ANEXO ACADÉMICO II.
"Título propio en Formación Permanente en Ciberseguridad"

Denominación del título

TÍTULO DE FORMACIÓN PERMANENTE EN CIBERSEGURIDAD POR LA UNIVERSIDAD DE LEÓN.

Departamento solicitante

Departamento de Ingeniería Mecánica, Informática y Aeroespacial.

Directores responsables:

Adriana Suárez Corona, profesor contratado doctor.

Luis Panizo Alonso, profesor titular.

Empresas colaboradoras: INCIBE colaboración económica mediante adenda nº 15 del convenio marco. PROCONSI, coordinación de las prácticas curriculares y colaboración económica en forma de 10 becas para alumnos.

Tipo de enseñanza

Presencial.

Número de plazas ofertadas

Número mínimo de estudiantes para su impartición:15

Señalar el número máximo de estudiantes admisibles:20

Número mínimo de créditos europeos de matrícula por estudiante y periodo lectivo

- *30 créditos.*

JUSTIFICACIÓN

El término ciberseguridad se utiliza para designar diversos campos de investigación, desarrollo e innovación relacionados con el tratamiento del ciberespacio desde el punto de vista de su seguridad y fiabilidad para el usuario y el dominio público.

Este campo engloba de manera transversal diversas disciplinas como la seguridad informática, la seguridad de infraestructuras y sistemas, la fiabilidad y robustez de sistemas, la interacción con sistemas ciber-físicos, métodos cuantitativos en análisis de datos, criptografía y criptoanálisis, matemática aplicada a la seguridad, computación digital analógica y cuántica, programación segura, hardware seguro, redes, redes definidas por software, sistemas operativos seguros y su bastionado, sistemas de gestión de la información, aspectos legales del ciberespacio, anonimato, protección y soberanía, etc.

El ciberespacio proporciona infinidad de oportunidades y dota de gran valor añadido a procesos de todo tipo (comerciales, industriales, de comunicación, de interacción social, sanitarios, científicos, culturales...), pero también es fuente de multitud de amenazas a individuos, ciudadanos, empresas y sector público.

Diversos gobiernos han establecido políticas ambiciosas para el adecuado tratamiento de tal problemática. Remarcamos como principales hitos que nos afectan la estrategia española de Ciberseguridad, la estrategia europea de Ciberseguridad, la Agenda Digital para España, La Agenda Digital para Europa, y entre otros los National Cyber Security Research Agenda — Trust and Security

for our Digital Life (The Netherlands), Trustworthy cyberspace: Strategic plan for the federal cybersecurity research and
development program (Executive Office of The President, National Science and Technology Council, 2011), Emerging cybersecurity research challenges (The Royal Society, UK, nov. 2013).
La propuesta de Diploma de Experto en Ciberseguridad está alineado con el Objetivo 4 y la línea de acción 5 de la Estrategia de Ciberseguridad Nacional, aprobada por Presidencia del Gobierno en 2019 y que estipula:

OBJETIVO IV: Cultura y compromiso con la ciberseguridad y potenciación de las capacidades humanas y tecnológicas.

LÍNEA DE ACCIÓN 5: Potenciar la industria española de ciberseguridad, y la generación y retención de talento, para el fortalecimiento de la autonomía digital.

En particular, la medida 6:

Identificar las necesidades de capacidades profesionales de ciberseguridad, fomentando la colaboración con las instituciones educativas y formativas impulsando la formación continua, la formación para el empleo y universitaria, promoviendo sistemas de acreditación y certificación profesional.

Además de la medida 7:

Promover la concienciación y formación en ciberseguridad en los centros de enseñanza, adaptada a todos los niveles formativos y especialidades.

Objetivos

El objetivo de la titulación es recoger la fuerte naturaleza interdisciplinar de la ciberseguridad, permitiendo a los estudiantes obtener conocimientos sobre los campos más relevantes en los que ésta es de aplicación: criptografía, sistemas confiables, redes, auditorías de seguridad y de sistemas, hacking, programación segura, derecho y ciberseguridad industrial.

Además, el título tiene una importante componente práctica a desarrollar en una empresa del sector para que los alumnos pongan en práctica los conocimientos adquiridos en el ámbito laboral.

