



EUROINNOVA
INTERNATIONAL ONLINE EDUCATION



INEAF
BUSINESS SCHOOL

Curso Experto en Derecho y Normativa del Tratamiento de Datos





Elige aprender en la escuela
líder en formación online

ÍNDICE

1 | Somos INEAF

2 | Rankings

3 | Alianzas y acreditaciones

4 | By EDUCA
EDTECH
Group

5 | Metodología
LXP

6 | Razones por
las que
elegir Ineaf

7 | Financiación
y Becas

8 | Métodos de
pago

9 | Programa
Formativo

10 | Temario

11 | Contacto

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.

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

[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.



Ver en la web

ALIANZAS Y ACREDITACIONES



Ver en la web



INEAF
BUSINESS SCHOOL

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.



ONLINE EDUCATION



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

4. Calidad AENOR

- ✓ Somos Agencia de Colaboración N°99000000169 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:



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



Nos adaptamos a todos los métodos de pago internacionales:



y muchos mas...



[Ver en la web](#)



INEAF
BUSINESS SCHOOL

Curso Experto en Derecho y Normativa del Tratamiento de Datos



DURACIÓN
250 horas



**MODALIDAD
ONLINE**



**ACOMPañAMIENTO
PERSONALIZADO**

Titulación

Titulación expedida por el Instituto Europeo de Asesoría Fiscal (INEAF), avalada por el Instituto Europeo de Estudios Empresariales (INESEM) "Enseñanza no oficial y no conducente a la obtención de un título con carácter oficial o certificado de profesionalidad."

Descripción

En virtud de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales encargada de desarrollar el RGPD en nuestro país, han sido muchas las nuevas obligaciones que deben aplicarse en materia de privacidad y datos personales en la empresa. Con esta normativa tan cambiante han surgido multitud de ofertas profesionales en este sector, con el Experto en Derecho y normativa del tratamiento de datos conocerá todas las herramientas y conceptos normativos para aplicar correctamente esta ley.

Objetivos

- Conocer en detalle la normativa en vigor en materia de protección de datos.
- Estudiar los principios de protección de datos, así como la base de esta legislación: la responsabilidad proactiva sobre la protección de datos.
- Aplicar técnicas de evaluación de impacto y gestión de riesgos en el tratamiento de datos personales.
- Adquirir conocimientos suficientes para aplicar un plan de cumplimiento en materia de protección de datos en una empresa.

Ver en la web



INEAF
BUSINESS SCHOOL

- Identificar las funciones y responsabilidades del Delegado de Protección de datos.
- Estudiar los principales conceptos de la ley de servicios de la sociedad de la información y de la Ley General de Telecomunicaciones.

A quién va dirigido

El Experto en Derecho y normativa del tratamiento de datos está orientada a cualquier persona interesada en privacidad, protección de datos en la empresa. Así mismo, está dirigido a estudiantes que deseen especializarse en esta área de gran importancia en la actualidad.

Para qué te prepara

Con la realización del Experto en Derecho y normativa del tratamiento de datos, el alumnado estará capacitado profesionalmente para conocer con todo detalle todos los aspectos en materia de protección de datos y privacidad, conocerá las principales funciones del delegado de Protección de datos, siendo capaz de asesorar, diseñar e implantar un plan de protección de datos personales en cualquier organización.

Salidas laborales

Experto en protección de datos y privacidad, Delegado de protección de datos, Abogado especializado en protección de datos personales, Asesor en materia de protección de datos, Compliance Officer

TEMARIO

MÓDULO 1. FUNDAMENTOS LEGALES PARA EL TRATAMIENTO DE DATOS PERSONALES

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
 1. - Antecedentes
 2. - Propuesta de reforma de la Directiva 95/46/CE
4. La Protección de Datos en España
5. Estándares y buenas prácticas

UNIDAD DIDÁCTICA 2. Reglamento Europeo de Protección de Datos (RGPD) y la Ley Orgánica 3/2018, de 5 diciembre, de protección de datos personales y garantía de los derechos digitales (LOPDGDD). Fundamentos

1. El Reglamento UE 2016/679
2. Ámbito de aplicación del RGPD
3. Definiciones
 1. - Otras 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 y la LOPDGDD

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
 1. - Impugnación de valoraciones
 2. - Tutela de derechos
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 y la LOPDGDD

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
 1. - Relaciones Responsable - Encargado
 2. - Encargados, sub-encargado, etc.
 3. - El contrato de Encargo
3. El Registro de Actividades de Tratamiento: identificación y clasificación del tratamiento de datos
 1. - 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
 1. - La supervisión de los códigos de conducta
 2. - Certificaciones

UNIDAD DIDÁCTICA 8. El Delegado de Protección de Datos (DPD, DPO o Data Privacy Officer) en el RGPD y la LOPDGDD

1. El Delegado de Protección de Datos (DPD)
2. Designación. Proceso de toma de decisión. Formalidades en el nombramiento, renovación y cese. Análisis de conflicto de intereses
3. Ejercicio de funciones: Obligaciones y responsabilidades. Independencia. Identificación y reporte a dirección
4. El DPD en el desarrollo de Sistemas de Información

