qualoom®

Inspiring Technology
for People

Frameworks de Ciberseguridad Comparados: **NIST, ISO 27001 y CIS Controls**

Área de Seguridad
Fecha 15/09/2025
Versión 1.0

Más información www.qualoom.es

qualoom®

Inspiring Technology
for People

ÍNDICE

qualoom®

Inspiring Technology
for People

Introducción.
¿Por qué lo necesitas?

Los ciberataques aumentan en sofisticación y frecuencia. Adoptar un marco de referencia estructurado permite establecer controles sólidos, cumplir con normativas y mejorar la resiliencia operativa.

Objetivo: Gestionar y reducir riesgos de ciberseguridad en infraestructuras críticas y organizaciones de cualquier tamaño.

Estructura: Basado en 5 funciones principales: Identify, Protect, Detect, Respond, Recover.

Objetivo: Establecer, implementar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI).

Estructura: Basado en el ciclo **PDCA** (Plan-Do-Check-Act).

CIS Controls

Objetivo: Proporcionar un conjunto de prácticas prioritarias para mejorar la ciberseguridad.

Estructura: 18 controles agrupados por niveles de implementación (IG1, IG2, IG3) según la madurez y recursos de la organización.

Más información www.qualoom.es

qualoom®

Inspiring Technology
for People

Introducción.
¿Por qué lo necesitas?

¿Cómo decidir cuál es el más adecuado para tu empresa? Compara los **principales marcos de ciberseguridad del mercado** y **fortalece tu postura defensiva.**

Característica	NIST CSF	ISO/IEC 27001	CIS Controls v8
Tipo de marco	Referencial, flexible	Normativo, certificable	Controles técnicos
Enfoque	Gestión de riesgos	Gestión de SGSI	Práctico y técnico
Certificación	No	Sí	No (pero sí autovalidación)
Nivel de detalle	Medio	Alto (gestión + controles)	Alto (controles técnicos)
Ideal para	Gobierno y empresas	Organizaciones reguladas	Implementación operativa

qualoom®

Inspiring Technology
for People

NIST CSF: Foco en la mejora continua

Ventajas: Adaptabilidad, orientación a la mejora continua

Aplicaciones: Sectores críticos, empresas con necesidades de cumplimiento (FISMA, HIPAA, etc.)

Identify

Gestiona activos, riesgos, entorno y gobernanza.

Protect

Aplica controles y medidas para proteger servicios críticos.

Detect

Detecta eventos de ciberseguridad oportunamente.

Respond

Contiene y responde a incidentes para reducir el impacto.

Recover

Restaura capacidades tras un incidente para volver a operar.

Más información www.qualoom.es

qualoom®

Inspiring Technology
for People

ISO 27001: Certificación internacional para SGSI

Enfoque: Gestión de la seguridad de la información (SGSI)

Puntos clave: Requiere análisis de riesgos, plan de tratamiento, controles del Anexo A

Certificación: Auditado externamente, alta reputación internacional

Ventajas: Reconocimiento global, formalización de procesos

Fases Clave del Proceso de Implementación y Certificación

1. INICIO

- Obtener apoyo de la alta dirección
- Definir el alcance del SGSI
- Identificar partes interesadas y requisitos

2. ANÁLISIS Y PLAN

- Evaluar riesgos de seguridad
- Establecer tratamiento de riesgos
- Crear Declaración de Aplicabilidad (SoA)

3. IMPLEMENTACIÓN

- Aplicar controles del Anexo A (ISO 27002)
- Redactar políticas y procedimientos
- Concienciar y formar al personal
- Establecer controles operacionales

4. MONITOREO

- Realizar auditorías internas
- Gestionar incidentes de seguridad
- Seguimiento y medición de controles
- Revisión por la dirección

5. CERTIFICACIÓN

- Seleccionar organismo certificador acreditado
- Superar auditoría de certificación
- Corregir no conformidades
- Obtener certificado ISO/IEC 27001

6. MANTENIMIENTO

- Auditorías de seguimiento anuales
- Mejora continua del SGSI (ciclo PDCA)
- Re-certificación cada 3 años

