



CURSO



Curso Experto en **Seguridad de los Datos y de la Información + Titulación Universitaria**



INEAF
BUSINESS SCHOOL

INEAF Business School



Índice

Curso Experto en **Seguridad de los Datos y de la Información + Titulación Universitaria**

1. Historia
2. Titulación Curso Experto en Seguridad de los Datos y de la Información + Titulación Universitaria

[Resumen](#) / [A quién va dirigido](#) / [Objetivos](#) / [Para que te prepara](#) / [Salidas Laborales](#) / [INEAF Plus](#)

3. Metodología de Enseñanza
4. Alianzas
5. Campus Virtual
6. Becas
7. Claustro Docente
8. Temario Completo



Historia

Ineaf Business School



En el año 1987 nace la primera promoción del Máster en Asesoría Fiscal impartido de forma presencial, a sólo unos metros de la histórica Facultad de Derecho de Granada. Podemos presumir de haber formado a profesionales de éxito durante las 27 promociones del Máster presencial, entre los que encontramos abogados, empresarios, asesores fiscales, funcionarios, directivos, altos cargos públicos, profesores universitarios...

El Instituto Europeo de Asesoría Fiscal INEAF ha realizado una apuesta decidida por la innovación y nuevas tecnologías, convirtiéndose en una Escuela de Negocios líder en formación fiscal y jurídica a nivel nacional.

Ello ha sido posible gracias a los cinco pilares que nos diferencian:

- **Claustro** formado por profesionales en ejercicio.
- **Metodología y contenidos** orientados a la práctica profesional.
- **Ejemplos y casos prácticos** adaptados a la realidad laboral.
- **Innovación** en formación online.
- **Acuerdos** con Universidades.



Curso Experto en **Seguridad de los Datos y de la Información + Titulación Universitaria**

DURACIÓN	450 H
PRECIO	1299 €
CRÉDITOS ECTS	16
MODALIDAD	Online

Entidad impartidora:

INEAF - Instituto Europeo de Asesoría Fiscal



Programa de Becas / Financiación 100% Sin Intereses

Titulación Curso Experto

Titulación Múltiple:

- Título Propio Experto en Seguridad de los Datos y de la Información expedido por el Instituto Europeo de Asesoría Fiscal(INEAF). “Enseñanza no oficial y no conducente a la obtención de un título con carácter oficial o certificado de profesionalidad.”
- Título Propio Universitario en Ciberseguridad: Seguridad desde el punto de vista empresarial y técnico Expedida por la Universidad Antonio de Nebrija con 8 créditos ECTS
- Título Propio Universitario en Compliance Officer Expedida por la Universidad Antonio de Nebrija con 8 créditos ECTS



Resumen

Los datos se han convertido en un activo muy importante a la hora de tomar decisiones que generen ventajas competitivas dentro del mundo empresarial, por lo que la información y la obtención de datos se han convertido en tarea imprescindible para las empresas. Con el Curso en Seguridad de los datos y de la información podrás gestionar la toma de información de la empresas y protegerla de forma segura.

A quién va dirigido

Dirigido a tanto al personal de la empresa, sobre todo a informáticos o empresarios, conocimientos de gran valor para el sector de la gestión de datos, además de servir como formación complementaria y especialización a estudiantes del Grado ingeniería informática o ADE que busquen incorporarse al mercado laboral.

Objetivos

Con el Curso Experto en ***Seguridad de los Datos y de la Información + Titulación Universitaria*** usted alcanzará los siguientes objetivos:

- Principios básicos de la seguridad informática
- Diseñar sistemas de gestión de seguridad de la información
- Conocimiento del marco normativo
- Implantar la figura del Compliance Officer
- Análisis de riesgos en el ámbito normativo

¿Y, después?

INEAF *Plus*. Descubre las ventajas

SISTEMA DE CONVALIDACIONES INEAF

La organización modular de nuestra oferta formativa permite formarse paso a paso; si ya has estado matriculado con nosotros y quieres cursar nuevos estudios solicita tu plan de convalidación. No tendrás que pagar ni cursar los módulos que ya tengas superados.

ACCESO DE POR VIDA A LOS CONTENIDOS ONLINE

Aunque haya finalizado su formación podrá consultar, volver a estudiar y mantenerse al día, con acceso de por vida a nuestro Campus y sus contenidos sin restricción alguna.

