Intedya
International Dynamic Advisors

ISO/IEC 27001 Extensión ISO/IEC 27701 - Sistemas de Gestión de Seguridad de la Información y Gestión de Información de Privacidad

Solicitar **Información**

Autoevaluación **On Line**

Descargar **Presentación**

Ver video de **Presentación**

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**

- Realización del análisis de riesgos de seguridad de la información.
- Realización de Evaluación de Impacto en la privacidad.
- Desarrollo del Registro de Actividades de Tratamiento de datos personales
- Formalización de contratos de confidencialidad y de tratamiento externo de datos con los empleados y proveedores.
- Formalización de acuerdos prestación de servicio.
- Nombramiento del Delegado de Protección de Datos y otras responsabilidades de seguridad.
- Desarrollo de textos informativos para el cumplimiento del derecho de información.
- Desarrollo de mecanismos para la atención al ejercicio de los derechos de los afectados.
- Uso de credenciales de acceso a las instalaciones para visitantes.
- Mecanismos que obstaculicen el acceso a las áreas seguras: dispositivos biométricos, etc.
- Uso de dispositivos de alimentación interrumpida.
- Uso de controladores de temperatura CPD.
- Uso de licencias legales.
- Realización de planes de continuidad
- Planes de prueba: caída de suministro eléctrico, fallos en los servidores, fallo comunicaciones, incendio edificio, etc.
- Política de gestión de contraseñas.
- Limitar la utilización de usuarios genéricos y los permisos de administración.
- Restringir los puertos USB a puestos determinados.
- Implantar y configurar un antivirus para todos los equipos de la organización, incluyendo los dispositivos móviles
- Instalación de Firewalls, VPN.
- Controlar y prohibir el acceso remoto hacia la propia organización.
- Limitar la navegación a páginas de ciertos contenidos y Sistemas de Detección de Intrusos.
- Realización de copias de seguridad.

- Segmentación de redes y conexiones seguras.
- Proteger las claves de acceso a sistemas, datos y servicios, almacenándolas de forma cifrada.
- Uso certificado digitales para el intercambio de información.

*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**

- Gestión de forma segura de la información crítica y sensible de nuestros clientes, garantizado que se establecen todos los controles necesarios para su preservación.
- Confianza de los clientes en cuanto a la gestión de su información de privacidad y al respeto a sus derechos al honor, intimidad y privacidad.
- Mantenimiento de la integridad y disponibilidad de la información de los clientes según sus necesidades
- Garantía de los derechos de los afectados en cuanto al tratamiento de sus datos (acceso, rectificación, cancelación, información,...)

Ventajas para **EL MERCADO**

- Empresas comprometidas con la seguridad de la información, que garantizan una adecuada gestión de la información con la que trabajan.
- Elemento distintivo frente a la competencia.
- Imágen de empresa comrpometida con la protección de la privacidad.
- Garantía a terceros del cumplimiento de la normativa de protección de datos.

Sectores **DE APLICACIÓN**

La **norma ISO 27001**, tiene **vocación universal**, aplicable a organizaciones de **todos los sectores y tamaños,** y que describe de qué debe constar un **sistema de gestión de la seguridad de la información en cualquier tipo de organización.** La norma es especialmente útil cuando la **protección de la información es crítica,** como por ejemplo, en las áreas de **gobierno, banca y finanzas, salud, empresas de servicios de tecnología de la información o comunicaciones** , o cualquier otro ámbito donde los activos de información requieran de una adecuada protección.

La extensión ISO 27701, adquiere mayor importancia en aquellas organizaciones que dispongan de datos personales especialmente críticos o en volúmenes elevados, sin embargo, es perfectamente aplicable en cualquier ámbito, considerando que el tratamiento de datos personales es inherente a cualquier organización independientemente de su tamaño o sector.