas y Automática, Escuela de Ingeniería Industrial, Escola Aberta de Formación Permanente** |
| Teléfono de contacto: **986-812244** |
| Correo electrónico de contacto: armesto@uvigo.es |

# 1. DATOS GENERALES

## 1.1. DATOS BÁSICOS

| | |
|---|---|
| NÚMERO DE CRÉDITOS QUE OFERTA EL TÍTULO: **33 ECTS** | |
| Nº DE CRÉDITOS TEÓRICOS: **17 ECTS** | Nº DE CRÉDITOS PRÁCTICOS: **13 ECTS** |
| Nº DE CRÉDITOS TRABAJO FINAL: **3 ECTS** | |
| FECHA DE INICIO: **13/01/2022** | |
| FECHA DE FINALIZACIÓN: **02/09/2022** | |
| MODALIDAD: **Síncrona virtual** | |
| ÁMBITO DE CONOCIMIENTO: **Tecnológico** | |
| HORAS SÍNCRONAS PRESENCIALES: **0H**<br>HORAS SÍNCRONAS VIRTUALES: **300H**<br>HORAS DE PRÁCTICAS: **0H**<br>HORAS DE PRÁCTICAS EXTERNAS: **0H** ☐ Prácticas externas obligatorias | |
| COORDINADORES/AS ACADÉMICOS/AS: **José Ignacio Armesto Quiroga \| Miguel Díaz-Cacho Medina** | |
| CENTRO ORGANIZADOR: **ESCOLA ABERTA DE FORMACIÓN PERMANENTE** | |
| LUGAR DE IMPARTICIÓN (modalidade presencial): **Online**<br>PLATAFORMAS VIRTUALES: **Campus Remoto** e **MooVi** | |
| IDIOMA DE IMPARTICIÓN: **Castelán** | |
| WEB DEL TÍTULO: http://ecsi.uvigo.es/ (en construcción) | |
| DENOMINACIÓN DEL TÍTULO EN INGLÉS: **Industrial Cybersecurity Specialist** | |

# 2. JUSTIFICACIÓN DEL TÍTULO

## 2.1. BREVE DESCRICIÓN DEL TÍTULO

**La introducción de las nuevas tecnologías en los procesos productivos ha supuesto a 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 cómo Universitaria, tratando así de adecuarlos a las propias necesidades del comprado. 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 Universidad de Vigo, consciente de la importancia de la formación continua en este sector, ofrece la posibilidad de formarse a través de este y otros cursos. El profesorado que va a impartir este curso tiene una titulación, conocimientos y experiencia industrial adecuados al contenido del curso que se pretende impartir y, aunque la ciberseguridad industrial es una parte del contenido de algunas materias, es imposible impartirlo, en un curso de primero o segundo ciclo, con la profundidad y extensión que se va a hacer aquí.**

## 2.2. OBJETIVOS DEL TÍTULO

**Este curso pretende ser una amplia introducción sobre el estado actual de las técnicas de ciberseguridad aplicadas en las plantas industriales (OT). Los conocimientos teóricos impartidos en este curso llevarán a la práctica utilizando herramientas y tecnologías de diversos fabricantes (FORTINET, MICROSOFT, NOZOMI NETWORKS y SIEMENS entre las más destacadas). El objetivo final de este curso es proporcionar al profesional de este sector conocimientos prácticos, actualizados y eficaces sobre algunas de las soluciones actuales del comprado de la ciberseguridade industrial en el campo del control, operación y comunicación de procesos industriales.**

## 2.3. JUSTIFICACIÓN SOCIAL

**Este curso puede ser una buena oportunidad de mantenerse al día y renovar los conocimientos para los personales de 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.**

## 2.4. PERFIL DE EGRESO:

**Este curso pretende cubrir el hueco que hay entre los perfiles formativos industrial y de las tecnologías de la información y comunicaciones, generando un nuevo perfil especialista en ciberseguridad industrial. Al finalizar este curso, el alumnado adquirirá los siguientes conocimientos y competencias: Conocimiento de la falta de ciberseguridad en los entornos industriales y los enormes riesgos que eso conlleva; Conocimiento de los principales organismos generadores de buenas prácticas y normativas de aplicación en los distintos entornos industriales; Conocimientos sobre cómo aplicar la ciberseguridad en los distintos niveles de las fábricas, utilizando para lo eres las últimas tecnologías habilitadoras de la industria 4.0; Capacidad para diseñar y desplegar arquitecturas de control industrial de forma cibersegura y/o ayudar a mitigar los riesgos asociados a la implantación de nuevas tecnologías en la industria; Capacidad para seleccionar, configurar y gestionar diversas tecnologías comerciales de vanguardia en la industria en el ámbito de las comunicaciones, virtualización de equipos, monitorización de infraestructuras, firewalls de nueva generación, detección de intrusiones, gestión de eventos e información de seguridad.**

## 2.5. COMPETENCIAS:

| CÓDIGO | COMPETENCIA |
|---|---|
| CE1 | Conocer los conceptos, principios y herramientas propios de los más modernos sistemas de fabricación industrial basados en la Industria 4.0. |
| CE2 | Conocer el rol da ciberseguridad industrial en las fábricas do futuro. |
| CE3 | Conocer los principales sistemas de control utilizados para la automatización de las plantas de fabricación industrial. |
| CE4 | Capacidad para diseñar y proyectar sistemas de producción automatizados. |
| CE5 | Conocer los principales conjuntos de buenas prácticas para el diseño ciberseguro de los sistemas de control. |
| CE6 | Conocer los conceptos, principios y herramientas de la norma ISA/IEC 62443. |
| CE7 | Capacidad para integrar la ciberseguridad industrial en un plan integral. |
| CE8 | Conocer el funcionamiento de las redes industriales basadas en ethernet. |
| CE9 | Capacidad para desarrollar una red cibersegura para la fábrica. |
| CE10 | Capacidad para configurar y gestionar equipos de la familia Scalance de Siemens. |
| CE11 | Conocer los conceptos y herramientas que otorga la virtualización de sistemas en un entorno industrial. |
| CE12 | Capacidad para configurar y gestionar entornos virtuales de VMware. |
| CE13 | Conocer los conceptos, principios y herramientas para la monitorización de una infraestructura de control industrial. |
| CE14 | Capacidad para configurar y gestionar un entorno de monitorización completo con Zabbix. |
| CE15 | Conocer los conceptos, principios y herramientas que proporcionan los firewalls de nueva generación (NGFW). |
| CE16 | Capacidad para configurar y gestionar equipos de la familia Fortigate de Fortinet. |
| CE17 | Conocer los conceptos, principios y herramientas que proporcionan los sistemas de detección de intrusiones (IDS) para entornos industriales. |
| CE18 | Capacidad para configurar y gestionar equipos de la familia Scada Guardian de Nozomi Networks. |
| CE19 | Conocer los conceptos, principios y herramientas que proporcionan los sistemas de gestión de eventos e información de seguridad (SIEM) en entornos industriales. |
| CE20 | Capacidad para configurar una herramienta SIEM comercial. |
| CE21 | Conocer cómo aplicar los conocimientos aprendidos en un caso práctico similar a uno real. |

## 2.6. XUSTIFICACIÓN DA PROPUESTA NA UVIGO

**En la Universidad de Vigo se imparte un máster interuniversitario en ciberseguridad que incluye una única materia, optativa y de 3 créditos ECTS, relativa a la aplicación de técnicas de ciberseguridad en entornos industriales. El curso de especialista en ciberseguridad industrial profunda nos objetivos y competencias necesarios para la implantación de sistemas de ciberseguridad industrial en el ámbito de los sistemas de producción mediante herramientas específicas de firmas líderes como FORTINET, MICROSOFT, NOZOMI NETWORKS, SIEMENS y VMWARE.**

# 3. DESTINATARIOS:

## 3.1. PERFIL DE INGRESO

| |
|---|
| PERFIL DE INGRESO:<br>**Orientado a Titulados Universitarios de primero y segundo ciclo y Profesionales del sector que reúnan los requisitos de habilitación de acceso a la Universidad, y cuya dedicación esté encaminada a la implantación, mantenimiento y gestión de sistemas automáticos en el ámbito industrial y acrediten un mínimo de 3 años de experiencia profesional.** |
| REQUISITOS DE ACCESO:<br>**1) Estar en posesión de un título universitario dentro del Espacio Europeo de Educación Superior (EEES) que otorgue el acceso a enseñanzas oficiales de posgrado.**<br>**2) Estar en posesión de un título extranjero, ajeno al EEES, homologado a un título universitario oficial del EEES.**<br>**3) 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.**<br>**4) Tener superados un mínimo de 120 ECTS en una titulación universitaria oficial dentro del EEES.**<br>**5) Ser profesionales de reconocida y acreditada experiencia laboral, siempre que la citada experiencia esté relacionada con las competencias inherentes al título y cumplan los requisitos de acceso a la universidad segundo la normativa vigente.** |
| NÚMERO DE PLAZAS: Mínimo **21** Máximo **30** |

