# Guía Ampliada y Profunda de ISO 27001

### ¿Qué es ISO 27001?

ISO/IEC 27001 es el estándar internacional más reconocido para la gestión de la seguridad de la información (SGSI), publicado por la Organización

Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (IEC).

* **Enfoque**: Basado en **riesgos** (identificar, evaluar y tratar amenazas).
* **Estructura**: Sigue el ciclo PDCA (Planificar-Hacer-Verificar-Actuar).
* **Certificación**: Las organizaciones pueden obtener una certificación externa mediante auditorías de entidades acreditadas.

### Evolución y Versiones

* **2005**: Primera versión (ISO/IEC 27001:2005).
* **2013**: Revisión importante (alineación con anexo SL, misma estructura que ISO 9001).
* **2022**: Actualización con nuevos controles (ej: seguridad en la nube, IA).

### Beneficios Clave

**Para la organización**:

* Reduce costos por brechas de seguridad.
* Evita multas por incumplimiento (ej: GDPR hasta 4% de ingresos globales).
* Mejora la eficiencia operativa con procesos estandarizados.

### Para clientes y partes interesadas:

* Demuestra compromiso con la protección de datos.
* Facilita contratos con gobiernos y grandes empresas (requisito en licitaciones).

## Sectores con Mayor Adopción

### Sector Casos de Uso

|  |  |
| --- | --- |
| Banca y Finanzas | Protección de datos de clientes (PCI DSS + ISO 27001). |
| Salud | Cumplimiento de HIPAA (EE.UU.) o LOPDGDD (España). |
| Tecnología | Seguridad en desarrollo de software (ISO 27001 + ISO 27034). |
| Retail | Protección de pagos electrónicos y datos de tarjetas. |

## Requisitos y Controles (Profundización)

## Estructura de la Norma

* **Capítulos 1-3**: Introducción y alcance.
* **Capítulos 4-10**: Requisitos obligatorios del SGSI (contexto, liderazgo, planificación, etc.).
* **Anexo A**: 114 controles en 14 dominios (no obligatorios, pero esenciales para la certificación).

## Controles Críticos por Dominio

**A.5 – Gobernanza de Seguridad**

* **A.5.1**: Políticas documentadas (ej: "Política de Uso Aceptable de TI").
* **A.5.3**: Revisión anual por la dirección.

**A.9 – Control de Accesos**

* **A.9.2.1**: Provisión y revocación de accesos (ej: desactivar cuentas de empleados que salen).
* **A.9.4.4**: Uso de MFA (Autenticación Multifactor) para accesos remotos.

**A.12 – Seguridad Operacional**

* **A.12.3.1**: Copias de seguridad automatizadas y pruebas de restauración.
* **A.12.6.1**: Gestión de vulnerabilidades (ej: parcheo mensual de sistemas).

**A.17 – Continuidad del Negocio**

* **A.17.1.2**: Plan de Recuperación ante Desastres (RTO y RPO definidos).

**A.18 – Cumplimiento Legal**

* **A.18.1.4**: Protección de datos personales (alineación con GDPR, CCPA).

## Auditoría ISO 27001: Enfoque Práctico

### Tipos de Auditorías

1. **Interna**: Realizada por auditores de la organización.
2. **Externa (Certificación)**: Por una entidad acreditada (ej: DNV, BSI).

## Checklist de Evidencias

### Requisito Ejemplo de Evidencia

|  |  |
| --- | --- |
| Contexto | Matriz de partes interesadas y requisitos legales. |
| Planificación | Registro de riesgos (ej: "Fuga de datos por phishing" → riesgo alto). |
| Operación | Logs de acceso a servidores críticos. |
| Evaluación | Informe de auditoría interna con no conformidades. |

## Preguntas Clave por Área

**Gestión de Riesgos**:

* ¿Cómo se actualiza la evaluación de riesgos ante nuevas amenazas (ej: ransomware)?

**Terceros**:

* ¿Los proveedores en la nube tienen certificación ISO 27001 o SOC 2?

**Incidentes**:

* ¿Cuántos incidentes se registraron en el último año? ¿Cuál fue el tiempo de respuesta?

## Integración con Otros Marcos

## ISO 27001 + COBIT

• **COBIT** (Control Objectives for Information and Related Technologies) complementa ISO 27001 con: o Métricas de desempeño (KPI/KRI). o Gobierno de TI (alineación con objetivos de negocio).

