

Máster en Análisis Estratégico y Ciberseguridad Legal en Entornos Jurídicos



ÍNDICE

1 | Somos Educa Business School

2 | Rankings

3 | Alianzas y acreditaciones

4 | By EDUCA EDTECH Group

5 | Metodología LXP

6 | Razones por las que elegir Educa Business School

7 | Programa Formativo

8 | Temario

9 | Contacto

SOMOS EDUCA BUSINESS SCHOOL

EDUCA Business School es una institución de formación online especializada en negocios. Como miembro de la Comisión Internacional de Educación a Distancia y con el prestigioso Certificado de Calidad AENOR (normativa ISO 9001) nuestra institución se distingue por su compromiso con la excelencia educativa.

Nuestra **oferta formativa**, además de **satisfacer las demandas del mercado laboral** actual, puede bonificarse como formación continua para el personal trabajador, así como ser homologados en Oposiciones dentro de la Administración Pública. Las titulaciones de EDUCA Business School se pueden certificar con la Apostilla de La Haya dotándolos de validez internacional en más de 160 países.

Más de

18

años de
experiencia

Más de

300k

estudiantes
formados

Hasta un

98%

tasa
empleabilidad

Hasta un

100%

de financiación

Hasta un

50%

de los estudiantes
repite

Hasta un

25%

de estudiantes
internacionales

RANKINGS DE EDUCA BUSINESS SCHOOL

Educa Business School se engloba en el conjunto de EDUCA EDTECH Group, que ha sido reconocido por su trabajo en el campo de la formación online.

Todas las entidades bajo el sello EDUCA EDTECH comparten la misión de democratizar el acceso a la educación y apuestan por la transferencia de conocimiento, por el desarrollo tecnológico y por la investigación. Gracias a ello ha conseguido el reconocimiento de diferentes rankings a nivel nacional e internacional.



ALIANZAS Y ACREDITACIONES



FONDO
SOCIAL
EUROPEO



BY EDUCA EDTECH

Educa Business School es una marca avalada por **EDUCA EDTECH Group**, que está compuesto por un conjunto de experimentadas y reconocidas instituciones educativas de formación online. Todas las entidades que lo forman comparten la misión de democratizar el acceso a la educación y apuestan por la transferencia de conocimiento, por el desarrollo tecnológico y por la investigación.



ONLINE EDUCATION



METODOLOGÍA LXP

La metodología **EDUCA LXP** permite una experiencia mejorada de aprendizaje integrando la AI en los procesos de e-learning, a través de modelos predictivos altamente personalizados, derivados del estudio de necesidades detectadas en la interacción del alumnado con sus entornos virtuales.

EDUCA LXP es fruto de la **Transferencia de Resultados de Investigación** de varios proyectos multidisciplinares de I+D+i, con participación de distintas Universidades Internacionales que apuestan por la transferencia de conocimientos, desarrollo tecnológico e investigación.



1. Flexibilidad

Aprendizaje 100% online y flexible, que permite al alumnado estudiar donde, cuando y como quiera.



2. Accesibilidad

Cercanía y comprensión. Democratizando el acceso a la educación trabajando para que todas las personas tengan la oportunidad de seguir formándose.



3. Personalización

Itinerarios formativos individualizados y adaptados a las necesidades de cada estudiante.



4. Acompañamiento / Seguimiento docente

Orientación académica por parte de un equipo docente especialista en su área de conocimiento, que aboga por la calidad educativa adaptando los procesos a las necesidades del mercado laboral.



5. Innovación

Desarrollos tecnológicos en permanente evolución impulsados por la AI mediante Learning Experience Platform.



6. Excelencia educativa

Enfoque didáctico orientado al trabajo por competencias, que favorece un aprendizaje práctico y significativo, garantizando el desarrollo profesional.

RAZONES POR LAS QUE ELEGIR EDUCA BUSINESS SCHOOL

1. FORMACIÓN ONLINE ESPECIALIZADA

Nuestros alumnos acceden a un modelo pedagógico innovador **de más de 20 años de experiencia educativa con Calidad Europea.**



2. METODOLOGÍA DE EDUCACIÓN FLEXIBLE

Con nuestra metodología estudiarán **100% online** y nuestros alumnos/as tendrán acceso los 365 días del año a la plataforma educativa.



3. CAMPUS VIRTUAL DE ÚLTIMA TECNOLOGÍA



Contamos con una **plataforma avanzada** con material adaptado a la realidad empresarial, que fomenta la participación, interacción y comunicación con alumnos de distintos países.

4. DOCENTES DE PRIMER NIVEL

Nuestros docentes están acreditados y formados en **Universidades de alto prestigio en Europa**, todos en activo y con una amplia experiencia profesional.



5. TUTORÍA PERMANENTE



Contamos con un **Centro de Atención al Estudiante CAE**, que brinda atención personalizada y acompañamiento durante todo el proceso formativo.

6. DOBLE MATRICULACIÓN

Algunas de nuestras acciones formativas cuentan con la llamada **Doble matriculación**, que te permite obtener dos formaciones, ya sean de masters o curso, al precio de una.



Máster en Análisis Estratégico y Ciberseguridad Legal en Entornos Jurídicos



DURACIÓN
1500 horas



MODALIDAD
ONLINE



ACOMPAÑAMIENTO
PERSONALIZADO

Titulación

Titulación de Máster en Análisis Estratégico y Ciberseguridad Legal en Entornos Jurídicos con 1500 horas expedida por EDUCA BUSINESS SCHOOL como Escuela de Negocios Acreditada para la Impartición de Formación Superior de Postgrado, con Validez Profesional a Nivel Internacional



EDUCA BUSINESS SCHOOL

como centro acreditado para la impartición de acciones formativas
expide el presente título propio

NOMBRE DEL ALUMNO/A

con número de documento XXXXXXXXX ha superado los estudios correspondientes de

Nombre del curso

con una duración de XXX horas, perteneciente al Plan de Formación de Educa Business School.