## 3.2. PRECIOS DE MATRÍCULA

| **PRECIO DEL TÍTULO DE ESPECIALISTA:** | | |
|---|---|---|
| General: **2.500€** | Comunidad Universitaria UVIGO: **2.125€** | Comunidad Alumni UVIGO: **2.250€** |

## 3.3. PREINSCRIPCIÓN Y MATRÍCULA:

| |
|---|
| FECHA DE INICIO DE LA PREINSCRICIÓN: **15/10/2021** |
| FECHA DE FIN DE LA PREINSCRICIÓN: **27/12/2021** |
| DOCUMENTACIÓN REQUERIDA:<br>1) **Titulados/as universitarios: título oficial.**<br>2) **Alumnos/as de grado, licenciatura o equivalente: expediente académico.**<br>3) **Profesionales: informe de vida laboral y certificados expedidos por la/s empresa/s en las que se haga/n constar las funciones desarrolladas relacionadas con el título.** |
| CRITERIOS DE ADMISIÓN:<br>1)**Para quellos/as que cumplan las condiciones de acceso, a selección se hará por riguroso orden de abono de las tasas de matriculación hasta completar la oferta de plazas disponibles.** |
| PRUEBAS DE ADMISIÓN (se procede): **No procede** |
| FECHA DE INICIO DE MATRÍCULA: **15/11/2021** |
| FECHA DE FINAL DE MATRÍCULA: **27/12/2021** |

# 4. COORDINACIÓN

| | |
|---|---|
| **COORDINADOR/A DEL TÍTULO DE ESPECIALISTA:** | |
| NOMBRE: **José Ignacio Armesto Quiroga** | |
| CATEGORÍA: **Profesor Titular Universidad** | DEPARTAMENTO: **T07 – D.I.S.A.** |
| CORREO-E: **armesto@uvigo.es** | Nº TELÉFONO: **986-812244** |

# 5. PROGRAMA ACADÉMICO

## 5.1. MATERIAS:

| MÓDULO/ ESPECIALIDAD | Obligatoria | NOMBRE DE LA MATERIA | ECTS |
|---|---|---|---|
| **T01** | ☒ | **Introducción a la Industria 4.0** | **1** |
| **T02** | ☒ | **Introducción a los sistemas de control industrial** | **2** |
| **T03** | ☒ | **Cumplimiento y gestión de la ciberseguridad industrial** | **6** |
| **T04** | ☒ | **Redes Industriales (Familia SCALANCE de SIEMENS)** | **5** |
| **T05** | ☒ | **Virtualización en arquitecturas de control industrial (Familia VSPHERE de VMWARE)** | **4** |
| **T06** | ☒ | **Sistemas de supervisión (Soluciones ZABBIX)** | **4** |
| **T07** | ☒ | **Firewalls de nueva generación (Familia FORTIGATE de FORTINET)** | **3** |
| **T08** | ☒ | **Sistemas de detección de intrusiones (Familia SCADA GUARDIAN de NOZOMI NETWORKS)** | **3** |
| **T09** | ☒ | **Sistemas de gestión de eventos e información de seguridad (Soluciones MICROSOFT AZURE SENTINEL)** | **2** |
| **TFC** | ☒ | **Trabajo final de curso** | **3** |
| | | TOTAL ECTS OFERTADOS: | **33** |

## 5.2. CALENDARIO Y HORARIO

**La docencia se impartirá de forma no presencial, en formato síncrono (en el horario y rango de fechas indicado) mediante las plataformas de teledocencia (Campus Remoto y Moovi) de la Universidade de Vigo.**

**Jueves y Viernes, de 16:00 h a 21:00 h**
**Sábados, de 9:00 h a 14:00 h**

**Fecha de inicio del curso:**
**Jueves, 13 de enero de 2022**

**Fecha de finalización del curso:**
**Viernes, 2 de septiembre de 2022**

## 5.3. CALENDARIO DE EVALUACIÓN

**Todas las pruebas y/o entrega de trabajos se realizarán de modo virtual mediante las plataformas Campus Remoto y/o Moovi.**

1) **Primera oportunidad**
   a) **Entrega de Trabajos (Plataforma Moovi)**
      **Fecha límite (Módulos T01 a T04): 21 de abril de 2022**
      **Fecha límite (Módulos T05 a T09): 23 de junio de 2022**
   b) **Pruebas Teóricas (Campus Remoto y/o Moovi):**
      **Módulos T01 a T04: 23, 25, 26 e 27 de abril de 2022**
      **Módulos T05 a T09: 1,4, 5 e 6 de julio de 2022**
   c) **Trabajos fin de curso (Campus Remoto y/o Moovi):**
      **18 e 19 de julio de 2022**

2) **Segunda oportunidad**
   a) **Entrega de Trabajos (Plataforma Moovi)**
      **Fecha límite (Módulos T01 a T09): 8 de julio de 2022**
   b) **Pruebas Teóricas (Campus Remoto y/o Moovi):**
      **Módulos T01 a T09: 11,12,13,14 e 15 de julio de 2022**
   c) **Trabajos fin de curso (Campus Remoto y/o Moovi):**
      **1 y 2 de septiembre de 2022**

# 6. RECURSOS HUMANOS

## 6.1. PERSONAL DE LA UNIVERSIDADE DE VIGO

| NÚMERO | NOMBRE | APELLIDOS | Doctor/a | Área de conocimiento | Perfil/méritos en relación con el título |
|---|---|---|---|---|---|
| 1 | José Ignacio | Armesto Quiroga | ☒ | Ing. Sist. e Automática | Se adjunta breve Bio |
| 2 | Manuel | Caeiro Rodríguez | ☒ | Ing. Telemática | Se adjunta breve Bio |
| 3 | Enrique | Costa Montenegro | ☒ | Ing. Telemática | Se adjunta breve Bio |
| 4 | Miguel Ramón | Díaz-Cacho Medina | ☒ | Ing. Sist. e Automática | Se adjunta breve Bio |
| 5 | Manuel | Fernández Veiga | ☒ | Ing. Telemática | Se adjunta breve Bio |
| 6 | Ana | Fernández Vilas | ☒ | Ing. Telemática | Se adjunta breve Bio |

## 6.2. PERSOAL DOCENTE EXTERNO

| NÚMERO | NOMBRE | APELLIDOS | Doctor/a | Empresa/institución | Perfil/méritos en relación con el título |
|---|---|---|---|---|---|
| 1 | Víctor Manuel | Aguilar Gutiérrez | ☐ | NOZOMI NETWORKS | Se adjunta breve Bio |
| 2 | Ignacio | Álvarez Vargas | ☐ | SIEMENS | Se adjunta breve Bio |
| 3 | Víctor Javier | Calvo Querol | ☐ | MUUTECH | Se adjunta breve Bio |
| 4 | Juan | de la Peña Gayo | ☐ | MICROSOFT | Se adjunta breve Bio |
| 5 | Fernando | Fernández-Valdés Pedrosa | ☐ | MUUTECH | Se adjunta breve Bio |
| 6 | Juan Manuel | Ferrer Miralles | ☐ | ISA SPAIN | Se adjunta breve Bio |
| 7 | Iago | Fortes Caramés | ☐ | INPROTECH | Se adjunta breve Bio |
| 8 | Sergio | García Irigoyen | ☐ | PROFESIONAL INDEP. | Se adjunta breve Bio |
| 9 | Javier | Larrea Arias | ☐ | GADISA | Se adjunta breve Bio |
| 10 | David | Marco Freire | ☐ | ACCENTURE | Se adjunta breve Bio |
| 11 | Juan Jesús | Pardo Expósito | ☐ | TECDESOFT | Se adjunta breve Bio |
| 12 | Belén | Pérez Rodríguez | ☐ | GRUPO NUEVA PESCANOVA | Se adjunta breve Bio |
| 13 | Juan Carlos | Pozas Bustos | ☐ | SIEMENS | Se adjunta breve Bio |
| 14 | Adriel | Regueira Suárez | ☐ | TECDESOFT | Se adjunta breve Bio |
| 15 | Jacobo | Rodríguez Souto | ☐ | TECDESOFT | Se adjunta breve Bio |

# CURSO ESPECIALISTA EN CIBERSEGURIDAD INDUSTRIAL

## PROFESORADO

### Víctor Manuel Aguilar Gutiérrez

*Director Regional de Nozomi Networks en Iberia y Turquía*

NOZOMI NETWORKS

Ingeniero de Telecomunicación por la Universidad de Alcalá completo su formación en la universidad Técnica de Estambul. Con más de 15 años de experiencia en ciberseguridad, actualmente dirige Nozomi Networks en las regiones de Iberia y Turquía.

