



CURSO



Curso Experto en
**Derecho y Normativa
del Tratamiento de
Datos**



INEAF
BUSINESS SCHOOL

INEAF Business School



Índice

Curso Experto en **Derecho y Normativa del Tratamiento de Datos**

1. Historia
2. Titulación Curso Experto en Derecho y Normativa del Tratamiento de Datos
[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 Derecho y Normativa del Tratamiento de Datos

DURACIÓN	250 H
PRECIO	975 €
MODALIDAD	Online

Entidad impartidora:

INEAF - Instituto Europeo de Asesoría Fiscal



Programa de Becas / Financiación 100% Sin Intereses

Titulación Curso Experto

- 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."



Resumen

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 Curso en Derecho y Normativa del Tratamiento de Datos conocerá todas las herramientas y conceptos normativos para aplicar correctamente esta ley.

A quién va dirigido

El Curso en Derecho y Normativa del Tratamiento de Datos está orientada a cualquier persona interesada en privacidad, protección de datos en la empresa. Por tanto, esta formación está indicada tanto a profesionales en activo de este sector como a estudiantes que quieren especializarse en esta área de gran importancia en la actualidad.

Objetivos

Con el Curso Experto en ***Derecho y Normativa del Tratamiento de Datos*** usted alcanzará los siguientes objetivos:

- Conocer en detalle la normativa en vigor en materia de protección de datos.
- Estudia 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.
- 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.



¿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 objeto de 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.

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

¿PARA QUÉ TE PREPARA?

Con la realización del Curso 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.

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.

BE
CAS

BECA DESEMPLEADOS Y ESTUDIANTES	BECA ANTIGUOS ALUMNOS	BECA AUTÓNOMOS	BECA FORMATIVA DE COLABORACIÓN
<p>Para aquellos que se encuentre en situación de desempleo o estén cursando estudios y decidan invertir su tiempo en actualizar sus conocimientos o reorientar su carrera profesional.</p>	<p>Queremos que sigas formándote con nosotros, por ello INEAF te ofrece un 20% dto. en todo nuestro catálogo y te garantiza la beca en los programas Máster.</p>	<p>Valoramos a aquellos que inician su propia aventura empresarial y ven en la formación un valor añadido a sus servicios. INEAF ofrece a los autónomos una beca del 15% dto.</p>	<p>Colaboradores y personal asociado. Tanto por ciento de beca acordado en función del convenio de colaboración.</p>
<p>Documentación a aportar:</p> <ul style="list-style-type: none">• Justificante de encontrarse en situación de desempleo• Documentación que acredite la situación de estudiante	<p>Documentación a aportar:</p> <ul style="list-style-type: none">• No tienes que aportar nada. ¡Eres parte de INEAF!	<p>Documentación a aportar:</p> <ul style="list-style-type: none">• Copia del último recibo de autónomo	<p>Documentación a aportar:</p> <ul style="list-style-type: none">• Consulta información sobre el convenio de colaboración
20%	20%	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 around a wooden conference table in a room with bookshelves. They are dressed in business attire. The man on the left is wearing glasses and a suit. The woman in the middle has curly hair and is wearing a pink top. The man on the right is wearing glasses and a suit. There are papers, a calculator, and a pen holder on the table.

"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 sección Claustro docente de nuestra web desde

[aquí](#)



Temario

Curso Experto en **Derecho y Normativa del Tratamiento de Datos**



PROGRAMA ACADEMICO

Módulo 1. Fundamentos legales para el tratamiento de datos personales

Módulo 2. Responsabilidad proactiva en el tratamiento de datos

Módulo 3. Auditoría en el rgpd

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
4. - Antecedentes
5. - Propuesta de reforma de la Directiva 95/46/CE
6. La Protección de Datos en España
7. 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
4. - Otras definiciones
5. Sujetos obligados
6. 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
2. - Impugnación de valoraciones
3. - Tutela de derechos
4. Transparencia e Información
5. Acceso, Rectificación, Supresión (Olvido)
6. Oposición
7. Decisiones individuales automatizadas
8. Portabilidad de los Datos
9. Limitación del tratamiento
10. Excepciones a los derechos
11. Casos específicos
12. 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
3. - Relaciones Responsable - Encargado
4. - Encargados, sub-encargado, etc.
5. - El contrato de Encargo
6. El Registro de Actividades de Tratamiento: identificación y clasificación del tratamiento de datos
7. - 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
8. - La supervisión de los códigos de conducta
9. - 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
6. - Supuestos sometidos a información previa
7. Autorización de la autoridad de control
8. - Procedimiento de autorización a la AEPD
9. Suspensión temporal
10. Cláusulas contractuales
11. Ejercicio resuelto: Transferencias internacionales de datos

UNIDAD DIDÁCTICA 10.