Y para que surta los efectos pertinentes queda registrado con número de expediente XXXXX/XXXX-XXXX-XXXXXX.

Con una calificación XXXXXXXXXXXXXXXX.

Y para que conste expido la presente titulación en Granada, a (día) de (mes) del (año).

Firma del Alumno/a
NOMBRE ALUMNO/A

La Dirección Académica
NOMBRE DE AREA MANAGER



Con Examen Convulsivo, Categoría Especial del Consejo Económico y Social de la URBECOT (Plan: Postgrado 1000)

Descripción

El Máster en Análisis Estratégico y Ciberseguridad Legal en Entornos Jurídicos responde a la creciente demanda de profesionales capacitados en la protección de datos y la ciberseguridad, dos áreas críticas en la era digital. Con un enfoque integral, este máster te prepara para enfrentar los desafíos legales de la protección de datos, el business intelligence y la gestión de ciberseguridad, proporcionándote herramientas para analizar y proteger información sensible en un entorno global. La importancia de la ciberseguridad y la protección de datos no solo está en auge, sino que es esencial para el funcionamiento seguro y eficiente de cualquier organización. Este máster online te ofrece flexibilidad y acceso a un conocimiento actualizado, preparándote para destacar en un mercado laboral competitivo. Con esta formación, desarrollarás habilidades clave para identificar, gestionar y mitigar riesgos, además de adquirir un profundo entendimiento del marco normativo vigente, lo que te convertirá en un profesional indispensable en el sector jurídico digital.

Objetivos

'- Desarrollar estrategias de protección de datos alineadas con el RGPD y derechos digitales. - Identificar la responsabilidad proactiva en el tratamiento de datos en entornos jurídicos. - Analizar el impacto del know-how y la protección intelectual en un mercado digital. - Implementar herramientas de Business Intelligence para la toma de decisiones estratégicas. - Comprender y gestionar riesgos de ciberseguridad en sistemas de información. - Diseñar un proceso de respuesta ante incidentes de seguridad informática eficaz. - Evaluar servicios LegalTech y su impacto en el sector jurídico.

Para qué te prepara

El Máster en Análisis Estratégico y Ciberseguridad Legal en Entornos Jurídicos está dirigido a profesionales del ámbito jurídico y tecnológico, incluidos abogados, consultores y responsables de cumplimiento que buscan profundizar en la protección de datos, ciberseguridad, y el uso de Business Intelligence en la gestión de riesgos legales en un entorno digital global.

A quién va dirigido

El Máster en Análisis Estratégico y Ciberseguridad Legal en Entornos Jurídicos te prepara para afrontar desafíos complejos en protección de datos y derechos digitales, garantizando el cumplimiento normativo del RGPD. Desarrollarás habilidades para gestionar ciberseguridad en despachos jurídicos, analizar big data y aplicar inteligencia de negocio. También adquirirás conocimientos sobre propiedad intelectual y servicios legaltech, mejorando tu capacidad para proteger información confidencial y gestionar incidentes de seguridad informática.

Salidas laborales

'- Consultor en protección de datos y derechos digitales - Responsable de ciberseguridad en entornos legales - Auditor de cumplimiento RGPD para despachos - Experto en propiedad intelectual en mercados digitales - Analista de Business Intelligence y Big Data - Especialista en LegalTech y servicios tecnológicos legales - Gestor de proyectos de ciberseguridad y protección de datos

TEMARIO

MÓDULO 1. PROTECCIÓN DE DATOS Y DERECHOS DIGITALES

UNIDAD DIDÁCTICA 1. PROTECCIÓN DE DATOS: CONTEXTO NORMATIVO

1. Normativa General de Protección de Datos
2. Privacidad y protección de datos en el panorama internacional
3. La Protección de Datos en Europa
4. La Protección de Datos en España
5. Estándares y buenas prácticas

UNIDAD DIDÁCTICA 2. REGLAMENTO EUROPEO DE PROTECCIÓN DE DATOS (RGPD). FUNDAMENTOS

1. El Reglamento UE 2016/679
2. Ámbito de aplicación del RGPD
3. Definiciones
4. Sujetos obligados
5. Ejercicio Resuelto. Ámbito de Aplicación

UNIDAD DIDÁCTICA 3. PRINCIPIOS DE LA PROTECCIÓN DE DATOS

1. El binomio derecho/deber en la protección de datos
2. Licitud del tratamiento de los datos
3. Lealtad y transparencia
4. Finalidad del tratamiento de los datos: la limitación
5. Minimización de datos
6. Exactitud y Conservación de los datos personales

UNIDAD DIDÁCTICA 4. LEGITIMACIÓN PARA EL TRATAMIENTO DE LOS DATOS PERSONALES EN EL RGPD

1. El consentimiento del interesado en la protección de datos personales
2. El consentimiento: otorgamiento y revocación
3. El consentimiento informado: finalidad, transparencia, conservación, información y deber de comunicación al interesado
4. Eliminación del Consentimiento tácito en el RGPD
5. Consentimiento de los niños
6. Categorías especiales de datos
7. Datos relativos a infracciones y condenas penales
8. Tratamiento que no requiere identificación
9. Bases jurídicas distintas del consentimiento

UNIDAD DIDÁCTICA 5. DERECHOS DE LOS CIUDADANOS EN LA PROTECCIÓN DE SUS DATOS PERSONALES

1. Derechos de las personas respecto a sus Datos Personales

2. Transparencia e Información
3. Acceso, Rectificación, Supresión (Olvido)
4. Oposición
5. Decisiones individuales automatizadas
6. Portabilidad de los Datos
7. Limitación del tratamiento
8. Excepciones a los derechos
9. Casos específicos
10. Ejercicio resuelto. Ejercicio de Derechos por los Ciudadanos

