UNIVERSIDAD COMPLUTENSE MADRID

Título Propio de la Universidad Complutense de Madrid

MÁSTER ONLINE EN PROTECCIÓN DE DATOS Y SEGURIDAD DE LA INFORMACIÓN

Inicio del Máster: Octubre 2021
Fin del Máster: Junio 2022

60 ETCS

Abierto plazo de preinscripción | **PLAZAS LIMITADAS**

isms forum

UNIVERSIDAD COMPLUTENSE MADRID

AENOR Confía

Índice

UNIVERSIDAD COMPLUTENSE MADRID

1º Universidad presencial con más alumnos de España.

3º Universidad presencial con más alumnos de Europa.

500 Años de Historia

La Universidad Complutense de Madrid

La UCM cuenta con más de 80 títulos de Grado y doble Grado, a lo que se le suma una oferta de formación superior de más de 140 Másteres. Con más de 500 años de historia y reconocimiento social, la Universidad Complutense de Madrid es la universidad española de referencia en 5 continentes.

El prestigio de la universidad está avalado por 7 Premios Nobel, 20 Príncipes de Asturias, 7 Premios Cervantes, Premios Nacionales de Investigación y a la Excelencia. La Universidad Complutense de Madrid tiene estudiantes de más de 90 países y convenios con universidades de los 5 continentes.

QS World University Ranking

La Universidad Complutense de Madrid ocupa la posición 206 en el QS World University Ranking de un total de 26.000 universidades evaluadas. Este resultado sitúa a la Complutense en la élite de la educación superior, entre el 1% de las mejores universidades del mundo.

En este mismo ranking, la Universidad Complutense de Madrid ocupa la posición 94 del mundo por su reputación en empleabilidad.

La clasificación se publica en la web https://www.topuniversities.com

UNIVERSIDAD COMPLUTENSE MADRID

1º Universidad presencial con más alumnos de España.

3º Universidad presencial con más alumnos de Europa.

500 Años de Historia

Título Propio

La Universidad Complutense de Madrid ofrece los títulos propios para responder a la demanda social de formación especializada en campos de conocimiento no cubiertos por titulaciones oficiales convencionales.

La flexibilidad y autonomía de los títulos propios, fuera de los rígidos y burocráticos esquemas de los títulos oficiales, permiten adaptarse con rapidez a las necesidades de formación o especialización que el mercado laboral exige.

Para acceder a un título propio de Máster es necesario contar con un título universitario oficial, y cumplir con las normas de acceso y matriculación de la propia universidad.

Emisión del título

Una vez finalizados y superados estos estudios, la Universidad Complutense de Madrid emitirá el título, conforme a las normas de admisión y matriculación de los títulos propios de la UCM.

Certificados expedidos por la UCM:

UNIVERSIDAD COMPLUTENSE MADRID

Máster Online en Protección de Datos y Seguridad de la Información UCM

UNIVERSIDAD COMPLUTENSE MADRID

+250 Empresas asociadas **+1.250** Profesionales asociados **14** Años de recorrido

ISMS Forum

La Asociación Española para el Fomento de la Seguridad de la Información, ISMS Forum, es una organización sin ánimo de lucro fundada en enero de 2007 para promover el desarrollo, conocimiento y cultura de la Seguridad de la Información en España y actuar en beneficio de toda la comunidad implicada en el sector.

Creada con una vocación plural y abierta, se configura como un foro especializado de debate para empresas, organizaciones públicas y privadas, investigadores y profesionales donde colaborar, compartir experiencias y conocer los últimos avances y desarrollos en materia de Seguridad de la Información. Toda su actividad se desarrolla en base a los valores de transparencia, independencia, objetividad y neutralidad.

Certificados expedidos por ISMS Forum:

Certified Data Privacy Professional ISMS

Consíguelo en el bloque 1

Certified Cyber Security Professional ISMS

Consíguelo en el bloque 2

UNIVERSIDAD COMPLUTENSE MADRID

AENOR Confía

100% Aprobación en el sector B2B

70% Reconocimiento en el público general

35 Años de recorrido

AENOR

AENOR es una empresa de servicios profesionales que identifica y ayuda a corregir las brechas de competitividad del tejido económico de las sociedades de las que formamos parte.

El valor añadido que aporta AENOR en la solución de dichas brechas es generar confianza entre los agentes económicos de una sociedad sobre la base del conocimiento, los valores y la competitividad.

Cuando el tejido económico llega a una masa crítica suficiente en la incorporación de esos conocimientos y valores, adquiere cotas de eficiencia que le permiten competir en igualdad de condiciones con los demás actores internacionales.