CONTENIDOS ACTUALIZADOS

Toda nuestra oferta formativa e información se actualiza permanentemente. El acceso ilimitado a los contenidos objetode estudio es la mejor herramienta de actualización para nuestros alumno/as en su trabajo diario.

DESCUENTOS EXCLUSIVOS

Los antiguos alumno/as acceden de manera automática al programa de condiciones y descuentos exclusivos de INEAF Plus, que supondrá un importante ahorro económico para aquellos que decidan seguir estudiando y así mejorar su currículum o carta de servicios como profesional.



OFERTAS DE EMPLEO Y PRÁCTICAS

Desde INEAF impulsamos nuestra propia red profesional entre nuestros alumno/as y profesionales colaboradores. La mejor manera de encontrar sinergias, experiencias de otros compañeros y colaboraciones profesionales.

NETWORKING

La bolsa de empleo y prácticas de INEAF abre la puerta a nuevas oportunidades laborales. Contamos con una amplia red de despachos, asesorías y empresas colaboradoras en todo el territorio nacional, con una importante demanda de profesionales con formación cualificada en las áreas legal, fiscal y administración de empresas.

¿PARA QUÉ TE PREPARA?

El curso en Seguridad de los datos y de la Información aporta los conocimientos teóricos y prácticos para diseñar y definir las estrategias en materia de seguridad de la información dentro de la empresa, para obtener un entorno de seguridad de los datos, gestionando todos los datos que se nos proporcionen a la empresa manteniendo siempre una correcta normativa.

SALIDAS LABORALES

En INEAF ofrecemos oportunidades de formación sin importar horarios, movilidad, distancia geográfica o conciliación.

Nuestro método de estudio online se basa en la integración de factores formativos y el uso de las nuevas tecnologías. Nuestro equipo de trabajo se ha fijado el objetivo de integrar ambas áreas de forma que nuestro alumnado interactúe con un CAMPUS VIRTUAL ágil y sencillo de utilizar. Una plataforma diseñada para facilitar el estudio, donde el alumnado obtenga todo el apoyo necesario, ponemos a disposición del alumnado un sinfín de posibilidades de comunicación.

Nuestra metodología de aprendizaje online, está totalmente orientada a la práctica, diseñada para que el alumnado avance a través de las unidades didácticas siempre prácticas e ilustradas con ejemplos de los distintos módulos y realice las Tareas prácticas (Actividades prácticas, Cuestionarios, Expedientes prácticos y Supuestos de reflexión) que se le irán proponiendo a lo largo del itinerario formativo.

Al finalizar el máster, el alumnado será capaz de transformar el conocimiento académico en conocimiento profesional.

metodología INEAF



Profesorado y servicio de tutorías

Todos los profesionales del Claustro de INEAF compatibilizan su labor docente con una actividad profesional (Inspectores de Hacienda, Asesores, Abogados ...) que les permite conocer las necesidades reales de asesoramiento que exigen empresas y particulares. Además, se encargan de actualizar continuamente los contenidos para adaptarlos a todos los cambios legislativos, jurisprudenciales y doctrinales.

Durante el desarrollo del programa el alumnado contará con el apoyo permanente del departamento de tutorización. Formado por especialistas de las distintas materias que ofrecen al alumnado una asistencia personalizada a través del servicio de tutorías on-line, teléfono, chat, clases online, seminarios, foros ... todo ello desde nuestro CAMPUS Online.

Materiales didácticos

Al inicio del programa el alumnado recibirá todo el material asociado al máster en papel. Estos contenidos han sido elaborados por nuestro claustro de expertos bajo exigentes criterios de calidad y sometido a permanente actualización. Nuestro sistema de Campus online permite el acceso ilimitado a los contenidos online y suministro gratuito de novedades y actualizaciones que hacen de nuestros recursos una valiosa herramienta para el trabajo diario.

Alianzas

En INEAF, las **relaciones institucionales** desempeñan un papel fundamental para mantener el máximo grado de excelencia en nuestra oferta formativa y situar a nuestros alumno/as en el mejor escenario de oportunidades laborales y relaciones profesionales.



ASOCIACIONES Y COLEGIOS PROFESIONALES

Las alianzas con asociaciones, colegios profesionales, etc. posibilitan el acceso a servicios y beneficios adicionales a nuestra comunidad de alumno/as.



EMPRESAS Y DESPACHOS

Los acuerdos estratégicos con empresas y despachos de referencia nos permiten nutrir con un especial impacto todas las colaboraciones, publicaciones y eventos de INEAF. Constituyendo INEAF un cauce de puesta en común de experiencia.