COMPETENCIAS GENERALES

CG 1. Transmitir soluciones al entorno industrial y empresarial en el campo de la ciberseguridad

CG2. Desarrollar proyectos de seguridad informática y de las comunicaciones.

CG3. Trabajar en equipo

CG4. Aprender de forma autónoma

CG5. Aplicar los conocimientos adquiridos y su capacidad de resolución de problemas en entornos nuevos o poco conocidos relacionados con su área de estudio.

COMPETENCIAS ESPECÍFICAS

CE1: Conocer los conceptos básicos del Hardware y el Software
CE2: Conocer los nuevos sistemas de computación
CE3: Analizar y clasificar las posibilidades de virtualización, almacenamiento y computación en la nube
CE4: Conocimiento teórico y aplicado de la arquitectura, servicios y protocolos de las redes de comunicaciones
CE5: Conocer los conceptos básicos de Ciberseguridad
CE6: Conocer los organismos implicados en la Ciberseguridad
CE7: Analizar y clasificar la gestión de los incidentes y soluciones en Ciberseguridad.
CE8: Entender, aplicar protocolos criptográficos.
CE9: Conocer los fundamentos de Blockchain
CE10: Detectar, analizar y prevenir amenazas de seguridad y tecnologías.
CE11: Prevenir fraudes en comercio electrónico.
CE12: Manejar redes y servicios informáticos desde el punto de vista de seguridad informática y de las comunicaciones.
CE13: Detectar, analizar y prevenir amenazas de seguridad y tecnologías.
C14: Desarrollar un sistema en red seguro.
CE15: Conocer y valorar diversos sistemas de gestión de seguridad.
CE16: Gestionar sistemas operativos, redes y servicios informáticos en el área de seguridad informática y de las comunicaciones.
CE17: Detectar, analizar y prevenir amenazas de seguridad y tecnológicas. Conocer y valorar diversos sistemas de gestión de seguridad.
CE18: Analizar la fiabilidad y robustez de sistemas informáticos complejos. Conocer herramientas científico técnicas para el análisis de robustez de sistemas
CE19: Conocer los principales conceptos de auditoría y certificación de seguridad.
CE20: Realizar auditorías y elaborar informes de auditorías.
CE21: Realizar acciones correctoras de auditorías.
CE22: Conocer la regulación jurídica europea y española de la seguridad y de la ciberseguridad.
CE23: Saber interpretar y aplicar la normativa europea y española en materia de infraestructuras críticas, seguridad de redes y sistemas de información.
CE24: Saber desarrollar habilidades y actitudes personales y profesionales que garanticen la protección de la privacidad y la protección de datos en el ámbito laboral.
CE25: Ser capaz de aplicar los derechos digitales en el ámbito laboral y en el teletrabajo
CE26: Conocer los principales conceptos de auditoría de sistemas de seguridad.

CE27: Analizar la fiabilidad y robustez de sistemas informáticos complejos
C28: Ser capaz de diseñar y planificar aplicaciones seguras en todas las etapas del desarrollo software desde el punto de vista del desarrollador.
C29: Ser capaz de desarrollar software seguro en diversos lenguajes de programación evitando generar las vulnerabilidades software más comunes.
C30: Ser capaz de realizar ejercicios sencillos de ingeniería inversa en el contexto de la ciberseguridad.
CE31: Conocer las amenazas y vulnerabilidades de seguridad específicas en los entornos industriales y de infraestructuras crítucas.
CE32: Conocer las principales iniciativas, programas y procedimientos en seguridad enfocadas a sistemas, redes y aplicaciones en entornos industriales.

ACCESO Y ADMISIÓN DE ESTUDIANTES

Acceso

Puede solicitar la admisión en el curso cualquier estudiante o profesional que cumpla alguno de los siguientes requisitos:

- Ser titulado o estudiante universitario
- Tener un título de Técnico Superior de Formación Profesional en las ramas de Informática y Comunicaciones.
- Disponer del título de Bachillerato y haber superado la EBAU
- Haber superado la prueba de acceso a la universidad para mayores de 25 años o la de 45 años
- Tener más de 40 años, disponer de experiencia profesional relacionada con la titulación universitaria que se quiera estudiar y superar una entrevista
- Tener estudios homologados o equivalentes a Bachillerato en el extranjero
- Cualquier otra vía de acceso a la universidad de entre las establecidas en el R.D. 412/2014

Admisión

Señalar los **procedimientos y criterios de admisión** a la correspondiente: enseñanza.

