GUIA

ISO 27001:2022

Sistemas de gestión de seguridad de la información — Requisitos.

La norma ISO/IEC 27001:2022 es el estándar internacional líder para la creación, implementación y mejora continua de un Sistema de Gestión de Seguridad de la Información (SGSI).

Esta actualización sustituye por completo a la antigua versión de 2013.

Su objetivo principal es proteger la confidencialidad, integridad y disponibilidad de los datos frente a ciberamenazas modernas.

Estructura de la Norma

Mantiene la estructura de alto nivel (Anexo SL) para facilitar la integración con otras normas como ISO 9001.

Las cláusulas obligatorias son:

Cláusula 4: Contexto de la organización.

Define el alcance del SGSI y los requisitos de las partes interesadas.

Cláusula 5: Liderazgo.

Establece el compromiso de la alta dirección y las políticas de seguridad.

Cláusula 6: Planificación.

Evalúa los riesgos y define los objetivos de seguridad de la información.

Cláusula 7: Soporte.

Gestiona los recursos, competencias y la concienciación del personal.

Cláusula 8: Operación.

Ejecuta las acciones de tratamiento de riesgos planificadas.

Cláusula 9: Evaluación del desempeño.

Monitorea la efectividad mediante auditorías internas.

Cláusula 10: Mejora.

Gestiona las no conformidades y aplica acciones correctivas.

Reestructuración del Anexo A (Los Objetivos de Control y Controles)

El mayor cambio de la versión 2022 radica en su Anexo A, el cual reduce y reorganiza los controles de seguridad, pasando de 114 controles a 93 controles distribuidos en solo 4 categorías temáticas:

Organizacionales (37 controles):

Tratan las políticas de seguridad, gestión de accesos y relaciones con proveedores.

Tecnológicos (34 controles):

Se centran en la infraestructura TI, cifrado, redes y desarrollo seguro.

Físicos (14 controles):

Protegen los perímetros de las instalaciones, equipos y áreas críticas.

De Personas (8 controles):

Regulan la contratación, formación y responsabilidades del personal.

11 Nuevos Controles Tecnológicos y Operativos:

Para responder al auge del trabajo remoto y la infraestructura en la nube, se añadieron 11 controles específicos:

1. **Inteligencia de amenazas (*Threat intelligence*):**

   Recopilación de datos sobre ciberataques actuales.

2. **Seguridad en la nube:**

   Protección específica para el uso de servicios Cloud.

3. **Preparación de las TIC para la continuidad del negocio:**

   Resiliencia tecnológica.

4. **Monitoreo de seguridad física:**

   Vigilancia activa de las instalaciones corporativas.

5. **Gestión de configuraciones:**

   Control de los parámetros de seguridad de los sistemas.

6. **Eliminación segura de la información:**

   Borrado definitivo para evitar recuperación de datos.

7. **Enmascaramiento de datos (*Data masking*):**

   Ocultar datos sensibles mediante técnicas de seudonimización.

8. **Prevención de fuga de datos (DLP):**

   Herramientas para evitar la salida no autorizada de información.

9. **Monitoreo de actividades:**

   Supervisión de redes, sistemas y aplicaciones en tiempo real.

10. **Filtrado web: Restricción de acceso a sitios de internet maliciosos.**

11. **Codificación segura (*Secure coding*): Directrices de seguridad en el desarrollo de software.**

Para ver el contenido completo de información específica contáctanos, la Norma **ISO 27001:2022 se incluye en Gap Analysis.**

Atención a Clientes
Lic. Alejandra Morales / Ing Gerardo García
Dirección Comercial WST / Dirección Operaciones WST
55 6581 0662 / 55 6581 0123
licmorales@iso-irca.com / inggarcia@iso-irca.com