INESEM

BUSINESS SCHOOL

Curso Superior en Protección de Datos (RGPD) para el Departamentos de Informática, Sistemas y Comunicación

+ Información Gratis

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

Curso Superior en Protección de Datos (RGPD) para el Departamentos de Informática, Sistemas y Comunicación

duración total: 120 horas ***horas teleformación:*** 60 horas

precio: 0 € *

modalidad: Online

* hasta 100 % bonificable para trabajadores.

descripción

Como consecuencia de la actualización normativa y el cambiante entorno digital es indiscutible que las empresas tengan la necesidad de establecer protocolos de seguridad informática y tratamiento de datos personales. Un tratamiento de datos personales adecuado a la normativa y una gestión correcta de brechas de seguridad de la información permitirá a cualquier organización realizar su labor empresarial con un respaldo legal y práctico de alto rango.
Con esta formación, Curso Protección de Datos en Sistemas Informáticos y de Comunicación, tanto teórica como técnica se convertirá en el profesional asesor que todas las empresas necesitan, sabrá aplicar todas las herramientas e infraestructuras de protección contra incidentes de seguridad y gestión eficaz de tratamientos de datos personales.

a quién va dirigido

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

objetivos

- Conocer los conceptos básicos en materia de protección de datos personales.
- Identificar los principios básicos de la seguridad informática.
- Reconocer las vulnerabilidades y los posibles ataques a las redes y a los sistemas libres.
- Estudiar el protocolo de gestión de protección de datos.
- Conocer la normativa de aplicación sobre el SGSI.
- Estudiar dentro de las políticas de seguridad el protocolo de implantación del SGSI.

para qué te prepara

Informáticos, Técnicos Informáticos, Técnicos de seguridad informática, Analistas de Datos, Abogados, Asesores legales, Consultores en protección de datos, Economistas, Empresarios, profesionales liberales, responsables y personal de los departamentos de marketing, recursos humanos y administración de cualquier tipo de empresa.

salidas laborales

Esta formación pormenorizada le habilita profesionalmente para conocer el área de la protección de datos en el entorno informático, desde los conceptos básicos que establece la ley de protección de datos y garantía de derechos digitales y los protocolos de gestión informática y brechas de seguridad. Actualmente todas las empresas precisan de técnicos informáticos y asesores en protección de datos, por lo que, con esta formación obtendrá las competencias necesarias y know-how para enfrentarse a las amenazas informáticas y brechas de seguridad de datos personales.

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 direccion General

MARIA MORENO HIDALGO

Sello

Firma del alumno/a

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 'Protección de Datos (RGPD) para el Departamentos de Informática, Sistemas y Comunica

profesorado y servicio de tutorías

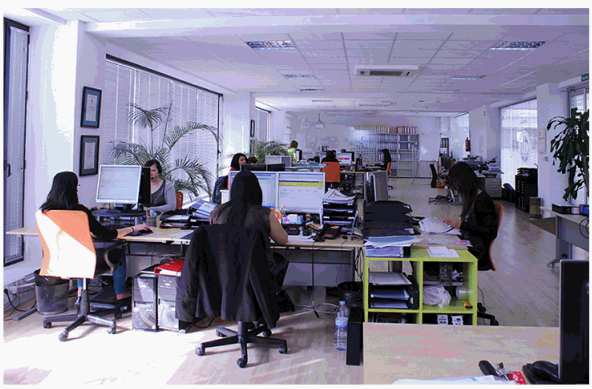
Nuestro equipo docente estará a su disposición para resolver cualquier consulta o ampliación de contenido que pueda necesitar relacionado con el curso. Podrá ponerse en contacto con nosotros a través de la propia plataforma o Chat, Email o Teléfono, en el horario que aparece en un documento denominado “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. 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. 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 Tratamien sus representantes. Relaciones entre ellos y formalización
3.El Registro de Actividades de Tratamiento: identificación y clasificación del tratamiento de datos

UNIDAD DIDÁCTICA 3. 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 Riesg
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 4. METODOLOGÍAS DE ANÁLISIS Y GESTIÓN DE RIESGOS

1.Metodologías de Análisis y Gestión de riesgos
2.Incidencias y recuperación
3.Principales metodologías

UNIDAD DIDÁCTICA 5. 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 6. SEGURIDAD DE LA INFORMACIÓN

1.Marco normativo. Esquema Nacional de Seguridad y directiva NIS: Directiva (UE) 2016/1148 relativa a las medida destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión. Ám de aplicación, objetivos, elementos principales, principios básicos y requisitos mínimos
2.Ciberseguridad y gobierno de la seguridad de la información. Generalidades, Misión, gobierno efectivo de la Segu de la información (SI). Conceptos de SI. Alcance. Métricas del gobierno de la SI. Estado de la SI. Estrategia de la SI
3.Puesta en práctica de la seguridad de la información. Seguridad desde el diseño y por defecto. El ciclo de vida de Sistemas de Información. Integración de la seguridad y la privacidad en el ciclo de vida. El control de calidad de los S

UNIDAD DIDÁCTICA 7. 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 documentación
3.Recuperación de desastres y continuidad del Negocio. Protección de activos técnicos y documentales. Planificaci gestión de la Recuperación de Desastres

UNIDAD DIDÁCTICA 8. NORMATIVA SOBRE EL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI)

1.Estándares y Normas Internacionales sobre los SGSI

1.- Familia de Normas ISO 27000
2.- La Norma UNE-EN-ISO/IEC 27001:2014
3.- Buenas prácticas en seguridad de la información, Norma ISO/IEC 27002

2.Normativa aplicable a los SGSI
1.- Normativa comunitaria sobre seguridad de la información
2.- Legislación Española sobre seguridad de la información
3.- El Instituto Nacional de Ciberseguridad (INCIBE)

UNIDAD DIDÁCTICA 9. 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