CALIDAD

PRÁCTICO

ACTUALIZADO

Si desea conocer mejor nuestro Campus Virtual puede acceder como invitado al curso de demostración a través del siguiente enlace:

alumnos.ineaf.es

campus virtual

En nuestro afán por adaptar el aprendizaje a la filosofía 3.0 y fomentar el empleo de los nuevos recursos tecnológicos en la empresa, **hemos desarrollado un Campus virtual (Plataforma Online para la Formación 3.0) exclusivo de última generación con un diseño funcional e innovador.**

Entre las herramientas disponibles encontrarás: servicio de tutorización, chat, mensajería y herramientas de estudio virtuales (ejemplos, actividades prácticas – de cálculo, reflexión, desarrollo, etc., vídeo-ejemplos y videotutoriales, además de “supercasos”, que abarcarán módulos completos y ofrecerán al alumnado una visión de conjunto sobre determinadas materias).

El Campus Virtual permite establecer contacto directo con el equipo de tutorización a través del sistema de comunicación, permitiendo el intercambio de archivos y generando sinergias muy interesantes para el aprendizaje.

El alumnado dispondrá de **acceso ilimitado a los contenidos** contando además con manuales impresos de los contenidos teóricos de cada módulo, que le servirán como apoyo para completar su formación.

En INEAF apostamos por tu formación y ofrecemos un **Programa de becas y ayudas al estudio**. Somos conscientes de la importancia de las ayudas al estudio como herramienta para garantizar la inclusión y permanencia en programas formativos que permitan la especialización y orientación laboral.

BECA DESEMPLEO, DISCAPACIDAD Y FAMILIA NUMEROSA	BECA ALUMNI	BECA EMPRENDE, GRUPO	BECA RECOMIENDA
Documentación a aportar (desempleo): • Justificante de encontrarse en situación de desempleo Documentación a aportar (discapacidad): • Certificado de discapacidad igual o superior al 33 %. Documentación a aportar (familia numerosa): • Se requiere el documento que acredita la situación de familia numerosa.	Documentación a aportar: • No tienes que aportar nada. ¡Eres parte de INEAF!	Documentación a aportar (emprende): • Estar dado de alta como autónomo y contar con la última declaración-liquidación del IVA. Documentación a aportar (grupo): • Si sois tres o más personas, podréis disfrutar de esta beca.	Documentación a aportar: • No se requiere documentación, tan solo venir de parte de una persona que ha estudiado en INEAF previamente.
20%	25%	15%	15%

Para más información puedes contactar con nosotros en el teléfono 958 050 207 y también en el siguiente correo electrónico: formacion@ineaf.es

El Claustro Docente de INEAF será el encargado de analizar y estudiar cada una de las solicitudes, y en atención a los **méritos académicos y profesionales** de cada solicitante decidirá sobre la concesión de **beca**.

A photograph of three people (two men and one woman) sitting at a wooden desk in a library or office setting. They are looking towards the camera. The background shows bookshelves filled with books. The text is overlaid on the image.