UNIDAD DIDÁCTICA 6. PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL: MEDIDAS DE CUMPLIMIENTO EN EL RGPD

1. Las políticas de Protección de Datos
2. Posición jurídica de los intervinientes. Responsables, corresponsables, Encargados, subencargado del Tratamiento y sus representantes. Relaciones entre ellos y formalización
3. El Registro de Actividades de Tratamiento: identificación y clasificación del tratamiento de datos

UNIDAD DIDÁCTICA 7. LA RESPONSABILIDAD PROACTIVA

1. El Principio de Responsabilidad Proactiva
2. Privacidad desde el Diseño y por Defecto. Principios fundamentales
3. Evaluación de Impacto relativa a la Protección de Datos (EIPD) y consulta previa. Los Tratamientos de Alto Riesgo
4. Seguridad de los datos personales. Seguridad técnica y organizativa
5. Las Violaciones de la Seguridad. Notificación de Violaciones de Seguridad
6. El Delegado de Protección de Datos (DPD). Marco normativo
7. Códigos de conducta y certificaciones

UNIDAD DIDÁCTICA 8. TRANSFERENCIAS INTERNACIONALES DE DATOS EN EL RGPD

1. El Movimiento Internacional de Datos
2. El sistema de decisiones de adecuación
3. Transferencias mediante garantías adecuadas
4. Normas Corporativas Vinculantes
5. Excepciones
6. Autorización de la autoridad de control
7. Suspensión temporal
8. Cláusulas contractuales

UNIDAD DIDÁCTICA 9. LAS AUTORIDADES DE CONTROL

1. Autoridades de Control: Aproximación
2. Potestades
3. Régimen Sancionador
4. Comité Europeo de Protección de Datos (CEPD)
5. Procedimientos seguidos por la AEPD
6. La Tutela Jurisdiccional
7. El Derecho de Indemnización

UNIDAD DIDÁCTICA 10. DERECHOS DIGITALES RELACIONADOS CON LA PROTECCIÓN DE DATOS

1. Derecho de Rectificación en Internet
2. Derecho a la Actualización de informaciones en medios de comunicación digitales
3. Derecho al Olvido en búsquedas de Internet
 1. - Derecho al Olvido en Google
 2. - Proceso ante Google

UNIDAD DIDÁCTICA 11. DERECHOS DIGITALES DE LOS TRABAJADORES

1. Derecho a la intimidad y uso de dispositivos digitales en el ámbito laboral
2. Derecho a la desconexión digital en el ámbito laboral
3. Derecho a la intimidad frente al uso de dispositivos de video-vigilancia y de grabación de sonido en el lugar de trabajo
4. Derecho a la intimidad ante la utilización de sistemas de geolocalización en el ámbito laboral
 1. - Medidas de seguridad sobre los datos de geolocalización
 2. - La Geolocalización acorde con la Agencia Española de Protección de Datos
5. Ejercicio resuelto: Geolocalización acorde con la AEPD
6. Derechos digitales en la negociación colectiva

UNIDAD DIDÁCTICA 12. DERECHOS DIGITALES DE LOS MENORES DE EDAD

1. Protección de los menores en Internet
2. Protección de datos de los menores en Internet
 1. - Tratamiento de datos por los centros educativos
 2. - Tratamiento de datos por Asociaciones de Madres y Padres de Alumnos (AMPA)
3. Ejercicio resuelto: Tratamiento de datos por Asociaciones de Madres y Padres de Alumnos (AMPA)

UNIDAD DIDÁCTICA 13. CUESTIONES PRÁCTICAS SOBRE DERECHOS DIGITALES

1. Video tutorial: Introducción a la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales
2. Video tutorial: Esquema normativo de Derechos Digitales
3. Sentencias Imprescindibles de Derechos Digitales

MÓDULO 2. PROTECCIÓN DE DATOS PARA DESPACHOS, ABOGADOS Y PROFESIONALES DEL SECTOR JURÍDICO

UNIDAD DIDÁCTICA 1. DESPACHOS, ABOGADOS Y PROFESIONALES COMO RESPONSABLES O ENCARGADOS DEL TRATAMIENTO

1. Cuestiones generales: RGPD, Despachos, Abogados y profesionales
 1. - Novedades introducidas por el RGPD
2. Las políticas de protección de Datos
 1. - Principios relativos al tratamiento de datos
 2. - Diseño del tratamiento
 3. - Intervinientes en el tratamiento de datos
3. Legitimación del tratamiento: Profesionales del Sector jurídico como Responsable o encargado del tratamiento

1. - Profesionales del Sector jurídico como Responsable o encargado del tratamiento
4. Delegado de Protección de Datos (DPD). Marco normativo
 1. - Conocimiento y designación
 2. - Funciones del Delegado de Protección de datos
 3. - Responsabilidad y conflicto
 4. - DPD externo o interno
 5. - Checklist de cumplimiento normativo
5. Tratamiento de los datos en el proceso y en el juicio
 1. - Acceso a las grabaciones de los actos judiciales por los clientes
6. Secreto profesional y confidencialidad
 1. - Límites a la comunicación de datos que impone el secreto profesional

UNIDAD DIDÁCTICA 2. RESPONSABILIDAD ACTIVA EN DESPACHOS, ABOGADOS Y PROFESIONALES DEL SECTOR JURÍDICO

1. El principio de Responsabilidad Proactiva
2. Privacidad desde el Diseño y por Defecto. Principios fundamentales
3. Análisis de riesgo en los Despachos de abogados y Procuradores
 1. - Aspectos generales del análisis de riesgos
 2. - Gestión de las amenazas y del riesgo
 3. - Riesgos en el despacho profesional
4. Evaluación de Impacto relativa a la Protección de Datos (EIPD) y consulta previa. Los tratamientos de alto riesgo
 1. - Contenido de la Evaluación de impacto
5. Seguridad de los datos personales. Seguridad técnica y organizativa
6. Brechas de seguridad en el Despacho de Abogados. Violaciones de seguridad
 1. - Fuga de información
 2. - Origen y motivos
 3. - Causas y formas de prevenirlas
 4. - Mitigar la fuga de información. El principio del mínimo privilegio
 5. - Gestión de la fuga de información
7. Registro de actividades de tratamiento: Identificación y clasificación del tratamiento de datos
 1. - Obligaciones
 2. - Campos que componen el registro de actividades de tratamiento
 3. - Exenciones
8. Códigos de conducta y certificaciones
 1. - Contenido de los códigos de conducta
 2. - Incentivos de los códigos de conducta

