Guía Práctica

para Pymes

Seguridad de la Información e ISO 27001

www.ursspain.com

Índice

1. Introducción

La **seguridad de la información** es un factor crítico en cualquier organización, sin importar su tamaño. Para las pymes, una brecha de datos o un ciberataque puede tener consecuencias económicas, legales y de reputación devastadoras.

ISO 27001 ofrece un marco reconocido internacionalmente para **proteger la confidencialidad, integridad y disponibilidad** de la información. Implantar un Sistema de Gestión de Seguridad de la Información (SGSI) ayuda a prevenir riesgos, cumplir requisitos legales y demostrar confianza ante clientes y socios.

Esta guía ha sido elaborada específicamente para ayudar a las **pymes españolas** a entender qué exige la legislación en materia de protección de datos y seguridad de la información, y cómo aplicar ISO 27001 de forma realista, adaptada a sus recursos.

2. Fundamentos legales en España

Legislación básica:

- **Reglamento General de Protección de Datos (RGPD – UE 2016/679):** regula la protección de datos personales.
- **Ley Orgánica 3/2018,** de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD).
- **Esquema Nacional de Seguridad (ENS):** obligatorio en el sector público y aplicable a proveedores tecnológicos de la Administración.
- **Ley de Servicios de la Sociedad de la Información (LSSI):** obligaciones en materia de seguridad y comunicaciones electrónicas.

Obligaciones esenciales para pymes:

1. Identificar y clasificar la información sensible.
2. Adoptar medidas técnicas (contraseñas robustas, copias de seguridad, cifrado).
3. Garantizar la formación y concienciación del personal.
4. Disponer de procedimientos para gestión de incidentes.
5. Mantener un registro actualizado de tratamientos y accesos.

3. Qué es ISO 27001 y por qué es útil para una pyme

ISO 27001 es la norma internacional que establece los requisitos para implementar un **Sistema de Gestión de Seguridad de la Información (SGSI).**

Beneficios concretos:

- Reducción de riesgos de ciberataques y fugas de información.
- Cumplimiento legal (RGPD, LOPDGDD, ENS).
- Mayor confianza de clientes y acceso a contratos que exigen certificación.
- Mejora de la continuidad del negocio.
- Ventaja competitiva frente a la competencia.

Mito: "ISO 27001 es solo para grandes empresas"

✗ **FALSO.** Su estructura es escalable y aplicable a cualquier pyme

4. Paso a paso: Cómo implementar ISO 27001 en una pyme

Etapa 1: Análisis del contexto y partes interesadas

- Define qué información manejas y quién depende de su seguridad.
- Herramienta: “mapa de partes interesadas y activos críticos”.

Etapa 2: Análisis de riesgos

- Identifica amenazas (ciberataques, errores humanos, fallos técnicos).
- Herramienta: matriz de riesgos (probabilidad x impacto).

Etapa 3: Política de Seguridad de la Información

- Documento oficial firmado por la dirección.
- Herramienta: modelo editable de política.

Etapa 4: Planificación y objetivos

- Ej.: reducir incidentes de phishing, implantar copias en la nube, formación anual.
- Herramienta: plan de

Etapa 5: Roles y responsabilidades

- Nombra un Responsable de Seguridad de la Información.
- Herramienta: organigrama de responsabilidades.

Etapa 6: Controles técnicos y organizativos

- Accesos, contraseñas, antivirus, cifrado, clasificación de la información.
- Evidencia: registros de pruebas, inventario de activos.

Etapa 7: Preparación y respuesta ante incidentes

- Protocolo de notificación, investigación y medidas correctivas.
- Herramienta: procedimiento tipo de gestión de incidentes.

Etapa 8: Evaluación y mejora continua

- Auditorías internas, revisión de la dirección y acciones de mejora.
- Herramienta: checklist de auditoría + plantilla de no conformidades.

5. Checklist de preparación para certificación

Este checklist está diseñado como una herramienta de autoevaluación para pymes que desean implementar ISO 27001. Cada ítem debe valorarse con base en el siguiente sistema

Método de evaluación

Respuesta	Puntuación	Significado
Si	2 pts.	Completamente implementado
Parcial	1 pts.	En proceso o parcialmente aplicado
No	0 pts.	No implementado aún

Interpretación de resultados

- **30–40 puntos:** Preparación avanzada. Puede estar lista para una auditoría interna o certificación.
- **15–29 puntos:** En progreso. Es recomendable reforzar varias áreas antes de una auditoría formal.
- **0–14 puntos:** Etapa inicial. Se sugiere formación y diagnóstico

A continuación se detalla un checklist ampliado para que una pyme pueda autoevaluarse antes de iniciar un proceso de certificación ISO 27001:

- ☐ Política de seguridad aprobada.
- ☐ Análisis de riesgos actualizado.
- ☐ Inventario de activos críticos.
- ☐ Control de accesos documentado.
- ☐ Plan de respuesta ante incidentes.
- ☐ Formación al personal realizada.
- ☐ Auditorías internas programadas.
- ☐ Evidencias de mejora continua.

6. Recursos adicionales

Para facilitar la implementación de un Sistema Seguridad de la Información basado en la norma ISO 27001, ponemos a disposición de las pymes una selección de recursos clave:

- **Guía oficial INCIBE sobre ciberseguridad para pymes:** www.incibe.es
- **Guía práctica de la AEPD sobre RGPD y LOPDGDD:** https://www.aepd.es/guias-y-herramientas/guias

Todas estas plantillas están diseñadas para ser fácilmente adaptables según el tamaño y actividad de la empresa.

- **Plantillas editables URS SPAIN:**
  - Matriz de riesgos de seguridad de la información
  - Modelo de política de seguridad para pymes
  - Procedimiento básico de gestión de incidentes.

- **Servicio de diagnóstico gratuito URS SPAIN:**
  - Revisión inicial del nivel de seguridad.
  - Identificación de áreas críticas.
  - Recomendaciones prácticas para iniciar el SGSI.