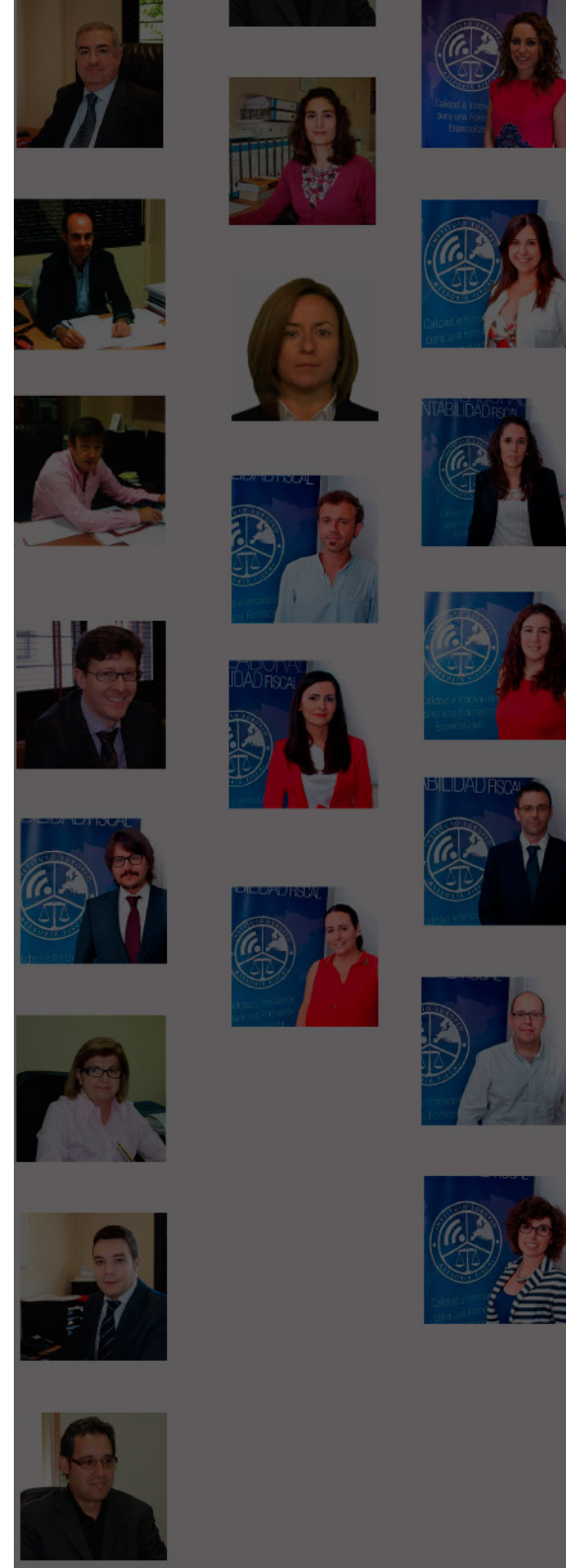
"Preparamos profesionales con casos prácticos,
llevando la realidad del mercado laboral a
nuestros Cursos y Másteres"

Claustro docente

Nuestro equipo docente está formado por Inspectores de Hacienda, Abogados, Economistas, Graduados Sociales, Consultores, ... Todos ellos profesionales y docentes en ejercicio, con contrastada experiencia, provenientes de diversos ámbitos de la vida empresarial que aportan aplicación práctica y directa de los contenidos objeto de estudio, contando además con amplia experiencia en impartir formación a través de las TICs.

Se ocupará además de resolver dudas al alumnado, aclarar cuestiones complejas y todas aquellas otras que puedan surgir durante la formación.

Si quieres saber más sobre nuestros docentes accede
a la seccion Claustro docente de nuestra web desde
aquí



Temario

Curso Experto en **Seguridad de los Datos y de la Información + Titulación Universitaria**



PROGRAMA ACADEMICO

Módulo 1. Ciberseguridad: seguridad desde el punto de vista empresarial y técnico

Módulo 2. Protección de datos en la empresa (rgpd)

Módulo 3. Derechos digitales

Módulo 4. Compliance officer

Módulo 1.

Ciberseguridad: seguridad desde el punto de vista empresarial y técnico

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
- 2. - ¿Qué es la seguridad de la información?
- 3. - Importancia de la seguridad de la información
- 4. Seguridad de la información: Diseño, desarrollo e implantación
- 5. - Descripción de los riesgos de la seguridad
- 6. - Selección de controles
- 7. Factores de éxito en la seguridad de la información
- 8. 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
- 2. - Familia de Normas ISO 27000
- 3. - La Norma UNE-EN-ISO/IEC 27001:2014
- 4. - Buenas prácticas en seguridad de la información, Norma ISO/IEC 27002
- 5. Normativa aplicable a los SGSI
- 6. - Normativa comunitaria sobre seguridad de la información
- 7. - Legislación Española sobre seguridad de la información
- 8. - 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
- 3. - Análisis de riesgos: Aproximación
- 4. - Principales tipos de vulnerabilidades, fallos de programa, programas maliciosos y su actualización permanente, así como criterios de programación segura
- 5. - Particularidades de los distintos tipos de código malicioso
- 6. - Principales elementos del análisis de riesgos y sus modelos de relaciones
- 7. - Metodologías cualitativas y cuantitativas de análisis de riesgos
- 8. - Identificación de los activos involucrados en el análisis de riesgos y su valoración
- 9. - Identificación de las amenazas que pueden afectar a los activos identificados previamente
- 10. - Análisis e identificación de las vulnerabilidades existentes en los sistemas de información que permitirían la materialización de amenazas, incluyendo el análisis local
- 11. - Optimización del proceso de auditoría y contraste de vulnerabilidades e informe de auditoría
- 12. - 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
- 13. - Establecimiento de los escenarios de riesgo entendidos como pares activo-amenaza susceptibles de materializarse
- 14. - Determinación de la probabilidad e impacto de materialización de los escenarios
- 15. - Establecimiento del nivel de riesgo para los distintos

