EUROINNOVA
INTERNATIONAL ONLINE EDUCATION

INEAF
BUSINESS SCHOOL

Curso Experto en Business Intelligence y Seguridad de la información + Titulación Universitaria

Elige aprender en la escuela
líder en formación online

ÍNDICE

Ver en la web

INEAF BUSINESS SCHOOL

SOMOS INEAF

INEAF es una institución especializada en **formación online fiscal y jurídica.** El primer nivel de nuestro claustro y un catálogo formativo en constante actualización nos hacen convertirnos en una de las principales instituciones online del sector.

Los profesionales en activo y recién graduados reciben de INEAF una alta cualificación que se dirige a la formación de especialistas que se integren en el mercado laboral o mejoren su posición en este. Para ello, empleamos **programas formativos prácticos y flexibles con los que los estudiantes podrán compaginar el estudio con su vida personal y profesional.** Un modelo de formación que otorga todo el protagonismo al estudiante.

Ver en la web

INEAF BUSINESS SCHOOL

Fórmate, crece, desafía lo convencional,

Elige INEAF

QS, sello de excelencia académica

INEAF: 5 estrellas en educación online

RANKINGS DE INEAF

La empresa **INEAF** ha conseguido el reconocimiento de diferentes rankings a nivel nacional e internacional, gracias a sus programas formativos y flexibles, así como un modelo de formación en el que el alumno es el protagonista.

Para la elaboración de estos rankings, se emplean indicadores como la reputación online y offline, la calidad de la institución, el perfil de los profesionales.

QS STARS™ RATING SYSTEM

★ ★ ★ ★ ★

Online Learning

EL MUNDO

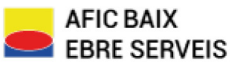
NOSOLOMASTER | RANKING Y OPINIONES SOBRE MASTER

FM

Ver en la web

INEAF BUSINESS SCHOOL

ALIANZAS Y ACREDITACIONES



Ver en la web

BY EDUCA EDTECH

INEAF 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.

EDUCA EDTECH Group

ONLINE EDUCATION

EUROINNOVA INTERNATIONAL ONLINE EDUCATION

inesem business school

INEAF BUSINESS SCHOOL

red educa.net

inesalud

EDU SPORT

EDUCA business school

educaopen tech school

Educa.Pro

ceupe European Business School

ESIBE ESCUELA IBEROAMERICANA DE POSTGRADO

CAPMAN testing solutions

UDAVINCI

Structuralia Engineering eLearning

Ver en la web

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.

Programas

PROPIOS UNIVERSITARIOS OFICIALES

RAZONES POR LAS QUE ELEGIR INEAF

1. Nuestra Experiencia

- ✓ Más de **18 años** de experiencia
- ✓ Más de **300.000** alumnos ya se han formado en nuestras aulas virtuales
- ✓ Alumnos de los 5 continentes
- ✓ **25%** de alumnos internacionales.
- ✓ **97%** de satisfacción
- ✓ **100% lo recomiendan.**
- ✓ Más de la mitad ha vuelto a estudiar en INEAF.

2. Nuestro Equipo

En la actualidad, INEAF cuenta con un equipo humano formado por más de **400 profesionales.** Nuestro personal se encuentra sólidamente enmarcado en una estructura que facilita la mayor calidad en la atención al alumnado.

3. Nuestra Metodología

100% ONLINE

Estudia cuando y desde donde quieras. Accede al campus virtual desde cualquier dispositivo.

APRENDIZAJE

Pretendemos que los nuevos conocimientos se incorporen de forma sustantiva en la estructura cognitiva

EQUIPO DOCENTE

INEAF cuenta con un equipo de profesionales que harán de tu estudio una experiencia de alta calidad educativa.

NO ESTARÁS SOLO

Acompañamiento por parte del equipo de tutorización durante toda tu experiencia como estudiante

Ver en la web

INEAF BUSINESS SCHOOL

4. Calidad AENOR

- ✓ Somos Agencia de Colaboración Nº99000000169 autorizada por el Ministerio de Empleo y Seguridad Social.
- ✓ Se llevan a cabo auditorías externas anuales que garantizan la máxima calidad AENOR.
- ✓ Nuestros procesos de enseñanza están certificados por **AENOR** por la ISO 9001.

5. Confianza

Contamos con el sello de **Confianza Online** y colaboramos con la Universidades más prestigiosas, Administraciones Públicas y Empresas Software a nivel Nacional e Internacional.

6. Somos distribuidores de formación

Como parte de su infraestructura y como muestra de su constante expansión Euroinnova incluye dentro de su organización una **editorial y una imprenta digital industrial.**

MÉTODOS DE PAGO

Con la Garantía de:

educapay

Fracciona el pago de tu curso en cómodos plazos y sin interéres de forma segura.

mastercard maestro VISA PayPal

bizum amazon pay Pay G Pay

Nos adaptamos a todos los métodos de pago internacionales:

OXXO mercado pago DISCOVER efecty Diners Club INTERNATIONAL CMR Falabella

y muchos mas...

