EXECUTIVE MASTER EN

# AUDITORÍA Y PROTECCIÓN DE DATOS

En colaboración con:

Quint ACADEMY

DPI Data Privacy Institute
AN ISMS FORUM INITIATIVE

COORGANIZADO CON:

IAITG
INSTITUTE OF AUDIT & IT-GOVERNANCE

CEU
Escuela de Negocios
Madrid

# Escuela de Negocios CEU

**La Escuela de Negocios CEU es el centro que aglutina la formación de postgrado empresarial del grupo educativo CEU, una institución con más de 75 años de experiencia en el ámbito educativo de formación superior.**

**La Escuela de Negocios CEU desarrolla la formación basándose en tres pilares: excelencia, innovación y el desarrollo profesional y personal de los alumnos de acuerdo con los valores del humanismo cristiano.**

**La propuesta formativa para directivos y profesionales de la Escuela de Negocios CEU se desarrolla en un doble ámbito, a través de sus programas Executive Master, que profundizan en la dirección empresarial, ya sea desde el ámbito funcional o sectorial, y de los programas de Formación Directiva, un amplio elenco de programas especializados de formación que permiten la adaptación permanente a las nuevas realidades de la dirección y la gestión empresarial.**

**La Escuela de Negocios CEU realiza su actividad en sedes propias en las principales ciudades españolas, Madrid y Valencia, lo que refuerza su compromiso con la formación de los directivos desde un punto de vista profesional.**

# Executive MAPD

La información es uno de los bienes más importantes de una empresa. La integridad y la fiabilidad de esta información y de los sistemas que la generan, condicionan el éxito de la empresa.

Con el incremento de la complejidad en los sistemas de información y de los riesgos asociados, las organizaciones buscan profesionales con experiencia y conocimientos probados para identificar y evaluar los riesgos, y sepan minimizar las vulnerabilidades de estos sistemas. En momento en que los costes se reducen la seguridad de la información y el tratamiento de datos de carácter personal es una de las principales preocupaciones de los directivos.

La auditoría de los sistemas de información se define como la disciplina que estudia los principios y los procedimientos metodológicos y técnicos usados en la recopilación y evaluación de evidencias para determinar si los sistemas de información y recursos relacionados protegen adecuadamente los activos, mantienen la integridad, fiabilidad y disponibilidad de los datos y procesos, alcanzan las metas de la organización y consumen los recursos de manera eficiente.

Se trata de una materia multidisciplinar, que abarca áreas de conocimiento como:

- Informática
- Telecomunicaciones
- Contabilidad y Auditoría financiera
- Auditoría Interna
- Derecho
- Gestión de la empresa
- Gestión de riesgos y seguridad
- Comunicación

Las Tecnologías de la Información y las Comunicaciones (TIC) están impactado en los procesos de las entidades públicas y privadas en:

- La capacidad que dan para capturar, almacenar, analizar y procesar cantidades ingentes de datos y información, así como para intercambiarla con el entorno (clientes, proveedores, socios, ciudadanos...) ha hecho que las TIC hayan llegado a ser un componente crítico de gran parte de los procesos productivos y de toma de decisiones.

- Las TIC han impactado significativamente en los procesos de control de las entidades. Los objetivos de control se han mantenido, sin embargo las TIC han alterado la forma en la que los procesos han de ser controlados (palabras de paso, cortafuegos, firmas digitales, encriptación...).

- Las TIC han influido también en la profesión de auditoría interna y externa, modificando la forma como las auditorías son realizadas (captura y análisis de la información, aspectos para ser controlados) y los conocimientos necesarios del equipo auditor.

- Consciente de los crecientes riesgos de las nuevas tecnologías, la Administración ha promulgado legislación sobre privacidad y protección de datos (LORTAD en el 1992 y LOPD en el 1999), servicios de la sociedad de la información y comercio electrónico (LSSICE en el 2002), Telecomunicaciones (2003) y Firma electrónica (2003).

- Por otra parte, existe regulación y legislación de ámbito internacional que indirectamente, establece la necesidad de una adecuada medida de riesgos y diseño y auditoría de los controles de los sistemas de información, como son el segundo acuerdo de capital del Comité de Supervisión Bancaria de Basilea (Basel II), que afecta a las entidades financieras, y la ley americana Sarbanes-Oxley Act, de protección de los inversores, que afecta a les compañías que cotizan en las bolsas de los EUA.