En caso de que el número de solicitudes de matrícula rebase el número máximo de plazas ofertadas, la selección entre los aspirantes se hará con arreglo a los siguientes criterios:

- Poseer un título oficial de FP o un título oficial universitario preferiblemente de la rama informática y comunicaciones.
- Adecuación del candidato al título propio, teniendo en cuenta la realización de una entrevista y/o prueba técnica.
- Tener experiencia profesional en el campo de la informática.
- Ser o haber sido estudiante universitario de la rama informática
- Ser o haber sido estudiante en un título de FP de la rama informática
- Justificación de tener conocimientos y habilidades informáticas
- Fecha de preinscripción

El Plan de Estudios (15 ECTS) se organizará de la siguiente forma:

Denominación del módulo o materia	**INTRODUCCION A LA INGENIERIA INFORMATICA APLICADA A LA CIBERSEGURIDAD**
Departamento/s responsable/s	Dpto. Ingeniería Eléctrica y de Sistemas y Automática y Dpto. Ingeniería Mecánica, Informática y Aeroespacial
Contenidos	Bloque 1. Arquitecturas de ordenadores Tema 1. Arquitectura de terminales. Tema 2. Sistemas operativos. Tema 3. Programación: principales lenguajes y entornos. Bloque II. Redes de ordenadores. Tema 1. Introducción a las redes. Tema 2. Principales protocolos de las redes TCP/IP. Bloque III. Sistemas móviles y empotrados. Tema 1. Los nombres de dominio. Tema 2. Sistemas móviles. Smartphones. Tema 3. Sistemas empotrados y sistemas de control industrial.

	Bloque IV. Computación distribuida. Tema 1. Virtualización. Tema 2. Computación y almacenamiento en la nube
Descripción de las competencias	CE1: Conocer los conceptos básicos del Hardware y el Software CE2: Conocer los nuevos sistemas de computación
	CE3: Analizar y clasificar las posibilidades de virtualización, almacenamiento y computación en la nube CE4: Conocimiento teórico y aplicado de la arquitectura, servicios y protocolos de las redes de comunicaciones

Denominación del módulo o materia	**FUNDAMENTOS DE CIBERSEGURIDAD**
Departamento/s responsable/s	Dpto. Ingeniería Mecánica, Informática y Aeroespacial
Créditos ECTS	1
Contenidos	Bloque I: Fundamentos de ciberseguridad Tema 1: Introducción a la ciberseguridad, a la ciberdefensa y el cibercrimen. Tema 2: Conceptos clave Bloque II: Taxonomías Tema 3: Taxonomía de ciberseguridad. Tema 4: Taxonomía de gestión de incidentes de ciberseguridad. Tema 5: Taxonomía de soluciones de ciberseguridad. Bloque III: Buenas prácticas

Descripción de las competencias	CE5: Conocer los conceptos básicos de Ciberseguridad CE6: Conocer los organismos implicados en la Ciberseguridad CE7: Analizar y clasificar la gestión de los incidentes y soluciones en Ciberseguridad.

Denominación del módulo o materia	**ASPECTOS TÉCNICOS DE LA CIBERSEGURIDAD**
Departamento/s responsable/s	Dpto. Ingeniería Mecánica, Informática y Aeroespacial, Dpto. Ingeniería Eléctrica y de Sistemas y Automática y Dpto. Matemáticas
Créditos ECTS	1
Contenidos	Bloque I: Criptografía y Blockchain Tema 1.- Criptografía. Tema 2.- Introducción a la "blockchain". Bloque II: Gestión de seguridad de activos Tema 1.- Sistemas de anonimización: VPN, redes TOR, Deep web y similares. Tema 2.- Peritaje informático.
Descripción de las competencias	CE8: Entender, aplicar protocolos criptográficos. CE9: Conocer los fundamentos de Blockchain CE10: Detectar, analizar y prevenir amenazas de seguridad y tecnologías. CE11: Prevenir fraudes en comercio electrónico.
Denominación del módulo o materia	**SISTEMAS CONFIABLES**
Departamento/s responsable/s	Dpto. Ingeniería Mecánica, Informática y Aeroespacial y Dpto. Ingeniería Eléctrica y de Sistemas y Automática
Créditos ECTS	2