Más información www.qualoom.es

qualoom®

Inspiring Technology
for People

CIS Controls: Seguridad táctica y priorizada

Enfoque: 18 controles priorizados en niveles (IG1, IG2, IG3)

Uso recomendado: Entornos operativos con necesidad de acción rápida

Ventajas: Implementación directa, clara priorización por nivel de madurez

Grupo IG1

Objetivo principal:
Protección básica, fácil de implementar

Ejemplos de Controles (CIS v8)
- Inventario de activos (Control 1)
- Configuración segura (Control 4)
- Gestión de accesos (Control 6)

Grupo IG2

Objetivo principal:
Gestión proactiva, más profundidad técnica

Ejemplos de Controles (CIS v8)
- Supervisión continua (Control 8)
- Defensa contra malware (Control 10)
- Respuesta a incidentes (Control 17)

Grupo IG3

Objetivo principal:
Madurez avanzada y gestión compleja de riesgos

Ejemplos de Controles (CIS v8)
- Detección de amenazas (Control 13)
- Pruebas de penetración (Control 18)
- Análisis de comportamiento

Más información www.qualoom.es

qualoom®

Inspiring Technology for People

Comparativa **Frameworks de Ciberseguridad (2025)**

Criterio	NIST CSF 2.0	ISO/IEC 27001:2022	CIS Controls v8
Alcance	Gestión de riesgos de ciberseguridad a nivel organizacional.	Sistema de Gestión de Seguridad de la Información (SGSI).	Controles técnicos y operativos concretos para proteger sistemas y datos.
Requisitos de certificación	No certificable (orientado a autoevaluación y mejora continua).	Certificable mediante auditorías por terceros acreditados (ISO).	No certificable como tal, aunque se puede evaluar el cumplimiento.
Nivel de detalle técnico	Medio: proporciona funciones, categorías y subcategorías con resultados deseados.	Bajo a medio: requiere interpretación, especialmente técnica.	Alto: controles detallados y específicos, con medidas técnicas directas.
Escalabilidad	Alta: adaptable a organizaciones de todos los tamaños y sectores.	Alta, pero puede ser más complejo para pequeñas empresas.	Alta: diseñado con tres niveles de implementación según madurez y tamaño.
Aplicabilidad por sector	Multisectorial, incluidos sectores críticos.	Universal, aunque requiere adaptación según el sector.	Muy utilizado en sector público, salud, educación, y pymes.
Coste de implementación	Bajo a medio (mayor si se integran otras normas y herramientas).	Medio a alto (incluye formación, documentación, auditorías, etc.).	Bajo a medio (recursos disponibles gratuitamente, requiere poco formalismo).

qualoom®

Inspiring Technology
for People

Observaciones clave de los **Frameworks**

NIST CSF 2.0

Rediseñado para mayor internacionalización y alineación con otros marcos. Ideal como base de gestión del riesgo cibernético, pero no entra en detalles técnicos concretos.

ISO/IEC 27001

Marco formal y globalmente reconocido. Excelente para demostrar cumplimiento y madurez de la seguridad, pero puede ser costoso y burocrático.

CIS Controls

CIS Controls v8

Extremadamente práctico. Popular para organizaciones que quieren implementar controles rápidamente, aunque no tiene el mismo reconocimiento formal que ISO.

qualoom®

Inspiring Technology
for People

¿Qué framework **es más adecuado para tu empresa?**

Tipo de Empresa	Recomendación
Empresa global con fuerte foco en cumplimiento	ISO 27001
Empresa mediana en entorno regulado o crítico	NIST CSF
Pyme con recursos limitados pero enfoque táctico	CIS Controls

CONSEJO EXPERTO:

Consejo experto: Muchos líderes optan por **combinar frameworks**: usar NIST como modelo base, complementado por controles CIS para acciones rápidas y certificación ISO a medio plazo.

qualoom®

Inspiring Technology
for People

Asegura tu futuro digital **con el marco adecuado**

CONTACTA CON NOSOTROS

www.qualoom.es

contacto@qualoom.es

(+34) 91 236 4808

Más información www.qualoom.es