Desde el comienzo de su carrera se especializó en seguridad de las redes en empresas como Cisco Systems para focalizarse posteriormente en la protección de redes en entornos industriales e IoT. Víctor Manuel cuenta en su haber numerosas certificaciones de seguridad y redes.

https://www.linkedin.com/in/vmaguilar/

### Ignacio Álvarez Vargas

*Director of Automation and Industrial Digitalization & Product and Solutions Security Officer*

SIEMENS

Ingeniero Industrial en la especialidad de Organización Industrial y Grado en Ingeniería Electrónica Industrial y Automática. Dentro de su vida profesional ocupa el cargo de Director técnico de Automatización y Digitalización en la Business Unit de Factory Automation y a la vez es Product & Solution Security Officer de la División de Digital Industries, ambos en Siemens. Adicionalmente colabora como experto en el CCI.

Entre otras formaciones adicionales posee un MBA Executive por la Universidad de Alcalá de Henares, Máster en Comunicaciones Industriales por Siemens Nixdorf y Máster en Ciberseguridad por el CCI.

https://www.linkedin.com/in/ignacioa1/

### José Ignacio Armesto Quiroga

*Profesor Titular de Universidad*

UNIVERSIDADE DE VIGO

Doctor Ingeniero Industrial y Profesor Titular de Universidad (Departamento de Ingeniería de Sistemas y Automática) en la Universidad de Vigo. Organizador de las Jornadas JAI (Tecnologías y soluciones para la automatización industrial). Coordinador del máster universitario en mecatrónica. Representante en España de OPC Foundation. Miembro del comité IEC SC65B WG7. Premio ISA Sección Española al mejor profesional (año 2019).

https://www.linkedin.com/in/armesto/

## Manuel Caeiro Rodríguez

*Profesor Contratado Doctor*

UNIVERSIDADE DE VIGO

Ingeniero de Telecomunicación, especialidad de Ingeniería Telemática (1999) y Doctor Ingeniero de Telecomunicación (2007), ambos por la Universidad de Vigo. Docente desde el año 2000 en la Escuela de Ingeniería de Telecomunicación y desde el 2017 en el Máster Universitario en Ciberseguridad de la Universidad de Vigo. Ha participado de forma continuada en más de 40 proyectos de investigación, tanto de convocatorias europeas, como nacionales y autonómicas, y ha publicado más de 200 publicaciones en congresos y revistas científicas. Ha sido presidente del Capítulo Español de la Sociedad de la Educación del IEEE entre 2018-2020.

https://www.linkedin.com/in/mcaeiro/

## Víctor J. Calvo Querol

*CEO*

MUUTECH

Ingeniero de Telecomunicación por la Universidad de Vigo, Máster en Ciberseguridad y en Gestión y Dirección TIC por la Universitat Oberta de Catalunya, trabajó durante 10 años en una de las empresas gallegas más potentes del sector telecomunicaciones, liderando su departamento de sistemas.
En la actualidad es el CEO de Muutech, empresa especialista en monitorización de sistemas industriales y de información, cuya misión es trasladar las tecnologías, los conocimientos y experiencia de su equipo en recogida, análisis y visualización de los datos del mundo TI al mundo industrial.

https://www.linkedin.com/in/vjcalvo/

## Enrique Costa Montenegro

*Profesor Contratado Doctor*

UNIVERSIDADE DE VIGO

Doctor Ingeniero de Telecomunicación (2007) por la Universidad de Vigo.
Actualmente imparte docencia en la Escuela de Ingeniería de Telecomunicación de la Universidad de Vigo en el Grado en Ingeniería de Tecnologías de Telecomunicación, Máster Universitario en Ingeniería de Telecomunicación y Máster InterUniversitario en Ciberseguridad.
Sus principales líneas de investigación son los dispositivos personales, el procesado de lenguaje natural, los sistemas recomendadores y los servicios móviles.

https://www.linkedin.com/in/enriquec2/

## Juan de la Peña Gayo

*Account Technology Strategist*

MICROSOFT

Ingeniero Informático y MBA, con más de 15 años de experiencia en el sector industrial, especialista en automatización industrial, IIoT, Cloud, Data & AI aplicado al sector industrial. Los primeros diez años de carrera, los desempeñó en Siemens en distintas posiciones, siendo miembro del comité de expertos de Industria 4.0 de España y Portugal.
Desde hace cinco años trabaja en Microsoft, donde los primeros cuatro años los ha desempeñado como responsable de consultoría en proyectos de IoT & Data & IA, y actualmente, es Technology Strategist ayudando a clientes a definir su estrategia a la nube, donde la palanca de seguridad juega un papel fundamental.

https://www.linkedin.com/in/juandelapg/

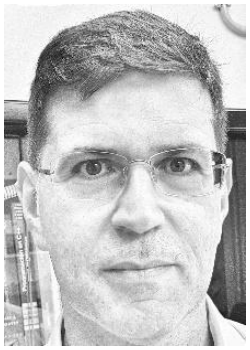
## Miguel Ramón Díaz-Cacho Medina

*Profesor Contratado Doctor*

UNIVERSIDADE DE VIGO

Ingeniero de Telecomunicación y Doctor Ingeniero Industrial por la Universidad de Vigo. Participa como docente en el Máster Universitario en Ciberseguridad de la Universidad de Vigo. Su investigación está focalizada en redes, protocolos y sistemas con retardos temporales para sistemas de control en red y teleoperación. Tiene publicaciones indexadas y ponencias en congresos nacionales e internacionales. Trabajó en diversas compañías de Tecnologías de la Información y Comunicaciones entre 1995 y 2007, destacando Bosch Telecom, Airtel (ahora Vodafone), Fujitsu ICL, Visual MS y Velneo.

https://www.linkedin.com/in/miguel-d%C3%ADaz-cacho-a1296b6/



## Manuel Fernández Veiga

*Profesor Titular de Universidad*

UNIVERSIDADE DE VIGO

Profesor titular del Departamento de Ingeniería Telemática (2001). Imparte docencia en la Escuela de Ingeniería de Telecomunicación en las áreas de ingeniería de Internet, seguridad de la información y teoría de la información. Es autor de alrededor de 50 artículos de investigación en revistas internacionales, de 60 contribuciones a congresos, de cuatro libros de texto y ha participado en proyectos de investigación, de transferencia tecnológica y de cooperación educativa a lo largo de más de veinte años. Ha sido subdirector de organización académica de la Escuela y coordinador del programa de doctorado del departamento.

https://www.linkedin.com/in/manuel-fern%C3%A1ndez-veiga-6b4bbb16/

## Ana Fernández Vilas

*Profesora Titular de Universidad*

UNIVERSIDADE DE VIGO

Doctor Ingeniero de Telecomunicación y Profesora Titular de Universidad del área de Ingeniería Telemática de la Universidad, impartiendo docencia en el Grado de Tecnologías de las Telecomunicación, Máster de Ingeniería de Telecomunicación y Máster InterUniversitario en Ciberseguridad. Desarrolla su investigación en el centro de investigación de la Universidad de Vigo AtlantTIC, en el grupo Information & Computing Lab.

Actualmente sus actividad investigadora se sitúa en la aplicación de técnicas de análisis de datos y aprendizaje máquina en distintos ámbitos de aplicación.

https://www.linkedin.com/in/anafernandezvilas/

## Fernando Fernández-Valdés Pedrosa

*CTO & Technical Director*

MUUTECH

Ingeniero de Telecomunicación y Máster en Ingeniería Telemática por la Universidad de Vigo, Máster en Ciberseguridad por la Universitat Oberta de Catalunya, Cisco CCNA y CCNP, trabajó durante varios años como docente e investigador en la Universidad de Vigo, para continuar su carrera en una de las empresas gallegas más potentes del sector telecomunicaciones, desarrollando productos de testing automática y monitorización de equipos de telecomunicación.

En la actualidad es el CTO de Muutech, empresa especialista en monitorización de sistemas industriales y de información, cuya misión es trasladar las tecnologías, los conocimientos y experiencia de su equipo en recogida, análisis y visualización de los datos del mundo TI al mundo industrial.

https://www.linkedin.com/in/fernandofernandezvaldes/

## Iago Fortes Caramés

*Socio Consultor*

INPROSEC

Ingeniero de Telecomunicación por la Universidad de Vigo y MBA. Socio Consultor y Director Gerente de Inprosec, empresa especializada en Seguridad SAP & SAP GRC. En 2005 forma parte de la división de TSRS de Ernst & Young en España durante 3 años. Posteriormente, asume el puesto de Information Security Process Manager a nivel Europeo en Unilever (multinacional del Fortune 500). En 2010 funda Inprosec, habiendo gestionado más de 20 proyectos directamente en el área de Seguridad y GRC y consiguiendo posicionar a la compañía como referente en el sector. También realiza asesoramiento como parte del Comité de Seguridad de algunas compañías multinacionales usuarias de SAP.