- Conocer la regulación de los diversos ámbitos de aplicación y de participación de las nuevas tecnologías, de la gestión de la información, de los procesos de control de las entidades y de la gestión de riesgos en los sistemas de información tienes una principal importancia. Es imprescindible el conocimiento de las normas y su aplicación para poder garantizar el respeto y cumplimiento y evitar la producción de resultados no deseados, tomando conciencia de las consecuencias jurídicas de los actos realizados u omitidos.

Por estos motivos, las organizaciones necesitan disponer de un número creciente de profesionales cualificados en la identificación y evaluación de los riesgos de los sistemas de información y en el diseño y evaluación independiente de los controles necesarios para asegurar la eficacia, eficiencia, legalidad y seguridad de los sistemas.

Esta situación contrasta con la falta de estudios oficiales sobre auditoría y control de sistemas, la dispersión de la oferta de estudios existentes y la falta de regulación de la profesión. Así pues, se necesita afrontar estos retos, promoviendo unos estudios universitarios de auditoría y control de sistemas adaptados a las necesidades de la sociedad.

# Objetivos

El programa pretende formar y preparar a los alumnos para desarrollar con eficiencia la gestión y organización de la seguridad de los sistemas de información con especial énfasis en lo que hace referencia a los datos de carácter personal.

Se quiere formar a profesionales que puedan llevar a término con todas las garantías una Auditoría de protección de datos y poder alcanzar la función de responsable de seguridad.

Asimismo, y con una preparación específica, se han de poder presentar si lo consideran necesario, a los exámenes internacionales para obtener el certificado CISA (Certified Information Systems Auditor) o CISM (Certified Information Security Manager).

## Destinatarios

Ingenieros en informática y telecomunicaciones, titulados en económicas y empresariales, abogados, profesionales en auditoría informática y financiera, profesionales en seguridad informática, graduados universitarios en prevención y seguridad integral, responsables de seguridad, y encargados del tratamiento de datos de carácter personal.

## Metodología docente

Esta preparación requerirá del equipo docente una metodología dentro del aula muy dinámica, ya que se plantearán las clases desde la triple perspectiva: técnica, jurídica y práctica.

Se combinarán el estudio de casos, sesiones lectivas, clases magistrales, conferencias y trabajos en grupo de los participantes.

Se han establecido acuerdos con organizaciones, Administración Pública y Autoridades de Control para que los alumnos puedan realizar su proyecto de final de curso tutelados por los principales profesionales del sector.

## Evaluación

Dependerá de cuatro parámetros:

- Asistencia a un 80% de las actividades académicas.
- Evaluación continuada del trabajo y de la participación de los alumnos.
- Exámenes modulares.
- Memoria y defensa del proyecto final.

## Acreditación académica.

La Fundación Universitaria San Pablo CEU expedirá un título de Executive Master en Auditoría y Protección de Datos, para todos aquellos alumnos que estén en posesión del título de graduado, licenciado, ingeniero, diplomado o equivalente y superen los requisitos académicos.

# Programa

## Módulo 1: Fundamentos

- **INTRODUCCIÓN A LA PROTECCIÓN DE DATOS**
  La protección de datos como derecho fundamental
  Marco europeo de desarrollo de los derechos y libertades de las personas
  La evolución del TC
  Las sentencias 290 y 292/2000 de 30 de noviembre
  El Convenio 108 del Consejo de Europa
  La Directiva 95/46/CE
  La LOPD

## Módulo 2: Marco Español

- **ÁMBITO DE APLICACIÓN DE LA LOPD**
  Concepto de dato personal
  Persona física identificable
  Los empresarios individuales
  Ámbito de aplicación objetivo y subjetivo
  Tratamientos excluidos: En particular datos personales o domésticos
  Concepto de fichero y tratamiento
  La anonimización o disociación
- **LOS SUJETOS DE LA LOPD**
  Responsable del fichero y del tratamiento
  Responsable y encargado del tratamiento
  La evolución de la jurisprudencia del TS
  El Reglamento de desarrollo de la LOPD
- **EL SISTEMA DE GARANTÍAS**
  Finalidad del Registro
  El Registro General de Protección de Datos
  Los Registros autonómicos
  Los ficheros de titularidad pública y privada
  Situaciones dudosas (Colegios profesionales, Cámaras de Comercio, Fundaciones, Universidades, etc)
  La coordinación entre las Autoridades de protección de datos
  El sistema NOTA
- **LA LEGITIMACIÓN PARA EL TRATAMIENTO DE DATOS PERSONALES**
  La regla general del consentimiento
  Consentimiento tácito y consentimiento reforzado
  La experiencia legal
  La relación jurídica
  Las fuentes accesibles al público