## ISO 27001 + NIST CSF

• El **NIST Cybersecurity Framework** (EE.UU.) mapea controles con ISO 27001:

**Identificar** → A.8 (Gestión de activos). o **Proteger** → A.9 (Control de accesos).

## ISO 27001 + GDPR

• **Artículo 32 GDPR**: "Medidas técnicas y organizativas" se cubren con:

**A.18.1.4** (Protección de datos personales).

**A.12.4** (Cifrado de datos).

## Casos Reales de Implementación

## Caso 1: Empresa de SaaS

* **Problema**: Necesitaba certificarse para competir en Europa.
* **Solución**: Implementó **A.14 (Seguridad en desarrollo)** → Revisiones de código. Certificación en 9 meses con 3 no conformidades menores.

## Caso 2: Hospital

* **Problema**: Riesgo de filtración de historias clínicas.
* **Solución**:

**A.13 (Comunicaciones seguras)**: Cifrado de emails. **A.11 (Seguridad física)**: Biométricos para acceso a salas de servidores.

**Formulario de Evaluación ISO 27001 – Escala Likert (1 a 5)**

|  |  |  |
| --- | --- | --- |
| Dominio | Pregunta | Opciones de Respuesta (1 a 5) |
| A.5 Gobernanza de Seguridad | ¿Existe una política documentada y aprobada de seguridad de la información? | 1 = No cumple ··· 5 = Cumple y supera expectativas |
|  | ¿Se revisa la política de seguridad al menos una vez al año? | 1 = No cumple ··· 5 = Cumple y supera expectativas |
|  | ¿La alta dirección participa en la gestión de la seguridad de la información? | 1 = No cumple ··· 5 = Cumple y supera expectativas |
| A.9 Control de Accesos | ¿Se revocan los accesos inmediatamente cuando un empleado deja la organización? | 1 = No cumple ··· 5 = Cumple y supera expectativas |
|  | ¿Se utiliza autenticación multifactor (MFA) para accesos remotos? | 1 = No cumple ··· 5 = Cumple y supera expectativas |
|  | ¿Los accesos a los sistemas están definidos según roles o perfiles? | 1 = No cumple ··· 5 = Cumple y supera expectativas |
| A.12 Seguridad Operacional | ¿Se realizan respaldos automáticos de la información crítica? | 1 = No cumple ··· 5 = Cumple y supera expectativas |
|  | ¿Se prueban periódicamente los respaldos para garantizar su restauración? | 1 = No cumple ··· 5 = Cumple y supera expectativas |
|  | ¿Existe un plan de gestión de vulnerabilidades actualizado? | 1 = No cumple ··· 5 = Cumple y supera expectativas |

# A.5– Gobernanza de Seguridad

#### **1. ¿Existe una política documentada y aprobada de seguridad de la información?**

|  |  |
| --- | --- |
| Nivel | Recomendación |
| 1. No cumple | Elaborar una política formal, documentarla y someterla a aprobación de la alta dirección. |
| 2. Cumple parcialmente | Verificar si la política está completa, actualizada y correctamente distribuida. |
| 3. Cumple mínimamente | Incluir responsables, objetivos claros y revisión periódica en la política. |
| 4. Cumple bien | Asegurar que la política esté alineada con otras normativas internas y con ISO 27001. |
| 5. Cumple y supera | Mantener revisiones proactivas, difundirla ampliamente y auditar su cumplimiento. |

#### **2. ¿Se revisa la política de seguridad al menos una vez al año?**

|  |  |
| --- | --- |
| Nivel | Recomendación |
| 1. No cumple | Establecer un cronograma anual obligatorio de revisión. |
| 2. Cumple parcialmente | Nombrar responsables y establecer fechas formales de revisión. |
| 3. Cumple mínimamente | Documentar revisiones pasadas y aplicar mejoras sugeridas. |
| 4. Cumple bien | Asociar revisión a cambios de riesgos, incidentes o tecnología. |
| 5. Cumple y supera | Integrar revisión continua con métricas de desempeño y validación externa. |

