ISO 27701:2019

Sistema de Gestión de la Privacidad de los Datos

ISO 27701:2019 Sistema de Gestión de la Privacidad de los Datos

ISO 27701:2019 es una norma internacional que establece los requisitos y proporciona orientación para implementar, mantener y mejorar un sistema de gestión de la información de privacidad (SGIP) dentro de una organización. Desarrollada por la Organización Internacional de Normalización (ISO), esta norma complementa a ISO/IEC 27001 e ISO/IEC 27002 y se centra en garantizar que una organización gestione adecuadamente la información personal identificable (PII), cumpliendo con las expectativas de privacidad de las partes interesadas, así como con los requisitos legales, reglamentarios y contractuales aplicables.

Los principales objetivos son:

- Planificación y diseño de controles de privacidad: Establecer procesos efectivos para planificar e implementar medidas de protección de la información personal identificable (PII), alineados con los requisitos legales, regulatorios y contractuales, así como con las expectativas de las partes interesadas.
- Transición de procesos de tratamiento de PII: Gestionar de forma controlada la incorporación o modificación de procesos que involucren el tratamiento de PII, asegurando que se mantenga la confidencialidad, integridad y disponibilidad de la información durante los cambios.
- Entrega y mejora continua del sistema de gestión de privacidad: Garantizar la protección efectiva y eficiente de la PII, promoviendo la mejora continua del sistema de gestión de la información de privacidad (SGIP) para adaptarse a cambios normativos, tecnológicos y organizativos.

Las priincipales ventajas:

- Protección fortalecida de la privacidad: Proporciona un marco sólido para proteger la información personal, mejorando la confianza de clientes, usuarios y otras partes interesadas.
- Alineación con requisitos legales y normativos: Facilita el cumplimiento de leyes de protección de datos como el Reglamento General de Protección de Datos (GDPR) de la UE u otras normativas locales e internacionales.
- Mejora continua de la gestión de privacidad: Promueve la evaluación y mejora constante de los controles de privacidad, adaptándose a nuevas amenazas, tecnologías o requisitos legales.

Un SGIP se enfoca diferentes aspectos clave:

1. Enfoque al cliente

La Norma Internacional ISO 27701:2019 establece los requisitos y proporciona orientación para implementar y mantener un sistema de gestión de la información de privacidad (SGIP). Su objetivo principal es permitir que las organizaciones demuestren su capacidad para gestionar de forma segura y responsable la información personal identificable (PII), cumpliendo con los requisitos legales, contractuales y las expectativas de las partes interesadas.

La norma promueve la mejora continua del sistema de gestión, fortaleciendo la confianza en el tratamiento de la información personal y reduciendo riesgos relacionados con la privacidad.

ISO 27701:2019 es una norma genérica, aplicable a todo tipo y tamaño de organizaciones, tanto públicas como privadas, y puede ser adoptada por responsables y encargados del tratamiento de datos, independientemente del sector al que pertenezcan.

2. Liderazgo

La alta dirección debe demostrar liderazgo y compromiso con respecto al Sistema de Gestión de la Información de Privacidad (SGIP). Para ello, debe definir una visión clara y una dirección estratégica orientada a la protección de la información personal identificable (PII), estableciendo los objetivos de privacidad y la política de protección de datos personales de la organización.

Los líderes en todos los niveles deben fomentar una cultura de protección de la privacidad, estableciendo una unidad de propósito y dirección que permita la participación activa de las personas en el cumplimiento de los objetivos relacionados con la gestión de la privacidad.

3. Compromiso con las personas

La alta dirección debe revisar el Sistema de Gestión de la Información de Privacidad (SGIP) de la organización en intervalos planificados, con el fin de asegurarse de su conveniencia, adecuación, eficacia y alineación continua con la dirección estratégica y los objetivos de privacidad de la organización.

El compromiso de las personas, entendido como la participación activa, informada y responsable de todos los miembros de la organización, es fundamental para el éxito del SGIP. La protección de la información personal requiere una cultura organizacional que promueva la conciencia, el cumplimiento y el respeto por la privacidad.

Las personas competentes, comprometidas y empoderadas son un recurso clave para garantizar el cumplimiento de los requisitos legales, regulatorios y contractuales en materia de privacidad.

4. Enfoque a procesos

El enfoque a procesos en el contexto de ISO 27701:2019 implica la definición, implementación y gestión sistemática de los procesos relacionados con el tratamiento de la información personal identificable (PII), así como sus interacciones, con el objetivo de alcanzar los resultados previstos conforme a la política de privacidad y la dirección estratégica de la organización.

El logro de un desempeño eficaz en la protección de la privacidad requiere que los procesos sean evaluados continuamente con base en datos, evidencias y resultados medibles, permitiendo identificar oportunidades de mejora y garantizar el cumplimiento de los requisitos legales y contractuales.

Los procesos de mejora en el SGIP deben seguir un enfoque estructurado y coherente, aplicando metodologías apropiadas para todos los procesos involucrados en la recolección, almacenamiento, uso, transferencia y eliminación de la PII, asegurando así la integridad, confidencialidad y disponibilidad de la información.

5. Mejora continua

La organización debe mejorar continuamente la conveniencia, adecuación y eficacia del Sistema de Gestión de la Información de Privacidad (SGIP), garantizando que se mantenga alineado con los objetivos de privacidad, los cambios normativos y las expectativas de las partes interesadas.

