

Los Sistemas de Gestión de la Seguridad de la Información (ENS e ISO 27001) y el cumplimiento del RGPD | ONLINE - Oferta especial!

La mejor herramienta para la gestión de riesgos tecnológicos y la protección de los datos personales.

FINALIDAD

¡ APROVECHA AHORA LA NUEVA OFERTA ESPECIAL «AEC REIMPULSA» !

-20% TODOS | -35% SOCIOS | -50% ERTES, DESEMPLEADOS Y AUTÓNOMOS CON BAJA ACTIVIDAD

El **Reglamento General de Protección de Datos de la Unión Europea** 2016/679, (RGPDUE), aprobado en abril de 2016, requiere el establecimiento de medidas de seguridad para la protección de los datos personales respecto a los riesgos tecnológicos.

Tradicionalmente los Sistemas de Gestión de Seguridad de la Información (SGSIs) han servido al propósito de poder determinar, **en función del riesgo, los controles o medidas de seguridad** más relevantes en el contexto específico de una organización.

El alcance de los SGSIs incluye la protección de los tipos de información relevantes para la organización (registros vitales) y sus procesos pudiendo quedar incluidos, por tanto, los datos personales objeto de protección en el RGPD. El principal marco de referencia internacional respecto a los requisitos mínimos que debe tener un SGSI es el estándar **UNE ISO/IEC 27001:2017**, ampliamente adoptado en el sector privado.

En España resulta de muy especial relevancia el **Esquema Nacional de Seguridad (ENS)**, regulado mediante el Real Decreto 3/2010, que requiere la adopción de un SGSI a las administraciones públicas y también a los operadores del sector privado que contribuyen en las distintas fases del ciclo de vida del dato o el sistema de información responsabilidad de la administración, conforme al ámbito objetivo y subjetivo de aplicación. El ENS se constituye en un SGSI, alineado con ISO/IEC 27001:2013, pero con un gran número de requisitos muy significativos que le otorgan un corpus propio y una relevancia en el contexto público y empresarial español muy notorio.

Durante este curso se estudiará de forma eminentemente práctica cómo contribuye un SGSI conforme al ENS o ISO/IEC 27001 en **la protección de los datos de carácter personal frente a riesgos tecnológicos**, cómo realizar una apreciación (identificación, análisis, evaluación) y tratamiento del riesgo, así como el proceso de implantación de estos y su certificación.

Este programa proporciona una actualización demostrable de los conocimientos establecidos por la **AEPD** en el Esquema de Certificación de Delegados de Protección de Datos para la **renovación** de la certificación.

OBJETIVOS

OBJETIVOS DEL CURSO

Al finalizar el curso, el alumno podrá:

- > Aprender a **gestionar la protección de los datos personales** amparados por el Reglamento (UE) 2016/679, de 27 de abril de 2016 mediante la implantación de un Sistema de Gestión de Seguridad de la Información conforme a ENS o ISO 27001.
- > Conocer los **requisitos de un SGSI** conforme a **UNE ISO/IEC 27001:2017** y al **Esquema Nacional de Seguridad (ENS)** y su proceso de certificación, destacando las diferencias entre ambas.
- > Aprender a realizar una Apreciación (**Identificación, Análisis, Evaluación**) del Riesgo Tecnológico alineada con los requisitos del RGPD.
- > Aprender a gestionar **Incidentes y Brechas** de Seguridad.

Uno de los **requisitos para la renovación de la certificación es justificar que se ha realizado un mínimo de 60 horas de formación**, en materias objeto del Programa del Esquema, durante el periodo de validez del certificado.

Los participantes en el programa recibirán un **Diploma** con el reconocimiento de la **Asociación Española para la Calidad**.

DIRIGIDO A

La necesidad de gestionar el riesgo tecnológico sobre los datos personales es común a los sectores público y privado. Resultando especialmente relevante en el contexto de:

- > Empresas y entidades con tratamientos sensibles desde la perspectiva RGPD.
- > Prestadores de servicios a las administraciones públicas / operadores privados.
- > Empresas y centros relacionados con la salud, entidades financieras, servicios de marketing y prospección comercial.
- > Empresas desarrolladoras de páginas web, Apps y software en general.
- > Implantadores de soluciones que integren Big Data o tratamientos masivos de datos.

Por todo ello, el curso está dirigido a:

- > Los Delegados de Protección de Datos y sus equipos, y en general, a los profesionales que quieran capacitarse en el ámbito del nuevo enfoque en protección de datos.



Para cualquier duda o consulta llamar al
912 108 120 / 21

Además, puedes consultar en nuestra web
otros programas formativos www.aec.es

AEC
ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD

Los Sistemas de Gestión de la Seguridad de la Información (ENS e ISO 27001) y el cumplimiento del RGPD | ONLINE - Oferta especial!

La mejor herramienta para la gestión de riesgos tecnológicos y la protección de los datos personales.

- > Directores y Responsables de Calidad
- > Directores y Responsables de Seguridad
- > Directores y Responsables de Compliance
- > Directores y Responsables de Sistemas
- > Personal Directivo

METODOLOGÍA Y PROFESORADO

METODOLOGÍA

Nuestra metodología de formación online tutorizada combina a la perfección la flexibilidad y practicidad de la formación online con el acompañamiento personalizado de un tutor especializado, para sacar el máximo rendimiento a tu formación.