#### **¿La alta dirección participa en la gestión de la seguridad de la información?**

|  |  |
| --- | --- |
| Nivel | Recomendación |
| 1. No cumple | Sensibilizar a la alta dirección sobre su rol en la seguridad. |
| 2. Cumple parcialmente | Involucrarla en reuniones de seguridad o asignarle funciones específicas. |
| 3. Cumple mínimamente | Solicitar su apoyo en decisiones clave y recursos. |
| 4. Cumple bien | Alta dirección lidera o respalda proyectos de seguridad. |
| 5. Cumple y supera | Participa activamente y promueve la cultura de seguridad en toda la organización. |

# A.9 – Control de Accesos

#### **¿Se revocan los accesos inmediatamente cuando un empleado deja la organización?**

|  |  |
| --- | --- |
| Nivel | Recomendación |
| 1. No cumple | Implementar procedimientos obligatorios de revocación inmediata. |
| 2. Cumple parcialmente | Notificar de forma automática a TI ante bajas de personal. |
| 3. Cumple mínimamente | Mantener un registro de revocaciones y su tiempo de ejecución. |
| 4. Cumple bien | Verificar el cumplimiento mediante auditorías internas. |
| 5. Cumple y supera | Automatizar la revocación mediante integración con RRHH y sistemas de acceso. |

#### **¿Se utiliza autenticación multifactor (MFA) para accesos remotos?**

|  |  |
| --- | --- |
| Nivel | Recomendación |
| 1. No cumple | Aplicar MFA en todos los accesos remotos de inmediato. |
| 2. Cumple parcialmente | Extender MFA a todo el personal, no solo usuarios críticos. |
| 3. Cumple mínimamente | Evaluar herramientas MFA más seguras y fáciles de usar. |
| 4. Cumple bien | Implementar MFA en todos los sistemas de información críticos. |
| 5. Cumple y supera | Usar MFA adaptativo según ubicación, horario o dispositivo. |

#### **¿Los accesos a los sistemas están definidos según roles o perfiles?**

|  |  |
| --- | --- |
| Nivel | Recomendación |
| 1. No cumple | Aplicar el modelo de acceso basado en roles (RBAC). |
| 2. Cumple parcialmente | Revisar que cada usuario tenga los accesos mínimos necesarios. |
| 3. Cumple mínimamente | Documentar roles y permisos en un sistema centralizado. |
| 4. Cumple bien | Auditar accesos regularmente y validar con los jefes de área. |
| 5. Cumple y supera | Automatizar asignación/revisión de roles según cambios de función. |

# A.12 – Seguridad Operacional

#### **¿Se realizan respaldos automáticos de la información crítica?**

|  |  |
| --- | --- |
| Nivel | Recomendación |
| 1. No cumple | Establecer respaldo automático diario/semanal de información crítica. |
| 2. Cumple parcialmente | Asegurar que toda la información crítica esté incluida en los respaldos. |
| 3. Cumple mínimamente | Supervisar logs de respaldo y configurar alertas ante fallos. |
| 4. Cumple bien | Usar almacenamiento externo o en la nube para mayor seguridad. |
| 5. Cumple y supera | Implementar respaldo automatizado, cifrado y con redundancia geográfica. |

#### **¿Se prueban periódicamente los respaldos para garantizar su restauración?**

|  |  |
| --- | --- |
| Nivel | Recomendación |
| 1. No cumple | Programar pruebas de restauración al menos trimestralmente. |
| 2. Cumple parcialmente | Documentar resultados de las pruebas y revisar los errores detectados. |
| 3. Cumple mínimamente | Incluir distintas muestras de información y pruebas simuladas. |
| 4. Cumple bien | Asociar las pruebas a los planes de continuidad de negocio. |
| 5. Cumple y supera | Realizar simulacros completos y documentar evidencia de restauración exitosa. |

#### **¿Existe un plan de gestión de vulnerabilidades actualizado?**

|  |  |
| --- | --- |
| Nivel | Recomendación |
| 1. No cumple | Crear un plan de gestión de vulnerabilidades documentado. |
| 2. Cumple parcialmente | Establecer revisiones periódicas del plan (mínimos semestrales). |
| 3. Cumple mínimamente | Ejecutar escaneos automáticos y manuales de vulnerabilidades. |
| 4. Cumple bien | Clasificar vulnerabilidades y aplicar acciones correctivas en tiempos definidos. |
| 5. Cumple y supera | Integrar con herramientas de monitoreo y respuesta automática a incidentes. |