Implementar y gestionar un proyecto ISO 27001:2013
Preparación para las certificaciones

Seminario de 3 días - 21h
Ref.: ASE - Precio 2024: 2 020€ sin IVA

La norma internacional de control de riesgos ISO/IEC 27001 relativa a la seguridad de la información describe las buenas prácticas que deben aplicarse para que una organización gestione eficazmente los riesgos relacionados con la información. Este curso presenta las normas ISO de seguridad de los sistemas de Información y los elementos para establecer un sistema de gestión de riesgos de seguridad de la información (SGSI).

OBJETIVOS PEDAGÓGICOS

Al término de la formación, el alumno podrá:

Explicar los componentes de un Sistema de Gestión de la Seguridad de la Información (SGSI) conforme a la norma ISO 27001

Explicar el contenido y la correlación entre las normas ISO 27001 y 27002, así como con otras normas y marcos normativos

Adaptar los requisitos de la norma ISO 27001 al contexto específico de una organización

Interpretar los requisitos de la norma ISO 27001 en el marco de una auditoría de un SGSI

Armonizar los diferentes enfoques de la gobernanza de los SI (ISO, LPM, NIS, etc.)

CER

Preparación para la obtención de los certificados ISO 27001 Lead Implementer y Lead Auditor.

CERTIFICACIÓN

En la modalidad a distancia, el candidato deberá adquirir todas las normas necesarias (ISO 27000, ISO 27001, ISO 27002, ISO 27005, ISO 27006, ISO 19011, ISO 17021 e ISO 27006). En modo presencial, en Orsys, las normas se prestan en formato papel durante la formación.

PROGRAMA

última actualización: 01/2023

1) Introducción

- Recordatorios. Terminología de la norma ISO 27000 y de la Guía ISO 73.
- Definiciones: amenaza, vulnerabilidad y protección.
- El concepto de riesgo (consecuencia, impacto y probabilidad).
- La clasificación mínima CID (Confidencialidad, Integridad y Disponibilidad).
- Gestión de riesgos (reducción, mantenimiento, rechazo y reparto).
- Análisis de la siniestralidad. Tendencias. Desafíos.
- La reglamentación sectorial PCI-DSS y COBIT. ¿Para quién? ¿Por qué? Interacción con ISO.
- Hacia la gobernanza de las TI, vínculos con ITIL® e ISO 20000.

2) Las normas BS 7799, sus aportaciones a la ISO.

- Las normas fundacionales (ISO 27001, 27002).
- Las normas indispensables (ISO 27005, 27004, 27003, etc.).
- Convergencia con las demás normas del «Sistema de Gestión».

3) La norma ISO 27001:2013

- Definición de un Sistema de Gestión de la Seguridad (SGSI).

PARTICIPANTES

Responsables de seguridad de la Información, gestores de riesgos, directores o responsables informáticos, gestores de proyectos, ingenieros o corresponsales de seguridad, jefes de proyectos, auditores internos y externos y futuros «auditados».

REQUISITOS PREVIOS

Conocimientos básicos de seguridad informática.

COMPETENCIAS DEL FORMADOR

Los expertos que imparten la formación son especialistas en las materias tratadas. Han sido validados por nuestros equipos pedagógicos, tanto en el plano de los conocimientos profesionales como en el de la pedagogía, para cada curso que imparten. Cuentan al menos con entre cinco y diez años de experiencia en su área y ocupan o han ocupado puestos de responsabilidad en empresas.

MODALIDADES DE EVALUACIÓN

El formador evalúa los progresos pedagógicos del participante a lo largo de toda la formación mediante preguntas de opción múltiple, escenificaciones de situaciones, trabajos prácticos, etc.
El participante también completará una prueba de posicionamiento previo y posterior para validar las competencias adquiridas.

MEDIOS PEDAGÓGICOS Y TÉCNICOS

• Los medios pedagógicos y los métodos de enseñanza utilizados son principalmente: ayudas audiovisuales, documentación y soporte de cursos, ejercicios prácticos de aplicación y ejercicios corregidos para los cursillos prácticos, estudios de casos o presentación de casos reales para los seminarios de formación.
• Al final de cada cursillo o seminario, ORSYS facilita a los participantes un cuestionario de evaluación del curso que analizarán luego nuestros equipos pedagógicos.
• Al final de la formación se entrega una hoja de presencia por cada media jornada de presencia, así como un certificado de fin de formación si el alumno ha asistido a la totalidad de la sesión.

MODALIDADES Y PLAZOS DE ACCESO

La inscripción debe estar finalizada 24 horas antes del inicio de la formación.

ACCESIBILIDAD DE LAS PERSONAS CON DISCAPACIDAD

¿Tiene alguna necesidad específica de accesibilidad? Póngase en contacto con la Sra. FOSSE, interlocutora sobre discapacidad, en la siguiente dirección psh-accueil@orsys.fr para estudiar de la mejor forma posible su solicitud y su viabilidad.

- Objetivos que debe alcanzar su SGSI.
- El enfoque de mejora continua como principio fundacional, el modelo PHVA (Planificar, Hacer, Verificar y Actuar) o rueda de Deming.
- La norma ISO 27001 forma parte de un enfoque global de gobernanza del SGSI.
- Detalles de las fases Plan-Do-Check-Act (Planificar-Hacer-Verificar-Actuar).
- Desde la especificación del alcance del SGSI hasta la Declaración de Aplicabilidad (SoA).
- Las recomendaciones de la norma ISO 27001 para la gestión de riesgos.
- La importancia de la evaluación de riesgos. Elección de un método tipo ISO 27005:2018.
- La aportación de los métodos publicados (por ejemplo, EBIOS RM) en su proceso de valoración.
- La adopción de medidas de seguridad técnicas y organizativas eficientes.

Mejora del SGSI. Aplicación de acciones correctivas y preventivas.

4) Buenas prácticas, norma ISO 27002:2013

- Objetivos de seguridad: Disponibilidad, integridad y confidencialidad.
- Estructuración en dominios/capítulos (nivel 1), objetivos de control (nivel 2) y controles (nivel 3).
- Las nuevas buenas prácticas de la norma ISO 27002:2013, las medidas suprimidas de la norma ISO 27001:2005. Los cambios.
- La norma ISO 27002:2013: los 14 dominios y las 114 buenas prácticas.
- Ejemplos de aplicación de la norma a su empresa: las principales medidas de seguridad indispensables.
- Medidas de la reducción de riesgos para los activos de apoyo, como las personas, los bienes y la informática.
- Medidas indispensables para compartir a través del dominio 15.

5) La aplicación de la seguridad en un proyecto de SGSI

- De las especificaciones de seguridad a la aceptación de la seguridad.
- ¿Cómo cumplir la Política de Seguridad de los Sistemas de Información y las exigencias de seguridad del cliente/dirección del proyecto?
- Del análisis de riesgos a la construcción de la declaración de aplicabilidad.
- Integración de medidas de seguridad en desarrollos específicos.
- La normas que deben respetarse para la subcontratación.
- Seguimiento del proyecto durante su ejecución y funcionamiento.
- Las reuniones de «seguridad» antes de la aceptación.
- Integrar el ciclo PHVA en el ciclo de vida del proyecto.

Preparación de los indicadores. Mejora continua.

FECHAS

Contacto