



INESEM

BUSINESS SCHOOL

Curso Superior en Auditoría en el RGPD

+ Información Gratis

titulación de formación continua bonificada expedida por el instituto europeo de estudios empresariales

Curso Superior en Auditoría en el RGPD

duración total: 150 horas

horas teleformación: 75 horas

precio: 0 € *

modalidad: Online

* hasta 100 % bonificable para trabajadores.

descripción

Con una perspectiva de responsabilidad proactiva y privacidad desde el diseño, esta formación curso auditor RGPD, teórico-práctica de gestión de riesgos y auditoría de protección de datos, le proporcionará los conocimientos y competencias necesarias para afrontar cualquier auditoría en materia de privacidad. Adquirirá las pautas y herramientas necesarias para realizar un protocolo de seguimiento y seguridad de datos desde el punto de vista legal y técnico.



+ Información Gratis

a quién va dirigido

Todos aquellos trabajadores y profesionales en activo que deseen adquirir o perfeccionar sus conocimientos técnicos en este área.

objetivos

- Conocer las previsiones normativas sobre la auditoría en un tratamiento de datos personales.
- Analizar el cumplimiento práctico de los principios responsabilidad proactiva.
- Estudiar las principales técnicas y herramientas de la auditoría de protección de datos.
- Aplicar técnicas de detección de deficiencias, riesgos y brechas de seguridad.
- Dotar al alumnado de todos los conocimientos sobre normativa y Protección de Datos que le permitirán realizar con solvencia una auditoría de protección de datos personales.
- Estudiar la evaluación y verificación del cumplimiento de los objetivos de seguridad.

para qué te prepara

Este curso auditor RGPD prepara al alumnado para conocer todos los aspectos teóricos-prácticos relativos a la auditoría de protección de datos personales. Le ofrecerá las capacidades y competencias necesarias para auditar a organizaciones empresariales, aplicando correctamente los estándares y medidas de seguridad precisas a cada caso en concreto.

A su vez, le prepara para comprender todos los fundamentos, alcances, obligaciones, y necesidades de una auditoría dentro de una empresa. Además, el objetivo primordial será estudiar el procedimiento propio para la redacción de un informe de auditoría de protección de datos personales.

salidas laborales

Auditor especializado en protección de datos; Asesor legal en materia protección de datos; Abogado experto en protección de datos; Emprendedor con conocimiento en materia de protección de datos; Informáticos expertos en protección de datos; Delegado de protección de Datos;

titulación

Una vez finalizado el curso, el alumno recibirá por parte de INESEM vía correo postal, la Titulación Oficial que acredita el haber superado con éxito todas las pruebas de conocimientos propuestas en el mismo.

Esta titulación incluirá el nombre del curso/máster, la duración del mismo, el nombre y DNI del alumno, el nivel de aprovechamiento que acredita que el alumno superó las pruebas propuestas, las firmas del profesor y Director del centro, y los sellos de la instituciones que avalan la formación recibida (Instituto Europeo de Estudios Empresariales).



INSTITUTO EUROPEO DE ESTUDIOS EMPRESARIALES

como centro de Formación acreditado para la impartición a nivel nacional de formación
EXPIDE LA SIGUIENTE TITULACIÓN

NOMBRE DEL ALUMNO/A

con D.N.I. XXXXXXXX ha superado los estudios correspondientes de

Nombre de la Acción Formativa

de XXX horas, perteneciente al Plan de Formación INESEM en la convocatoria de XXXX
Y para que surta los efectos pertinentes queda registrado con número de expediente XXXX- XXXX-XXXX-XXXXXX

Con una calificación de SOBRESALIENTE

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

La dirección General

MARIA MORENO HIDALGO

Firma del alumno/a

Sello



NOMBRE DEL ALUMNO/A



forma de bonificación

- Mediante descuento directo en el TC1, a cargo de los seguros sociales que la empresa paga cada mes a la Seguridad Social.