Curso Experto en Business Intelligence y Seguridad de la información + Titulación Universitaria

DURACIÓN
350 horas

MODALIDAD
ONLINE

ACOMPAÑAMIENTO PERSONALIZADO

CREDITOS
8 ECTS

Titulación

Titulación Múltiple: Título Propio Experto en Business Intelligence y Seguridad de la información expedido por el Instituto Europeo de Asesoría Fiscal(INEAF) + Título Propio Universitario en Curso Superior Universitario en Protección de Datos en la Empresa (RGPD) con 200 horas y 8 créditos ECTS por la Universidad Católica de Murcia

Descripción

En la actualidad, es infinita la cantidad de información que puede obtenerse a través de un móvil o cualquier otro aparato electrónico. Con ello, la realidad ha dado lugar al llamado Business Intelligence, Ciberseguridad y a la Protección de Datos. La nueva normativa en este campo y las necesidades de las empresas han provocado una revolución en el mercado laboral, solicitando, cada vez más, profesionales en la materia, para así atender a las necesidades y obligaciones exigidas. Sin duda, este curso responde a las necesidades del sector.

Ver en la web

Objetivos

- Ofrecer un concepto de Business Intelligence y las necesidades que origina en la actualidad.
- Conocer el nuevo marco normativo de protección de datos personales y el cumplimiento de obligaciones en la empresa.
- Ampliar la información sobre la
- Gestionar y conocer las distintas herramientas aplicables para la seguridad de la información.
- Aprender a gestionar las Incidentes de Seguridad Informática

A quién va dirigido

Dirigido a directivos y altos mandos de empresas que recaben y traten datos personales y otro tipo de información. También útil para informáticos y futuros trabajadores del sector de la informática. Estudiantes del Grado en Ingeniería Informática.

Para qué te prepara

El mundo de la seguridad de la información ha sufrido en estos últimos años una importante transformación. El alumno de este curso desarrollará todos los conocimientos necesarios para obtener, tratar y analizar los datos existentes, de una forma segura y bajo las exigencias impuestas con arreglo a la normativa actualizada, utilizando los mecanismos y herramientas adecuadas. Se convertirá con ello en un profesional en el sector y así alcanzar sus objetivos laborales.

Salidas laborales

Expertos en la seguridad de la información y Delegados de Protección de Datos. Informáticos y personal del departamento de informática de todo tipo de empresas que traten con datos. Empleados de empresas relacionadas con el sector Mobile.

TEMARIO

MÓDULO 1. 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 2. 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 adopta
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 3. PROTECCIÓN DE DATOS EN LA EMPRESA (RGPD)

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. ANÁLISIS Y GESTIÓN DE RIESGOS DE LOS TRATAMIENTOS DE DATOS PERSONALES

1. Introducción. Marco general de la Evaluación y Gestión de Riesgos. Conceptos generales
2. Evaluación de Riesgos. Inventario y valoración de activos. Inventario y valoración de amenazas. Salvaguardas existentes y valoración de su protección. Riesgo resultante
3. Gestión de Riesgos. Conceptos. Implementación. Selección y asignación de salvaguardas a amenazas. Valoración de la protección. Riesgo residual, riesgo aceptable y riesgo asumible

UNIDAD DIDÁCTICA 11. PROGRAMA DE CUMPLIMIENTO DE PROTECCIÓN DE DATOS Y SEGURIDAD EN UNA ORGANIZACIÓN

1. El diseño y la Implantación del Programa de Protección de Datos en el contexto de la organización
2. Objetivos del Programa de Cumplimiento
3. Accountability: La Trazabilidad del Modelo de Cumplimiento

UNIDAD DIDÁCTICA 12. EVALUACIÓN DE IMPACTO DE PROTECCIÓN DE DATOS “EIPD”

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

UNIDAD DIDÁCTICA 13. LA AUDITORÍA DE PROTECCIÓN DE DATOS

1. La Auditoría de Protección de Datos
2. El Proceso de Auditoría. Cuestiones generales y aproximación a la Auditoría. Características básicas de la Auditoría
3. Elaboración del Informe de Auditoría. Aspectos básicos e importancia del Informe de Auditoría
4. Ejecución y seguimiento de Acciones Correctoras

Solicita información sin compromiso

¡Matricularme ya!

Teléfonos de contacto

España	+34 900 831 200	Argentina	54-(11)52391339
Bolivia	+591 50154035	Estados Unidos	1-(2)022220068
Chile	56-(2)25652888	Guatemala	+502 22681261
Colombia	+57 601 50885563	Mexico	+52-(55)11689600
Costa Rica	+506 40014497	Panamá	+507 8355891
Ecuador	+593 24016142	Perú	+51 1 17075761
El Salvador	+503 21130481	República Dominicana	+1 8299463963

!Encuéntranos aquí!

Edificio Educa Edtech

Camino de la Torrecilla N.º 30 EDIFICIO EDUCA EDTECH,
C.P. 18.200, Maracena (Granada)

formacion@euroinnova.com

www.euroinnova.com

Horario atención al cliente

Lunes a viernes: 9:00 a 20:00h Horario España

¡Síguenos para estar al tanto de todas nuestras novedades!

España

Latino America

Reública Dominicana

Ver en la web

INEAF BUSINESS SCHOOL

INEAF
BUSINESS SCHOOL

By
EDUCA EDTECH
Group