  El régimen de las cesiones de datos
  El principio de información como presupuesto para la prestación del consentimiento
- **EL PRINCIPIO DE CALIDAD DE DATOS**
  La regla de la proporcionalidad en el tratamiento de los datos (datos ordenados, pertinentes y no excesivos)
  El principio de finalidad
  La cancelación de los datos innecesarios
- **LOS PRINCIPIOS DE SEGURIDAD Y SECRETO**
  La doble imputación en caso de incumplimiento de los principios de seguridad y secreto
- **COMPETENCIA Y FUNCIONES DE LAS AUTORIDADES DE CONTROL**
  Inscripción de ficheros
  Tutela de Derechos
  Control de oficio. Planes sectoriales
  Procedimiento sancionador
  Inspección
  Instrucción
- **LOS CÓDIGOS TIPO**
  La naturaleza de la autorregulación
  La exigencia de valor añadido
  La experiencia de la AEPD
- **OTRAS OBLIGACIONES**
  Ley 56/2007 LISI
  Ley 34/2002 LSSI
  Ley 34/2003 LGT
  Ley 11/2007

## Módulo 3: Aplicación Sectorial

- **ENTORNO PÚBLICO**
  Seguridad pública
  Ficheros policiales
  Delitos y protección de datos
  Justicia
  Hacienda
  Administración electrónica
  Servicios sociales
  Salud
  Educación
  Universidades
- **ENTORNO PRIVADO**
  Seguridad privada
  Video-vigilancia
  Colegios profesionales, asociaciones y fundaciones
  Marketing
  Comercio y servicios al consumo
  Hostelería y servicios turísticos
  Telecomunicaciones e Internet
  Seguros y mutuas
  Banca y Servicios finanzas. Basilea II, SOX
  Otros sectores

## Módulo 4: Internacional

Transferencias internacionales de datos
Autoridades de control
Europol
IWGDPT (International Working Group of Data Protection and Telecommunications)
Red Iberoamericana
Grupo del artículo 29
Las regulaciones europeas
Las regulaciones norteamericanas: USA, Canadá
Las regulaciones latinoamericanas
Otras regulaciones

## Módulo 5: Prácticum

El Documento de Seguridad
Modificaciones según el nuevo reglamento

## Módulo 6: Protección de los Activos de Información

- **GESTIÓN DE RIESGOS**
  Conceptos Generales
  Tipos de Riesgo
  Análisis de Riesgos
  Metodologías y Estándares
  Elementos y Fases
  Tecnologías
  Outsourcing y SLA (Acuerdos de Nivel de Servicio)
  Implementación
  Monitorización y Comunicación
- **SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN**
  Confidencialidad, Integridad y Disponibilidad
  Inventario y clasificación de activos
  Funciones y responsabilidades del personal
  Concienciación y Formación
  Componentes y Arquitectura Hardware
  Arquitectura y Software de Sistemas de Información
  Infraestructura de Redes de Sistemas de Información
- **EXPOSICIONES Y ACCESOS**
  Permisos de Acceso al Sistema
  Riesgos y Controles de Acceso al Sistema
  Seguridad de las redes de área local
  Seguridad Inalámbrica
  Seguridad en Internet
- **CRIPTOGRAFÍA**
  Sistemas de Clave Privada
  Sistemas de Clave Pública
  Infraestructura de Clave Pública
- **FIRMA DIGITAL**
  Concepto, regulación y clases.
  La identificación electrónica.
  La certificación digital
  Los prestadores de servicio
- **PLAN DE BACKUP**
  Procedimientos periódicos de copias
  Frecuencia y método de rotación

## Módulo 7: Gestión y Respuesta ante Incidentes


- **ANÁLISIS PREVIO**
  BIA (Análisis del impacto en el negocio)
  PIA (Análisis del impacto en la privacidad)
- **FUNCIONES**
  Detección y Notificación
  Jerarquización
  Análisis
  Respuesta
- **PLANIFICACIÓN DE LA CONTINUIDAD**
  Desastres y otras interrupciones
  Punto de recuperación y tiempo de recuperación
  Estrategias de recuperación