Por todo ello, AENOR es una empresa de gestión del conocimiento que actúa en el ámbito de las brechas de competitividad; tanto del conjunto del tejido económico como sectoriales.

Certificados expedidos por AENOR:

AENOR Confía

Auditor Líder ISO 27001

Consíguelo en el bloque 3.

IQNet ACADEMY

IQNET ISO 27001 Lead Auditor

Consíguelo en el bloque 3.

UNIVERSIDAD COMPLUTENSE MADRID

Información general

Fechas

Inicio: Octubre de 2021

Fin: Junio de 2022

Duración

Inicio: Octubre de 2021

Fin: Junio de 2022

Modalidad

100% Online

Precio

Precio: 4500€+ 40€ de tasas.

Facilidad de pago: Paga en 2 veces sin intereses

Objetivos del Máster

El objetivo principal del Máster es formar profesionales especializados en el ámbito de la privacidad, de acuerdo con la normativa española en protección de datos de carácter personal, de cara al ejercicio tanto en el contexto nacional, como en el europeo e internacional, obteniendo así mismo un dominio de los fundamentos que rigen la Seguridad de la Información en las organizaciones.

Así, se integra también como objetivo la formación de profesionales en el gobierno de la ciberseguridad.

Metodología 100% Online

La formación se realizará de forma tutorizada por los profesores. Se utilizará una plataforma de formación virtual para la comunicación entre los alumnos y profesores, creando una comunidad virtual de trabajo.

UNIVERSIDAD COMPLUTENSE MADRID

¿Para quién es este Máster?

El Máster está dirigido principalmente (aunque no en exclusiva) a los siguientes perfiles:

- Licenciados y Graduados en Derecho (o especialistas en alguna de sus ramas) con interés en dirigir o extender su actividad profesional hacia la protección de datos.

- Licenciados y Graduados en Administración y Dirección de Empresas, Ciencias Políticas, Relaciones Laborales-Estudios Sociales y/o Criminología, que tengan inquietud por la seguridad de la información y el cumplimiento normativo.

- Postgraduados en ámbitos afines como el derecho de las telecomunicaciones o el comercio electrónico, que busquen integrar la protección de datos en su práctica laboral.

- Postgraduados en áreas de tecnologías de la información y las comunicaciones con interés por el marco regulatorio y la actividad empresarial en materia de protección de datos.

UNIVERSIDAD COMPLUTENSE MADRID

Salidas profesionales

- **Delegado de Protección de Datos (DPD):** Figura clave del RGPD que debe incluirse en un número importante de organismos gubernamentales, empresas, asociaciones y entidades que traten datos personales, de acuerdo con lo señalado en el artículo 34 de la norma. El DPD podrá ser un profesional interno contratado por la organización responsable, o bien externo.

- **Consultor en Protección de Datos:** Presta funciones de asesoramiento en materia de conformidad con el RGPD y la LOPDGDD para las empresas que traten permanentemente datos personales y que requieran una orientación completa, detallada y especializada en esta materia para el mejor cumplimiento de la normativa.

- **Abogado Especialista en Protección de Datos:** Ofrece asesoramiento jurídico en materia de protección de datos, administración electrónica, propiedad intelectual, telecomunicaciones, firma electrónica, contratos informáticos y similares.

- **Auditor en Protección de datos:** Como parte del cumplimiento proactivo de las empresas de sus compromisos sobre protección de datos de carácter personal, se plantea la necesidad de realizar auditorías anuales para evaluar el grado de cumplimiento del RGPD, la cual se realizará por profesionales internos o externos que cuenten con la debida cualificación.

- **Empleados que procesan datos personales en una organización, que trabajan en el área de cumplimiento normativo, o en el sector de la ciberseguridad:** Todos estos tipos de empleados exigen una formación adecuada para el tratamiento de los datos personales de los consumidores, proveedores y empleados, así como para el desarrollo de protocolos, productos y sistemas que garanticen un tratamiento correcto y adecuado de los datos.

Titulaciones y certificados

Una vez completado el Máster, **además del título de la UCM,** obtendrás de manera adicional y gratuita, las siguientes certificaciones: **Certified Data Privacy Professional** (CDPP, de ISMS), **Certified Cyber Security Professional** (CCSP, de ISMS), **Auditor Líder ISO 27001 AENOR** y **IQNET ISO 27001 Lead Auditor.**

Máster Online en Protección de Datos y Seguridad de la Información UCM

Certified Data Privacy Professional ISMS

Consíguelo en el bloque 1.