UNIDAD DIDÁCTICA 3. LOS DESPACHOS DE PROFESIONALES DEL SECTOR JURÍDICO: CUESTIONES RELEVANTES EN SU FUNCIONAMIENTO

1. Páginas web y cookies
 1. - Comunicaciones comerciales electrónicas
 2. - Dispositivos de almacenamiento y recuperación de datos
2. Comunicaciones electrónicas entre profesionales del Sector Jurídico y clientes
3. El cloud computing
 1. - Tipos de cloud computing
 2. - Portabilidad de la información

3. - Garantías contractuales
4. - Riesgo de la computación en la nube
5. - Estrategia para el cliente de servicios de Cloud Computing
4. Publicación de sentencias en internet
 1. - Centro de documentación Judicial del CGPJ (CENDOJ)
 2. - Informes de la AEPD
 3. - Difusión de sentencias por un particular
5. Tratamiento de datos derivados de la aplicación de la Ley de Prevención del Blanqueo de Capitales
 1. - Comunicación al SEPBLAC
 2. - Obligaciones de control interno
6. Cesión de Datos a la Agencia Tributaria (AEAT)
 1. - Informes de la AEPD
7. Colegios Profesionales: publicación de datos de los colegiados
 1. - Publicación en ventanilla única

UNIDAD DIDÁCTICA 4. MODELOS HABITUALES PARA EL CUMPLIMIENTO DEL RGPD

1. Modelo de contrato de encargo con cláusula informativa
2. Modelos para el uso y la navegación en páginas web
3. Modelo de acuerdo de encargo de tratamiento
4. Modelos para el ejercicio de derechos
 1. - Modelo ejercicio del derecho de acceso
 2. - Modelo ejercicio del derecho de oposición
 3. - Modelo ejercicio del derecho de rectificación
 4. - Modelo ejercicio del derecho de supresión "derecho al olvido"
 5. - Modelo ejercicio del derecho de limitación del tratamiento
 6. - Modelo ejercicio derecho de portabilidad
 7. - Modelo ejercicio derecho a no ser objeto de decisiones automatizadas
5. Modelos de respuesta para el ejercicio de derechos
 1. - Modelo de respuesta para el ejercicio del derecho de acceso
 2. - Modelo de respuesta para el ejercicio del derecho de oposición
 3. - Modelo de respuesta para el ejercicio del derecho de rectificación
 4. - Modelo de respuesta para el ejercicio del derecho de supresión "derecho al olvido"
 5. - Modelo de respuesta para el ejercicio derecho de limitación del tratamiento
 6. - Modelo de respuesta para el ejercicio derecho de portabilidad
 7. - Modelo de respuesta para el ejercicio derecho a no ser objeto de decisiones individuales automatizadas
 8. - Modelo de respuesta requiriendo al afectado para que aporte documentación o subsane defectos en la solicitud

MÓDULO 3. KNOW-HOW, PROPIEDAD INTELECTUAL E INDUSTRIAL EN UN MERCADO DIGITAL GLOBAL

UNIDAD DIDÁCTICA 1. INTRODUCCIÓN AL KNOW-HOW

1. Introducción teórica al concepto de know-how
2. Entorno de Innovación Abierta
3. Política de Gestión de Propiedad Intelectual e Industrial

4. Gestión de Propiedad Intelectual e Industrial en Proyectos de I+D+I
5. Patent Box

UNIDAD DIDÁCTICA 2. SECRETOS EMPRESARIALES E INFORMACIÓN CONFIDENCIAL

1. Jurisdicción Europea Y Española
2. Relevancia del secreto
3. Requisitos del secreto empresarial

UNIDAD DIDÁCTICA 3. PROTECCIÓN DEL KNOW-HOW

1. Gestión de la protección
2. Protección de la Propiedad Intelectual e Industrial en la era digital
3. Gestión de la Propiedad Intelectual e Industrial en explotación y defensa
4. Non Disclosure Agreement (NDA)

UNIDAD DIDÁCTICA 4. INTERACCIÓN ENTRE LA LSSI Y LA LEY DE PROPIEDAD INTELECTUAL

1. Ley de Servicios de la Sociedad de la Información y Ley de Propiedad Intelectual: una doble perspectiva
2. Derechos de propiedad intelectual sobre las páginas web
3. Acceso a contenidos desde la perspectiva de la LSSI
4. La Ley Sinde: Ley 2/2011, de 4 de marzo, de Economía Sostenible
5. Impacto de la Reforma
6. Reforma del TRLGDCU impacto en los negocios online

UNIDAD DIDÁCTICA 5. PATENTES, DISEÑOS INDUSTRIALES Y MODELOS DE UTILIDAD

1. Requisitos de una patente
2. Clases de patentes
3. Procedimiento de registro de patentes
4. Diseños industriales
5. Modelos de utilidad

UNIDAD DIDÁCTICA 6. MARCA NACIONAL Y NOMBRES COMERCIALES

1. Marco normativo La Ley 17/2001, de 7 de diciembre, de Marcas
2. Concepto de marca
3. Clases de marcas
4. Concepto de nombre comercial
5. Prohibiciones absolutas de registro
6. Prohibiciones relativas de registro
7. Marca notoria y marca renombrada
8. Marcas colectivas y de garantía

