MOORE

LEGAL Y COMPLIANCE

ISO 27701:2019 TÉCNICAS DE SEGURIDAD – EXTENSIÓN A ISO/IEC 27001 E ISO/IEC 27002 PARA LA GESTIÓN DE LA INFORMACIÓN

ISO (International Organization for Standardization) ha publicado el pasado día 6 de agosto la norma ISO 27701, llamada ISO 27552 durante el período de redacción de la misma, constituye una extensión de la norma de requisitos ISO/IEC 27001 y de la guía ISO/IEC 27002 sobre sistemas de Gestión de Seguridad de la Información, que está **diseñado para permitir la adición de requisitos específicos del sector**, sin la necesidad de desarrollar un nuevo Sistema de Gestión, **aportando a las organizaciones los requisitos para administrar, gestionar los datos y proteger la privacidad de la información de identificación personal (PII)** contribuyendo al cumplimiento con otras normas, en especial con el Reglamento General de Protección de Datos.

Establece un marco para que los responsables y encargados del tratamiento de datos de carácter personal gestionen los controles de privacidad, a fin de reducir el riesgo para los derechos de privacidad de las personas.

El incremento exponencial que se está dando a la información personal y el tratamiento que se está dando debido a la necesidad de intercambio entre departamentos de una misma empresa o más si cabe, entre diferentes organizaciones para una correcta prestación de los servicios, hace necesario verificar que esta información esté debidamente gestionada y protegida mediante un Sistema de Gestión de Información de Privacidad (PIMS), acorde con la legislación y regulaciones específicas de cada país.

La necesidad de certificar el modelo de gestión sobre la privacidad en una organización, ha hecho necesaria la publicación de una nueva norma que establezca los requisitos y proporcione orientación para establecer, implementar, mantener y mejorar continuamente un Sistema de Gestión de Información de Privacidad (PIMS).

Los responsables del tratamiento y/o los Encargados del tratamiento que han implementado ISO 27001 podrán usar ISO 27701 para ampliar sus esfuerzos de seguridad para cubrir la gestión de la privacidad, incluido su procesamiento de datos personales / PII (información de identificación personal), lo que les ayudará a demostrar el cumplimiento (responsabilidad proactiva) de las leyes de protección de datos como RGPD.

Las organizaciones sin un SGSI también pueden implementar ISO 27001 e ISO 27701 de forma conjunta como un solo proyecto de implementación. La razón es que la ISO 27701 simplemente extiende los requisitos y la orientación proporcionados por ISO 27001 y su código de práctica, ISO 27002, por lo que no hay necesidad de combinar dos sistemas de gestión separados.

Ha sido diseñado para ser utilizado por todos responsables del tratamiento y/o los Encargados **del tratamiento que traten datos personales** y es **aplicable a todos los tipos y tamaños de organizaciones**, incluidas empresas públicas y privadas, entidades gubernamentales y organizaciones sin fines de lucro, con independencia de la complejidad o el país en el que operen.

Al igual que ISO 27001**, aboga por un enfoque basado en el riesgo** para que cada organización conforme aborde los riesgos específicos que enfrenta, así como los riesgos para los datos personales y la privacidad.

Estructura de la norma ISO 27701

De una manera más detallada, la ISO 27701 amplía los requisitos de la ISO 27001 e ISO 27002 para tener en cuenta la protección de la privacidad, potencialmente afectada por el tratamiento y procesamiento de información de carácter personal, en los siguientes apartados:

Cláusula 5: Los requerimientos establecidos en este apartado tienen trazabilidad con los apartados 4 al 10 de la norma ISO 27001, ampliando los requerimientos sobre protección de la información específicamente para el apartado 4 sobre el contexto organizacional y el apartado 6 relativo a la planificación de la gestión de riesgos, no aportando necesidades adicionales en el resto de los apartados.

Cláusula 6: Este apartado amplía los requerimientos establecidos en la guía de buenas prácticas ISO 27002 y los controles establecidos en el Anexo A de la ISO 27001, haciendo un repaso de los 114 controles y ampliando los requisitos sobre la protección de la información en controles puntuales de los dominios 5 al 18, con excepción del dominio 17 (Seguridad de la información en la continuidad del negocio) donde no se establecen medidas adicionales a las ya existentes.

Cláusula 7: Determina controles adicionales y la guía de implementación de estos para los propietarios de la Información de identificación personal (PII). Estos controles no han de ser implementados en su totalidad, sino que su aplicabilidad o exclusión deben ser debidamente justificadas.

Cláusula 8: De manera similar a los requerimientos de la cláusula 7, este apartado establece controles adicionales y una recomendación de implantación para los encargados de tratar información personal de terceros contratados, teniendo en cuenta también si éstos, a su vez, subcontratan servicios.

La norma, hace referencia a la legislación sobre protección de datos vigente en el país donde se implemente, los que supone una base ideal para todas aquellas organizaciones que quieran aportar una confianza en sus clientes, apoyado en un proceso de mejora continua y transparencia de sus procesos y procedimientos, ya que se estima que esta norma pueda cubrir futuras certificaciones asociadas al Reglamento General de Protección de Datos (RGPD) al ser una norma certificable asociada a la ISO 27001.