En 2017, dentro del grupo Inprosec, lanza la nueva iniciativa de ciberseguridad Industrial denominada InprOTech.

https://www.linkedin.com/in/iagofortes/


## Sergio García Irigoyen

*Security and technology consultant - Cybersecurity services*

PROFESIONAL INDEPENDIENTE

ingeniero Técnico en Informática de Sistemas por la URJC, Posgrado de Seguridad informática por la UOC y posee, entre otras, las certificaciones CISSP de (ISC)2 y CISM de ISACA. Especialista de Ciberseguridad con dos décadas de experiencia a sus espaldas tanto en tareas técnicas (diseño de infraestructuras, bastionado, pentesting, etc) como de gestión, habiendo trabajado como consultor de seguridad, formador e integrador de sistemas de seguridad.
También ha ocupado el cargo de CISO en varias entidades, entre ellas dos grandes bancos con gran presencia digital, como son EVO Banco e ING España & Portugal.

https://www.linkedin.com/in/sergio-garcia-irigoyen-b497665/

## Javier Larrea Arias

*Administrador de Sistemas*

GADISA

Administrador de sistemas en Gadisa, vExpert de VMware desde el año 2012 hasta 2020, líder del VMware Users Group Galicia y Miembro de la junta de ISMS Forum Galicia. Dispone de certificaciones CCNA, VCP-410, VCP5-DV.
Entre sus especialidades destacan: Administración de sistemas: Linux, Windows, AS/400, VMware. Redes: Cisco, HP, switched Wireless. Seguridad: Firewalls Stonegate y Checkpoint.

https://www.linkedin.com/in/javierlarrea/

## David Marco Freire

*Iberia OT/ICS/IOT/IIOT (Industrial Cybersecurity) and Industry X Security Lead*

ACCENTURE

Ingeniero técnico en informática (Higher Colleges of Technology de Abu Dhabi). Aterrizó en el mundo de la CiberSeguridad Industrial hace más de 12 años. Empezó implementado medidas de ciberseguridad en proyectos de Oil&Gas con Técnicas Reunidas para clientes como SABIC, ARAMCO, GALP, PEMEX, PETRONAS, TOTAL, etc. Ahora es OT Security  Manager en Accenture Security. David es uno de los expertos reconocidos a nivel nacional e internacional dentro de la ciberseguridad industrial. Es colaborador con el Centro de Ciberseguridad Industrial, miembro del comité de ISA99 (IEC 62443), evaluador externo de la comisión europea sobre proyectos de ciberseguridad y profesor en varias universidades además de ponente internacional.

https://www.linkedin.com/in/davidmarcofreire/

## Juan Jesús Pardo Expósito

*Director Técnico y Director de Negocio*

TECDESOFT AUTOMATION

Ingeniero en Automática y Electrónica Industrial. Director Técnico y Director de Negocio en la empresa TECDESOFT. Trabajando desde el año 2001 en el sector de la digitalización y automatización industrial. Dirección de más de 150 proyectos relacionados con la automatización de procesos industriales y digitalización en sectores como la minería, automóvil, agua, energía, madera, químico y alimentación. ISA Member desde 2008, CMSE Certified Machinery Safety Expert TUV Nord, Expert in ATEX systems, Auditor de Sistemas de Gestión de PRL y experto en seguridad funcional. PDD IESE Business School y MBA by Bureau Veritas.
En los últimos años se ha volcado en llevar al sector industrial las últimas tendencias en ciberseguridad industrial e inteligencia artificial aplicada a procesos de fabricación.

https://www.linkedin.com/in/juan-jes%C3%BAs-pardo-a6b98b23/

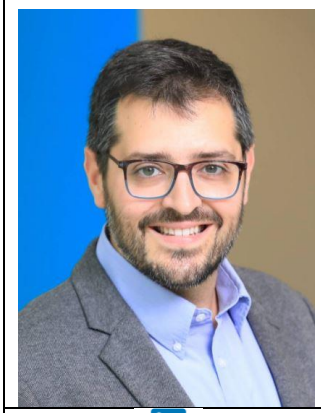
## Belén Pérez Rodríguez

*CISO*

Grupo Nueva Pescanova (CEH, CHFI, CPN)

Ingeniero Técnico Industrial (Universidad de A CORUÑA) y Grado en Ingeniería electrónica Industrial y Automática (Universidad de León). Máster Profesional de Ciberseguridad Industrial (CCI). Certificaciones profesionales: CCNA, CCNA-Security y CCNP-Routing&Switching de CISCO, QRadar de IBM. En la actualidad es CISO en Grupo Nueva Pescanova. Anteriormente: Consultora, auditora y gestora de proyectos de Ciberseguridad, Ingeniero QA, Técnico de O&M y docente.
En el ámbito de la Ciberseguridad Industrial, formadora tanto en el ámbito educativo (Universidad, Centros de Formación Profesional...) como en diferentes organizaciones Industriales y Ponente en algunos de los principales congresos de seguridad en España (Navaja Negra, SecAdmin, TizonaCOnf, MakerFaire Galicia...).

https://www.linkedin.com/in/belenpr/



## Juan Carlos Pozas Bustos

*Responsable de producto, Sistemas de comunicaciones y Ciberseguridad Industrial*

SIEMENS

Ingeniero Superior en Telecomunicaciones por la universidad Carlos III de Madrid, especialista en planificación y gestión de redes de comunicaciones, y aplicación de algoritmos genéticos para detección y clasificación. Trabajando en SIEMENS desde hace 13 años, siempre vinculado a la línea de las comunicaciones y ciberseguridad industrial. Actualmente desempeñando el cargo de responsable de producto, Sistemas de comunicaciones y Ciberseguridad industrial, así como responsable del desarrollo de negocio a través del programa de Industrial Strength Networks Solution Partners.

https://www.linkedin.com/in/juan-carlos-pozas-b456817/

## Adriel Regueira Suárez

*Head of IT & Cybersecurity*

TECDESOFT AUTOMATION

Ingeniero de Telecomunicación por la Universidad de Vigo. Dirige el departamento de Sistemas y Ciberseguridad de Tecdesoft. Ha dedicado toda su carrera a la aplicación de tecnología y comunicaciones al entorno de la fábrica, haciendo realidad la industria 4.0.
Ha gestionado y participado en multitud de proyectos en ciberseguridad industrial incluyendo algunas de las mayores infraestructuras críticas del país. Es miembro ISA y del comité internacional de ISA99 (IEC 62443) y participa en foros y ponencias evangelizando sobre la materia.

https://www.linkedin.com/in/adriel-regueira/

## Jacobo Rodríguez Souto

*Ingeniero de Sistemas y Ciberseguridad*

TECDESOFT AUTOMATION

Ingeniero Industrial por la Universidad de la Coruña (UDC). Trabaja como Ingeniero de Sistemas y Ciberseguridad de Tecdesoft. Ha participado en multitud proyectos de I+D europeos, así como en proyectos de ciberseguridad para importantes multinacionales del sector del automóvil y de la energía.
Es ingeniero certificado de Nozomi Networks, y en su día a día está acostumbrado a solucionar problemas en entornos complejos dónde la fabricación no puede parar. Experto en sistemas de comunicación Siemens así como en las mejores prácticas recogidas en la IEC 62443.

https://www.linkedin.com/in/jacobo-rodr%C3%ADguez-souto-286b4775/

Escola Aberta
de Formación Permanente
Universidade Vigo

# FICHA MATERIA TÍTULO DE ESPECIALISTA

| |
|---|
| MATERIA: **Introducción a la Industria 4.0** |
| Módulo: |
| Tipo: ☒Obligatoria ☐Optativa |
| ECTS: 1 |
| Modalidad: **Síncrona virtual** |
| COMPETENCIAS ASOCIADAS: **CE1, CE2**<br>Indicar códigos da táboa 2.3 da proposta |
| Descripción general:<br>**Esta materia tiene como objetivo introducir al alumnado en los conceptos básicos y principales tecnologías habilitadoras de la industria 4.0, haciendo especial hincapié en la relevancia que tiene la aplicación de tecnologías y soluciones específicas para la ciberseguridad en el ámbito de las plantas de fabricación.** |
| Coordinador/a: **José Ignacio Armesto Quiroga**<br>Profesores/as:<br>1) **José Ignacio Armesto Quiroga** |

| |
|---|
| Resultados de aprendizaje:<br>**Conocimiento del marco histórico y de los conceptos básicos de la Industria 4.0. Conocimiento de las principales tecnologías habilitadoras relacionadas con la Industria 4.0 y la fábrica conectada. Capacidad para comprender la relevancia de la ciberseguridad industrial en el contexto de las fábricas conectadas.** |

| |
|---|
| Programa académico:<br>**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.** |