Certified Cyber Security Professional ISMS

Consíguelo en el bloque 2.

Auditor Líder ISO 27001

Consíguelo en el bloque 3.

IQNET ISO 27001 Lead Auditor

Consíguelo en el bloque 3.

UNIVERSIDAD COMPLUTENSE MADRID

Plataforma Online

Como estudiante, dispondrás de una plataforma virtual donde el claustro subirá vídeos y documentación explicativa de cada uno de los módulos del Máster. Tendrás acceso a recursos individuales y personalizados de mensajería, actividades, videotutoriales y contacto directo con el profesorado mediante mensajería, foros y chat.

Mensajería individual

Lecciones en video

Video-tutorías

Documentación

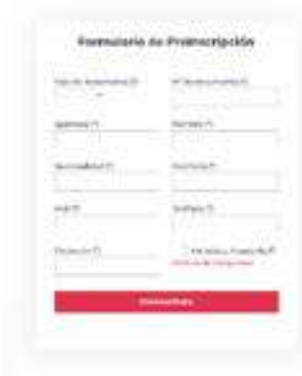
Ejercicios y cuestionarios

Comunicación directa con profesores

UNIVERSIDAD COMPLUTENSE MADRID

Proceso de admisión

Tanto la preinscripción como la prematrícula quedan abiertas hasta comenzar el curso académico o completar plazas, estableciéndose lista de espera si procede.



1. Rellenar el formulario

El primer paso para estudiar el Máster en Protección de Datos y Seguridad de la Información de la UCM es rellenar **el formulario de preinscripción.**

2. Enviar Documentación

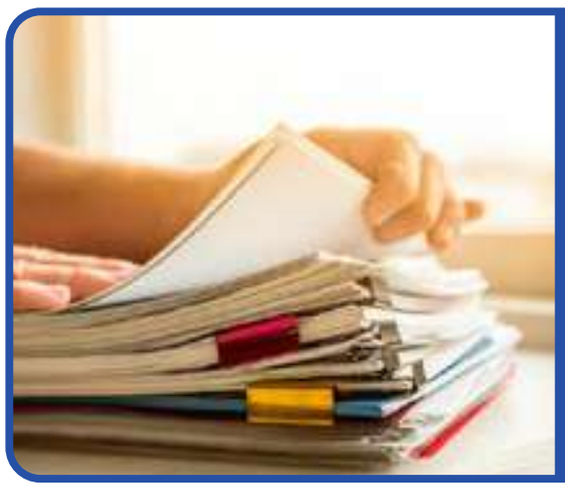
Enviar la documentación que se te solicitará vía e-mail para evaluar tu solicitud. Más información en la página siguiente.

3. Entrevista Online

Enviada la documentación que se te pidió por e-mail, se te citará para una **entrevista con el Director del Máster** para evaluar tu candidatura y resolver cualquier cuestión que se plantee.

4. Reserva de plaza

Confirmada tu idoneidad como candidato/a a la plaza del Máster, tendrás que reservarla ingresando 500€ como reserva, cantidad que **se descontará del total del Máster** una vez completado el proceso.



5. ¡Bienvenido!

¡Enhorabuena!
Ya formas parte del **Máster en Protección de Datos y Seguridad de la Información** de la Universidad Complutense de Madrid.

UNIVERSIDAD COMPLUTENSE MADRID

Documentación requerida

Si tienes titulación en España

- Fotocopia del documento de identidad/pasaporte
- Certificado de notas oficial.
- Título universitario o resguardo de solicitud de título.
- Currículum Vitae.

⬇ Si tienes titulación fuera de España

Si tienes titulación dentro de la Unión Europea

Tanto el título como el certificado de notas tienen deben ir acompañados de una traducción jurada.

Si tienes una titulación fuera de la Unión Europea

- DNI o NIE. En el caso de estudiantes extranjeros a los que no sea de aplicación el régimen comunitario se admitirá, con carácter provisional, el pasaporte como documento identificativo.

- El título y el certificado de notas tiene que estar legalizado con la Apostilla de la Haya.

- Si están en otro idioma que no sea español deben ir acompañados de una traducción jurada.

Programa del Máster

El programa del Máster en Protección de Datos y Seguridad de la Información se desarrolla y actualiza en colaboración con **ISMS Forum** y **Aenor.**

El enfoque de las clases y actividades es eminentemente práctico, y se imparten en su inmensa mayoría por profesionales en ejercicio en este campo, a fin de incluir en todo momento las mejores prácticas empleadas por las empresas en la realidad de su día a día. de trabajo.