UNIDAD DIDÁCTICA 7. NOMBRES DE DOMINIO

1. Clases de nombres de dominio
2. Conflictos en nombres de dominio

UNIDAD DIDÁCTICA 8. INTRODUCCIÓN AL BIG DATA

1. ¿Qué es Big Data?
2. La era de las grandes cantidades de información: historia del big data
3. La importancia de almacenar y extraer información
4. Big Data enfocado a los negocios
5. Open Data
6. Información pública
7. IoT (Internet of Things - Internet de las cosas)

MÓDULO 4. BUSSINESS INTELLIGENCE: DATOS, INFORMACIÓN Y CONOCIMIENTO

UNIDAD DIDÁCTICA 1. MINERÍA DE DATOS O DATA MINING Y EL APRENDIZAJE AUTOMÁTICO

1. Introducción a la minería de datos y el aprendizaje automático
2. Proceso KDD
3. Modelos y Técnicas de Data Mining
4. Áreas de aplicación
5. Minería de textos y Web Mining
6. Data mining y marketing

UNIDAD DIDÁCTICA 2. DATAMART. CONCEPTO DE BASE DE DATOS DEPARTAMENTAL

1. Aproximación al concepto de DataMart
2. Bases de datos OLTP
3. Bases de Datos OLAP
4. MOLAP, ROLAP & HOLAP
5. Herramientas para el desarrollo de cubos OLAP

UNIDAD DIDÁCTICA 3. DATAWAREHOUSE O ALMACÉN DE DATOS CORPORATIVOS

1. Visión General. ¿Por qué DataWarehouse?
2. Estructura y Construcción
3. 3. Fases de implantación
4. Características
5. Data Warehouse en la nube

UNIDAD DIDÁCTICA 4. INTELIGENCIA DE NEGOCIO Y HERRAMIENTAS DE ANALÍTICA

1. Tipos de herramientas para BI
2. Productos comerciales para BI
3. Productos Open Source para BI

UNIDAD DIDÁCTICA 5. BUSINESS INTELLIGENCE CON POWERBI

1. Business Intelligence en Excel
2. Herramienta Powerbi

UNIDAD DIDÁCTICA 6. HERRAMIENTA TABLEAU

1. Herramienta Tableau

UNIDAD DIDÁCTICA 7. HERRAMIENTA QLIKVIEW

1. Instalación y arquitectura
2. Carga de datos
3. Informes
4. Transformación y modelo de datos
5. Análisis de datos

MÓDULO 5. BIG DATA: CUESTIONES FUNDAMENTALES

UNIDAD DIDÁCTICA 1. INTRODUCCIÓN AL BIG DATA

1. ¿Qué es Big Data?
2. La era de las grandes cantidades de información. Historia del big data
3. La importancia de almacenar y extraer información
4. Big Data enfocado a los negocios
5. Open Data
6. Información pública
7. IoT (Internet of Things-Internet de las cosas)

UNIDAD DIDÁCTICA 2. FUENTES DE DATOS

1. Definición y relevancia de la selección de las fuentes de datos
 1. - Relevancia o Importancia de la selección de las fuentes
2. Naturaleza de las fuentes de datos Big Data

UNIDAD DIDÁCTICA 3. OPEN DATA

1. Definición, Beneficios y Características
 1. - Principios Básicos del Open Data
 2. - Beneficios del Open Data
 3. - Relación Linked Data
 4. - Lenguaje de consulta
2. Ejemplo de uso de Open Data

UNIDAD DIDÁCTICA 4. FASES DE UN PROYECTO DE BIG DATA

1. Diagnóstico inicial
2. Diseño del proyecto
3. Proceso de implementación
4. Monitorización y control del proyecto
5. Responsable y recursos disponibles
6. Calendarización
7. Alcance y valoración económica del proyecto

UNIDAD DIDÁCTICA 5. BUSINESS INTELLIGENCE Y LA SOCIEDAD DE LA INFORMACIÓN

1. Definiendo el concepto de Business Intelligence y sociedad de la información

2. Arquitectura de una solución de Business Intelligence
3. Business Intelligence en los departamentos de la empresa
4. Conceptos de Plan Director, Plan Estratégico y Plan de Operativa Anual
5. Sistemas operacionales y Procesos ETL en un sistema de BI
6. Ventajas y Factores de Riesgos del Business Intelligence

UNIDAD DIDÁCTICA 6. PRINCIPALES PRODUCTOS DE BUSINESS INTELLIGENCE

1. Cuadros de Mando Integrales (CMI)
2. Sistemas de Soporte a la Decisión (DSS)
3. Sistemas de Información Ejecutiva (EIS)

UNIDAD DIDÁCTICA 7. BIG DATA Y MARKETING

1. Apoyo del Big Data en el proceso de toma de decisiones
2. Toma de decisiones operativas
3. Marketing estratégico y Big Data
4. Nuevas tendencias en management

UNIDAD DIDÁCTICA 8. DEL BIG DATA AL LINKED OPEN DATA

1. Concepto de web semántica
2. Linked Data Vs Big Data
3. Lenguaje de consulta SPARQL

UNIDAD DIDÁCTICA 9. INTERNET DE LAS COSAS

1. Contexto Internet de las Cosas (IoT)
2. ¿Qué es IoT?
3. Elementos que componen el ecosistema IoT
4. Arquitectura IoT
5. Dispositivos y elementos empleados
6. Ejemplos de uso
7. Retos y líneas de trabajo futuras

MÓDULO 6. CIBERSEGURIDAD: GESTIÓN, HERRAMIENTAS E INCIDENTES DE SEGURIDAD INFORMÁTICA

UNIDAD FORMATIVA 1. CIBERSEGURIDAD: GESTIÓN Y HERRAMIENTAS

UNIDAD DIDÁCTICA 1. GESTIÓN Y HERRAMIENTAS DE CIBERSEGURIDAD: INTRODUCCIÓN Y CONCEPTOS BÁSICOS

1. La sociedad de la información
 1. - ¿Qué es la seguridad de la información?
 2. - Importancia de la seguridad de la información
2. Seguridad de la información: Diseño, desarrollo e implantación
 1. - Descripción de los riesgos de la seguridad
 2. - Selección de controles
3. Factores de éxito en la seguridad de la información

