# GUÍA DE IMPLANTACIÓN ISO/IEC 27701

50,000 CERTIFICATES GLOBALLY

100% TRANSPARENT FEES

1000+ EMPLOYEES WORLDWIDE

AVERAGE CUSTOMER PARTNERSHIP 10 YEARS

OVER 90 OPERATING COUNTRIES

# GESTIÓN DE INFORMACIÓN PERSONAL ISO/IEC 27701

Desde 2016 y en un período de tiempo relativamente corto, se han aprobado leyes de protección de datos en muchos países. El más notable es el Reglamento General de Protección de Datos (rgpd) de la UE, que ha dado forma a los requisitos para que las organizaciones garanticen los derechos de los interesados cuando procesan sus datos personales. La velocidad a la que se ha establecido esta legislación ha dejado a algunas empresas sin poder adaptarse adecuadamente y se han producido infracciones.

A pesar de la implementación del GDPR, este no brinda una guía específica sobre qué medidas deben tomarse para garantizar el cumplimiento de sus requisitos. Además, los estándares existentes no tienen un conjunto de cláusulas o controles lo suficientemente robustos para garantizar que la privacidad de los datos se aborde por completo mediante la implementación de sistemas de gestión.

La Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (IEC) han desarrollado la ISO 27701 para proporcionar la orientación necesaria para que las empresas aborden eficazmente la privacidad de los datos y se aseguren cerrar las deficiencias entre los requisitos de los sistemas de gestión existentes y la legislación de privacidad de datos global.

## RGPD: descripción de la legislación

El RGPD fue adoptado por la UE en abril de 2016 y reemplazó a la Directiva de Protección de Datos de la UE 95/46/EC. Esta nueva legislación impone obligaciones para cualquier organización con responsabilidades de procesamiento de datos, y también es aplicable a organizaciones fuera de la UE. Ha armonizado la legislación sobre privacidad en todo el EEE.

Cualquier entidad fuera de la UE que ofrezca bienes o servicios a personas ubicadas en la UE también está sujeta a los requisitos del RGPD. Las empresas y organizaciones con requisitos de procesamiento de datos personales se ven especialmente afectadas y es primordial garantizar la conformidad con la legislación.

Las organizaciones deben tener una base legal para procesar datos personales y procesarlos para un propósito específico. Las personas tienen derecho a solicitar una copia de todos los datos que se guardados incluida una explicación de cómo se utilizan dichos datos y si es accesible por terceros. Las personas pueden solicitar que su perfil de datos se transfiera a otro procesador de datos y también tienen derecho a retirar su consentimiento para dicho procesamiento.

Las organizaciones y las personas que procesan datos personales ahora deben contar con controles de seguridad adecuados para garantizar la confidencialidad de los datos que tienen o procesan. Los datos personales se pueden transferir fuera de la UE, pero solo a países que se considera que tienen una legislación adecuada para preservar los derechos de los interesados de la UE.

Las notificaciones sobre violaciones de datos deben enviarse a la autoridad supervisora dentro de un periodo de 72 horas posteriores al reconocimiento de la infracción. EL Supervisor Europeo de Protección de Datos (SEPD) es la autoridad europea encargada de garantizar que, a la hora de tratar datos personales, las instituciones y organismos de la UE respeten el derecho a la intimidad de los ciudadanos.

# ¿QUÉ ES LA ISO 27701 Y POR QUÉ ES NECESARIA?

Al igual que muchas legislaciones de privacidad en todo el mundo, hay muy poca orientación sobre cómo implementar procesos para cumplir con el RGPD. La ISO 27701:2019 es una extensión de privacidad de la norma internacional de gestión de seguridad de la información, ISO 27001 (ISO 27701 Técnicas de seguridad - Extensión de ISO 27001 e ISO 27002 para la gestión de privacidad dela información - Requisitos y directrices).

La ISO 27701 detalla los requisitos y brinda la orientación necesaria para el establecimiento, implementación, mantenimiento y mejora de un Sistema de Gestión de la Información Confidencial (SGIC). El estándar se basa en los requisitos, objetivos de control y controles del estándar ISO 27001 e incluye un conjunto de requisitos de privacidad, controles y objetivos de control.

Los conceptos de seguridad de la información son familiares para las organizaciones que ya tienen un Sistema de Gestión de Seguridad de la Información (SGSI) operativo. El SGIC garantizará que las organizaciones tengan una gobernanza de datos integral y universalmente aplicable que se corresponda directamente con los requisitos legislativos de sus jurisdicciones.

La norma se redactó con aportaciones de expertos y autoridades de protección de datos de todo el mundo, incluida la Junta Europea de Protección de Datos. Se tuvieron en cuenta las legislaciones de protección de datos de todos los continentes. Es cercana al RGPD, pero cada cláusula se relaciona con un artículo del mismo.