Bloque 1:

Especialización en Protección de Datos CDPP por ISMS Forum

Bloque 2:

Especialización en Ciberseguridad CCSP por ISMS Forum

Bloque 3:

Módulo Auditor Líder ISO 27001

Data Protection

Programa

1.- NORMATIVA GENERAL DE PROTECCIÓN DE DATOS.

En este caso se aborda todo el contexto normativo de la protección de datos. En particular, se profundiza en el RGPD y la actualización de la LOPD con los fundamentos, principios, legitimación, medidas de cumplimiento, responsabilidad proactiva, los Delegados de Protección de Datos (DPD, DPO o Data Privacy Officer), las transferencias internacionales de datos, las Autoridades de Control, y las directrices de interpretación del RGPD. Se analizan los derechos de los individuos, y también las normativas sectoriales afectadas por la protección de datos, así como la normativa española y europea con implicaciones en este campo.

Contexto normativo.

- Privacidad y protección de datos en el panorama internacional.
- La protección de datos en Europa.
- La protección de datos en España.
- Estándares y buenas prácticas.

El Reglamento Europeo de Protección de datos y actualización de LOPD. Fundamentos.

- Ámbito de aplicación.
- Definiciones.
- Sujetos obligados.

El Reglamento Europeo de Protección de datos y actualización de LOPD. Principios.

- El binomio derecho/deber en la protección de datos.
- Licitud del tratamiento.
- Lealtad y transparencia.
- Limitación de la finalidad.
- Minimización de datos.
- Exactitud.

El Reglamento Europeo de Protección de datos y actualización de LOPD. Legitimación.

- El consentimiento: otorgamiento y revocación.
- El consentimiento informado: finalidad, transparencia, conservación, información y deber de comunicación al interesado.
- Consentimiento de los niños.
- Categorías especiales de datos.
- Datos relativos a infracciones y condenas penales.
- Tratamiento que no requiere identificación.
- Bases jurídicas distintas del consentimiento.

Derechos de los individuos.

- Transparencia e información
- Acceso, rectificación, supresión (olvido).
- Oposición.

- Decisiones individuales automatizadas.
- Portabilidad.
- Limitación del tratamiento.
- Excepciones a los derechos.

El Reglamento Europeo de Protección de datos y actualización de LOPD. Medidas de cumplimiento.

- Las políticas de protección de datos.
- Posición jurídica de los intervinientes. Responsables, co-responsables, encargados, subencargado del tratamiento y sus representantes. Relaciones entre ellos y formalización.
- El registro de actividades de tratamiento: identificación y clasificación del tratamiento de datos.

El Reglamento Europeo de Protección de datos y actualización de LOPD. Responsabilidad proactiva.

- Privacidad desde el diseño y por defecto. Principios fundamentales.
- Evaluación de impacto relativa a la protección de datos y consulta previa. Los tratamientos de alto riesgo.
- Seguridad de los datos personales. Seguridad técnica y organizativa.
- Las violaciones de la seguridad. Notificación de violaciones de seguridad.
- El Delegado de Protección de Datos (DPD). Marco normativo.
- Códigos de conducta y certificaciones.

El Reglamento Europeo de Protección de datos. Delegados de Protección de Datos (DPD, DPO o Data Privacy Officer).

- Designación. Proceso de toma de decisión. Formalidades en el nombramiento, renovación y cese. Análisis de conflicto de intereses.
- Obligaciones y responsabilidades. Independencia. Identificación y reporte a dirección.
- Procedimientos. Colaboración, autorizaciones previas, relación con los interesados y gestión de reclamaciones.
- Comunicación con la autoridad de protección de datos.
- Competencia profesional. Negociación. Comunicación. Presupuestos.
- Formación.
- Habilidades personales, trabajo en equipo, liderazgo, gestión de equipos.

El Reglamento Europeo de Protección de datos y actualización de LOPD. Transferencias

internacionales de datos.

- El sistema de decisiones de adecuación.
- Transferencias mediante garantías adecuadas.
- Normas Corporativas Vinculantes.
- Excepciones.
- Autorización de la autoridad de control.
- Suspensión temporal
- Cláusulas contractuales

El Reglamento Europeo de Protección de datos y actualización de LOPD.
Las Autoridades de Control.

- Autoridades de Control.
- Potestades.
- Régimen sancionador.
- Comité Europeo de Protección de Datos.
- Procedimientos seguidos por la AEPD.
- La tutela jurisdiccional.
- El derecho de indemnización.