La tutorización del curso actúa como apoyo principal al autoestudio para favorecer, junto a la realización de ejercicios, el correcto aprendizaje de todos los conceptos. Los alumnos contarán con:

- > Un aula virtual en la que se ordenan los contenidos teóricos en un formato amigable y fácil de interiorizar.
- > Una evaluación continua que ayudará a reforzar los conocimientos adquiridos a través de ejercicios de autoevaluación para consolidar los principales conceptos y pruebas de evaluación para superar cada uno de los módulos.
- > Casos prácticos de aplicación real a empresas y organizaciones.
- > Material audiovisual de ayuda a la interiorización de los principales conceptos.
- > Foros de resolución de dudas e intercambio de experiencias con tutores y alumnos.
- > Acceso gratuito a la prueba para obtener la Titulación propia AEC

Este programa formativo también está disponible en modalidad In Company, formación a medida para tu empresa.

PROFESORES

- > **Miguel A. Lubian Rueda.** Socio en www.institutocies.es dirigiendo el área de Governance, Risk management, and Compliance.
- > **Javier Cao Avellaneda.** Cybersecurity, Privacy and IT Risk Leader en Govertis Advisory Services, S.L.
- > **Lucía Arias Gil.** Management, Governance- IT Advisor en Govertis Advisory Services, S.L.
- > **Borja Romano Arenas.** Information, Security & Risk Consultant en GOVERTIS Advisory Services
- > **José Luis Colom Planas.** Director de auditoría y cumplimiento normativo at AUDERTIS

PROGRAMA

UNIDAD 1. CONCEPTO DE SGSI. CONTEXTO NORMATIVO DEL ENS Y SU RELACIÓN CON EL RGPD

- > **Clase online en directo: Contexto normativo del ENS y su relación con el RGPD.**
- > Qué es un Sistema de Gestión de Seguridad de la Información (SGSI).
- > Requisitos conforme a UNE-EN ISO/IEC 27001:2017.
- > El Esquema Nacional de Seguridad (ENS). Ámbito objetivo y subjetivo de Aplicación. Cuerpo doctrinal (Reales Decretos, Instrucciones Técnicas de Seguridad) y documentación de referencia (serie CCN-STIC-800).
- > Relación del SGSI con el RGPD y otros marcos normativos (Infraestructuras Críticas, Ley NIS).

UNIDAD 2. IMPLANTACIÓN Y MEJORA CONTINUA DE UN SGSI

- > **Clase online en directo: Implantación y mejora continua de un SGSI.**
- > Sistemas de Gestión y Mejora Continua. PDCA.
- > Plan de adecuación al ENS.
- > Implantación de ISO/IEC 27001:2013 conforme a ISO/IEC 27003:2017.

UNIDAD 3. APRECIACIÓN (IDENTIFICACIÓN, ANÁLISIS, EVALUACIÓN) DEL RIESGO TECNOLÓGICO EN EL CONTEXTO DEL ENS Y EL RGPD

- > **Clase online en directo: Apreciación del Riesgo Tecnológico en el contexto del ENS y el RGPD.**
- > Evaluaciones de Impacto en la Protección de Datos (EIPD).
- > El Riesgo Tecnológico y la protección de datos personales.
- > Activos Esenciales (tipos de Información, Servicios y Sistemas) y su relación con las Actividades de Tratamiento de Datos Personales.



Para cualquier duda o consulta llamar al
912 108 120 / 21

Además, puedes consultar en nuestra web
otros programas formativos www.aec.es



ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD

Los Sistemas de Gestión de la Seguridad de la Información (ENS e ISO 27001) y el cumplimiento del RGPD | ONLINE - Oferta especial!

La mejor herramienta para la gestión de riesgos tecnológicos y la protección de los datos personales.

- > Determinación de la Criticidad: Valoración y Categorización de Sistemas. Segregación de sistemas en subsistemas.
- > Apreciación del Riesgo en el contexto de un SGSI.
- > Tratamiento del Riesgo.
- > Controles de Seguridad: estado de implantación, eficacia y evaluación continua.
- > **Caso Práctico 1. Apreciación y Tratamiento del Riesgo de una organización**

UNIDAD 4. GESTIÓN DE INCIDENTES Y BRECHAS DE SEGURIDAD EN UN CONTEXTO MULTI-NORMA

- > **Clase online en directo: Brechas de seguridad en un contexto multi-norma.**
- > Evento, incidente y brecha de seguridad.
- > Fases de gestión de un incidente:
- > Determinación de la peligrosidad y el nivel de impacto de un incidente.
- > Escalado de incidentes.
- > Notificación de brechas de seguridad.
- > Comunicación a terceros y gestión de crisis.
- > **Caso Práctico 2. ¿Podemos hacer un caso práctico sobre Gestión de Incidentes y Brechas de Seguridad?**

UNIDAD 5. CERTIFICACIÓN DE SISTEMAS DE INFORMACIÓN EN EL ENS Y DE SGSIS CONFORME A UNE-EN ISO/IEC 27001:2017

- > **Clase online en directo: Certificación de Sistemas de Información en el ENS.**
- > Diferencia sustantiva entre un sistema de gestión y un sistema de información. Comparativa entre la norma ISO 27001 y el ENS. Diferencia en el proceso de certificación.
- > Obligación legal para la certificación de sistemas en el ámbito del ENS. La ITS de Conformidad con el ENS. Diferencias entre Declaración y Certificación de conformidad. Diferencias entre el Sector Público y el Sector Privado.
- > Entidades de certificación acreditadas en ISO 27001. Autorización del CCN para la certificación de sistemas de información del ENS.
- > Proceso de Certificación del ENS.
- > Proceso de Certificación de ISO 27001.
- > Certificación de la Cadena de Suministro.
- > Obtención y publicidad de la certificación.
- > Auditoría del RGPD. Auditorías concurrentes ENS y RGPD.

La exposición en la sesión formativa se hará de forma que estos contenidos puedan ser aplicados a través del software de gestión SandaS GRC.



Para cualquier duda o consulta llamar al
912 108 120 / 21

Además, puedes consultar en nuestra web
otros programas formativos www.aec.es