# GUIA

# ISO 27032:2023

**Sistemas de gestión de seguridad de ciberseguridad — Requisitos.**

**La norma ISO/IEC 27032:2023 es un estándar internacional publicado por la Organización Internacional de Normalización (ISO) que proporciona las directrices esenciales para la seguridad en Internet.**

**Esta segunda edición actualiza y reemplaza la versión original del año 2012 para abordar los riesgos cibernéticos modernos y el panorama de amenazas tecnológicas actuales.**

## Objetivos principales del estándar

**Establecer relaciones claras:**

Explica detalladamente las diferencias y vínculos entre la ciberseguridad, la seguridad en la red, la seguridad web y la seguridad en Internet.

**Mitigar amenazas comunes:**

Ofrece guías de alto nivel para identificar, evaluar y tratar riesgos críticos en el entorno digital.

**Definir roles y funciones:**

Identifica a los actores relevantes y detalla las responsabilidades que les corresponden en el espacio cibernético.

**Fomentar la colaboración:**

Promueve la cooperación activa entre empresas, usuarios y autoridades gubernamentales para mejorar la seguridad colectiva.

## Áreas clave de protección e infraestructura

**Activos de información digital:**

Protege datos confidenciales, software corporativo, hardware, plataformas web y centros de datos físicos.

**Infraestructuras críticas globales:**

Cubre sistemas vitales para la economía social como redes de transporte, servicios financieros y telecomunicaciones inalámbricas.

**Servicios en línea corporativos:**

Asegura las operaciones de comercio electrónico, banca en línea, redes sociales y sistemas de correo electrónico empresarial.

**Integración tecnológica emergente:**

Alinea estrategias de protección considerando los retos de la Inteligencia Artificial (IA) y el Internet de las Cosas (IoT).

## Niveles y tipos de controles contemplados

**La norma agrupa sus recomendaciones de ciberseguridad en cuatro enfoques prácticos y específicos para las organizaciones:**

**Controles a nivel de aplicación:**

Prácticas dirigidas a blindar el código de los programas y software.

**Controles a nivel de servidor:**

Configuraciones de infraestructura para resistir ataques externos directos.

**Controles de usuario final:**

Mecanismos de protección en los dispositivos y terminales de los empleados.

**Controles contra ingeniería social:**

Estrategias organizacionales y de capacitación de personal contra el phishing y engaños de identidad.

**Relación con otras normativas**

**A diferencia de ISO/IEC 27001, que define los requisitos para establecer un Sistema de Gestión de la Seguridad de la Información (SGSI) certificable, la norma ISO/IEC 27032:2023 opera como una guía técnica extendida.**

**Los ingenieros e implementadores utilizan esta norma como un banco de controles avanzados para enriquecer el Anexo A de la ISO 27001, cubriendo vacíos operativos específicos del entorno Internet.**

**Para ver el contenido completo de información específica contáctanos, la** Norma **ISO 27032:2023 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