Metodología docente:
**Lección magistral e Seminarios: exposición de los contenidos de la materia. Estudio de casos: realización de un trabajo basado en los contenidos de la materia. Prueba teórica: realización de una prueba síncrona de evaluación mediante as plataformas Campus Remoto y/o Moovi de la Universidade de Vigo.**

| Actividades formativas SÍNCRONAS | Horas síncronas presenciales | Horas síncronas virtuales | Horas de trabajo autónomo del estudante |
|---|---|---|---|
| **Lección magistral** | | **4** | **6** |
| **Seminarios** | | **4** | **4** |
| **Estudio de casos** | | **1** | **5** |
| **Prueba teórica** | | **1** | |
| ECTS TOTALES = 1,00 | 0,00 | 10,00 | 15,00 |

***Las horas síncronas deben ser entre 8 y 12 por ECTS en modalidad síncrona***

| Actividades formativas ASÍNCRONAS | Horas tutorización | Horas de trabajo autónomo del estudiante |
|---|---|---|
| | | |
| ECTS TOTALES = 0,00 | 0,00 | 0,00 |

***Las horas de titorización serán entre 4 e 8 por ECTS en modalidad asíncrona***

Metodología de evaluación:
**La asistencia y participación en las actividades formativas síncronas supondrá el 15% de la cualificación. El estudio de casos consistirá en la realización de un trabajo basado en los contenidos de la materia, que será evaluado y supondrá el 60% de la cualificación. La evaluación de la prueba teórica supondrá el 25% de la cualificación.**

| Pruebas de evaluación | % Ponderación |
|---|---|
| **Asistencia actividades formativas síncronas** | **15** |
| **Estudio de casos: trabajo basado en los contenidos de la materia** | **60** |
| **Prueba teórica** | **25** |
| | 100% |

Plataformas de Teledocencia y tutorización:
**Las actividades síncronas se realizarán en el Campus Remoto de la Universidade de Vigo. La entrega de trabajos se realizará en la plataforma Moovi de la Universidade de Vigo. Las tutorías se concertarán por correo electrónico y tendrán lugar en el Campus Remoto de la Universidade de Vigo.**

Escola Aberta
de Formación Permanente
Universidade Vigo

# FICHA MATERIA TÍTULO DE ESPECIALISTA

| |
|---|
| MATERIA: **Introducción a los sistemas de control industrial** |
| Módulo: |
| Tipo: ☒Obligatoria ☐Optativa |
| ECTS: 2 |
| Modalidad: **Síncrona virtual** |
| COMPETENCIAS ASOCIADAS: **CE3, CE4**<br>Indicar códigos da táboa 2.3 da proposta |
| Descripción general:<br>**Esta materia tiene como objetivo introducir al alumnado en los fundamentos de los principales sistemas electrónicos de control utilizados para la automatización y control de las plantas de fabricación industrial, haciendo especial hincapié en los apartados relativos a su integración en el contexto de la industria 4.0 y la fábrica conectada.** |
| Coordinador/a: **José Ignacio Armesto Quiroga**<br>Profesores/as:<br>1) **José Ignacio Armesto Quiroga**<br>2) **Miguel Ramón Díaz-Cacho Medina** |

| |
|---|
| Resultados de aprendizaje:<br>**Conocimientos generales sobre los sistemas de control utilizados en la automatización de plantas industriales. Conocimientos generales sobre las redes de comunicación industrial utilizadas en los sistemas de control. Capacidad para analizar las necesidades de un proyecto de automatización industrial. Capacidad para especificar las distintas tecnologías de control y comunicación necesarias para la implantación de un proceso de fabricación automatizado.** |

| |
|---|
| Programa académico:<br>**Sistemas de control industrial: sistema de control distribuido (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.** |

Metodología docente:
**Lección magistral y Seminarios: exposición de los contenidos de la materia. Estudio de casos: realización de un trabajo basado en los contenidos de la materia. Prueba teórica: realización de una prueba síncrona de evaluación mediante las plataformas Campus Remoto y/o Moovi de la Universidad de Vigo.**

| Actividades formativas SÍNCRONAS | Horas síncronas presenciales | Horas síncronas virtuales | Horas de trabajo autónomo del estudiante |
|---|---|---|---|
| **Lección magistral** | | **14** | **18** |
| **Seminarios** | | **4** | **6** |
| **Estudio de casos** | | **1** | **6** |
| **Proba teórica** | | **1** | |
| ECTS TOTALES = 2,00 | 0,00 | 20,00 | 30,00 |

***Las horas síncronas deben ser entre 8 y 12 por ECTS en modalidad síncrona***

| Actividades formativas ASÍNCRONAS | Horas tutorización | Horas de trabajo autónomo del estudiante |
|---|---|---|
| | | |
| ECTS TOTALES = 0,00 | 0,00 | 0,00 |

***Las horas de titorización serán entre 4 e 8 por ECTS en modalidad asíncrona***

Metodología de evaluación:
**La asistencia y participación en las actividades formativas síncronas supondrá el 15% de la cualificación. El estudio de casos consistirá en la realización de un trabajo basado en los contenidos de la materia, que será evaluado y supondrá el 60% de la cualificación. La evaluación de la prueba teórica supondrá el 25% de la cualificación.**

| Pruebas de evaluación | % Ponderación |
|---|---|
| **Asistencia actividades formativas síncronas** | **15** |
| **Estudio de casos: trabajo basado en los contenidos de la materia** | **60** |
| **Prueba teórica** | **25** |
| | 100% |

Plataformas de Teledocencia y tutorización:
**Las actividades síncronas se realizarán en el Campus Remoto de la Universidad de Vigo. La entrega de trabajos se realizará en la plataforma Moovi de la Universidad de Vigo. Las tutorías se concertarán por correo electrónico y tendrán lugar en el Campus Remoto de la Universidad de Vigo.**

Escola Aberta
de Formación Permanente
Universidade Vigo

# FICHA MATERIA TÍTULO DE ESPECIALISTA

| |
|---|
| MATERIA: **Cumplimiento y gestión de la ciberseguridad industrial** |
| Módulo: |
| Tipo: ☒Obligatoria ☐Optativa |
| ECTS: 6 |
| Modalidad: **Síncrona virtual** |
| COMPETENCIAS ASOCIADAS: **CE5, CE6, CE7**<br>Indicar códigos da táboa 2.3 da proposta |
| Descripción general:<br>**Esta materia tiene como objetivo introducir al alumnado en los conceptos básicos de las distintas normativas y compendios de buenas prácticas más utilizadas en el sector industrial, así como sus principales características y cómo aplicarlas en la realidad.** |
| Coordinador/a: **Belén Pérez Rodríguez**<br>Profesores/as:<br>1) **Ana Fernández Vilas**<br>2) **Manuel Caeiro Rodríguez**<br>3) **Belén Pérez Rodríguez**<br>4) **David Marco Freire**<br>5) **Juan de la Peña Gayo** |

| |
|---|
| Resultados de aprendizaje:<br>**Conocimiento de los distintos organismos que aglutinan normativas y buenas prácticas. Conocimiento para saber distinguir cuándo es preciso utilizar normativa y cuando las buenas prácticas. Conocimiento de cómo aplicar este conjunto de buenas prácticas y normativa en la industria gallega. Conocimientos sobre cómo funciona la normativa ISA/ IEC 62443. Conocimientos sobre cómo apoyarse en las buenas prácticas para asentar la mejor base para la digitalización.** |

| |
|---|
| Programa académico:<br>**Introducción. Evaluación de riesgos: inventario de activos, identificación de vulnerabilidades y amenazas, evaluación de riesgos. 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 da Ciberseguridad-SGCI: administrativo, operacional y técnico.** |

Metodología docente:
**Lección magistral y Seminarios: exposición de los contenidos de la materia. Estudio de casos: realización de un trabajo basado en los contenidos de la materia. Prueba teórica: realización de una prueba síncrona de evaluación mediante las plataformas Campus Remoto y/o Moovi de la Universidad de Vigo.**

| Actividades formativas SÍNCRONAS | Horas síncronas presenciales | Horas síncronas virtuales | Horas de trabajo autónomo del estudiante |
|---|---|---|---|
| **Lección magistral** | | **54** | **72** |
| **Seminarios** | | **4** | **6** |
| **Estudio de casos** | | **1** | **12** |
| **Prueba teórica** | | **1** | |
| ECTS TOTALES = 6,00 | 0,00 | 60,00 | 90,00 |

***Las horas síncronas deben ser entre 8 y 12 por ECTS en modalidad síncrona***

| Actividades formativas ASÍNCRONAS | Horas tutorización | Horas de trabajo autónomo del estudiante |
|---|---|---|
| Descrición da actividade formativa | | |
| ECTS TOTALES = 0,00 | 0,00 | 0,00 |

