Intedya
International Dynamic Advisors

Ampliación a ISO 27701 Sistema de Gestión de Información de Privacidad - Extensión a ISO / IEC 27001 e ISO / IEC 27002

Solicitar **Información**

Autoevaluación **On Line**

Descargar **Presentación**

Ver video de **Presentación**

Intedya
International Dynamic Advisors

La protección de los datos de carácter personal se ha convertido en un aspecto fundamental que debe ser considerado por cualquier organización durante el desarrollo de sus actividades. El elevado volumen de información que se maneja en cualquier actividad empresarial (en particular de clientes, proveedores, trabajadores,...) así como la creciente complejidad e interconexión de los sistemas de información, ha hecho necesaria la definición de una normativa de protección de datos consistente y que permita **asegurar una protección adecuada de la privacidad de las personas, y de derechos fundamentales como el derecho al honor y la intimidad**.

El incumplimiento de los requisitos de estas normativas puede suponer, atendiendo a lo establecido por las normativas, **elevadas infracciones o sanciones, que pueden poner en riesgo la continuidad de cualquier organización**.

Obtener la certificación según los requisitos de ISO 27701 como extensión de ISO 27001 permite evidenciar a terceros un cumplimiento efectivo de las normativas de protección de datos, consiguiendo consolidar **la confianza de los clientes, proteger la reputación de una organización**, y **protegerse contra la responsabilidad legal y contra las sanciones que puedan derivarse del incumplimiento de la normativa.**

Principales **REQUISITOS**

- La consideración del **CONTEXTO** incluyendo en el mismo los tratamientos de datos realizados por la organización;
- Identificación de **ACTIVIDADES DE TRATAMIENTO;**
- Identificación de **LEGITIMACIÓN** en el tratamiento de datos personales;
- EVALUACIÓN, GESTIÓN y TRATAMIENTO de los **RIESGOS**, que pueden afectar a la privacidad;
- **EVALUACIÓN DE IMPACTO EN LA PRIVACIDAD**
- **DEFINICIÓN DE RESPONSABILIDADES** en materia de seguridad de la información;
- Establecimiento de **MECANISMOS DE CONTROL** de acceso físico, lógico, control en red y criptográficos adecuados al nivel de criticidad de los datos;
- Asegurar la seguridad de la información en el **SERVICIO A TERCEROS;**
- Asegurar el cumplimiento de los derechos de los afectados en cuanto al tratamiento de sus datos;
- Disponer de **CONTRATOS DE CONFIDENCIALIDAD** con los empleados;
- Cumplimiento con la **LEGISLACIÓN APLICABLE**;
- **GESTIÓN DE INCIDENCIAS** relativas a la seguridad de la información y a la privacidad de las personas;
- **TOMA DE CONCIENCIA Y COMPROMISO**;
- Proporcionar la **FORMACIÓN** necesaria para **garantizar la competencia de las personas;**
- **PRESERVACIÓN DE LA CONTINUIDAD** de las operaciones de la organización y de las actividades de tratamiento de datos.

Ejemplos de **ACCIONES PRÁCTICAS A IMPLEMENTAR**

- Asegurar que en el análisis de riesgos se consideran los riesgos asociados a la privacidad de las personas y a la protección de datos de carácter personal.
- Complementar las Políticas de Seguridad de la Información con Políticas específicas de Protección de Datos de carácter personal.
- Realizar una Evaluación de Impacto de la Privacidad, en los casos que sea requerido por la normativa
- Establecer los procedimientos y mecanismos necesarios para interactuar con las autoridades y grupos de interés especial (Agencias de Protección de Datos).
- Formalizar los acuerdos y contratos necesarios para asegurar la protección de datos personales cuando exista acceso a los mismos por parte de terceros.
- Analizar la licitud de los tratamientos de datos personales, asegurando la legitimidad de los mismos según lo definido en las normativas de protección de datos (consentimiento, relación contractual, requisito legal, interés legítimo...)
- Aplicar las medidas de seguridad necesarias, acordes con la criticidad de los datos personales manejados por la organización.
- Desarrollar los procedimientos y mecanismos necesarios para asegurar el ejercicio de los derechos de los titulares de los datos (información, acceso, cancelación, oposición, rectificación,...).
- Desarrollo de textos informativos adecuados para el cumplimiento del derecho de información y el principio de transparencia.
- Reforzar las medidas de seguridad implementadas según lo definido en la ISO 27001 (Anexo A), con las medidas específicas necesarias para la adecuada protección de la información de privacidad.
- Desarrollar el Registro de Actividades de Tratamiento en los casos que sea necesario o requerido por la normativa.
- Definir los procedimientos, herramientas y registros necesarios para realizar una gestión adecuada de las brechas de seguridad que afecten a información de privacidad (incluyendo las notificaciones a las Autoridades de Control y partes afectadas).
- Definir las responsabilidades necesarias para asegurar la adecuada gestión de la información de privacidad, incluyendo las figuras requeridas por las normativas de protección de datos (Delegado de Protección de Datos).
- Formar y sensibilizar al personal en cuanto a la protección de los datos personales y al cumplimiento de las normativas

relacionadas.