4. Vídeo tutorial: relación entre la ciberseguridad y el Big Data

UNIDAD DIDÁCTICA 2. NORMATIVA SOBRE EL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI)

1. Estándares y Normas Internacionales sobre los SGSI
 1. - Familia de Normas ISO 27000
 2. - La Norma UNE-EN-ISO/IEC 27001:2014
 3. - Buenas prácticas en seguridad de la información, Norma ISO/IEC 27002
2. Normativa aplicable a los SGSI
 1. - Normativa comunitaria sobre seguridad de la información
 2. - Legislación Española sobre seguridad de la información
 3. - El Instituto Nacional de Ciberseguridad (INCIBE)

UNIDAD DIDÁCTICA 3. POLÍTICA DE SEGURIDAD: ANÁLISIS Y GESTIÓN DE RIESGOS

1. Plan de implantación del SGSI
2. Análisis de riesgos
 1. - Análisis de riesgos: Aproximación
 2. - Principales tipos de vulnerabilidades, fallos de programa, programas maliciosos y su actualización permanente, así como criterios de programación segura
 3. - Particularidades de los distintos tipos de código malicioso
 4. - Principales elementos del análisis de riesgos y sus modelos de relaciones
 5. - Metodologías cualitativas y cuantitativas de análisis de riesgos
 6. - Identificación de los activos involucrados en el análisis de riesgos y su valoración
 7. - Identificación de las amenazas que pueden afectar a los activos identificados previamente
 8. - Análisis e identificación de las vulnerabilidades existentes en los sistemas de información que permitirían la materialización de amenazas, incluyendo el análisis local
 9. - Optimización del proceso de auditoría y contraste de vulnerabilidades e informe de auditoría
 10. - Identificación de las medidas de salvaguarda existentes en el momento de la realización del análisis de riesgos y su efecto sobre las vulnerabilidades y amenazas
 11. - Establecimiento de los escenarios de riesgo entendidos como pares activo-amenaza susceptibles de materializarse
 12. - Determinación de la probabilidad e impacto de materialización de los escenarios
 13. - Establecimiento del nivel de riesgo para los distintos pares de activo y amenaza
 14. - Determinación por parte de la organización de los criterios de evaluación del riesgo, en función de los cuales se determina si un riesgo es aceptable o no
 15. - Relación de las distintas alternativas de gestión de riesgos
 16. - Guía para la elaboración del plan de gestión de riesgos
 17. - Exposición de la metodología NIST SP 800-30
 18. - Exposición de la metodología Magerit
3. Gestión de riesgos
 1. - Aplicación del proceso de gestión de riesgos y exposición de las alternativas más frecuentes
 2. - Metodologías comúnmente aceptadas de identificación y análisis de riesgos
 3. - Aplicación de controles y medidas de salvaguarda para obtener una reducción del riesgo

UNIDAD DIDÁCTICA 4. AUDITORÍA DE CIBERSEGURIDAD

1. Criterios Generales en la Auditoría de Seguridad de la Informática
 1. - Código deontológico de la función de auditoría
 2. - Relación de los distintos tipos de auditoría en el marco de los sistemas de información
 3. - Criterios a seguir para la composición del equipo auditor
 4. - Tipos de pruebas a realizar en el marco de la auditoría, pruebas sustantivas y pruebas de cumplimiento
 5. - Tipos de muestreo a aplicar durante el proceso de auditoría
 6. - Utilización de herramientas tipo CAAT (Computer Assisted Audit Tools)
 7. - Explicación de los requerimientos que deben cumplir los hallazgos de auditoría
 8. - Aplicación de criterios comunes para categorizar los hallazgos como observaciones o no conformidades
 9. - Relación de las normativas y metodologías relacionadas con la auditoría de sistemas de información comúnmente aceptadas
2. Aplicación de la normativa de protección de datos de carácter personal
 1. - Normativa de referencia: Reglamento General de Protección de Datos y Ley Orgánica de Protección de Datos 3/2018
 2. - Principios generales de la protección de datos de carácter personal
 3. - Legitimación para el tratamiento de datos personales
 4. - Medidas de responsabilidad proactiva
 5. - Los derechos de los interesados
 6. - Delegado de Protección de Datos
3. Herramientas para la auditoría de sistemas
 1. - Herramientas del sistema operativo tipo Ping, Traceroute, etc
 2. - Herramientas de análisis de red, puertos y servicios tipo Nmap, Netcat, NBTScan, etc
 3. - Herramientas de análisis de vulnerabilidades tipo Nessus
 4. - Analizadores de protocolos tipo WireShark, DSniff, Cain & Abel, etc
 5. - Analizadores de páginas web tipo Acunetix, Dirb, Parosproxy, etc
 6. - Ataques de diccionario y fuerza bruta tipo Brutus, John the Ripper, etc
4. Descripción de los aspectos sobre cortafuego en auditorías de sistemas de información
 1. - Principios generales de cortafuegos
 2. - Componentes de un cortafuegos de red
 3. - Relación de los distintos tipos de cortafuegos por ubicación y funcionalidad
 4. - Arquitecturas de cortafuegos de red
5. Guías para la ejecución de las distintas fases de la auditoría de sistemas de información
 1. - Normas para la implantación de la auditoría de la documentación
 2. - Instrucciones para la elaboración del plan de auditoría
 3. - Pruebas de auditoría
 4. - Instrucciones para la elaboración del informe de auditoría

UNIDAD DIDÁCTICA 5. COMUNICACIONES SEGURAS: SEGURIDAD POR NIVELES

1. Seguridad a nivel físico
 1. - Tipos de ataques
 2. - Servicios de Seguridad
 3. - Medidas de seguridad a adoptar
2. Seguridad a nivel de enlace
 1. - Tipos de ataques