metodología

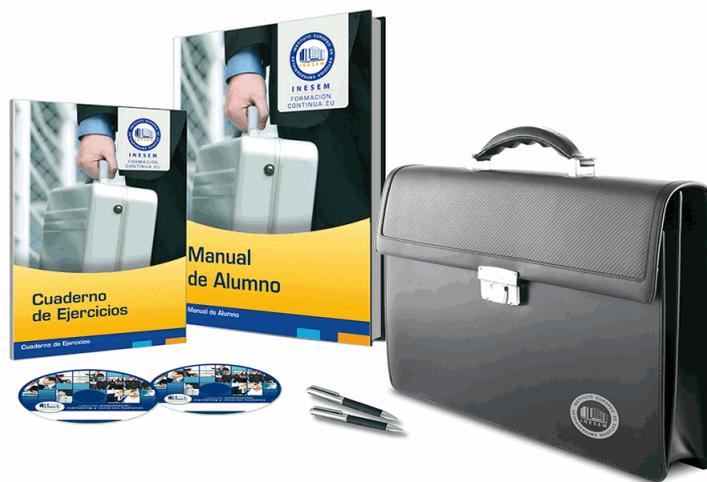
El alumno comienza su andadura en INESEM a través del Campus Virtual. Con nuestra metodología de aprendizaje online, el alumno debe avanzar a lo largo de las unidades didácticas del itinerario formativo, así como realizar las actividades y autoevaluaciones correspondientes. Al final del itinerario, el alumno se encontrará con el examen final, debiendo contestar correctamente un mínimo del 75% de las cuestiones planteadas para poder obtener el título.

Nuestro equipo docente y un tutor especializado harán un seguimiento exhaustivo, evaluando todos los progresos del alumno así como estableciendo una línea abierta para la resolución de consultas.

El alumno dispone de un espacio donde gestionar todos sus trámites administrativos, la Secretaría Virtual, y de un lugar de encuentro, Comunidad INESEM, donde fomentar su proceso de aprendizaje que enriquecerá su desarrollo profesional.

materiales didácticos

- Manual teórico 'Auditoría en el RGPD'



profesorado y servicio de tutorías

Nuestro equipo docente estará a su disposición para resolver cualquier consulta o ampliación de contenido que pueda necesitar relacionado con el curso. Podrá ponerse en contacto con nosotros a través de la propia plataforma o Chat, Email o Teléfono, en el horario que aparece en un documento denominado “Guía del Alumno” entregado junto al resto de materiales de estudio.

Contamos con una extensa plantilla de profesores especializados en las distintas áreas formativas, con una amplia experiencia en el ámbito docente.

El alumno podrá contactar con los profesores y formular todo tipo de dudas y consultas, así como solicitar información complementaria, fuentes bibliográficas y asesoramiento profesional. Podrá hacerlo de las siguientes formas:

- **Por e-mail:** El alumno podrá enviar sus dudas y consultas a cualquier hora y obtendrá respuesta en un plazo máximo de 48 horas.
- **Por teléfono:** Existe un horario para las tutorías telefónicas, dentro del cual el alumno podrá hablar directamente con su tutor.
- **A través del Campus Virtual:** El alumno/a puede contactar y enviar sus consultas a través del mismo, pudiendo tener acceso a Secretaría, agilizando cualquier proceso administrativo así como



plazo de finalización

El alumno cuenta con un período máximo de tiempo para la finalización del curso, que dependerá de la misma duración del curso. Existe por tanto un calendario formativo con una fecha de inicio y una fecha de fin.

campus virtual online

especialmente dirigido a los alumnos matriculados en cursos de modalidad online, el campus virtual de inesem ofrece contenidos multimedia de alta calidad y ejercicios interactivos.

comunidad

servicio gratuito que permitirá al alumno formar parte de una extensa comunidad virtual que ya disfruta de múltiples ventajas: becas, descuentos y promociones en formación, viajes al extranjero para aprender idiomas...

revista digital

el alumno podrá descargar artículos sobre e-learning, publicaciones sobre formación a distancia, artículos de opinión, noticias sobre convocatorias de oposiciones, concursos públicos de la administración, ferias sobre formación, etc.

secretaría

Este sistema comunica al alumno directamente con nuestros asistentes, agilizando todo el proceso de matriculación, envío de documentación y solución de cualquier incidencia.

Además, a través de nuestro gestor documental, el alumno puede disponer de todos sus documentos, controlar las fechas de envío, finalización de sus acciones formativas y todo lo relacionado con la parte administrativa de sus cursos, teniendo la posibilidad de realizar un seguimiento personal de todos sus trámites con INESEM

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

UNIDAD DIDÁCTICA 3. LA GESTIÓN DE LA SEGURIDAD DE LOS TRATAMIENTOS

- 1.Eschema 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.Recuperación de desastres y continuidad del Negocio. Protección de activos técnicos y documentales. 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 permanent 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 riesgo 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 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