Contenidos	Bloque I: Asegurando sistemas operativos Tema 1: Conceptos básicos de sistemas operativos y su seguridad. Tema 2: Manejos de las herramientas propias del SO (LINUX). Tema 3: Mecanismos de control de accesos y de autenticación. Tema 4: Contenedorización de aplicaciones. Bloque II: Asegurando redes de computadoras Tema 1: Conceptos básicos de creación de redes y su seguridad y confiabilidad. Tema 2: Cifrado de comunicaciones. Tema 3: Filtrado de comunicaciones. Tema 4: DMZS. Tema 5. Amenazas persistentes en redes de comunicación. Tema 6. Protocolos de compartición segura de información en redes. Ciberseguridad pasiva y activa. Bloque III: Análisis de sistemas confiables y de seguridad Tema 1: Detección de intrusiones y vulnerabilidades. Tema 2: HONEYPOTS
Descripción de las competencias	CE12: Manejar redes y servicios informáticos desde el punto de vista de seguridad informática y de las comunicaciones. CE13: Detectar, analizar y prevenir amenazas de seguridad y tecnologías. C14: Desarrollar un sistema en red seguro. CE15: Conocer y valorar diversos sistemas de gestión de seguridad. CE16: Gestionar sistemas operativos, redes y servicios informáticos en el área de seguridad informática y de las comunicaciones. CE17: Detectar, analizar y prevenir amenazas de seguridad y tecnológicas. Conocer y valorar diversos sistemas de gestión de seguridad. CE18: Analizar la fiabilidad y robustez de sistemas informáticos complejos. Conocer herramientas científico técnicas para el análisis de robustez de sistemas

Denominación del módulo o materia	**AUDITORÍA DE SEGURIDAD**
Departamento/s responsable/s	Dpto. Ingeniería Mecánica, Informática y Aeroespacial, Dpto. Derecho Público y Dpto. Derecho Privado y de la Empresa
Créditos ECTS	2
Contenidos	Bloque I: Auditoría y certificación Tema 1: Auditoría y certificación: Pasos para hacer una auditoría. Evidencias digitales. Tema 2: Métodos de trabajo Tema 3: Ejecución y seguimiento de auditorías. Tema 4: Elaboración de informes de auditoría Tema 5: Ejecución y seguimiento de acciones correctoras. Tema 6: El perfil profesional de auditor de sistemas de información. Bloque II. Sistemas de gestión de la seguridad de la información Tema 1. Sistemas de Gestión de la Seguridad de la Información (SGSI): ISO/IEC 27001:2013, ISO/IEC 27001:2014. Tema 2. El ciclo de vida de los Sistemas de Información. Tema 3. Seguridad desde el diseño y por defecto. Tema 4. Gestión de riesgos Tema 5. Gestión de la seguridad de la información y continuidad de la empresa. Tema 6. La responsabilidad de la dirección en la implantación de medidas de ciberseguridad en sus organizaciones. Bloque III: Marco normativo y legislativo Tema 1. Marco normativo y legislativo: ENS. NIS. Ley de protección de infraestructuras críticas. LSSI. RGPD

Descripción de las competencias	CE19: Conocer los principales conceptos de auditoría y certificación de seguridad. CE20: Realizar auditorías y elaborar informes de auditorías. CE21: Realizar acciones correctoras de auditorías. CE22: Conocer la regulación jurídica europea y española de la seguridad y de la ciberseguridad. CE23: Saber interpretar y aplicar la normativa europea y española en materia de infraestructuras críticas, seguridad de redes y sistemas de información.
	CE24: Saber desarrollar habilidades y actitudes personales y profesionales que garanticen la protección de la privacidad y la protección de datos en el ámbito laboral. CE25: Ser capaz de aplicar los derechos digitales en el ámbito laboral y en el teletrabajo