2. - Medidas de seguridad a adoptar
3. Seguridad a nivel de red
 1. - Datagrama IP
 2. - Protocolo IP
 3. - Protocolo ICMP
 4. - Protocolo IGMP
 5. - Tipos de Ataques
 6. - Medidas de seguridad a adoptar
4. Seguridad a nivel de transporte
 1. - Protocolo TCP
 2. - Protocolo UDP
 3. - Tipos de Ataques
 4. - Medidas de seguridad a adoptar
5. Seguridad a nivel de aplicación
 1. - Protocolo DNS
 2. - Protocolo Telnet
 3. - Protocolo FTP
 4. - Protocolo SSH
 5. - Protocolo SMTP
 6. - Protocolo POP
 7. - Protocolo IMAP
 8. - Protocolo SNMP
 9. - Protocolo HTTP
 10. - Tipos de Ataques
 11. - Medidas de seguridad a adoptar

UNIDAD FORMATIVA 2. CIBERSEGURIDAD: GESTIÓN DE INCIDENTES DE SEGURIDAD INFORMÁTICA

UNIDAD DIDÁCTICA 1. SISTEMAS DE DETECCIÓN Y PREVENCIÓN DE INTRUSIONES (IDS/IPS)

1. Conceptos generales de gestión de incidentes, detección de intrusiones y su prevención
2. Identificación y caracterización de los datos de funcionamiento del sistema
3. Arquitecturas más frecuentes de los IDS
4. Relación de los distintos tipos de IDS/IPS por ubicación y funcionalidad
5. Criterios de seguridad para el establecimiento de la ubicación de los IDS/IPS

UNIDAD DIDÁCTICA 2. IMPLANTACIÓN Y PUESTA EN PRODUCCIÓN DE SISTEMAS IDS/IPS

1. Análisis previo
2. Definición de políticas de corte de intentos de intrusión en los IDS/IPS
3. Análisis de los eventos registrados por el IDS/IPS
4. Relación de los registros de auditoría del IDS/IPS
5. Establecimiento de los niveles requeridos de actualización, monitorización y pruebas del IDS/IPS

UNIDAD DIDÁCTICA 3. CONTROL MALWARE

1. Sistemas de detección y contención de Malware
2. Herramientas de control de Malware
3. Criterios de seguridad para la configuración de las herramientas de protección frente a Malware

4. Determinación de los requerimientos y técnicas de actualización de las herramientas de protección frente a Malware
5. Relación de los registros de auditoría de las herramientas de protección frente a Malware
6. Establecimiento de la monitorización y pruebas de las herramientas de protección frente a Malware
7. Análisis de Malware mediante desensambladores y entornos de ejecución controlada

UNIDAD DIDÁCTICA 4. RESPUESTA ANTE INCIDENTES DE SEGURIDAD

1. Procedimiento de recolección de información relacionada con incidentes de seguridad
2. Exposición de las distintas técnicas y herramientas utilizadas para el análisis y correlación de información y eventos de seguridad
3. Proceso de verificación de la intrusión
4. Naturaleza y funciones de los organismos de gestión de incidentes tipo CERT nacionales e internacionales

UNIDAD DIDÁCTICA 5. PROCESO DE NOTIFICACIÓN Y GESTIÓN DE INTENTOS DE INTRUSIÓN

1. Establecimiento de las responsabilidades
2. Categorización de los incidentes derivados de intentos de intrusión
3. Establecimiento del proceso de detección y herramientas de registro de incidentes
4. Establecimiento del nivel de intervención requerido en función del impacto previsible
5. Establecimiento del proceso de resolución y recuperación de los sistemas
 1. - Respaldo y recuperación de los datos
 2. - Actualización del Plan de Recuperación
 3. - Errores comunes al formular un DRP
6. Proceso para la comunicación del incidente a terceros

UNIDAD DIDÁCTICA 6. ANÁLISIS FORENSE INFORMÁTICO

1. Conceptos generales y objetivos del análisis forense
 1. - Tipos de análisis forense
2. Exposición del Principio de Lockard
3. Guía para la recogida de evidencias electrónicas
 1. - Evidencias volátiles y no volátiles
 2. - Etiquetado de evidencias
 3. - Cadena de custodia
 4. - Ficheros y directorios ocultos
 5. - Información oculta del sistema
 6. - Recuperación de ficheros borrados
4. Guía para el análisis de las evidencias electrónicas recogidas
5. Guía para la selección de las herramientas de análisis forense

MÓDULO 7. SERVICIOS LEGALTECH

UNIDAD DIDÁCTICA 1. NECESIDADES DEL SECTOR LEGAL

1. La legislación española reguladora de la actividad debido a la aparición de necesidades determinadas del sector

2. El surgimiento de los bufetes online: necesidades legislativas
 1. - El ciberespacio
3. Grado de protección exigido legalmente
 1. - Legislación correspondiente

UNIDAD DIDÁCTICA 2. IDEAS DE NEGOCIO. BUSINESS IDEA

1. La generación de ideas de negocio
2. Elección de una estrategia de negocio viable
 1. - Estudio de viabilidad
 2. - Tipos de viabilidad
3. Focalización de la atención en un tipo de negocio concreto
 1. - Identificación de barreras de entrada
4. Business plan. El plan de negocio
5. La innovación en el desarrollo de proyectos
 1. - La importancia de la innovación en los negocios
 2. - La innovación en el desarrollo de proyectos legaltech: ciberabogado

UNIDAD DIDÁCTICA 3. VENTAJAS DE ESTOS PROYECTOS PARA PROFESIONALES Y CLIENTES

1. Requisitos para el éxito de los proyectos Legaltech: el despacho virtual
 1. - Puntos clave para el éxito o fracaso del proyecto
 2. - Definición de la misión del proyecto Legaltech para garantizar el éxito
2. Ventajas de los proyectos Legaltech para los profesionales
 1. - Tipos de ventajas
3. Ventajas de los proyectos Legaltech para los clientes
 1. - Tipos de ventajas