5. Procedimientos. Colaboración, autorizaciones previas, relación con los interesados y gestión de reclamaciones
6. Comunicación con la Autoridad de Protección de Datos
7. Competencia profesional. Negociación. Comunicación. Presupuestos
8. Capacitación y Desempeño del DPO: Formación, Habilidades personales, Trabajo en equipo, Liderazgo, Gestión de equipos

UNIDAD DIDÁCTICA 9. Transferencias Internacionales de datos en el RGPD y la LOPDGDD

1. El Movimiento Internacional de Datos
2. El sistema de decisiones de adecuación
3. Transferencias mediante garantías adecuadas
4. Normas Corporativas Vinculantes
5. Excepciones
 1. - Supuestos sometidos a información previa
6. Autorización de la autoridad de control
 1. - Procedimiento de autorización a la AEPD
7. Suspensión temporal
8. Cláusulas contractuales
9. Ejercicio resuelto: Transferencias internacionales de datos

UNIDAD DIDÁCTICA 10. Las Autoridades de Control en el RGPD y la LOPDGDD

1. Autoridades de Control: Aproximación
 1. - Cooperación y Coherencia entre las distintas autoridades de Control
 2. - Instrumentos de Asistencia Mutua
 3. - El Mecanismo de Coherencia
 4. - El Procedimiento de Urgencia
2. Potestades
3. Régimen Sancionador
 1. - Sujetos responsables
 2. - Infracciones
 3. - Prescripción de las infracciones y sanciones
 4. - Procedimiento en caso de vulneración de la normativa de protección de datos
4. Comité Europeo de Protección de Datos (CEPD)
 1. - Supervisor Europeo de Protección de Datos (SEPD)
5. Procedimientos seguidos por la AEPD
6. La Tutela Jurisdiccional
7. El Derecho de Indemnización

UNIDAD DIDÁCTICA 11. Directrices de interpretación del RGPD

1. Grupo Europeo de Protección de Datos del Artículo 29 (WP 29)
2. Opiniones del Comité Europeo de Protección de Datos (CEPD)
3. Criterios de Órganos Jurisdiccionales

UNIDAD DIDÁCTICA 12. Normativas sectoriales afectadas por la Protección de Datos

1. Normativas sectoriales sobre Protección de Datos

2. Sanitaria, Farmacéutica, Investigación
3. Protección de los menores
4. Solvencia Patrimonial
5. Telecomunicaciones
6. Videovigilancia
7. Seguros, Publicidad y otros

UNIDAD DIDÁCTICA 13. Normativa española con implicaciones en Protección de Datos

1. Aproximación a la normativa estatal con implicaciones en Protección de Datos
2. LSSI, Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico
3. LGT, Ley 9/2014, de 9 de mayo, General de Telecomunicaciones
4. Ley Firma-e, Ley 59/2003, de 19 de diciembre, de Firma Electrónica
5. Otras normas de interés

UNIDAD DIDÁCTICA 14. Normativa europea con implicaciones en Protección de Datos

1. Normas de Protección de Datos de la UE
2. Directiva e-Privacy: Directiva 2002/58/CE del Parlamento Europeo y del Consejo de 12 de julio de 2002
3. Directiva 2009/136/CE del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009
4. Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo de 27 de abril de 2016

MÓDULO 2. RESPONSABILIDAD PROACTIVA EN EL TRATAMIENTO DE DATOS

UNIDAD DIDÁCTICA 1. 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
 1. - Guía para implantar el programa de protección de datos
2. Objetivos del Programa de Cumplimiento
3. Accountability: La Trazabilidad del Modelo de Cumplimiento

UNIDAD DIDÁCTICA 2. Seguridad de la Información

1. 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
 1. - Esquema Nacional de Seguridad
 2. - Directiva INS: 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
2. 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 la SI
 1. - Diferencias entre Seguridad de la Información y Seguridad Informática
 2. - Conceptos de Seguridad de la Información

3. - Alcance
4. - Estrategia de SI. El modelo PDCA
3. 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
 1. - Puesta en práctica de la seguridad de la información
 2. - Seguridad desde el diseño y por defecto
 3. - El ciclo de vida de los Sistemas de Información
 4. - Integración de la seguridad y la privacidad en el ciclo de vida
 5. - El control de calidad de los SI

UNIDAD DIDÁCTICA 3. Análisis y Gestión de Riesgos de los Tratamientos de Datos Personales