Denominación del módulo o materia	**AUDITORIA DE SISTEMAS**
Departamento/s responsable/s	Dpto. Ingeniería Mecánica, Informática y Aeroespacial
Créditos ECTS	2
Contenidos	Bloque I: Introducción a la auditoría de sistemas Tema 1: Conceptos generales Bloque II: Preparación de auditorías de sistemas Tema 2: Preparación de auditorías de sistemas Bloque III: Pentesting Tema 3: Pentesting Bloque IV: Elaboración de informes de auditoría Tema 4: Elaboración de informes de auditoría
Descripción de las competencias	CE11: Prevenir fraudes en comercio electrónico. CE26: Conocer los principales conceptos de auditoría de sistemas de seguridad. CE27: Analizar la fiabilidad y robustez de sistemas informáticos complejos

Denominación del módulo o materia	**PROGRAMACION SEGURA**
Departamento/s responsable/s	Dpto. Ingeniería Mecánica, Informática y Aeroespacial
Créditos ECTS	2

Contenidos	Bloque I. Introducción a la seguridad en el software Tema 1. Presentación general Tema 2. Introducción a la seguridad en el desarrollo de software Bloque II. Definición de sistemas de software seguros Tema 1. Diseño de sistemas software Tema 2. Arquitectura de sistemas software Bloque III. Análisis de software Tema 1. Introducción al análisis de software Tema 2. Técnicas de análisis de código binario. Tema 3. Seguridad software. Tema 4. Principios de análisis de malware. Bloque IV. Metodologías de ingeniería del software segura Tema 1. Implementación Tema 2. Operaciones Tema 3. Automatización y Tests Bloque V. Programación segura
	Tema 1. Conceptos Generales Tema 2. C++ Tema 3. Java Tema 4. Python Tema 5. Errores en programación. TOP 25 OWASP y SANS Tema 6. Reglas y recomendaciones CMU Cert Tema 7: Programación segura e identificación de vulnerabilidades
Descripción de las competencias	C28: Ser capaz de diseñar y planificar aplicaciones seguras en todas las etapas del desarrollo software desde el punto de vista del desarrollador. C29: Ser capaz de desarrollar software seguro en diversos lenguajes de programación evitando generar las vulnerabilidades software más comunes. C30: Ser capaz de realizar ejercicios sencillos de ingeniería inversa en el contexto de la ciberseguridad.

Denominación del módulo o materia	**CIBERSEGURIDAD INDUSTRIAL**
Departamento/s responsable/s	Dpto. Ingeniería Eléctrica y de Sistemas y Automática
Créditos ECTS	4
Contenidos	Bloque I. Peculiaridades de los sistemas de control industrial desde el punto de vista de la seguridad Tema 1. Introducción y revisión de conceptos. Tema 2. Arquitecturas y tecnologías. Bloque II. Amenazas y vulnerabilidades en sistemas de control industrial e infraestructuras críticas Tema 1. Amenazas. Tema 2. Vulnerabilidades. Tema 3. Impacto. Riesgo. Bloque III. Iniciativas y estándares Tema 1. Legislación europea y española. Entidades relevantes y fuentes de recomendaciones e información. Tema 2. Estándares. IEC-62443 Bloque IV. Revisión crítica de incidentes relevantes. Tema 1. Incidentes. Bloque V. Introducción a los procedimientos y medidas de seguridad en el ámbito de los sistemas de control industrial Tema 1. Políticas y procedimientos. Privilegios y autenticación. Tema 2. Medidas de seguridad física. Medidas de seguridad de los equipos Tema 3. Seguridad de red. Bloque VI. Arquitectura de seguridad en profundidad.

	Tema 1. Seguridad perimetral y segmentación. Tema 2. Modelo de zonas y conductos Bloque VII. Medidas y tecnologías en el ámbito de la ciberseguridad industrial Tema 1. Tecnologías Tema 2. Seguridad de los equipos. Tema 3. Filtrado de protocolos. Tema 4. Detección de intrusiones. Bloque VIII. Detección y respuesta ante incidentes en entornos industriales Tema 1. Supervisión de eventos de seguridad. Tema 2. procedimiento de respuesta ante incidentes.
Descripción de las competencias	CE31: Conocer las amenazas y vulnerabilidades de seguridad específicas en los entornos industriales y de infraestructuras crítucas. CE32: Conocer las principales iniciativas, programas y procedimientos en seguirdad enfocadas a sistemas, redes y aplicaciones en entornos industriales.

Prácticas Externas

Las Prácticas Externas tendrán una dedicación de 15 ECTS.