***Las horas de titorización serán entre 4 e 8 por ECTS en modalidad asíncrona***

Metodología de evaluación:
**La asistencia y participación en las actividades formativas síncronas supondrá el 15% de la cualificación. El estudio de casos consistirá en la realización de un trabajo basado en los contenidos de la materia, que será evaluado y supondrá el 60% de la cualificación. La evaluación de la prueba teórica supondrá el 25% de la cualificación.**

| Pruebas de evaluación | % Ponderación |
|---|---|
| **Asistencia actividades formativas síncronas** | **15** |
| **Estudio de casos: trabajo basado en los contenidos de la materia** | **60** |
| **Prueba teórica** | **25** |
| | 100% |

Plataformas de Teledocencia y tutorización:
**Las actividades síncronas se realizarán en el Campus Remoto de la Universidad de Vigo. La entrega de trabajos se realizará en la plataforma Moovi de la Universidad de Vigo. Las tutorías se concertarán por correo electrónico y tendrán lugar en el Campus Remoto de la Universidad de Vigo.**

Escola Aberta
de Formación Permanente
Universidade Vigo

# FICHA MATERIA TÍTULO DE ESPECIALISTA

| |
|---|
| MATERIA: **Redes industriales (Familia SCALANCE de SIEMENS)** |
| Módulo: |
| Tipo: ☒Obligatoria ☐Optativa |
| ECTS: 5 |
| Modalidad: **Síncrona virtual** |
| COMPETENCIAS ASOCIADAS: **CE8, CE9, CE10**<br>Indicar códigos da táboa 2.3 da proposta |
| Descripción general:<br>**Esta materia tiene como objetivo introducir al alumnado en los conceptos básicos de las comunicaciones industriales basadas en ethernet, utilizando una de las tecnologías más ampliamente adoptadas en las fábricas. Se verá cómo utilizar estos conceptos para crear un esquema de defensa en seguridad y como aplicar y configurar en dispositivos reales las mejores prácticas.** |
| Coordinador/a: **Miguel Ramón Díaz-Cacho Medina**<br>Profesores/as:<br>1) **Miguel Ramón Díaz-Cacho Medina**<br>2) **Manuel Fernández Veiga**<br>3) **Ignacio Álvarez Vargas**<br>4) **Juan Carlos Pozas Bustos**<br>5) **Adriel Regueira Suárez**<br>6) **Jacobo Rodríguez Souto** |

| |
|---|
| Resultados de aprendizaxe:<br>**Conocimiento del modelo de referencia OSI de ISO. Conocimiento de la capa ethernet (VLAN, anillos MRP y HRP, ACL). Conocimiento de los principales dispositivos de red: hub, switch, router, gateway y firewall. Conocimiento de la capa IP (enrutado, VRRP, redundante en standby). Conocimientos básicos para la segurización y segmentación de redes industriales mediante NAT, VPN y conexionado remoto seguro. Conocimiento de las arquitecturas de referencia para el diseño de una red industrial segura.** |

| |
|---|
| Programa académico:<br>**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 e HRP. 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.** |

Metodología docente:
**Lección magistral y talleres prácticos: exposición de los contenidos teóricos y prácticos de la materia. Estudio de casos: realización de un trabajo basado en los contenidos de la materia. Prueba teórica: realización de una prueba síncrona de evaluación mediante las plataformas Campus Remoto y/o Moovi de la Universidad de Vigo.**

| Actividades formativas SÍNCRONAS | Horas síncronas presenciales | Horas síncronas virtuales | Horas de trabajo autónomo del estudiante |
|---|---|---|---|
| **Lección magistral** | | **43** | **60** |
| **Talleres prácticos** | | **5** | **6** |
| **Estudio de casos** | | **1** | **9** |
| **Prueba teórica** | | **1** | |
| ECTS TOTALES = 5,00 | 0,00 | 50,00 | 75,00 |

***Las horas síncronas deben ser entre 8 y 12 por ECTS en modalidad síncrona***

| Actividades formativas ASÍNCRONAS | Horas tutorización | Horas de trabajo autónomo del estudiante |
|---|---|---|
| | | |
| ECTS TOTALES = 0,00 | 0,00 | 0,00 |

***Las horas de titorización serán entre 4 e 8 por ECTS en modalidad asíncrona***

Metodología de evaluación:
**La asistencia y participación en las actividades formativas síncronas supondrá el 15% de la cualificación. El estudio de casos consistirá en la realización de un trabajo basado en los contenidos de la materia, que será evaluado y supondrá el 60% de la cualificación. La evaluación de la prueba teórica supondrá el 25% de la cualificación.**

| Pruebas de evaluación | % Ponderación |
|---|---|
| **Asistencia actividades formativas síncronas** | **15** |
| **Estudio de casos: trabajo basado en los contenidos de la materia** | **60** |
| **Prueba teórica** | **25** |
| | 100% |

Plataformas de Teledocencia y tutorización:
**Las actividades síncronas se realizarán en el Campus Remoto de la Universidad de Vigo. La entrega de trabajos se realizará en la plataforma Moovi de la Universidad de Vigo. Las tutorías se concertarán por correo electrónico y tendrán lugar en el Campus Remoto de la Universidad de Vigo.**

Escola Aberta
de Formación Permanente
Universidade Vigo

# FICHA MATERIA TÍTULO DE ESPECIALISTA

| |
|---|
| MATERIA: **Virtualización en arquitecturas de control industrial (Familia VSPHERE de VMWARE)** |
| Módulo: |
| Tipo: ☒Obligatoria ☐Optativa |
| ECTS: 4 |
| Modalidad: **Síncrona virtual** |
| COMPETENCIAS ASOCIADAS: **CE11, CE12**<br>Indicar códigos da táboa 2.3 da proposta |
| Descripción general:<br>**Esta materia tiene como objetivo introducir al alumnado en los conceptos básicos de virtualización, para comprender cómo utilizarla para mejorar la gestión y la disponibilidad de los sistemas de control industrial. Se utilizará una de las tecnologías más utilizadas en el comprado.** |
| Coordinador/a: **Ana Fernández Vilas**<br>Profesores/as:<br>1) **Manuel Fernández Veiga**<br>2) **Ana Fernández Vilas**<br>3) **Javier Larrea Arias** |

| |
|---|
| Resultados de aprendizaje:<br>**Conocimientos de teoría de la virtualización. Conocimientos de configuración de redes virtuales. Conocimientos de creación de máquinas virtuales. Capacidad para crear y gestionar un servidor de máquinas virtuales. Capacidad para crear, configurar y gestionar un sistema de almacenamiento virtual.** |

| |
|---|
| Programa académico:<br>**Introducción. Conceptos básicos. Tipos de hipervisores. Elementos da plataforma VMware: Hosts esxI, 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.** |

Metodoloxía docente:
**Lección magistral y Talleres prácticos: exposición de los contenidos teóricos y prácticos de la materia. Estudio de casos: realización de un trabajo basado en los contenidos de la materia. Prueba teórica: realización de una prueba síncrona de evaluación mediante las plataformas Campus Remoto y/o Moovi de la Universidad de Vigo.**

| Actividades formativas SÍNCRONAS | Horas síncronas presenciales | Horas síncronas virtuales | Horas de trabajo autónomo del estudiante |
|---|---|---|---|
| **Lección magistral** | | **10** | **15** |
| **Talleres prácticos** | | **24** | **35** |
| **Estudio de casos** | | **5** | **10** |
| **Prueba teórica** | | **1** | |
| ECTS TOTALES = 4,00 | 0,00 | 40,00 | 60,00 |

***Las horas síncronas deben ser entre 8 y 12 por ECTS en modalidad síncrona***

| Actividades formativas ASÍNCRONAS | Horas tutorización | Horas de trabajo autónomo del estudiante |
|---|---|---|
| | | |
| ECTS TOTALES = 0,00 | 0,00 | 0,00 |

***Las horas de titorización serán entre 4 e 8 por ECTS en modalidad asíncrona***

Metodología de evaluación:
**La asistencia y participación en las actividades formativas síncronas supondrá el 15% de la cualificación. El estudio de casos consistirá en la realización de un trabajo basado en los contenidos de la materia, que será evaluado y supondrá el 60% de la cualificación. La evaluación de la prueba teórica supondrá el 25% de la cualificación.**

| Pruebas de evaluación | % Ponderación |
|---|---|
| **Asistencia actividades formativas síncronas** | **15** |
| **Estudio de casos: trabajo basado en los contenidos de la materia** | **60** |
| **Prueba teórica** | **25** |
| | 100% |

Plataformas de Teledocencia y tutorización:
**Las actividades síncronas se realizarán en el Campus Remoto de la Universidad de Vigo. La entrega de trabajos se realizará en la plataforma Moovi de la Universidad de Vigo. Las tutorías se concertarán por correo electrónico y tendrán lugar en el Campus Remoto de la Universidad de Vigo.**