Directrices de interpretación del RGPD.

- Guías del GT art. 29.
- Opiniones del Comité Europeo de Protección de Datos.
- Criterios de órganos jurisdiccionales.

Normativas sectoriales afectadas por la protección de datos.

- Sanitaria, Farmacéutica, Investigación.
- Protección de los menores.
- Solvencia Patrimonial.
- Telecomunicaciones.
- Videovigilancia.
- Seguros.
- Publicidad, etc.

Normativa española con implicaciones en protección de datos.

- LSSI, Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
- LGT, Ley 9/2014, de 9 de mayo, General de Telecomunicaciones.
- Ley firma-e, Ley 59/2003, de 19 de diciembre, de firma electrónica.

Normativa europea con implicaciones en protección de datos.

- Directiva e-Privacy: Directiva 2002/58/CE del Parlamento Europeo y del Consejo de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre privacidad y las comunicaciones electrónicas) o Reglamento e-Privacy cuando se apruebe.
- Directiva 2009/136/CE del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009, por la que se modifican la Directiva 2002/22/CE relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas, la Directiva 2002/58/CE relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas y el Reglamento (CE) nº 2006/2004 sobre la cooperación en materia de protección de los consumidores.
- Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo.

2.- RESPONSABILIDAD ACTIVA

Este dominio se centra en el análisis y gestión de riesgos de los tratamientos de datos personales, las metodologías de análisis y gestión de riesgos, el Programa de cumplimiento de Protección de Datos y Seguridad en una organización, la seguridad de la información, y la Evaluación de Impacto de Protección de Datos o EIPD.

Análisis y gestión de riesgos de los tratamientos de datos personales.

- Introducción. Marco general de la evaluación y gestión de riesgos. Conceptos generales.
- Evaluación de riesgos. Inventario y valoración de activos. Inventario y valoración amenazas. Salvaguardas existentes y valoración de su protección. Riesgo resultante.
- Gestión de riesgos. Conceptos. Implementación. Selección y asignación de salvaguardas

a amenazas. Valoración de la protección. Riesgo residual, riesgo aceptable y riesgo inasumible.

Metodologías de análisis y gestión de riesgos.

- Programa de cumplimiento de Protección de Datos y Seguridad en una organización.
- El Diseño y la implantación del programa de protección de datos en el contexto de la organización.
- Objetivos del programa de cumplimiento.
- Accountability: La trazabilidad del modelo de cumplimiento

Seguridad de la información.

- Marco normativo. Esquema Nacional de Seguridad y directiva NIS: Directiva (UE) 2016/1148 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión. Ámbito de aplicación, objetivos, elementos principales, principios básicos y requisitos mínimos.
- Ciberseguridad y gobierno de la seguridad de la información. Generalidades, Misión, gobierno efectivo de la Seguridad de la Información (SI). Conceptos de SI. Alcance. Métricas del gobierno de la SI. Estado de la SI. Estrategia de SI.
- Puesta en práctica de la seguridad de la información. Seguridad desde el diseño y por defecto. El ciclo de vida de los Sistemas de Información. Integración de la seguridad y la privacidad en el ciclo de vida. El control de calidad de los SI.

Evaluación de Impacto de Protección de Datos “EIPD”.

- Introducción y fundamentos de las EIPD: Origen, concepto y características de las EIPD. Alcance y necesidad. Estándares.
- Realización de una evaluación de impacto. Aspectos preparatorios y organizativos, análisis de la necesidad de llevar a cabo la evaluación y consultas previas.

3.- TÉCNICAS PARA GARANTIZAR EL CUMPLIMIENTO DE LA NORMATIVA DE PROTECCIÓN DE DATOS.

Los contenidos principales en este caso son la auditoría de protección de datos, la auditoría de Sistemas de Información, la gestión de la seguridad de los tratamientos, y otros conocimientos (cloud computing, smartphones, “Internet de las Cosas” o IoT, big data y elaboración de perfiles, redes sociales, y tecnologías de seguimiento del usuario).

La auditoría de protección de datos.

- El proceso de auditoría. Cuestiones generales y aproximación a la auditoría. Características básicas de la Auditoría.
- Elaboración del informe de auditoría. Aspectos básicos e importancia del informe de auditoría.
- Ejecución y seguimiento de acciones correctoras.

Auditoría de Sistemas de Información.