1. Introducción. Marco general de la Evaluación y Gestión de Riesgos. Conceptos generales
 1. - Impacto en la Protección de Datos
 2. - ¿Qué entendemos por "Riesgo"?
 3. - ¿Qué debemos entender por "aproximación basada en el riesgo"?
 4. - Otros conceptos
2. Evaluación de Riesgos. Inventario y valoración de activos. Inventario y valoración de amenazas. Salvaguardas existentes y valoración de su protección. Riesgo resultante
 1. - Principales tipos de vulnerabilidades
 2. - Particularidades de los distintos tipos de código malicioso
 3. - Principales elementos del análisis de riesgos y sus modelos de relaciones
 4. - Identificación de los activos involucrados en el análisis de riesgos y su valoración
 5. - Identificación de las amenazas que pueden afectar a los activos identificados previamente
 6. - Análisis e identificación de las vulnerabilidades existentes en los sistemas de información que permitirían la materialización de amenazas, incluyendo el análisis local
 7. - 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
 8. - Establecimiento de los escenarios de riesgo entendidos como pares activo-amenaza susceptibles de materializarse
 9. - Determinación de la probabilidad e impacto de materialización de los escenarios
 10. - Establecimiento del nivel de riesgo para los distintos pares de activo y amenaza
 11. - 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
 12. - Relación de las distintas alternativas de gestión de riesgos
 13. - Guía para la elaboración del plan de gestión de riesgos
 14. - Ejercicio resuelto Análisis de Riesgo: FACILITA_RGPD
3. Gestión de Riesgos. Conceptos. Implementación. Selección y asignación de salvaguardas a amenazas. Valoración de la protección. Riesgo residual, riesgo aceptable y riesgo asumible
 1. - Etapas en la gestión de riesgos
 2. - Valoración del riesgo, valoración de probabilidad y valoración de gravedad
 3. - Implicaciones en la protección de datos de la gestión de riesgos
 4. - Gestión de riesgos por defecto
 5. - Aplicación del proceso de gestión de riesgos y exposición de las alternativas más frecuentes
 6. - Metodologías comúnmente aceptadas de identificación y análisis de riesgos
 7. - Aplicación de controles y medidas de salvaguarda para obtener una reducción del riesgo

UNIDAD DIDÁCTICA 4. Metodologías de Análisis y Gestión de Riesgos

1. Metodologías de Análisis y Gestión de riesgos
 1. - Análisis de riesgos
 2. - Aproximación basada en riesgo del RGPD
 3. - Asignación de responsabilidades mediante RACI
 4. - Describir el ciclo de vida de los datos
 5. - Gestión de riesgos: Identificar, evaluar y tratar
2. Incidencias y recuperación
 1. - Notificación de brechas de seguridad
3. Principales metodologías
 1. - Octave
 2. - NIST SP 800-30
 3. - Magerit versión 3

UNIDAD DIDÁCTICA 5. 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
 1. - Origen, Concepto y Características de la EIPD
 2. - Alcance y necesidad
 3. - 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
 1. - Aspectos preparatorios de la ejecución de la EIPD
 2. - Análisis de la necesidad de hacer una Evaluación de Impacto
 3. - Descripción sistemática de las operaciones de tratamiento
 4. - Objetivos y finalidades del tratamiento. Evaluación de la necesidad y proporcionalidad de las operaciones de tratamiento
 5. - Gestión de Riesgo. Informe de Evaluación
 6. - La Consulta Previa
 7. - Ejercicio resuelto EIPD: GESTIONA_RGPD

MÓDULO 3. AUDITORÍA EN EL RGPD

UNIDAD DIDÁCTICA 1. 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

UNIDAD DIDÁCTICA 2. Auditoría de Sistemas de Información

1. La función de la Auditoría en los Sistemas de Información. Conceptos básicos. Estándares y Directrices de Auditoría de SI
 1. - Conceptos básicos
 2. - Estándares y Directrices de Auditoría de SI

2. Control interno y mejora continua. Buenas prácticas. Integración de la auditoría de protección de datos en la auditoría de SI
 1. - Buenas prácticas
 2. - Integración de la auditoría de protección de datos en la auditoría de SI
3. Planificación, ejecución y seguimiento

UNIDAD DIDÁCTICA 3. La Gestión de la Seguridad de los Tratamientos

1. Esquema Nacional de Seguridad, ISO/IEC 27001:2013 (Actualización a la norma UNE-EN ISO/IEC 27001:2017 Requisitos de sistemas de Gestión de Seguridad de la Información, SGSI)
2. Gestión de la Seguridad de los Activos. Seguridad lógica y en los procedimientos. Seguridad aplicada a las TI y a la documentación
 1. - Seguridad lógica y en los procedimientos
 2. - Seguridad aplicada a las TI y a la documentación
3. Recuperación de desastres y continuidad del Negocio. Protección de activos técnicos y documentales. Planificación y gestión de la Recuperación de Desastres
 1. - Protección de activos técnicos y documentales
 2. - Planificación y gestión de la Recuperación de Desastres

UNIDAD DIDÁCTICA 4. 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 5. 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 6. 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 7. 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 8. 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 9. 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 10. 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 11. 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

Solicita información sin compromiso

iMatricularme 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

!Encuétranos 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!



Ver en la web



INEAF
BUSINESS SCHOOL



INEAF
BUSINESS SCHOOL



By
EDUCA EDTECH
Group