Escola Aberta
de Formación Permanente
Universidade Vigo

# FICHA MATERIA TÍTULO DE ESPECIALISTA

| |
|---|
| MATERIA: **Sistemas de supervisión (Soluciones ZABBIX)** |
| Módulo: |
| Tipo: ☒Obligatoria ☐Optativa |
| ECTS: 4 |
| Modalidad: **Síncrona virtual** |
| COMPETENCIAS ASOCIADAS: **CE13, CE14**<br>Indicar códigos da táboa 2.3 da proposta |
| Descripción general:<br>**Esta materia tiene como objetivo introducir al alumnado en la importancia de monitorizar los dispositivos de la infraestructura industrial y cómo hacerlo usando una de las tecnologías open source más utilizadas en el comprado.** |
| Coordinador/a: **Víctor Javier Calvo Querol**<br>Profesores/as:<br>1) **Víctor Javier Calvo Querol**<br>2) **Fernando Fernández-Valdés Pedrosa** |

| |
|---|
| Resultados de aprendizaje:<br>**Conocimiento de la necesidad de monitorizar. Conocimientos para la instalación de Zabbix. Conocimientos para la aplicación de Zabbix en entornos industriales. Conocimientos de las principales características de Zabbix. Experiencia configurando un entorno Zabbix completo.** |

| |
|---|
| Programa académico:<br>**Introducción. Necesidad. Tipos de sistemas de supervisión. Aplicabilidad en entornos industriales. Aplicabilidad en ciberseguridade industrial. Monitorización con Zabbix: Arquitectura, requisitos, modelos On-premise, Cloud, SaaS. Host, items e modelos. Triggers, macros, funcións 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.** |

Metodología docente:
**Lección magistral y Seminarios prácticos: exposición de los contenidos teóricos y prácticos de la materia. Estudio de casos: realización de un trabajo basado en los contenidos de la materia. Prueba teórica: realización de una prueba síncrona de evaluación mediante las plataformas Campus Remoto y/o Moovi de la Universidad de Vigo.**

| Actividades formativas SÍNCRONAS | Horas síncronas presenciales | Horas síncronas virtuales | Horas de trabajo autónomo del estudiante |
|---|---|---|---|
| **Lección magistral** | | **28** | **36** |
| **Talleres prácticos** | | **10** | **15** |
| **Estudio de casos** | | **1** | **9** |
| **Prueba teórica** | | **1** | |
| ECTS TOTALES = 4,00 | 0,00 | 40,00 | 60,00 |

***Las horas síncronas deben ser entre 8 y 12 por ECTS en modalidad síncrona***

| Actividades formativas ASÍNCRONAS | Horas tutorización | Horas de trabajo autónomo del estudiante |
|---|---|---|
| | | |
| ECTS TOTALES = 0,00 | 0,00 | 0,00 |

***Las horas de titorización serán entre 4 e 8 por ECTS en modalidad asíncrona***

Metodología de evaluación:
**La asistencia y participación en las actividades formativas síncronas supondrá el 15% de la cualificación. El estudio de casos consistirá en la realización de un trabajo basado en los contenidos de la materia, que será evaluado y supondrá el 60% de la cualificación. La evaluación de la prueba teórica supondrá el 25% de la cualificación.**

| Pruebas de evaluación | % Ponderación |
|---|---|
| **Asistencia actividades formativas síncronas** | **15** |
| **Estudio de casos: trabajo basado en los contenidos de la materia** | **60** |
| **Prueba teórica** | **25** |
| | 100% |

Plataformas de Teledocencia y tutorización:
**Las actividades síncronas se realizarán en el Campus Remoto de la Universidad de Vigo. La entrega de trabajos se realizará en la plataforma Moovi de la Universidad de Vigo. Las tutorías se concertarán por correo electrónico y tendrán lugar en el Campus Remoto de la Universidad de Vigo.**

Escola Aberta
de Formación Permanente
Universidade Vigo

# FICHA MATERIA TÍTULO DE ESPECIALISTA

| |
|---|
| MATERIA: **Firewalls de nueva generación (Familia FORTIGATE de FORTINET)** |
| Módulo: |
| Tipo: ☒Obligatoria ☐Optativa |
| ECTS: 3 |
| Modalidad: **Síncrona virtual** |
| COMPETENCIAS ASOCIADAS: **CE15, CE16**<br>Indicar códigos da táboa 2.3 da proposta |
| Descripción general:<br>**Esta materia tiene como objetivo introducir al alumnado en los principales conceptos de los firewalls de nueva generación (NGFW), utilizando una de las soluciones tecnológicas más ampliamente adoptadas en el entorno industrial para la creación de una red industrial cibersegura.** |
| Coordinador/a: **Sergio García Irigoyen**<br>Profesores/as:<br>1) **Sergio García Irigoyen** |

| |
|---|
| Resultados de aprendizaje:<br>**Conocimientos sobre los firewalls de nueva generación (NGFW). Conocimientos sobre las tablas y políticas de routing. Conocimientos sobre cómo funcionan y cómo se configuran túneles VPN e IPSEC. Conocimientos sobre cómo aplicar las seguridades a nivel de capa de aplicación para segurizar la infraestructura. Experiencia en la utilización de un firewall de nueva generación con casos prácticos.** |

| |
|---|
| Programa académico:<br>**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.** |

Metodología docente:
**Lección magistral y Seminarios prácticos: exposición de los contenidos teóricos y prácticos de la materia. Estudio de casos: realización de un trabajo basado en los contenidos de la materia. Prueba teórica: realización de una prueba síncrona de evaluación mediante las plataformas Campus Remoto y/o Moovi de la Universidad de Vigo.**

| Actividades formativas SÍNCRONAS | Horas síncronas presenciales | Horas síncronas virtuales | Horas de trabajo autónomo del estudiante |
|---|---|---|---|
| **Lección magistral** | | **18** | **24** |
| **Talleres prácticos** | | **10** | **15** |
| **Estudio de casos** | | **1** | **6** |
| **Prueba teórica** | | **1** | |
| ECTS TOTALES = 3,00 | 0,00 | 30,00 | 45,00 |

***Las horas síncronas deben ser entre 8 y 12 por ECTS en modalidad síncrona***

| Actividades formativas ASÍNCRONAS | Horas tutorización | Horas de trabajo autónomo del estudiante |
|---|---|---|
| | | |
| ECTS TOTALES = 0,00 | 0,00 | 0,00 |

***Las horas de titorización serán entre 4 e 8 por ECTS en modalidad asíncrona***

Metodología de evaluación:
**La asistencia y participación en las actividades formativas síncronas supondrá el 15% de la cualificación. El estudio de casos consistirá en la realización de un trabajo basado en los contenidos de la materia, que será evaluado y supondrá el 60% de la cualificación. La evaluación de la prueba teórica supondrá el 25% de la cualificación.**

| Pruebas de evaluación | % Ponderación |
|---|---|
| **Asistencia actividades formativas síncronas** | **15** |
| **Estudio de casos: trabajo basado en los contenidos de la materia** | **60** |
| **Prueba teórica** | **25** |
| | 100% |

Plataformas de Teledocencia y tutorización:
**Las actividades síncronas se realizarán en el Campus Remoto de la Universidad de Vigo. La entrega de trabajos se realizará en la plataforma Moovi de la Universidad de Vigo. Las tutorías se concertarán por correo electrónico y tendrán lugar en el Campus Remoto de la Universidad de Vigo. .**

Escola Aberta
de Formación Permanente
Universidade Vigo

# FICHA MATERIA TÍTULO DE ESPECIALISTA

| |
|---|
| MATERIA: **Sistemas de detección de intrusiones (Familia SCADA GUARDIAN de NOZOMI NETWORKS)** |
| Módulo: |
| Tipo: ☒Obligatoria ☐Optativa |
| ECTS: 3 |
| Modalidad: **Síncrona virtual** |
| COMPETENCIAS ASOCIADAS: **CE17, CE18**<br>Indicar códigos da táboa 2.3 da proposta |
| Descripción general:<br>**Esta materia tiene como objetivo introducir al alumnado en los conceptos básicos y principales de los sistemas de detección de intrusiones (IDS) y la necesidad de su utilización con protocolos de comunicación específicos de la industria. Se utilizará para eso una de las soluciones IDS más extendida en el ámbito industrial.** |
| Coordinador/a: **Adriel Regueira Suárez**<br>Profesores/as:<br>1) **Enrique Costa Montenegro**<br>2) **Víctor Manuel Aguilar Gutiérrez**<br>3) **Adriel Regueira Suárez** |

| |
|---|
| Resultados de aprendizaje:<br>**Conocimiento de la necesidad de utilización de sistemas de detección de intrusiones (IDS). Conocimientos sobre su aplicación en el marco normativo y de buenas prácticas. Conocimientos sobre que es necesario modificar en las infraestructuras para instalar un sistema IDS. Experiencia en la configuración y gestión de un sistema IDS real.** |

| |
|---|
| Programa académico:<br>**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, integraciones de terceros. Taller práctico.** |