Pero la ISO 27701 no es específica al RGPD, es un estándar global y un referente en términos de privacidad. Las organizaciones que lo implementan demostrarán un enfoque proactivo en la protección de datos personales.

# ÉNFASIS EN LA ISO 27001

La ISO 27701requiere de un sistema de gestión existente al que adherirse. No todas las cláusulas y controles son aplicables en todos los casos.

Los requisitos de la norma se dividen en los cuatro grupos que se enumeran a continuación:

1. Los requisitos del SGIC relacionados con ISO 27001 se describen en la cláusula 5.
2. Los requisitos del SGIC relacionados con ISO 27002 se describen en la cláusula 6.
3. La guía del SGIC para controladores de información personal se describen en la cláusula 7.
4. La guía del SGIC para procesadores de información confidencial se describe en la cláusula 8.

Además, los controles aplicables se describen en los anexos del cuerpo principal de la norma. Puede utilizar como guía los siguientes:

1. Anexo A: enumera los controles para controladores.
2. Anexo B: enumera los controles para procesadores.
3. Anexo C: esquematiza las disposiciones de ISO 27701 comparándolas con la ISO 29100.
4. Anexo D: esquematiza las dispociones de ISO 27701 comparandolo con el RGPD.
5. Anexo E: esquematiza las disposiciones de ISO 27701 contra la ISO 27018 e ISO 29151.
6. Anexo F: Proporciona directrices para aplicar la ISO 27701 a la ISO 27001 e ISO 27002.

En la mayoría de casos, las organizaciones con certificación ISO 27001 deben comenzar en el Anexo F para comprender cómo la aplicación del SGIC encaja en su SGSI ISO 27001 existente. Este anexo se refiere a tres instancias de aplicación de la norma:

- Aplicación de estándares de seguridad.
- Adiciones a los estándares de seguridad.
- Refinamiento de los estándares de seguridad.

Las cláusulas 5 a 8 del SGIC amplían los requisitos de ISO 27001 para incorporar consideraciones de información personal. La cláusula 5 proporciona orientación específica al SGIC con respecto a los requisitos de seguridad de la información en ISO 27001 apropiados para una organización que actúa como controlador o procesador de información personal. Las organizaciones deben implementar una Declaración de Aplicabilidad (SoA) determinando si son controladores o procesadores (o ambos). La organización también puede integrar sus sistemas ISO 27001 e ISO 27701.

