



INESEM

BUSINESS SCHOOL

Curso Práctico de Responsabilidad Proactiva en el Tratamiento de Datos

+ Información Gratis

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

Curso Práctico de Responsabilidad Proactiva en el Tratamiento de Datos

duración total: 50 horas

horas teleformación: 26 horas

precio: 0 € *

modalidad: Online

* hasta 100 % bonificable para trabajadores.

descripción

El Reglamento General de Protección de Datos describe el principio de responsabilidad proactiva como la necesidad de que el responsable del tratamiento aplique medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el RGPD. En términos prácticos, este principio requiere que las organizaciones analicen qué datos tratan, con qué finalidades lo hacen y qué tipo de operaciones de tratamiento llevan a cabo. A partir de este conocimiento deben determinar de forma explícita la forma en que aplicarán las medidas que el Reglamento y la LOPD prevén, asegurándose de que esas medidas son las adecuadas para cumplir con las mismas y de que pueden demostrarlo ante los interesados y ante las autoridades de supervisión.



+ 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

- Diseñar e implantar un programa de protección de datos en el contexto de la organización.
- Comprender el concepto “accountability” y las obligaciones derivadas del mismo.
- Analizar y gestionar los riesgos de los tratamientos de datos personales.
- Conocer las distintas metodologías de análisis y gestión de riesgos.
- Llevar a la práctica la protección de datos desde el diseño y por defecto.
- Identificar los pasos necesarios para llevar a cabo una evaluación de impacto “EIPD”.

para qué te prepara

El Curso práctico en responsabilidad proactiva en el tratamiento de datos te prepara para, teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas, aplicar medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el Reglamento General de protección de datos. Proporciona al alumnado las herramientas necesarias para adoptar una actitud consciente, diligente y proactiva frente a los tratamientos de datos personales que se lleven a cabo.

salidas laborales

Delegado de Protección de datos; Técnico de protección de datos, Compliance Officer; Responsable del dpto. jurídico; asesor de empresas en materia de protección de datos; Consultor en materia de protección de datos; Auditor 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 'Curso Práctico de Responsabilidad Proactiva en el Tratamiento de Datos'
- Guía didáctica



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. PROGRAMA DE CUMPLIMIENTO DE PROTECCIÓN DE DATOS Y SEGURIDAD EN UNA ORGANIZACIÓN

- 1.El diseño y la Implantación del Programa de Protección de Datos en el contexto de la organización
 - 1.- Guía para implantar el programa de protección de datos
- 2.Objetivos del Programa de Cumplimiento
- 3.Accountability: La Trazabilidad del Modelo de Cumplimiento

UNIDAD DIDÁCTICA 2. SEGURIDAD DE LA INFORMACIÓN

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

UNIDAD DIDÁCTICA 3. ANÁLISIS Y GESTIÓN DE RIESGOS DE LOS TRATAMIENTOS DE DATOS PERSONALES

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

- 11.- Determinación por parte de la organización de los criterios de evaluación del riesgo, en función de los cuales determina si un riesgo es aceptable o no
 - 12.- Relación de las distintas alternativas de gestión de riesgos
 - 13.- Guía para la elaboración del plan de gestión de riesgos
 - 14.- Ejercicio resuelto Análisis de Riesgo: FACILITA_RGPD
3. Gestión de Riesgos. Conceptos. Implementación. Selección y asignación de salvaguardas a amenazas. Valoración de la protección. Riesgo residual, riesgo aceptable y riesgo asumible
- 1.- Etapas en la gestión de riesgos
 - 2.- Valoración del riesgo, valoración de probabilidad y valoración de gravedad
 - 3.- Implicaciones en la protección de datos de la gestión de riesgos
 - 4.- Gestión de riesgos por defecto
 - 5.- Aplicación del proceso de gestión de riesgos y exposición de las alternativas más frecuentes
 - 6.- Metodologías comúnmente aceptadas de identificación y análisis de riesgos
 - 7.- Aplicación de controles y medidas de salvaguarda para obtener una reducción del riesgo

UNIDAD DIDÁCTICA 4. METODOLOGÍAS DE ANÁLISIS Y GESTIÓN DE RIESGOS

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

UNIDAD DIDÁCTICA 5. EVALUACIÓN DE IMPACTO DE PROTECCIÓN DE DATOS “EIPD”

1. Introducción y fundamentos de las EIPD: Origen, concepto y características de las EIPD. Alcance y necesidad. Estándares
 - 1.- Origen, Concepto y Características de la EIPD
 - 2.- Alcance y necesidad
 - 3.- Estándares
2. Realización de una Evaluación de Impacto. Aspectos preparatorios y organizativos, análisis de la necesidad de llevar a cabo la evaluación y consultas previas
 - 1.- Aspectos preparatorios de la ejecución de la EIPD
 - 2.- Análisis de la necesidad de hacer una Evaluación de Impacto
 - 3.- Descripción sistemática de las operaciones de tratamiento
 - 4.- Objetivos y finalidades del tratamiento. Evaluación de la necesidad y proporcionalidad de las operaciones de tratamiento
 - 5.- Gestión de Riesgo. Informe de Evaluación
 - 6.- La Consulta Previa
 - 7.- Ejercicio resuelto EIPD: GESTIONA_RGPD

