Ciberseguridad, ISO 27032, certificación

Curso práctico de 5 días - 35h
Ref.: CYB - Precio 2024: 2 790€ sin IVA

Este curso intensivo le proporcionará los conocimientos y competencias necesarios para implementar y gestionar un programa de ciberseguridad basado en la norma ISO 27032. Le permitirá obtener la certificación ISO 27032.

OBJETIVOS PEDAGÓGICOS

Al término de la formación, el alumno podrá:

Conocer los componentes y el funcionamiento de un programa de ciberseguridad conforme a la norma ISO 27032

Explicar la finalidad, el contenido y la correlación entre la norma ISO 27032 y otras normas y referencias

Dominar conceptos, métodos, normas y técnicas para gestionar un programa de ciberseguridad

Control de un programa de ciberseguridad según la norma ISO 27032

MÉTODOS PEDAGÓGICOS

Curso magistral apoyado por una presentación ilustrada con ejemplos concretos, salpicada de debates, preguntas y respuestas tanto de teoría como de práctica.

Anatomía de un ataque a una empresa internacional de telecomunicaciones. Ejercicios para identificar lagunas y manejar conceptos clave.

CERTIFICACIÓN

Se obtiene la certificación PECB «Certified ISO 27032 Lead Cybersecurity Manager» si se supera el examen de certificación.

PARTICIPANTES

Profesionales de la ciberseguridad, expertos en seguridad de la información, gestores de proyectos y consultores de seguridad de TI.

REQUISITOS PREVIOS

Conocimientos de seguridad de la información.

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.

PROGRAMA

última actualización: 01/2023

1) Conceptos de ciberseguridad y norma ISO 27032

- Objetivos y estructura del curso.
- Marco reglamentario y normativo.
- Definición de los conceptos fundamentales de la ciberseguridad.
- Planificar un programa de ciberseguridad.

2) Iniciar un programa de ciberseguridad

- Estructura organizativa.
- Definir las funciones y responsabilidades de las partes interesadas en la ciberseguridad.
- Establecer políticas y principios que rijan la ciberseguridad.
- Gestión de los riesgos de ciberseguridad en el marco de la gestión del riesgo empresarial.
- Evaluación de los riesgos de ciberseguridad.

3) Implementación de un programa de ciberseguridad

- Implementación de un marco de gestión documental.
- Intercambio de información y coordinación de los actores clave.
- Desarrollo de un programa de formación y sensibilización del personal y de los actores clave.
- Aplicación de controles específicos de ciberseguridad.

- Gestión de incidentes de ciberseguridad y su integración en la gestión ordinaria de incidentes.
- Gestión de la continuidad del negocio.

4) Evaluación de los resultados del programa de ciberseguridad

- Mediciones del rendimiento de las acciones emprendidas.
- Autoevaluación de los controles.
- Implantación de un entorno de garantía.
- Evaluación del nivel de preparación frente a las ciberamenazas.
- Adecuación de la implementación de la mejora continua.
- Medición del nivel de integración de los controles de ciberseguridad en los controles de seguridad de la información.
- Presentación del sistema de certificación PECB.

5) Realización del examen de certificación

- Área 1: conceptos básicos de ciberseguridad.
- Área 2: orientación para iniciar, implementar y gestionar un programa de ciberseguridad.
- Área 3: directrices sobre las funciones y responsabilidades de las partes interesadas en la ciberseguridad.
- Área 4: gestión de riesgos de ciberseguridad.
- Área 5: supervisión de las actividades del programa de ciberseguridad.

Examen : Examen en papel consistente en 12 preguntas abiertas, que deberán responder en 3 horas, en francés. Formato «libro abierto» (se permite utilizar material y notas personales tomadas durante el curso).

FECHAS

Contacto