LAS AUTORIDADES DE CONTROL EN EL RGPD Y LA LOPDGDD

1. Autoridades de Control: Aproximación
2. - Cooperación y Coherencia entre las distintas autoridades de Control
3. - Instrumentos de Asistencia Mutua
4. - El Mecanismo de Coherencia
5. - El Procedimiento de Urgencia
6. Potestades
7. Régimen Sancionador
8. - Sujetos responsables
9. - Infracciones
10. - Prescripción de las infracciones y sanciones
11. - Procedimiento en caso de vulneración de la normativa de protección de datos
12. Comité Europeo de Protección de Datos (CEPD)
13. - Supervisor Europeo de Protección de Datos (SEPD)
14. Procedimientos seguidos por la AEPD
15. La Tutela Jurisdiccional
16. 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
2. - Guía para implantar el programa de protección de datos
3. Objetivos del Programa de Cumplimiento
4. 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
2. - Esquema Nacional de Seguridad
3. - 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
4. 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
5. - Diferencias entre Seguridad de la Información y Seguridad Informática
6. - Conceptos de Seguridad de la Información
7. - Alcance
8. - Estrategia de SI. El modelo PDCA
9. 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
10. - Puesta en práctica de la seguridad de la información
11. - Seguridad desde el diseño y por defecto

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
2. - Impacto en la Protección de Datos
3. - ¿Qué entendemos por “Riesgo”?
4. - ¿Qué debemos entender por “aproximación basada en el riesgo”?
5. - Otros conceptos
6. Evaluación de Riesgos. Inventario y valoración de activos. Inventario y valoración de amenazas. Salvaguardas existentes y valoración de su protección. Riesgo resultante
7. - Principales tipos de vulnerabilidades
8. - Particularidades de los distintos tipos de código malicioso
9. - Principales elementos del análisis de riesgos y sus modelos de relaciones
10. - Identificación de los activos involucrados en el análisis de riesgos y su valoración
11. - Identificación de las amenazas que pueden afectar a los activos identificados previamente
12. - Análisis e identificación de las vulnerabilidades existentes en los sistemas de información que permitirían la materialización de amenazas, incluyendo el análisis local
13. - 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
14. - Establecimiento de los escenarios de riesgo entendidos como pares activo-amenaza susceptibles de materializarse
15. - Determinación de la probabilidad e impacto de materialización de los escenarios

20. - Ejercicio resuelto Análisis de Riesgo: FACILITA_RGPD
21. Gestión de Riesgos. Conceptos. Implementación. Selección y asignación de salvaguardas a amenazas. Valoración de la protección. Riesgo residual, riesgo aceptable y riesgo asumible
22. - Etapas en la gestión de riesgos
23. - Valoración del riesgo, valoración de probabilidad y valoración de gravedad
24. - Implicaciones en la protección de datos de la gestión de riesgos
25. - Gestión de riesgos por defecto
26. - Aplicación del proceso de gestión de riesgos y exposición de las alternativas más frecuentes
27. - Metodologías comúnmente aceptadas de identificación y análisis de riesgos
28. - Aplicación de controles y medidas de salvaguarda para obtener una reducción del riesgo

- 12. - El ciclo de vida de los Sistemas de Información
- 13. - Integración de la seguridad y la privacidad en el ciclo de vida
- 14. - El control de calidad de los SI

- 16. - Establecimiento del nivel de riesgo para los distintos pares de activo y amenaza
- 17. - 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
- 18. - Relación de las distintas alternativas de gestión de riesgos
- 19. - Guía para la elaboración del plan de gestión de riesgos

UNIDAD DIDÁCTICA 4.

METODOLOGÍAS DE ANÁLISIS Y GESTIÓN DE RIESGOS

- 1. Metodologías de Análisis y Gestión de riesgos
- 2. - Análisis de riesgos
- 3. - Aproximación basada en riesgo del RGPD
- 4. - Asignación de responsabilidades mediante RACI
- 5. - Describir el ciclo de vida de los datos
- 6. - Gestión de riesgos: Identificar, evaluar y tratar
- 7. Incidencias y recuperación
- 8. - Notificación de brechas de seguridad
- 9. Principales metodologías
- 10. - Octave
- 11. - NIST SP 800-30
- 12. - 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
- 2. - Origen, Concepto y Características de la EIPD
- 3. - Alcance y necesidad
- 4. - Estándares
- 5. Realización de una Evaluación de Impacto. Aspectos preparatorios y organizativos, análisis de la necesidad de llevar a cabo la evaluación y consultas previas
- 6. - Aspectos preparatorios de la ejecución de la EIPD
- 7. - Análisis de la necesidad de hacer una Evaluación de Impacto
- 8. - Descripción sistemática de las operaciones de tratamiento
- 9. - Objetivos y finalidades del tratamiento. Evaluación de la necesidad y proporcionalidad de las operaciones de tratamiento
- 10. - Gestión de Riesgo. Informe de Evaluación
- 11. - La Consulta Previa
- 12. - 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
- 2. - Conceptos básicos
- 3. - Estándares y Directrices de Auditoría de SI
- 4. Control interno y mejora continua. Buenas prácticas. Integración de la auditoría de protección de datos en la auditoría de SI
- 5. - Buenas prácticas
- 6. - Integración de la auditoría de protección de datos en la auditoría de SI
- 7. 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
3. - Seguridad lógica y en los procedimientos
4. - Seguridad aplicada a las TI y a la documentación
5. Recuperación de desastres y continuidad del Negocio. Protección de activos técnicos y documentales. Planificación y gestión de la Recuperación de Desastres
6. - Protección de activos técnicos y documentales
7. - 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
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 9.

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 10. 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 11. 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 adoptar
- 15. Seguridad a nivel de transporte
- 16. - Protocolo TCP
- 17. - Protocolo UDP
- 18. - Tipos de Ataques
- 19. - 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.

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

www.ineaf.es



INEAF BUSINESS SCHOOL

958 050 207 · formacion@ineaf.es