Denominación del módulo o materia	PRÁCTICA Experto en Ciberseguridad
Departamento/s responsable/s	Departamento de Sistemas y Ciberseguridad de Proconsi. Luis Angel Martínez Cancelo.
Créditos ECTS	15
Requisitos previos	Haber completado y superado los 15 ECTS de formación teórica.
Carácter	Carácter práctico

Actividades Formativas	1. Técnica Realización de análisis de vulnerabilidades sobre sistemas. Implementación de planes de Disaster Recovery, Configuración de dispositivos UTM con diferentes servicios de protección. Práctica de análisis forense sobre una estación de trabajo.Contenido en ECTS – 2 2. Práctica sobre el desarrollo de auditoría de cumplimiento con el ENS. Contenido en ECTS – 2 3. Práctica sobre elaboración de un análisis de riesgos. Contenido en ECTS – 1
	4. Práctica sobre la elaboración de contenidos para la formación continua en ciberseguridad para usuarios. Contenido en ECTS – 0,5 5. Práctica creación de campaña de ingeniería social para el phishing. Contenido en ECTS – 0,5
Contenidos	1. Técnica: seguridad y monitorización de red. Control de acceso. Operaciones de Seguridad. Sistema de autenticación Biométrica. Benchmarking y soluciones de Ciberseguridad. Pentest. Prueba de estrés y planes de Disaster Recovery. Protección ante fuga de datos. Soluciones de Seguridad para la Navegación y el Correo Electrónico. Despliegue de Soluciones de Protección de Medios Extraibles. DFIR. Configuración Backup. Antivirus y Firewall. Acceso Remoto. 2. Auditoría: Auditorías de Seguridad de Sistemas. Auditoría RGPD, LOPDGDD. LSSICE. Auditoría ISO 27001. Auditoría Aplicación Web. Auditoría conformidad ENS. Auditoría del sello de ciberseguridad. 3. Consultoría: Consultoría en Ciberseguridad. SGSI. Servicios de Análisis y Gestión de Riesgos. Servicios de Estrategia en Ciberseguridad. Continuidad de Negocio. Consultoría RGPD. Consultoría DPO. Disaster Recovery. Consultoría para Infraestructura Física. Consultoría para Infraestructura Lógica. Apoyo a Equipos de Desarrollo en Ciberseguridad. 4. Concienciación: Plataforma Online de Introducción a la Ciberseguridad. 5. Formación: Ingeniería Social, Jornadas de concienciación, Concienciación en continuidad de negocio.

Descripción de las competencias	CG 1. Transmitir soluciones al entorno industrial y empresarial en el campo de la ciberseguridad CG2. Desarrollar proyectos de seguridad informática y de las comunicaciones. CG3. Trabajar en equipo CG4. Aprender de forma autónoma CG5. Aplicar los conocimientos adquiridos y su capacidad de resolución de problemas en entornos nuevos o poco conocidos relacionados con su área de estudio.
	CE 26 Conocer el funcionamiento de empresas que desarrollan su actividad en el ámbito de la ciberseguridad. Comprender los riesgos existentes y las medidas de prevención y recuperación aplicadas por la empresa en materia de ciberseguridad. CE 27 Aplicar al mundo laboral las competencias adquiridas en las enseñanzas

Profesorado de la Universidad de León

Departamento	Área	Categoría	Dedicación	Bloque temático	Nº. de horas que imparte
Ingeniería Eléctrica y de Sistemas y Automática	Ingeniería de Sistemas y Automática	PCU	A tiempo completo	Ciberseguridad Industrial	5
Ingeniería Eléctrica y de Sistemas y Automática	Ingeniería de Sistemas y Automática	PTU	A tiempo completo	Introducción a Ingeniería Informática aplicada la Ciberseguridad, Sistemas Confiables, Ciberseguridad Industrial	4+5+15
Ingeniería Eléctrica y de Sistemas y Automática	Ingeniería de Sistemas y Automática	PCD	A tiempo completo	Sistemas Confiables	5

