Normas de sistemas de gestión

ISO/IEC 27001:2022 — Requisitos

Dos días para comprender lo que exige ISO/IEC 27001:2022 y preparar la certificación de un sistema de gestión de la seguridad de la información. Alcance, evaluación y tratamiento de riesgos, declaración de aplicabilidad, 93 controles del anexo A, incidentes y continuidad: cada noción se aplica a sus activos, sus proveedores y sus procedimientos. Usted sale con una primera declaración de aplicabilidad y la lista de sus brechas prioritarias.

Duración : 2 días

Objetivos

1. Explicar la estructura de ISO/IEC 27001:2022 y el lugar del anexo A en el método
2. Definir el alcance del sistema a partir del contexto, de las partes interesadas y de las interfaces con los proveedores
3. Aplicar un método de evaluación y tratamiento de los riesgos de seguridad de la información
4. Construir una declaración de aplicabilidad justificada a partir de los 93 controles del anexo A
5. Preparar la gestión de incidentes, la continuidad, la auditoría interna y la revisión por la dirección

Programa

Día 1 — mañana

• Confidencialidad, integridad, disponibilidad: lo que un certificado ISO/IEC 27001 demuestra a sus clientes

• La familia ISO/IEC 27000: papeles respectivos de 27001, 27002 y 27005

• Contexto, partes interesadas, requisitos legales y contractuales, incluida la ley n.º 09-08 sobre datos personales

• Alcance: sitios, actividades, sistemas de información, proveedores

Día 1 — tarde

• Liderazgo, política de seguridad de la información, roles y responsabilidades

• Evaluación de riesgos: criterios, identificación, análisis, valoración

• Opciones de tratamiento, plan de tratamiento y aceptación de los riesgos residuales por sus propietarios

• Ejercicio: evaluación de riesgos de un proceso de su empresa

Día 2 — mañana

• Anexo A: 93 controles repartidos en cuatro temas: organizativo, de personas, físico y tecnológico

• Declaración de aplicabilidad: controles seleccionados, exclusiones justificadas, estado de implantación

• Controles que se examinan a menudo en auditoría: derechos de acceso, copias de seguridad, proveedores y servicios en la nube, registro de eventos

• Gestión de incidentes de seguridad y seguridad de la información durante una perturbación

Día 2 — tarde (taller)

• Seguimiento, medición, auditoría interna y revisión por la dirección del sistema

• No conformidades y acciones correctivas

• Taller: borrador de su declaración de aplicabilidad y lista de brechas prioritarias

• Prueba de conocimientos y presentación de los trabajos

Metodología

• Lectura comentada de los requisitos y del anexo A
• Ejercicios con sus activos, sus flujos de datos y los contratos con sus proveedores informáticos
• Construcción guiada de una declaración de aplicabilidad
• Caso práctico de un incidente de seguridad, de la detección a la acción correctiva
• Cuestionario de mitad de formación y prueba final sobre los requisitos del sistema

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, borrador de declaración de aplicabilidad y lista de brechas entregados a la empresa.

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

Conviene saber

Para profundizar en el método de evaluación de riesgos, la formación «ISO/IEC 27005:2022 — Riesgos de SI» (2 días) complementa esta. La protección de datos personales y la ley 09-08 se tratan en «ISO/IEC 27701:2025 y ley 09-08».

Información práctica

Duración	2 días
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

¿Hay que ser informático para seguir la formación?
No. Los requisitos de la norma se refieren ante todo a la organización: alcance, riesgos, roles, proveedores, incidentes. Los controles técnicos se explican sin jerga; la presencia del director de sistemas de información o del responsable de seguridad ayuda a vincularlos con su infraestructura.

¿Debe la declaración de aplicabilidad incluir los 93 controles?
No. Indica, para cada control del anexo A, si se selecciona o se excluye, y por qué. Estas decisiones se derivan de la evaluación y el tratamiento de los riesgos; el auditor de certificación verifica su coherencia.

¿Qué relación hay con la ley 09-08?
La ley n.º 09-08 regula el tratamiento de los datos de carácter personal. ISO/IEC 27001:2022 pide identificar los requisitos legales aplicables y tenerlos en cuenta: la ley entra en el contexto y en el tratamiento de riesgos, sin que la certificación equivalga a cumplimiento legal.

¿Puede un sitio ya certificado ISO 9001 apoyarse en su sistema?
Sí. Las dos normas comparten la estructura armonizada: control documental, auditoría interna, revisión por la dirección y acciones correctivas pueden ser comunes. El trabajo propio de ISO/IEC 27001 se refiere a los riesgos de seguridad de la información y a los controles del anexo A.