

Taller de Implantación de un Sistema de Gestión de Seguridad de la Información: ISO 27001

Gestiona los riesgos y protege tu organización mediante un SGSI basado en ISO 27001

FINALIDAD

Las organizaciones necesitan una **sólida gestión de la seguridad de la información** que vele por su protección, de forma que se optimicen sus áreas y sus procesos; planteando una estrategia de gestión de la seguridad de la información desde el inicio, desde la concepción de una idea hasta su consecución.

La 'Alta Dirección' de la organización debe proporcionar los mecanismos necesarios para ofrecer **productos y servicios seguros**, procesos de negocio **sólidos** que contribuyan a la seguridad de la información necesaria.

La mejor opción es implantar un Sistema de Gestión de Seguridad de la Información utilizando como referencia la norma **ISO/IEC 27001**; estándar internacionalmente reconocido y elaborado por expertos, **certificable** y con un sentido eminentemente **práctico**.

La norma ISO/IEC 27001 nos ayuda a garantizar una mayor **confianza de nuestros clientes y del mercado en general**, facilitando un marco de gestión que asegure la confidencialidad de la información y garantice la integridad, precisión y disponibilidad de ésta. Además se encuentra en armonía con otras normas de referencia como ISO 9001/ISO 14001 etc.

Este taller te ayudará a implantar un sistema de gestión que **cumpla con los requisitos** de esta norma, identificando el contexto de la Organización, sus activos esenciales, demostrando el liderazgo y la implicación de la Dirección, la gestión de riesgos, la mejora continua...etc.

Conoceremos **las mejores prácticas para gestionar los riesgos** de seguridad de la información en base al estándar ISO/IEC 27005, analizaremos las claves para la implantación de otros aspectos como métricas e indicadores, controles y medidas de seguridad, planes de contingencia etc., de modo que se pueda determinar el nivel de seguridad de la Organización en base a criterios objetivos y en función del riesgo detectado.

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

- > Entender los conceptos y fundamentos de un **Sistema de Gestión de Seguridad de la Información**.
- > Aprender a gestionar los Sistemas de Información mediante la implantación de un Sistema de Gestión de Seguridad de la Información conforme al estándar internacional **ISO/IEC 27001**.
- > Conocer los **requisitos de un SGSI** conforme a ISO/IEC 27001 y el proceso hacia su certificación.
- > Conocer los procesos necesarios para el establecimiento, implantación, operación, monitorización, revisión, gestión y mejora desde el punto de vista de la norma.
- > Conocer, identificar y valorar los **activos esenciales de la Organización**.
- > Aprender a documentar debidamente un **Sistema de Gestión de Seguridad de la Información (SGSI)**.
- > Aprender a realizar una **Apreciación del Riesgos en la Organización** en base a la identificación, análisis, evaluación y tratamiento del riesgo.
- > Aprender a gestionar las **No Conformidades (NC) y las Oportunidades de Mejora (OM)** detectadas.

DIRIGIDO A

- > Directores y Responsables de Seguridad.
- > Responsables de Sistema de Información y sus equipos.
- > Profesionales que quieran capacitarse en el ámbito de la Seguridad de la Información.
- > Consultores en seguridad de la información.
- > Auditores de seguridad.
- > Directores y responsables de Sistemas de Gestión.



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

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

Taller de Implantación de un Sistema de Gestión de Seguridad de la Información: ISO 27001

Gestiona los riesgos y protege tu organización mediante un SGSI basado en ISO 27001

En general, cualquier persona que quiera introducirse o ampliara conocimientos en el área de seguridad de la información.

METODOLOGÍA Y PROFESORADO

METODOLOGÍA

El programa está impartido por una selección de los más destacados profesionales de la materia, 100% activos en la disciplina que imparten, garantizando que el programa responda y se adecúe a la realidad de la actividad y de las empresas y organizaciones actuales.

El enfoque didáctico combina la asimilación del marco conceptual de la disciplina, su aplicabilidad en casos de éxito y talleres participativos individuales y grupales, haciendo del programa una experiencia dinámica, práctica y rica en experiencias.

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

PROFESORES

- > **Santiago Raúl de la Fuente Cagigós.** Lead Advisor Técnico. Consultor/Auditor Ciberseguridad, TI y GRC (Gobierno, Riesgo y Cumplimiento normativo)

PROGRAMA

CONCEPTO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI)

- > Qué es un Sistema de Gestión de Seguridad de la Información (SGSI).
- > Requisitos conforme a UNE-ISO/IEC 27001.
- > Ámbito objetivo y subjetivo de Aplicación.
- > Anexo SL.
- > Relación del SGSI con otros marcos normativos.

IMPLANTACIÓN Y MEJORA CONTINUA DE UN SGSI

- > Sistemas de Gestión y Mejora Continua. PDCA. Contexto de la organización, Liderazgo, Planificación y Soporte – Dominios 4, 5, 6 y 7 (PLAN). Operación. Dominio 8 (DO). Evaluación del desempeño – Dominio 9 (CHECK). Mejora – Dominio 10 (ACT).
- > Implantación de UNE-ISO/IEC 27001
 - > Contexto de la organización.
 - > Liderazgo.
 - > Planificación.
 - > Soporte.
 - > Operación.
 - > Evaluación del rendimiento.
 - > Mejora.
- > **Caso Práctico 1. Identificación del alcance y cómo abordar la implantación de un SGSI.**

UNE-ISO/IEC 27002 – RELACIÓN DE CONTROLES DENTRO DEL PROCESO DE IMPLANTACIÓN DE UN SGSI.

- > Organización de los controles: Estructura de la norma. Requisitos, selección y desarrollo de controles.
- > Relación de controles:
 - > Políticas de seguridad de la información
 - > Organización de la seguridad de la información
 - > Seguridad relativa a los recursos humanos



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

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

Taller de Implantación de un Sistema de Gestión de Seguridad de la Información: ISO 27001

Gestiona los riesgos y protege tu organización mediante un SGSI basado en ISO 27001

Gestión de activos

- > Control de acceso
- > Criptografía
- > Seguridad física y del entorno
- > Seguridad de las operaciones
- > Seguridad de las comunicaciones
- > Adquisición, desarrollo y mantenimiento de los sistemas de información
- > Relación con proveedores
- > Gestión de incidentes de seguridad de la información
- > Aspectos de seguridad de la información para la gestión de la continuidad del negocio. Visión general de (ISO 22301)
- > Cumplimiento
- > **Caso Práctico 2. Identificación de los controles necesarios para conseguir los objetivos definidos.**

APRECIACIÓN DEL RIESGO: IDENTIFICACIÓN, ANÁLISIS, EVALUACIÓN Y TRATAMIENTO DE RIESGOS.

- > Riesgo Tecnológico y la protección de datos.
- > Activos Esenciales (servicio e información).
- > Valoración y Categorización de los Sistemas. Determinación de su Criticidad.
- > Apreciación del Riesgo: Identificación del riesgo. Análisis del riesgo. Evaluación del riesgo. Tratamiento del riesgo (ISO/IEC 27005 – ISO/IEC 31000)
- > Controles de Seguridad: implantación, eficacia y evaluación continua.
- > **Caso Práctico 3. Gestión de riesgos: apreciación y tratamiento del riesgo.**

EL PROCESO DE CERTIFICACIÓN

- > Fase 1 de auditoría: Revisión de la documentación. Revisión documental del SGSI
- > Fase 2 de auditoría: Auditoría principal. Verificación del SGSI



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

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