## Módulo 8: Control y Auditoría de los Sistemas de Información

- **CONTROL**
  Control Interno
  Control sobre el personal
  Control sobre los proveedores
  Control de las TIC
  COBIT (Objetivos de Control)
  Métricas
  Limitaciones del Control
- **AUDITORÍA DE LOS SISTEMAS DE INFORMACIÓN**
  Tipos de Auditoría
  Metodologías
  Riesgos de auditoría
  Autoevaluación de Controles
  Control y auditoría de la adquisición y mantenimiento de la infraestructura de SI
  Control y auditoría de la operación de los SI
  Control y auditoría de la adquisición, desarrollo y mantenimiento de las aplicaciones
  Control y auditoría en las aplicaciones. Origen, entrada, procesos y salida
- **AUDITORÍA LOPD**
  Marco legal
  Metodologías
  Papeles de trabajo
  Informe final
  Archivos temporales y definitivos
- **EL DATA PROTECTION OFFICER**
  Funciones y responsabilidades
  Marco europeo e internacional
  Competencia profesional

## Módulo 9: Gestión y Gobierno de las TIC

- **PLAN ESTRATÉGICO**
  Definición de niveles de servicio
  Arquitectura de la información
  Dirección tecnológica
  Organización de TI
  Gestión de personal de TI
  Gestión de servicios externos
  Gestión económica de TI
  Gestión de la capacidad y el rendimiento
- **PLAN DIRECTOR DE SEGURIDAD**
  Recursos Humanos, tecnológicos y procesos
  Restricciones
  Hoja de ruta
  Plan de implementación
- **ADMINISTRACIÓN ELECTRÓNICA**
  El procedimiento administrativo y el uso de las nuevas tecnologías
  Las nuevas tecnologías y los procesos electorales (el voto electrónico)
  e-Negocios y e-Gestión
  Comunidades virtuales
- **ESTÁNDARES**
  ISO 38500
  ISO 20000, ITIL
  ISO 27000
  Estándares de Privacidad

## Módulo 10: Proyecto Final de Máster

# Profesorado

**Profesorado vinculado a la Escuela de Negocios CEU sujeto a posibles cambios en el desarrollo del curso.**

**Emilio Aced.**
Subdirector Gral. del Registro de Ficheros y Consultoría de la Agencia de Protección de Datos de Madrid. Presidente (04-06) de la Autoridad Común de Control Europol.

**Miguel Ángel Ballesteros.**
Ingeniero, analista de riesgos ISMS Forum, Auditor interno Sistemas de Información Grupo Cepsa.

**Julio J. Ballesteros.**
Ldo. en Ciencias Políticas y de la Administración. Consultor Senior de Quint Wellington Redwood. Especialista en Gobierno y Gestión de Servicios de TI. Auditor de Sistemas de Gestión de Calidad, Ambientales y de Seguridad de la Información Miembro del GT25 de AENOR y del Comité de Calidad del Software de la AEC.

**Mª José Blanco.**
Subdirectora General del Registro General de Protección de Datos de la Agencia Española de Protección de Datos.

**Antoni Bosch Pujol.**
Licenciado en Física Electrónica. Diplomado ADE. Técnico Superior en Prevención de Riesgos Laborales. CISA, CISM, CGEIT. Director IT-Governance. Institute of Law & Technology (UAB). Asesor de diferentes empresas y organismos. Presidente Fundador ISACA-Barcelona. Director Institute of Audit&IT-Governance (IAITG). Director Data Privacy Institute (DPI-ISMS).

**Miguel Cebrián.**
Lead Auditor, CISA, Seguridad de la Información y Gestión de Riesgos del Grupo FCC. Responsable de Riesgo y Cumplimiento Normativo.

**Gianluca D´Antonio.**
Licenciado en Derecho, CISA, CISM, Lead Auditor, Director de Seguridad de la Información y Gestión de Riesgos del Grupo FCC.

**Álvaro Écija.**
Licenciado en Derecho, Socio fundador y Director Gerente de Ecija, experto en Derecho de las TIC y Seguridad de la Información.

**Carlos Manuel Fernández.**
CISA, CISM. Gerente de TI AENOR. Dirección de Desarrollo.

**Antonio Fernández.**
Doctor en Informática. Coordina la implantación del GTI4U.

**Jesús Gómez.**
Especializado en Gestión y Gobierno de la TI y en Gestión por Competencias. Consultor y formador en Quint Wellington Redwood.

**Enric LLaudet.**
CISA, CISM. Consultor en Auditoría y Seguridad de la Información. Certificado CISA y CISM por ISACA y miembro de la Junta Directiva de ISACA Barcelona Chapter. Ha sido durante varios años Responsable de Ingeniería de Sistemas en BT.

**Ricard Martínez.**
Doctor en Derecho Constitucional. Consultor en la UOC. Técnico de Control de Bases de Datos de la Universitat de València. Premio Joan Lluis Vives 2004 de comunicación científica. Coordinador del Área de estudios AEPD.