- La Función de la Auditoría en los Sistemas de Información. Conceptos básicos. Estándares y Directrices de Auditoría de SI.
- Control interno y mejora continua. Buenas prácticas. Integración de la auditoria de protección de datos en la auditoria de SI.
- Planificación, ejecución y seguimiento.

La gestión de la seguridad de los tratamientos.

- Esquema Nacional de Seguridad, ISO/IEC 27001:2013 (UNE ISO/IEC 27001:2014: Requisitos de Sistemas de Gestión de Seguridad de la Información, SGSI).
- Gestión de la Seguridad de los Activos. Seguridad lógica y en los procedimientos. Seguridad aplicada a las TI y a la documentación.
- Recuperación de desastres y Continuidad del Negocio. Protección de los activos técnicos y documentales. Planificación y gestión de la Recuperación del Desastres.

Otros conocimientos.

- El cloud computing.
- Los Smartphones.
- Internet de las cosas (IoT).
- Big data y elaboración de perfiles.
- Redes sociales.
- Tecnologías de seguimiento de usuario.
- Blockchain y últimas tecnologías

Bloque 2:
Especialización en Ciberseguridad
CCSP por ISMS Forum

Contenido

1.- GOBIERNO DE SEGURIDAD

Se abordan las Arquitecturas de Seguridad, la introducción, gestión y gobierno de la ciberseguridad, la organización de roles y responsabilidades, la auditoría y control de la seguridad, la certificación y acreditación de productos y sistemas, y la seguridad en entornos cloud; (IaaS, PaaS, SaaS).

Estándares, Estrategia, Política de Ciberseguridad, Gestión, Auditorías, Terceras partes, Cloud.

- Arquitecturas de Seguridad.
- Introducción y Gestión de Ciberseguridad.
- Estándares y buenas prácticas de referencia.
- Organización Roles y Responsabilidades.
- Gobierno de Ciberseguridad.
- Auditoría y control de la seguridad.
- Certificación y acreditación de productos y sistemas .

2.- ANÁLISIS Y GESTIÓN DE RIESGOS

En este primer módulo de especialización en Ciberseguridad, aprenderás todo lo relacionado con los estándares del sector, las estrategias, la política de Ciberseguridad, gestión, auditorías, terceras partes, etc.

En este segundo dominio se explicarán las principales amenazas y riesgos tecnológicos, cómo llevar a cabo su identificación y gestión, y el proceso de análisis y gestión de riesgos y amenazas.

- La identificación y gestión de riesgos.
- Análisis y gestión de riesgos y amenazas.
- Riesgos Tecnológicos.

3.- CUMPLIMIENTO LEGAL Y NORMATIVO

Se analiza el Cumplimiento Legal, prestando atención a los aspectos legales y regulatorios asociados a la privacidad, seguridad, e IC, las técnicas, metodologías y herramientas del “compliance legal”, cómo llevar a cabo la notificación, reporte, denuncia y presentación en juzgado, y las cuestiones relativas al cibercrimen y los delitos informáticos.

Regulaciones y Leyes, Cibercrimen, Infraestructuras Críticas, la prueba digital.

- Cumplimiento Legal.
- Aspectos legales y regulatorios asociados a Privacidad, Seguridad, e IC.
- Técnicas, metodologías y herramientas del compliance legal.
- Notificación, reporte, denuncia y presentación en juzgado.
- Cibercrimen y delitos informativos.

4.- OPERATIVA DE CIBERSEGURIDAD

Incluye las temáticas de desarrollo seguro, criptografía, monitorización de seguridad, tecnologías de ciberseguridad, análisis de vulnerabilidades, hacking ético, seguridad del acceso directo y parque Windows, y seguridad en el acceso Remoto y el teletrabajo.

- Desarrollo seguro Criptografía Monitorización de seguridad.
- Tecnologías de Ciberseguridad.
- Análisis de vulnerabilidades.
- Hacking ético.

5.- CIBER INTELIGENCIA, COOPERACIÓN Y CAPACIDAD (OSINT, Inteligencia, IOCs, Ciberejercicios)

En este dominio se abordan las relaciones con organismos nacionales e internacionales, los distintos tipos de Ciberejercicios más relevantes, y el intercambio de información con terceros e indicadores de compromiso o IoCs por sus siglas en inglés.

- Relaciones con organismos nacionales e Internacionales.
- Ciber Ejercicios.
- Intercambio de información con terceros e IoCs.

6.- GESTIÓN EFICAZ DE INCIDENTES

El contenido de este dominio se centra en actividades esenciales para el manejo y remediación de ciberincidentes, como el análisis forense de sistemas, el análisis de malware, y la gestión y respuesta a incidentes de seguridad, con especial atención a las consecuencias no sólo técnicas, sino legales y de negocio.