- 20. - Exposición de la metodología Magerit
- 21. Gestión de riesgos
- 22. - Aplicación del proceso de gestión de riesgos y exposición de las alternativas más frecuentes
- 23. - Metodologías comúnmente aceptadas de identificación y análisis de riesgos
- 24. - 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
- 2. - Código deontológico de la función de auditoría
- 3. - Relación de los distintos tipos de auditoría en el marco de los sistemas de información
- 4. - Criterios a seguir para la composición del equipo auditor
- 5. - Tipos de pruebas a realizar en el marco de la auditoría, pruebas sustantivas y pruebas de cumplimiento
- 6. - Tipos de muestreo a aplicar durante el proceso de auditoría
- 7. - Utilización de herramientas tipo CAAT (Computer Assisted Audit Tools)
- 8. - Explicación de los requerimientos que deben cumplir los hallazgos de auditoría
- 9. - Aplicación de criterios comunes para categorizar los hallazgos como observaciones o no conformidades
- 10. - Relación de las normativas y metodologías relacionadas con la auditoría de sistemas de información comúnmente aceptadas
- 11. Aplicación de la normativa de protección de datos de carácter personal
- 12. - Normativa de referencia: Reglamento General de Protección de Datos y Ley Orgánica de Protección de Datos

- 20. - Herramientas de análisis de red, puertos y servicios tipo Nmap, Netcat, NBTScan, etc.
- 21. - Herramientas de análisis de vulnerabilidades tipo Nessus
- 22. - Analizadores de protocolos tipo WireShark, DSniff, Cain & Abel, etc.
- 23. - Analizadores de páginas web tipo Acunetix, Dirb, Parosproxy, etc
- 24. - Ataques de diccionario y fuerza bruta tipo Brutus, John the Ripper, etc.
- 25. Descripción de los aspectos sobre cortafuego en auditorías de sistemas de información
- 26. - Principios generales de cortafuegos
- 27. - Componentes de un cortafuegos de red
- 28. - Relación de los distintos tipos de cortafuegos por ubicación y funcionalidad
- 29. - Arquitecturas de cortafuegos de red
- 30. Guías para la ejecución de las distintas fases de la auditoría de sistemas de información
- 31. - Normas para la implantación de la auditoría de la documentación
- 32. - Instrucciones para la elaboración del plan de auditoría
- 33. - Pruebas de auditoría
- 34. - Instrucciones para la elaboración del informe de auditoría

- pares de activo y amenaza
- 16. - 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
- 17. - Relación de las distintas alternativas de gestión de riesgos
- 18. - Guía para la elaboración del plan de gestión de riesgos
- 19. - Exposición de la metodología NIST SP 800-30

UNIDAD DIDÁCTICA 5.

COMUNICACIONES SEGURAS: SEGURIDAD POR NIVELES

- 1. Seguridad a nivel físico
- 2. - Tipos de ataques
- 3. - Servicios de Seguridad
- 4. - Medidas de seguridad a adoptar
- 5. Seguridad a nivel de enlace
- 6. - Tipos de ataques
- 7. - Medidas de seguridad a adoptar
- 8. Seguridad a nivel de red
- 9. - Datagrama IP
- 10. - Protocolo IP
- 11. - Protocolo ICMP
- 12. - Protocolo IGMP
- 13. - Tipos de Ataques
- 14. - Medidas de seguridad a adopta
- 15. Seguridad a nivel de transporte
- 16. - Protocolo TCP
- 17. - Protocolo UDP
- 18. - Tipos de Ataques
- 19. - Medidas de seguridad a adoptar

- 20. Seguridad a nivel de aplicación
- 21. - Protocolo DNS
- 22. - Protocolo Telnet
- 23. - Protocolo FTP
- 24. - Protocolo SSH
- 25. - Protocolo SMTP
- 26. - Protocolo POP
- 27. - Protocolo IMAP
- 28. - Protocolo SNMP
- 29. - Protocolo HTTP
- 30. - Tipos de Ataques
- 31. - Medidas de seguridad a adoptar

- 13. - Principios generales de la protección de datos de carácter personal
- 14. - Legitimación para el tratamiento de datos personales
- 15. - Medidas de responsabilidad proactiva
- 16. - Los derechos de los interesados
- 17. - Delegado de Protección de Datos
- 18. Herramientas para la auditoría de sistemas
- 19. - Herramientas del sistema operativo tipo Ping, Traceroute, etc.