UNIDAD DIDÁCTICA 4. PROTECCIÓN JURÍDICA DEL SOFTWARE

1. El software de los proyectos Legaltech y su protección a nivel legal
2. Derecho de autor
 1. - Derechos protegidos
 2. - Limitaciones de los derechos
 3. - Vigencia, propiedad, ejercicio y cesión del derecho de autor
3. Patentes
 1. - Fundamentos jurídicos de las patentes
 2. - Fundamentos económicos de las patentes
4. LCD (Competencia desleal)
 1. - Modelos teóricos de competencia
 2. - Tipos y acciones de competencia desleal

UNIDAD DIDÁCTICA 5. PROTECCIÓN JURÍDICA DE LAS BASES DE DATOS

1. Las bases de datos
 1. - Tipos y características
 2. - Estructura de una base de datos
 3. - Funciones
 4. - Organización

2. Regulación normativa de la protección jurídica de las bases de datos
 1. - Derecho de autor
 2. - Derecho "sui generis"

UNIDAD DIDÁCTICA 6. CLOUD COMPUTING

1. Orígenes del cloud computing
2. Cloud computing: aspectos generales
 1. - Definición de cloud computing
3. Características del cloud computing
4. La nube y los negocios
 1. - Beneficios específicos
5. Modelos básicos en la nube

UNIDAD DIDÁCTICA 7. BIG DATA

1. ¿Qué es Big Data?
 1. - ¿Por qué se genera tanta información?
 2. - La era de las grandes cantidades de información: historia del big data
2. La importancia de almacenar y extraer información
 1. - Herramientas y tecnologías para manejo de Big Data
3. Reglas para los Big Data
4. Big Data enfocado a los negocios

MÓDULO 8. TECNOLOGÍA Y SECTOR LEGAL

UNIDAD DIDÁCTICA 1. SERVICIOS DE LA SOCIEDAD DE LA INFORMACIÓN

1. Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI): Ley - de 11 de Julio
 1. - Objeto de la LSSI-CE
 2. - Ámbito de aplicación de la LSSI-CE
 3. - Obligaciones de los prestadores de servicios respecto a la ley
 4. - Responsabilidad de los Prestadores de Servicios que realizan Copia Temporal de los Datos Solicitados por los Usuarios
 5. - Responsabilidad de los Prestadores de Servicios de Alojamiento o Almacenamiento de Datos
 6. - Responsabilidad de los Prestadores de Servicios que Faciliten Enlaces a Contenidos o Instrumentos de Búsqueda
 7. - Colaboración ente los Prestadores de Servicios de Intermediación
2. Régimen Sancionador
3. Principales Normas de Ordenación del Comercio Electrónico

UNIDAD DIDÁCTICA 2. ADMINISTRACIÓN ELECTRÓNICA I

1. El Derecho a la información: concepto y tipo de información administrativa
2. La Sociedad de la Información en la Administración Pública
3. Actuaciones que responden a la modernización de la atención en las Administraciones Públicas
4. Ventanilla única

5. Portal de información Administrativa
6. Elaboración y Actualización de Guías de Servicios
7. Teléfonos de información administrativa
8. Puntos de información administrativa
9. Medición de la satisfacción del ciudadano en la prestación del servicio
10. Sistema de Quejas y Sugerencias
11. Medición de la satisfacción del ciudadano
12. La implantación de un registro telemático único

UNIDAD DIDÁCTICA 3. ADMINISTRACIÓN ELECTRÓNICA II

1. Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas
2. Funcionamiento Electrónico del Sector Público
3. Sede Electrónica y Portal Internet
 1. - Sede Electrónica
 2. - Portal Internet
4. Sistema de identificación de las Administraciones Públicas
5. Actuación Administrativa Automatizada. Sistema de firma
6. Firma electrónica del personal al servicio de las Administraciones Públicas
7. Intercambio electrónico de datos en entornos cerrados de comunicación
8. Aseguramiento e interoperabilidad de la firma electrónica
9. Archivo electrónico de documentos
10. Funcionamiento Electrónico de la Administración. Herramientas Disponibles

UNIDAD DIDÁCTICA 4. NORMATIVA SOBRE TELECOMUNICACIONES

1. Normativa sobre Telecomunicaciones
2. Ley de 9 de mayo, General sobre Telecomunicaciones
3. Objeto y Ámbito de Aplicación
4. Objetivos y Principios de la Normativa
5. Servicios Públicos

UNIDAD DIDÁCTICA 5. CIBERSEGURIDAD Y CUMPLIMIENTO NORMATIVO I

1. Privacidad y seguridad de la información: marco legal y jurídico
 1. - Normas sobre gestión de la seguridad de la información: familia de las normas ISO 27000
 2. - Bases de datos: cloud computing
 3. - Direcciones de correo electrónico
 4. - El uso de Cookies
2. Gestión de sistemas de seguridad de la información y ciberinteligencia: introducción y conceptos básicos
 1. - ¿Qué es la seguridad de la información?
 2. - Importancia de la seguridad de la información
 3. - Diseño, desarrollo e implantación
3. Normativa esencial sobre el sistema de gestión de la seguridad de la información (SGSI)
 1. - Estándares y Normas Internacionales sobre los SGSI
 2. - Legislación: leyes aplicables a los SGSI

UNIDAD DIDÁCTICA 6. CIBERSEGURIDAD Y CUMPLIMIENTO NORMATIVO II

1. Política de seguridad: Análisis y gestión de riesgos
 1. - Plan de implantación del SGSI
 2. - Análisis de riesgos: Introducción
 3. - Gestión de riesgos
2. Auditoría de seguridad informática
 1. - Criterios generales
 2. - Herramientas para la auditoria de sistemas
 3. - Descripción de los aspectos sobre cortafuegos en auditorías de sistemas de información
 4. - Guías para la ejecución de las distintas fases de la auditoria de sistemas de información