Detección, tratamiento, análisis y notificación de brechas. Continuidad y Resiliencia.

- Análisis Forense de Sistemas.
- Análisis de malware.
- Gestión y respuesta a incidentes de Seguridad.

7.- Infraestructuras Críticas

Con este dominio, conocerás las instalaciones, redes, servicios y equipos cuya interrupción o destrucción tendría un impacto de gran calado en la salud, la seguridad o el bienestar económico de los ciudadanos. En particular, se abordará la ciberseguridad en infraestructuras críticas, OT e IoT.

- Ciberseguridad en IC.
- OT e IoT.

8.- CISO Soft Skills

Además de los conocimientos y habilidades técnicos tratados en los dominios anteriores, en este se abordarán las llamadas “habilidades blandas” o transversales que un responsable de seguridad de la información necesita para la Estrategia de Seguridad, y la planificación necesaria de una gestión de crisis.

- Estrategia de Seguridad.
- Planificación de una gestión de Crisis.
- Softskills.

9.- Sesión práctica y simulacro de examen

En esta última sección del Bloque de Especialización en Ciberseguridad pondrás en práctica todo lo aprendido a lo largo de los dominios anteriores en un simulacro de examen y un caso práctico, del que recibirás feedback por parte de expertos en la materia.

- Ejercicio práctico, Simulacro de examen y corrección.

Bloque 3:
Auditor Líder ISO 27001 por AENOR

Descripción del Bloque

El bloque, de 40 horas, se impartirá en 4 semanas.

El alumno deberá superar cada uno de ellos y realizar un examen final (para el que dispondrá de 2 convocatorias), con el fin de obtener 2 titulaciones: Titulación propia de Aenor **Auditor Líder ISO 27001** y diploma IQNet Academy **IQNET ISO 27001 Lead Auditor.**

El bloque está formado por los siguientes cursos:

1.- Fundamentos de la gestión de la seguridad de la información según ISO 27001 - S -01

2.- Implantación de un sistema de gestión de seguridad de la información según ISO 27001 - S-02

3.- Auditor interno ISO 77011 - S-05

UNIVERSIDAD COMPLUTENSE MADRID

Contenido

- **Conceptos de la seguridad de la información y de su gestión**
- **Origen, evolución y contenido de la Norma ISO/IEC 27002**
- **Marco de procesos para definir un SGSI según la Norma ISO/IEC 27001**
- **Definición del alcance de un SGSI**
- **Implementación del Sistema de Gestión de la Información según la Norma ISO/IEC 27001**
- **Criterios de éxito para la gestión efectiva y práctica de la seguridad de la información**
- **Auditoría de un sistema de Gestión de la Seguridad de la Información:**

  - Definición y tipos de auditoría.
  - Procesos y fases de la metodología que hay que seguir en las auditorías de un SGSI.
  - Criterios para la auditoría del sistema de gestión de continuidad del negocio.
  - Definición, objetivos y tipos de auditoría.
  - Normas aplicables a la auditoría de un SGSI: ISO 227001, UNE-EN ISO 19011, ISO 17021, ISO27006.

- **Gestión del programa de auditoría**

  - Planificación y realización de las auditorias de un SGCN.
  - Preparación de la auditoría.
  - Desarrollo de la auditoría.
  - Redacción y clasificación de las no conformidades.

- **Elaboración del informe de auditoría Proceso de certificación**

DIRECTOR

UNIVERSIDAD COMPLUTENSE MADRID

Pedro López Sáez

Director del Máster
Director de la Preincubadora de Empresas
UNIVERSIDAD COMPLUTENSE DE MADRID
Facultad de Comercio y Turismo

CV resumido:

Pedro López Sáez es Profesor Titular de Organización de Empresas de la Universidad Complutense de Madrid y Coordinador Máster en Comercio Electrónico que se imparte en dicha Universidad. Cuenta con una experiencia docente de más de quince años, centrada especialmente en las áreas de Dirección Estratégica y Creación de Empresas. Es Doctor en Dirección de Empresas por la Universidad Complutense de Madrid, con Premio Extraordinario de Doctorado en el año 2005, Licenciado en Administración y Dirección de Empresas por la Universidad Rey Juan Carlos y Diplomado en Estudios Empresariales por la Universidad Complutense de Madrid.