**Ángel Menéndez.**
Catedrático. Facultad de Derecho UAM.

**Roberto Moriyón.**
Dr. en Matemáticas por Princeton University. Catedrático de Lenguajes y Sistemas Informáticos, UAM.

**José Luis Piñar Mañas.**
Dr. en Derecho. Catedrático de la Universidad CEU San Pablo. Ex Director de la Agencia Española de Protección de Datos. Presidente Honorario de la Red Iberoamericana de Protección de Datos.

**Jorge Ramió.**
Dr. Ingeniero de Telecomunicación Diplomado (UPM). Profesor titular de la Universidad Politécnica de Madrid. Creador y Director de CriptoRed. Director de la Cátedra UPM Applus+ de Seguridad y Desarrollo de la Sociedad de la Información.

**Luis Miguel Rosa.**
Máster en Dirección de S.I. Máster en Gestión de la Calidad. Coordinador del CTN71/SC7/GT-25 de AENOR. Country Manager Exin Espanya.

**Juan Ignacio Rouyet.**
Ingeniero de Telecomunicación. Consultor de ITIL en Quint Wellington Redwood. Experto en consultoría estratégica en Gobierno y Gestión de Servicios de TI.

**Jesús Rubí.**
Director adjunto Agencia Española de Protección de Datos.

**Juan Salom.**
Tit. del Curso superior de Informática del Ejercito y máster de Seguridad de la información para la defensa. Comandante y Director de la Unidad Central Operativa de Policía Judicial de la Guardia Civil.

**Carlos Alberto Saiz.**
Ldo. en Derecho, Socio de Ecija, Responsable del Área de Compliance IT y Gobierno de la Seguridad, Vicepresidente del ISMS Forum y Subdirector del DPI (Data Privacy Institute).

**Jorge Uya.**
Ingeniero electrónico, por la Universidad Simón Bolívar de Venezuela y especialista en Dirección estratégica de las TIC (UPM). Instructor certificado de CERT/CC (Universidad Carnegie Mellon de EEUU). CISA y BS7799 Auditor. Director Latinoamérica TB Security S.A.

**Lluís Vera.**
Ingeniero Superior de Telecomunicaciones por la UPC. MBA y colaborador académico de Esade Business School. Codirector Master de Seguridad en Tecnologías de la Información esCERT UPC/TB-Security. Socio director TB Security S.A.

# Datos de interés

## Dirección

**ANTONI BOSCH.**

CISA, CISM, CGEIT. Ldo. en Física Electrónica (UB). Diplomado ADE (ESADE). Técnico Superior en Prevención de Riesgos Laborales (UOC). Director IT-Governance. Institute of Law&Technology (UAB). Asesor de diferentes empresas y organismos. Director de varios Másters y cursos de Postgrado. Presidente Fundador ISACA-Barcelona. Director Data Privacy Institute (DPI-ISMS.) Director Institute of Audit&IT-Governance (IAITG).

## Coordinación

**ÓSCAR DEL MORAL QUEIPO.**

Coordinador de Programas Master Escuela de Negocios CEU
E-mail: omoral.en@ceu.es

## Duración

El programa se desarrolla los viernes en la tarde y sábados en la mañana. Con un total de 300 horas lectivas.

## Derechos de Matrícula

9.800 euros. Incluye toda la documentación y materiales necesarios para el seguimiento del programa.

La Escuela de Negocios CEU tiene acuerdos con entidades financieras para la financiación del importe de la matrícula. Asimismo, la Escuela de Negocios ofrece diferentes modalidades de pago para adaptarse a diferentes circunstancias financieras de los alumnos.

La Escuela de Negocios CEU pone a disposición de las empresas la posibilidad de desarrollar acuerdos generales de formación para sus profesionales por el que se puede beneficiar de bonificaciones en los diferentes programas de formación.

Los antiguos alumnos de cualquier centro de la Fundación Universitaria San Pablo-CEU se bonifican con una reducción en el importe de la matrícula.

## Información y matrícula

**Coordinación del Programa**
Óscar del Moral Queipo. E-mail: omoral.en@ceu.es

**Escuela de Negocios CEU**
Carrera de San Francisco 2, 28005 Madrid
Teléfono: 91 354 07 18, Fax: 91 354 07 36. E-mail: en@ceu.es

www.en.ceu.es | www.ceu.es | www.postgradoceu.es

**Escuela de Negocios CEU**
Carrera de San Francisco, 2. 28005 Madrid
Teléfono: 91 354 07 18, Fax: 91 354 07 36
E-mail: en@ceu.es

**www.en.ceu.es**

CEU
*Escuela de Negocios*
*Madrid*