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
- 6. - Respaldo y recuperación de los datos
- 7. - Actualización del Plan de Recuperación
- 8. - Errores comunes al formular un DRP
- 9. Proceso para la comunicación del incidente a terceros

UNIDAD DIDÁCTICA 6.

ANÁLISIS FORENSE INFORMÁTICO

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

Módulo 2.

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

Módulo 3.

Derechos digitales

UNIDAD DIDÁCTICA 1.

DERECHOS BÁSICOS EN EL ENTORNO DIGITAL

- 1. Introducción. Los derechos en la Era digital
- 2. - Origen de la normativa
- 3. - La Agencia Española de Protección de Datos y los Derechos Digitales
- 4. Derecho a la Neutralidad de Internet
- 5. Derecho de Acceso universal a Internet
- 6. Ejercicio Resuelto: Derecho de Acceso universal a Internet
- 7. Derecho a la Seguridad Digital.
- 8. Derecho a la Educación Digital

UNIDAD DIDÁCTICA 2.

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
- 4. - Derecho al Olvido en Google
- 5. - Proceso ante Google

UNIDAD DIDÁCTICA 3.

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
5. - Medidas de seguridad sobre los datos de geolocalización
6. - La Geolocalización acorde con la Agencia Española de Protección de Datos
7. Ejercicio resuelto: Geolocalización acorde con la AEPD
8. Derechos digitales en la negociación colectiva

UNIDAD DIDÁCTICA 4.

DERECHOS DIGITALES EN LAS REDES SOCIALES

1. Derecho al olvido en servicios de redes sociales y servicios equivalentes
2. Derecho de portabilidad en servicios de redes sociales y servicios equivalentes

UNIDAD DIDÁCTICA 5.

DERECHOS DIGITALES DE LOS MENORES DE EDAD

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

UNIDAD DIDÁCTICA 6.

OTROS DERECHOS DIGITALES

1. Derecho al testamento digital
2. Utilización de medios tecnológicos y datos personales en las actividades electorales
3. Políticas de impulso de los Derechos Digitales
4. Compra Segura en Internet y Cloud Computing
5. - Compra segura en Internet: Detección de fraudes y precauciones en la contratación de servicios online y publicidad
6. - Ejercicio Resuelto: Compra segura en Internet
7. - Cloud Computing
8. Impuestos sobre determinados servicios digitales
9. Fingerprinting o Huella Digital del Dispositivo

UNIDAD DIDÁCTICA 7.

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

UNIDAD DIDÁCTICA 1. COMPLIANCE EN LA EMPRESA

- 1. Gobierno Corporativo
- 2. El Compliance en la empresa
- 3. Relación del compliance con otras áreas de la empresa
- 4. Compliance y Gobierno Corporativo

UNIDAD DIDÁCTICA 2. FUNCIONES DEL COMPLIANCE OFFICER

- 1. Funciones del Compliance Officer: Introducción
- 2. Estatuto y cualificación del Compliance Officer
- 3. - Estatuto del Compliance Officer
- 4. - La cualificación del Compliance Officer
- 5. El compliance officer dentro de la empresa
- 6. - Modelos de Compliance en la empresa
- 7. - Funciones del Compliance Officer en la empresa
- 8. La externalización del Compliance
- 9. Funciones Generales del Compliance officer
- 10. Responsabilidad del Compliance Officer
- 11. - Responsabilidad penal del Compliance Officer

UNIDAD DIDÁCTICA 3. LA FIGURA DEL COMPLIANCE OFFICER

- 1. Formación y Asesoramiento
- 2. - Asesoramiento
- 3. - Formación
- 4. Novedades de servicios, productos y proyectos
- 5. Servicio comunicativo y sensibilización
- 6. - Comunicación
- 7. - Sensibilización
- 8. Resolución práctica de incidencias e incumplimientos
- 9. - Detección
- 10. - Documentación
- 11. - Sistema Sancionador