Forma parte del Grupo de Investigación Complutense sobre Estrategia, Conocimiento e Innovación (ECI) y ha sido Research Fellow del Real Colegio Complutense at Harvard (Harvard University. Cambridge, Massachusetts – EE.UU.). Sus líneas de investigación se centran en: la Dirección Estratégica de la Empresa; la Dirección del Conocimiento, el Capital Intelectual y el Aprendizaje Organizativo; y las Capacidades Dinámicas, la Dirección de la Innovación y el Proceso Emprendedor.

Cuenta con dos tramos de investigación reconocidos (sexenios). Ha participado, como investigador principal o como miembro del equipo investigador, en diversos proyectos de investigación financiados por organismos públicos (Ministerio de Economía y Competitividad, Ministerio de Ciencia e Innovación, Comunidad de Madrid...) y privados (EADS, Fundación Rafael del Pino...). Sus investigaciones han sido publicadas en revistas como Technovation, Industrial Marketing Management, Journal of Knowledge Management, o Journal of Business Ethics.

PROFESORADO

UNIVERSIDAD COMPLUTENSE MADRID

Carlos Solé
CISO en Santander España

Alberto Francoso
Jefe del Servicio de Análisis de la Ciberseguridad y la Cibercriminalidad de la OCC en Ministerio del Interior

Ana Belén Galán
Security Manager en CISO CIB-BBVA

Patricia Muleiro Antón
DPO & Compliance Officer
Clinica Universidad de Navarra

Sol Fernandez-Rañada Lopez-Doriga
Asesora Legal

Raúl Siles
Founder & Senior Security Analyst at DinoSec

Víctor Fernández
Senior Manager Auditoria Interna Grupo Santander | MBA | CIA | GDPR

Francisco Lázaro Anguis
Profesor asociado en ETSI de Telecomunicación UPM
Presidente Gpo. Seguridad de AUTELSI.

Marta Fernández Núñez
Data Protection Officer - Head of the Data Protection and Privacy Department at BNP Paribas Group in Spain

Maica Aguilar Carneros
Experta en Ciberseguridad y Privacidad. Junta Directiva Women4Cyber Spain (W4C)

Javier Pinillos
Information Security Manager - CISA MBA

Ingrid González
Abogada, Área de Tecnología, Innovación y Economía Digital en Ceca Magán Abogados

PROFESORADO

UNIVERSIDAD COMPLUTENSE MADRID

Henry Velásquez Yanez
CIPP/E. International Data Privacy & Tech Lawyer (GDPO): Spain, Italy & Portugal at Publicis Groupe

Eduardo Di Monte
Coordinator of the Industrial Cybersecurity Center in Chile and Security and Continuity of Business Director of the Agbar Group, for Spain and Chile.

Gustavo Lozano García
CISO - Chief Information Security Officer at ING Spain & Portugal

Gonzalo Asensio Asensio
CISO en Bankinter Group

Gabriel E.M.
Director de CiberSeguridad (CISO) en Leroy Merlin

David Moreno
Experto en Tecnología y Ciberseguridad

Cristina Garcerán Ortega
Responsable de Privacidad y Protección de Datos | Admiral Europe Compañía de Seguros | Admiral Group | DPD Certificado

Tristan Ramaget
Senior specialist - Information Security Management and Continuity Management

Daniel Largacha Lamela
MAPFRE Global Control Center CERT Assitant Director

Ramón Miralles López
Socio | Director ECIX Catalunya

Carlos Alberto Saiz Peña
Abogado experto en Legal Tech, GRC (Governance, Risk & Compliance)

Berta Balanzategui Vidal
Senior Privacy Counsel

PROFESORADO

UNIVERSIDAD COMPLUTENSE MADRID

Antonio Muñoz
Data Protection Technical Director, Global DPO Office at Telefónica

Mariano Benito
Director Seguridad/CISO, GMV Soluciones Globales Internet. Coordinador CSA España. VP Comité Seguridad AMETIC

Rafael Hernández
Responsable de seguridad lógica en CEPSA

César Arquero
Alcalá de Henares, Comunidad de Madrid, España Información de contacto

David Corral
IT Security Manager, CISSP, CISM, CCISO at Repsol

Alfonso Menchen
Delegado de Protección de Datos en Iberdrola España

UNIVERSIDAD COMPLUTENSE MADRID

Información de Contacto

Teléfono

+34 687 30 04 04

E-mail

info@masterprotecciondedatosucm.com

Sitio Web

https://www.masterprotecciondedatosucm.com

***La dirección del Máster se reserva el derecho de modificar, suprimir y actualizar los profesores, la información y el programa del Máster