Metodología docente:
**Lección magistral y Seminarios prácticos: exposición de los contenidos teóricos y prácticos de la materia. Estudio de casos: realización de un trabajo basado en los contenidos de la materia. Prueba teórica: realización de una prueba síncrona de evaluación mediante las plataformas Campus Remoto y/o Moovi de la Universidad de Vigo.**

| Actividades formativas SÍNCRONAS | Horas síncronas presenciales | Horas síncronas virtuales | Horas de trabajo autónomo del estudiante |
|---|---|---|---|
| **Lección magistral** | | **18** | **24** |
| **Talleres prácticos** | | **10** | **15** |
| **Estudio de casos** | | **1** | **6** |
| **Prueba teórica** | | **1** | |
| ECTS TOTALES = 3,00 | 0,00 | 30,00 | 45,00 |

***Las horas síncronas deben ser entre 8 y 12 por ECTS en modalidad síncrona***

| Actividades formativas ASÍNCRONAS | Horas tutorización | Horas de trabajo autónomo del estudiante |
|---|---|---|
| | | |
| ECTS TOTALES = 0,00 | 0,00 | 0,00 |

***Las horas de titorización serán entre 4 e 8 por ECTS en modalidad asíncrona***

Metodología de evaluación:
**La asistencia y participación en las actividades formativas síncronas supondrá el 15% de la cualificación. El estudio de casos consistirá en la realización de un trabajo basado en los contenidos de la materia, que será evaluado y supondrá el 60% de la cualificación. La evaluación de la prueba teórica supondrá el 25% de la cualificación.**

| Pruebas de evaluación | % Ponderación |
|---|---|
| **Asistencia actividades formativas síncronas** | **15** |
| **Estudio de casos: trabajo basado en los contenidos de la materia** | **60** |
| **Prueba teórica** | **25** |
| | 100% |

Plataformas de Teledocencia y tutorización:
**Las actividades síncronas se realizarán en el Campus Remoto de la Universidad de Vigo. La entrega de trabajos se realizará en la plataforma Moovi de la Universidad de Vigo. Las tutorías se concertarán por correo electrónico y tendrán lugar en el Campus Remoto de la Universidad de Vigo.**

Escola Aberta
de Formación Permanente
Universidade Vigo

# FICHA MATERIA TÍTULO DE ESPECIALISTA

| |
|---|
| MATERIA: **Introducción a los sistemas de gestión de eventos e información de seguridad (Soluciones MICROSOFT AZURE SENTINEL e INPROTECH GUARDIAN)** |
| Módulo: |
| Tipo: ☒Obligatoria ☐Optativa |
| ECTS: 2 |
| Modalidad: **Síncrona virtual** |
| COMPETENCIAS ASOCIADAS: **CE19, CE20**<br>Indicar códigos da táboa 2.3 da proposta |
| Descripción general:<br>**Esta materia tiene como objetivo introducir al alumnado en los conceptos básicos y la necesidad de utilizar herramientas de gestión de eventos e información de seguridad (SIEM) en la industria. Aprenderá las ventajas de su utilización en la segurización de un entorno industrial y configurará una herramienta SIEM comercial.** |
| Coordinador/a: **Iago Fortes Caramés**<br>Profesores/as:<br>1) **Iago Fortes Caramés**<br>2) **Juan de la Peña Gayo** |

| |
|---|
| Resultados de aprendizaje:<br>**Conocimientos básicos sobre las principales características de los sistemas de gestión de eventos e información de seguridad (SIEM). Conocimientos sobre la aplicación de herramientas SIEM en la segurización de industrias. Experiencia en la configuración de un SIEM comercial.** |

| |
|---|
| Programa académico:<br>**Introducción a los sistemas de gestión de eventos e información de seguridad (SIEM): funcionamiento, diferencias entre IDS e SIEM. Necesidad. Casos de uso y elementos de un SIEM. Taller práctico.** |

Metodología docente:
**Lección magistral y talleres prácticos: exposición de los contenidos teóricos y prácticos de la materia. Estudio de casos: realización de un trabajo basado en los contenidos de la materia. Prueba teórica: realización de una prueba síncrona de evaluación mediante las plataformas Campus Remoto y/o Moovi de la Universidad de Vigo.**

| Actividades formativas SÍNCRONAS | Horas síncronas presenciales | Horas síncronas virtuales | Horas de trabajo autónomo del estudiante |
|---|---|---|---|
| **Lección magistral** | | **13** | **21** |
| **Talleres prácticos** | | **5** | **6** |
| **Estudio de casos** | | **1** | **3** |
| **Prueba teórica** | | **1** | |
| ECTS TOTALES = 2,00 | 0,00 | 20,00 | 30,00 |

***Las horas síncronas deben ser entre 8 y 12 por ECTS en modalidad síncrona***

| Actividades formativas ASÍNCRONAS | Horas tutorización | Horas de trabajo autónomo del estudiante |
|---|---|---|
| | | |
| ECTS TOTALES = 0,00 | 0,00 | 0,00 |

***Las horas de titorización serán entre 4 e 8 por ECTS en modalidad asíncrona***

Metodología de evaluación:
**La asistencia y participación en las actividades formativas síncronas supondrá el 15% de la cualificación. El estudio de casos consistirá en la realización de un trabajo basado en los contenidos de la materia, que será evaluado y supondrá el 60% de la cualificación. La evaluación de la prueba teórica supondrá el 25% de la cualificación.**

| Pruebas de evaluación | % Ponderación |
|---|---|
| **Asistencia actividades formativas síncronas** | **15** |
| **Estudio de casos: trabajo basado en los contenidos de la materia** | **60** |
| **Prueba teórica** | **25** |
| | 100% |

Plataformas de Teledocencia y tutorización:
**Las actividades síncronas se realizarán en el Campus Remoto de la Universidad de Vigo. La entrega de trabajos se realizará en la plataforma Moovi de la Universidad de Vigo. Las tutorías se concertarán por correo electrónico y tendrán lugar en el Campus Remoto de la Universidad de Vigo.**

Escola Aberta
de Formación Permanente
Universidade Vigo

# FICHA MATERIA TÍTULO DE ESPECIALISTA

| |
|---|
| MATERIA: **Trabajo final de curso** |
| Módulo: |
| Tipo: ☒Obligatoria ☐Optativa |
| ECTS: 3 |
| Modalidad: **Síncrona virtual** |
| COMPETENCIAS ASOCIADAS: **CE21**<br>Indicar códigos da táboa 2.3 da proposta |
| Descripción general:<br>**Esta materia tiene como objetivo que el alumnado ponga en práctica los distintos conocimientos adquiridos en un caso real. De este modo, verá como todo el aprendido se interrelaciona en la realidad y tendrá que afrontar decisiones sobre cómo segurizar una fábrica.** |
| Coordinador/a: **José Ignacio Armesto Quiroga**<br>Profesores/as:<br>1) **José Ignacio Armesto Quiroga**<br>2) **Miguel Ramón Díaz-Cacho Medina**<br>3) **Adriel Regueira Suárez**<br>4) ***El restante profesorado del curso puede también dirigir trabajos final de curso** |

| |
|---|
| Resultados de aprendizaje:<br>**Puesta en práctica de los conocimientos adquiridos en el desarrollo de un tema aplicado específico.** |

| |
|---|
| Programa académico:<br>**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.** |

Metodología docente:
**Trabajo tutelado: Tutorías para formulación y redacción del trabajo fin de curso.**

| Actividades formativas SÍNCRONAS | Horas síncronas presenciales | Horas síncronas virtuales | Horas de trabajo autónomo del estudiante |
|---|---|---|---|
| **Trabajo tutelado** | | **2** | **73** |
| ECTS TOTALES = 3,00 | 0,00 | 2,00 | 73,00 |

*Las horas síncronas deben ser entre 8 y 12 por ECTS en modalidad síncrona*

| Actividades formativas ASÍNCRONAS | Horas tutorización | Horas de trabajo autónomo del estudiante |
|---|---|---|
| | | |
| ECTS TOTALES = 0,00 | 0,00 | 0,00 |

*Las horas de titorización serán entre 4 e 8 por ECTS en modalidad asíncrona*

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

| Pruebas de evaluación | % Ponderación |
|---|---|
| **Evaluación de contenidos y presentación de la memoria del proyecto** | **100** |
| | 100% |

Plataformas de Teledocencia y tutorización:
**Las actividades síncronas se realizarán en el Campus Remoto de la Universidad de Vigo. La entrega de trabajos se realizará en la plataforma Moovi de la Universidad de Vigo. Las tutorías se concertarán por correo electrónico y tendrán lugar en el Campus Remoto de la Universidad de Vigo.**