Para lograrlo, la organización debe considerar los resultados del análisis y la evaluación del desempeño del SGIP, así como las salidas de la revisión por la dirección, con el fin de identificar necesidades u oportunidades de mejora que refuercen la protección de la información personal identificable (PII).

La mejora es una actividad orientada a incrementar el desempeño del sistema de gestión, ya sea a nivel de procesos, controles, medidas de seguridad, formación del personal o relaciones con terceros. La mejora del desempeño puede ayudar a la organización a anticiparse a riesgos, responder eficazmente a incidentes, y cumplir de manera proactiva con los requisitos legales y contractuales en materia de privacidad.

Mejorar los procesos del SGIP puede traducirse en beneficios como reducción de riesgos, mayor eficiencia operativa, ahorro de recursos, disminución de incidentes de seguridad y mayor confianza de clientes y partes interesadas.

Las actividades de mejora pueden ir desde ajustes incrementales hasta transformaciones significativas en la estructura, los procesos o los controles del SGIP. La organización debería establecer objetivos claros de mejora, basados en el análisis del desempeño, auditorías, revisiones, brechas identificadas y evolución de los requisitos regulatorios.

6. Toma de decisión basada en evidencia

Los objetivos del Sistema de Gestión de la Información de Privacidad (SGIP) deben ser coherentes con la política de privacidad de la organización, ser medibles, tener en cuenta los requisitos legales, regulatorios y contractuales aplicables, y ser pertinentes para asegurar el cumplimiento en el tratamiento de la información personal identificable (PII).

Dichos objetivos deben contribuir al fortalecimiento de la confianza de las partes interesadas y a la mejora continua de la protección de la privacidad, debiendo ser monitoreados, comunicados y actualizados periódicamente, según corresponda.

Uno de los pilares fundamentales de la ISO 27701:2019 es la toma de decisiones basada en evidencia, que busca asegurar que todas las decisiones en materia de privacidad se fundamenten en datos objetivos, verificables y pertinentes, y no en suposiciones o juicios intuitivos.

Este enfoque implica que las organizaciones deben recopilar, analizar y utilizar información confiable —como resultados de auditorías, análisis de riesgos, reportes de incidentes o evaluaciones de impacto en la privacidad— para sustentar decisiones estratégicas y operativas relacionadas con la gestión de la PII.

7. Gestión de las relaciones

La organización debe establecer y mantener procesos que fomenten el compromiso del personal con respecto al cumplimiento de los objetivos de privacidad y la protección de la información personal identificable (PII).

La participación activa de las personas que intervienen en el tratamiento de datos personales es esencial para asegurar el desempeño eficaz del Sistema de Gestión de la Información de Privacidad (SGIP). Los líderes en todos los niveles deben promover una cultura de privacidad, motivando a sus equipos a involucrarse en la mejora continua y en el cumplimiento de los requisitos legales, regulatorios y contractuales relacionados con la privacidad.

¿Beneficios de la certificación ISO 27701?

entajas de implementar y certificar un Sistema de Gestión de la Información de Privacidad

La implementación y certificación de la ISO 27701:2019 permite a las organizaciones demostrar altos estándares en la gestión de la privacidad y protección de datos personales, fortaleciendo su reputación y facilitando la generación de nuevas oportunidades de negocio, especialmente en contextos donde la confianza en el tratamiento de la información es esencial.

La certificación se obtiene tras una auditoría satisfactoria que verifica el cumplimiento con los requisitos establecidos por la norma. Entre sus principales ventajas se encuentran:

- Cumplimiento con los requisitos legales y reglamentarios en materia de protección de datos personales, tanto a nivel nacional como internacional.
- Facilidad para expandirse hacia nuevos mercados que requieren garantías en la gestión de la privacidad.
- Identificación y tratamiento proactivo de los riesgos relacionados con el tratamiento de información personal identificable (PII).
- Mejora en la gestión de relaciones con proveedores, mediante el establecimiento de requisitos claros sobre privacidad y seguridad de la información.
- Incremento de la eficacia operativa a través de procesos más seguros, estructurados y eficientes.
- Obtención de una ventaja competitiva frente a otras organizaciones que no cuentan con un sistema certificado de gestión de privacidad.
- Proyección de una imagen sólida y confiable respaldada por una entidad certificadora independiente.
- Incremento en la confianza de los clientes actuales y potenciales, al evidenciar el compromiso con la protección de sus datos personales.

¿Por qué elegir Intercet para realizar una auditoría de certificación de la norma ISO 27701?

Hemos perfeccionado nuestro enfoque para adaptarnos a las exigencias del mercado, por ello somos líderes en el servicio de certificación de sistemas de gestión, con el compromiso de asegurar la satisfacción de nuestros clientes.

Entendemos que la industria tiene sus propias particularidades y desafíos. Por lo tanto, nuestro servicio de certificación se adapta específicamente a las necesidades de su sector, asegurando una evaluación efectiva del estándar.

Acreditaciones

SCC
Consejo de normas de Canadá

UAF
Fundación de Acreditación USA

KAB
Junta de Acreditación de Corea

EXEMPLAR GLOBAL

Reconocimientos

IAF
Foro Internacional de Acreditación

APAC
Cooperación de Acreditación Asia-Pacífico

Proceso de Certificación