Normas de sistemas de gestión

ISO/IEC 27005:2022 — Riesgos de SI

Dos días para llevar a cabo la evaluación y el tratamiento de los riesgos de seguridad de la información que exige ISO/IEC 27001:2022, siguiendo las recomendaciones de ISO/IEC 27005:2022. Enfoque por eventos o por activos, escenarios, criterios, plan de tratamiento, aceptación de los riesgos residuales: el método se aplica a sus sistemas de información y a sus proveedores, hasta obtener un registro de riesgos utilizable.

Duración : 2 días

Objetivos

1. Explicar el papel de ISO/IEC 27005:2022 respecto a los requisitos de ISO/IEC 27001:2022
2. Definir el contexto, los criterios de aceptación y los criterios de evaluación de los riesgos
3. Identificar escenarios de riesgo según un enfoque por eventos o por activos
4. Analizar y valorar los riesgos y construir un plan de tratamiento vinculado a los controles del anexo A
5. Organizar el seguimiento, la revisión y la comunicación de los riesgos a lo largo del tiempo

Programa

Día 1 — mañana

• Por qué un método: lo que ISO/IEC 27001:2022 exige sobre la evaluación y el tratamiento de los riesgos

• Vocabulario: fuente de riesgo, amenaza, vulnerabilidad, evento, consecuencia, probabilidad

• Contexto, criterios de aceptación de los riesgos y criterios de evaluación

• Propietarios de los riesgos y papel de la dirección

Día 1 — tarde

• Enfoque por eventos y enfoque por activos: cuándo elegir uno u otro

• Activos, amenazas y vulnerabilidades; construcción de escenarios de riesgo

• Análisis: consecuencias, probabilidad, nivel de riesgo

• Ejercicio: escenarios de riesgo sobre un perímetro de su empresa (correo, ERP, datos de clientes)

Día 2 — mañana

• Valoración y priorización de los riesgos

• Opciones de tratamiento: reducir, evitar, compartir, retener

• Plan de tratamiento vinculado a los controles del anexo A y a la declaración de aplicabilidad

• Aceptación de los riesgos residuales e información a la dirección

Día 2 — tarde (taller)

• Seguimiento y revisión de los riesgos: indicadores, desencadenantes de actualización

• Comunicación y consulta sobre los riesgos

• Taller: registro de riesgos y plan de tratamiento de su perímetro

• Prueba de conocimientos y presentación del registro

Metodología

• Ejercicios con sus sistemas de información, sus flujos de datos y sus contratos de subcontratación informática

• Comparación de los dos enfoques sobre un mismo perímetro

• Modelo de registro de riesgos y de plan de tratamiento, adaptable a su herramienta

• Caso práctico: riesgo ligado a un proveedor de servicios en la nube

• Cuestionario de mitad de formación y prueba final sobre el método

Evaluación y documentos

Cuestionario de mitad de formación y prueba de conocimientos al final de la sesión, evaluación en caliente a J+1. Certificado de formación numerado, verificable en línea, para cada participante; informe de formación, registro de riesgos y plan de tratamiento surgidos del taller entregados a la empresa.

Materiales bilingües para cada participante; cada formación presencial incluye su gemelo digital en OmniLearn.

Conviene saber

Esta formación presupone conocer los requisitos de ISO/IEC 27001:2022: la formación «ISO/IEC 27001:2022 — Requisitos» (2 días) los presenta. El método general de gestión del riesgo se trata en «ISO 31000:2018 — Gestión del riesgo».

Información práctica

Duración	2 días
Público	Responsables de seguridad de la información, directores de sistemas de información, gestores de riesgos, responsables de cumplimiento, auditores internos del sistema de seguridad de la información
Requisitos previos	Conocimiento básico de ISO/IEC 27001:2022
Número de participantes	Grupos de 6 a 12 participantes, en la empresa
Formato	En la empresa, presencial en sus instalaciones
Idioma	Francés, darija o inglés; materiales bilingües
Financiación	Contratos especiales de formación de la OFPPT (TFP), GIAC, Maroc PME: preparamos los expedientes con usted, sin coste adicional.
Personalización del programa	Programa adaptado a sus procedimientos, sus equipos y su público

Preguntas frecuentes

¿Es certificable ISO/IEC 27005?
No. ISO/IEC 27005:2022 ofrece recomendaciones. Ayuda a cumplir los requisitos de ISO/IEC 27001:2022 sobre los riesgos, que sí se auditan en la certificación.

¿Hace falta un software de gestión de riesgos?
No. Una hoja de cálculo bien estructurada basta para empezar. La formación aporta un modelo; la elección de una herramienta viene después, según el tamaño del perímetro y el número de propietarios de riesgos.

¿Qué diferencia hay con ISO 31000:2018?
ISO 31000:2018 ofrece directrices generales de gestión del riesgo. ISO/IEC 27005:2022 las aplica a la seguridad de la información: activos, amenazas, vulnerabilidades, escenarios y vínculo con los controles del anexo A de ISO/IEC 27001:2022.

¿Quién debe participar?
El responsable de seguridad de la información, el director de sistemas de información, los gestores de riesgos y los propietarios de procesos de negocio. Los propietarios de los riesgos deben comprender el método para poder aceptar los riesgos residuales con conocimiento de causa.