*Las acciones indicadas son sólo ejemplos, estás deberán ser adaptadas a la realidad y necesidades de cada organización

Ventajas para **LA ORGANIZACIÓN**

Las organizaciones que complementan su SGSI con un Sistema de Gestión de Información de Privacidad (PIMS) según la norma ISO 27701 consiguen implementar los procesos necesarios para asegurar el cumplimiento de los requisitos internacionales relacionados con la protección de los datos de carácter personal y ofrecen cobertura a los derechos de los interesados. Igualmente se consiguen definir las responsabilidades necesarias para la gestión de la protección de datos personales en la organización, incluyendo figuras requeridas por la normativa, como el Delegado de Protección de Datos, se reduce la posibilidad de infracciones o sanciones derivadas de las normativas y permite evidenciar ante las Autoridades de Control una gestión proactiva. También facilita una gestión adecuada de los riesgos relativos a la privacidad, permitiendo el establecimiento de las medidas técnicas y organizativas adecuadas y definir procedimientos y mecanismos adecuados para la gestión de las incidencias o brechas de seguridad que afecten a los datos de carácter personal.

Ventajas para **LOS CLIENTES**

Implementar un Sistema de Gestión de la Información de Privacidad (PIMS) permite a sus clientes:

- Incrementar su confianza en cuanto a la gestión de la información personal por parte de la organización.
- Obtener garantías de que se respetan los derechos que la normativa de protección de datos otorga a los titulares de los datos (acceso, rectificación, cancelación, información,...).
- Tener evidencia fiable de la adecuada protección de sus derechos al honor, intimidad y privacidad.
- Mantenimiento de la integridad, confidencialidad y disponibilidad de la información de los clientes según sus necesidades.
- Tener un conocimiento claro de cómo se trata su información personal por parte de la organización.
- Tener evidencias de una gestión y protección adecuada frente a los riesgos que puedan afectar su información personal.
- Disponer de los mecanismos necesarios para una adecuada gestión de las posibles incidencias que puedan afectar a sus datos.

Ventajas para **EL MERCADO**

En general, en un mercado y en una sociedad cada vez más dependiente de la información y, en particular, de los datos de carácter personal, implementar un Sistema de Gestión de Información de Privacidad permite:

- Servir como elemento distintivo y diferenciador frente a la competencia, ofreciendo garantías de una gestión eficaz de los datos personales.
- En general, reforzar la imagen de la organización a terceros y a las diferentes partes interesadas.
- Evidenciar de forma eficaz el cumplimiento de los requisitos respecto a la normativa de protección de datos, siendo este un aspecto cada vez más requerido para posibilitar la participación en proyectos y, en especial, en concursos públicos.
- Favorece el mercado internacional, estableciendo requisitos de protección de datos con un enfoque internacional y considerando los requisitos de las diferentes normativas de protección de datos
- Imagen de empresa comprometida con la protección de la privacidad.

- Garantía a terceros del cumplimiento de la normativa de protección de datos.

Sectores **DE APLICACIÓN**

Hoy en día, prácticamente todas las organizaciones, independientemente de su sector o tamaño, manejan datos de carácter personal, ya sea de sus trabajadores, clientes u otras partes interesadas, por lo que podría decirse que cualquier organización se ve afectada por los requisitos de las cada vez más reguladas normativas de protección de datos.

Esta extensión de la ISO 27001, permite que aquellas organizaciones que tienen desarrollado (o que prevén desarrollar) un Sistema de Gestión de Seguridad de la Información (ISO 27001) complementen esta gestión con los procesos, políticas y medidas necesarias para asegurar una protección adecuada de los datos personales, y un cumplimiento efectivo de las normativas de aplicación.

Además, la Extensión ISO 27701, tiene vocación universal y pretende establecer requisitos generales que permitan dar cumplimiento a las diferentes normativas de protección de datos, independientemente del ámbito territorial de la organización. En particular, en algunos sectores donde la información de carácter personales es epecialmente crítica (sanitario, bancario, de telecomunicaciones, académico, asistencial,...)la implementación de esta gestión de la información de privacidad, se convierte en algo imprescindible.