Ingeniería Eléctrica y de Sistemas y Automática	Ingeniería de Sistemas y Automática	PAD	A tiempo completo	Aspectos técnicos de la Ciberseguridad, Ciberseguridad Industrial	5+10
Ingeniería Eléctrica y de Sistemas y Automática	Ingeniería de Sistemas y Automática	Profesor Asociado	A tiempo completo	Ciberseguridad Industrial	5
Ingeniería Eléctrica y de Sistemas y Automática	Ingeniería de Sistemas y Automática	Becario FPI	A tiempo completo	Ciberseguridad Industrial	5
Matemáticas	Matemática Aplicada	PCD	A tiempo completo	Aspectos técnicos de la Ciberseguridad	5
Derecho Público	Derecho Administrativo	PCU	A tiempo completo	Auditoría de Seguridad	2
Derecho Privado y de la Empresa	Derecho del Trabajo y de la Seguridad Social	PCU	A tiempo completo	Módulo jurídico (Marco normativo y legislativo)	2
Derecho Privado y de la Empresa	Derecho del Trabajo y de la Seguridad Social	PTU	A tiempo completo	Módulo jurídico (Marco normativo y legislativo)	2
Ingeniería Mecánica, Informática y Aeroespacial	ATC	PTU	Completa	Introducción a Ingeniería Informática aplicada la Ciberseguridad, Fundamentos de Ciberseguridad, Programación Segura	3+5+16
Ingeniería Mecánica, Informática y Aeroespacial	ATC	PCD	Completa	Introducción a Ingeniería Informática aplicada la Ciberseguridad	3

Ingeniería Mecánica, Informática y Aeroespacial	ATC	Titulado Superior Investigador	Completa	Auditoría de Sistemas, Programación Segura	20+4
Ingeniería Mecánica, Informática y Aeroespacial	ATC	Profesor Ayudante	Completa	Sistemas Confiables	20
Ingeniería Mecánica,	ATC	PAD	Completa	Auditoría de Sistemas	5
Informática y Aeroespacial					
Ingeniería Mecánica, Informática y Aeroespacial	ATC	Profesor Asociado	Parcial	Auditoría de Seguridad	16

Profesorado externo a la Universidad de León

Nombre y apellidos	Titulación	Empresa, entidad, universidad de procedencia	Bloque temático	Nº. de horas que imparte
Luis Ángel Martínez Cancelo	Titulado Superior Formación Profesional	PROCONSI	Prácticas en Empresa	50
Roberto Tovar Martín	Grado en Ingeniería Informática	PROCONSI	Prácticas en Empresa	50
Anabel Vázquez Iglesias	Ingeniería Informática	PROCONSI	Prácticas en Empresa	50

Lugar de impartición: Teoría (150 h) en el aula 301 del Edificio Tecnológico del Campus de Vegazana. Prácticas (150 h) en las instalaciones de la empresa Proconsi, situadas en el Parque Tecnológico y en el Campus de Vegazana (León).

Horario: la teoría se impartirá de lunes a viernes de 16:00 a 20:00 h, durante 8 semanas, en el aula 301 del Edificio Tecnológico y a continuación las prácticas en horario de mañana de 10 a 14 h en las instalaciones de la empresa Proconsi (Parque Tecnológico de León), durante otras 8 semanas.

Pruebas de evaluación: cada módulo tendrá su evaluación y que será necesario superar para obtener el título.

Qué nos diferencia: la formación está adaptada a las necesidades reales del mercado laboral. Es por ello que se ha diseñado siguiendo las directrices de las empresas más innovadoras en las áreas de las TIC. Esta formación está dentro del marco de la EARTIC (programa de especialización de alto rendimiento en tecnologías TIC), mediante la cual tendrás acceso, en función del nivel alcanzado, a un contrato laboral en PROCONSI o empresas asociadas al programa.

Fechas previstas:

Preinscripción hasta el 31 de agosto en https://preinscripcion.unileon.es/intro

Plazo de matrícula: desde el 2 al 11 de septiembre de 2024. Para ello es necesario ser admitido previamente.

Comienzo de las clases teóricas el 16 de septiembre hasta el 8 de noviembre.

Precio: 950 € (con derecho al título propio de la Universidad de León en Formación permanente en Ciberseguridad). Gracias a las becas y ayudas económicas de PROCONSI e INCIBE solo se tendrá que abonar el 50% de la matrícula, es decir, 475 €.

Más información:

- Universidad de León: https://www.unileon.es/estudiantes/oferta-academica/titulos-propios/oferta
  lpana@unileon.es 987.291916 y posgrado@unileon.es 987.293468
- PROCONSI: rrhh@proconsi.com