UNIDAD DIDÁCTICA 4. APROXIMACIÓN AL COMPLIANCE PROGRAM

- 1. Beneficios para mi empresa del compliance program
- 2. Ámbito de actuación
- 3. Materias incluídas en un programa de cumplimiento
- 4. - Normativa del Sector Financiero
- 5. - Normativa del Sector Asegurador
- 6. - Normativa del Sector Farmacéutico
- 7. Objetivo del compliance program

UNIDAD DIDÁCTICA 5. EVALUACIÓN DE RIESGOS

- 1. Riesgo empresarial. Concepto general
- 2. Tipos de riesgos en la empresa
- 3. Identificación de los riesgos en la empresa
- 4. Estudio de los riesgos
- 5. Impacto y probabilidad de los riesgos en la empresa
- 6. Evaluación de los riesgos

UNIDAD DIDÁCTICA 6. CONTROLES DE RIESGOS

- 1. Políticas y Procedimientos
- 2. Controles de Procesos
- 3. Controles de Organización
- 4. Código Ético
- 5. Cultura de Cumplimiento

UNIDAD DIDÁCTICA 7. CONTROLES INTERNOS EN LA EMPRESA

- 1. Conceptos de Controles Internos
- 2. Realización de Controles e Implantación
- 3. Plan de Monitorización
- 4. Medidas de Control de acceso físicas y lógico
- 5. Otras medidas de control

UNIDAD DIDÁCTICA 8.

INVESTIGACIONES Y DENUNCIAS DENTRO DE LA EMPRESA

1. Necesidad de implantar un canal de denuncias en la empresa
2. Implantar un canal de denuncias internas
3. - Cana del denuncias: Características
4. - Personal implicado en un canal de denuncias y funciones
5. - Confidencialidad
6. Gestión de canal de denuncias internas
7. - Deberes y derechos de las partes
8. - Gestión del canal de denuncias internas en un grupo de empresas
9. - Riesgos por incumplimientos
10. Recepción y manejo de denuncias
11. Como tratar las denuncias
12. Investigación de una denuncia

UNIDAD DIDÁCTICA 9.

RESPONSABILIDAD PENAL DE LAS PERSONAS JURÍDICAS: CRITERIOS DE APLICACIÓN, ATENUACIÓN Y EXONERACIÓN

1. Introducción: Reformas tras las Leyes Orgánicas 5/2010 y 1/2015
2. Transmisión de la responsabilidad penal a las personas jurídicas
3. Artículo 319 del Código Penal
4. Compatibilidad de sanciones penales y administrativas. Principio “Ne bis in ídem”
5. La persona jurídica en la legislación penal
6. Imputación de responsabilidad a la persona jurídica
7. - Delito cometido por representantes o personas con capacidad de decisión, organización y control
8. - Delito cometido por un empleado
9. Delimitación de los delitos imputables a personas jurídicas
10. - Delitos imputables a personas jurídicas
11. Penas aplicables a las personas jurídicas
12. - Determinación de la pena
13. El procedimiento penal
14. - Tipos de procesos penales

UNIDAD DIDÁCTICA 10.

DELITOS IMPUTABLES A LAS PERSONAS JURÍDICAS (I)

1. Delito de tráfico ilegal de órganos
2. Delito de trata de seres humanos
3. Delitos relativos a la prostitución y corrupción de menores
4. Delitos contra la intimidad, allanamiento informático y otros delitos informáticos
5. Delitos de estafas y fraudes
6. Delitos de insolvencias punibles
7. Delitos de daños informáticos

UNIDAD DIDÁCTICA 11.

DELITOS IMPUTABLES A LAS PERSONAS JURÍDICAS (II)

1. Delitos contra la propiedad intelectual e industrial, el mercado y los consumidores
2. Delitos de blanqueo de capitales
3. Delitos contra la hacienda pública y la Seguridad Social
4. Delitos contra los derechos de los ciudadanos extranjeros
5. Delitos de construcción, edificación o urbanización ilegal
6. Delitos contra el medio ambiente

UNIDAD DIDÁCTICA 12.

DELITOS IMPUTABLES A LAS PERSONAS JURÍDICAS (III)

1. Delitos Relativos a la energÍA solar y las radiaciones ionizantes
2. Delitos de tráfico de drogas
3. Delitos de falsedad en medios de pago
4. Delitos de cohecho
5. Delitos de tráfico de influencias
6. Delitos financiación del terrorismo

www.ineaf.es



INEAF BUSINESS SCHOOL

958 050 207 · formacion@ineaf.es