Anexo A + Cláusula 6 = **37 controles mejorados**

Anexo A + Cláusula 7 = **31 controles para controladores**

Anexo A - Cláusula 8 = **18 controles para procesadores**

# CONSIDERACIONES ADICIONALES

| | |
|---|---|
| **A continuación se detallan las consideraciones adicionales dentro de la cláusula 5 de la norma ISO 27701 que pueden observarse como adicionales a los requisitos existentes del SGSI:** | |
| **5.1** | Los requisitos de la norma ISO 27001 deben extenderse a la protección de la privacidad como potencialmente afectada por el procesamiento de información personal. El Anexo F proporciona una tabla muy visual. |
| **5.2.1** | Un requisito adicional a la cláusula 4.1 de la ISO 27001 es describir que la organización determinará su función como controlador y/o procesador de información personal. Además, se deben indicar los factores externos e internos que son relevantes para el contexto y afectan la capacidad de lograr resultados de su SGIC. Esto incluye cualquier cumplimiento legislativo como una consideración dentro del SGSI existente o los requisitos contractuales que hasta ahora se habían identificado en diferentes cláusulas o controles del anexo dentro de ISO 27001. |
| **Cuando una organización tiene identificados los roles de controlador y/o procesador de información personal, se deben determinar roles separados, cada uno de los cuales estará sujeto a un conjunto de controles diferentes.** | |
| **5.2.2** | Una consideración adicional a la cláusula 4.2 de ISO 27001 es el requisito de incluir a las partes interesadas con responsabilidades asociadas con el procesamiento de información personal. Esto puede incluir a los clientes, lo que nuevamente no es algo que se haya considerado previamente en un SGSI ISO 27001. Además, los requisitos relevantes para el procesamiento pueden ser determinados por requisitos legales,contractuales u objetivos. |
| **5.2.3** | El alcance del SGSI es requerido por la cláusula 4.3 de ISO 27001. Los factores del SGIC adicionales para el alcance incluyen el procesamiento de información. La determinación del alcance del SGIC puede requerir una revisión del SGSI debido a la interpretación de la seguridad de la información en la cláusula 5.1 de ISO 27701. |
| **5.2.4** | Además de la cláusula 4.4 de la ISO 27001, se requiere que una organización dentro de la nueva norma establezca, implemente, mantenga y mejore continuamente un SGIC de acuerdo con los requisitos de las cláusulas 4 a 10 de la norma ISO 27001:2013, ampliadas por los requisitos de la cláusula 5. |
| **5.3** | Dentro de la ISO 27001, las organizaciones deben demostrar su compromiso con el SGSI a través de iniciativas de liderazgo y la creación de políticas, roles, responsabilidades y orientación. Asimismo, el SGIC requiere un aporte similar de la gerencia junto con interpretaciones específicas relevantes como se indica en el punto 5.1 de la norma ISO 27701, que cubre todos los aspectos reflejados de la cláusula 5 del SGSI. |
| **5.4.1** | Los requisitos de la ISO 27001 para abordar riesgos y oportunidades requieren un aumento con las consideraciones de la cláusula 5.1 en la ISO 27701. Además, las evaluaciones de riesgos de seguridad de la información identificadas en la ISO 27001 son aplicables con los siguientes requisitos adicionales:<br>1. La organización debe evaluar los riesgos de seguridad de la información para identificar los riesgos asociados con la pérdida de confidencialidad, integridad y disponibilidad, dentro del alcance del SGIC.<br>2. La organización debe evaluacr los riesgos de privacidad para identificar los riesgos relacionados con el procesamiento de la información personal, dentro del alcance del SGIC.<br>3. La organización debe garantizar a lo largo de los procesos de evaluación de riesgos que la relación entre la seguridad de la información y la protección de la informacion personal se gestiona de forma adecuada.<br>Puede ser un proceso de evaluación de riesgos integrado o procesos paralelos que se controlan por separado, dependerá de lo que la organización quiera.<br>Además, la cláusula 6.1.2.d de la norma ISO 27001 se refinó para incluir una evaluación de las posibles consecuencias tanto para la organización como para los directores de información personal que resultarían si los riesgos identificados durante la 6.1.2.c (ISO 27001) se materializaran.<br>Se dan más consideraciones a la Declaración de Aplicabilidad de la organización al implementar la ISO 27001. Como una organización habría encontrado un enfoque de “exclusión y justificación” para producir el SoA en primera instancia, del mismo modo para el PIMS, no es necesario incluir todos los objetivos de control y controles enumerados en las áreas del Anexo durante la implementación del PIMS. Se puede identificar la justificación de la exclusión cuando los controles no se consideran necesarios. |
| **5.4.2** | Se deben considerar los objetivos de seguridad de la información de la organización contenido en la cláusula 6.2, aumentados por la interpretación de la cláusula 5.1 de la ISO 27701. |
| **5.5** | Las consideraciones de apoyo de la norma ISO 27001 en la cláusula 7 son aplicables junto con la interpretación adicional especificada en la cláusula 5.1 de la norma ISO 27701. |
| **5.6** | La operativa de la ISO 27001 en la cláusula 8, incluida la planificación del tratamiento de riesgos, es requerida de manera similar por la ISO 27701 junto con información adicional de la cláusula 5.1 de esta última norma. |
| **5.7/5.8** | Las consideraciones de seguimiento/medición y mejora del SGSI existente requieren un aumento de las consideraciones dadas en la cláusula 5.1 de la ISO 27701. |

**Los procesos identificados anteriormente indican que la cláusula 5.1 del nuevo estándar es un punto clave para la implementación del SGIC. La extensión de la protección de la privacidad para el procesamiento de información personal es un elemento clave para la implementación. Proporciona orientación en la consideración que se debe dar al abordar las cláusulas adicionales de la ISO 27701.**

| La siguiente tabla proporciona una descripción de la información de la página anterior: | |
|---|---|
| **Cláusula ISO 27001** | **Extensión ISO 27701** |
| **5.1**<br>**5.2**<br>**5.3**<br>**7.1**<br>**7.4** | Compromiso de la gerencia con la política de privacidad y la integración del SGIC en el SGSI, incluyendo:<br>**1.** Dotación de recursos / establecimiento de roles.<br>**2.** Comunicación (interna / externa).<br>**3.** Resultado esperado.<br>**4.** Control y orientación.<br>**5.** Mejora continua del SGIC. |
| **6.2** | SGIC/Objetivos de privacidad. |
| **7.2** | Perfiles de competencia de las personas asignadas a roles de privacidad. |
| **7.3** | Conocimiento de la política SGIC y cómo contribuye el personal al establecimiento y mejora del sistema. |
| **7.5** | Documentación del SGIC con consideraciones adicionales sobre información y documentación no orgánica para la organización. |
| **8.1** | Activación del tratamiento de riesgos del SGIC. |
| **8.2** | Proceso de evaluación de riesgos del SGIC. |
| **8.3** | Plan de tratamiento de riesgos del SGIC con modificaciones en los registros de riesgos existentes. |
| **9.1**<br>**9.2**<br>**9.3** | Rendimiento del SGIC y análisis de la eficacia del SGIC, incluyendo:<br>**1.** Auditoría interna.<br>**2.** Revisión por la dirección. |
| **10** | Consideraciones de mejora continua del SGIC. |