Certificación ISO / IEC 27701 – Protección de la privacidad

Hace pocos días HostDime Brasil obtuvo esta certificación ISO / IEC 27701(y seguramente otras ramas de la compañía también lo hagan en el futuro próximo).

HostDime es una empresa global de cloud computing ubicada en distintas partes del mundo, que opera en el mercado tecnológico desde hace más de 14 años y atiende a miles de clientes. La misión de la organización es garantizar la disponibilidad total de los sistemas críticos y ofrecer soluciones de TI estructurales lógicas a empresas de todo el mundo.

Introducción

Brinde a sus clientes la confianza que se merecen beneficiándose de una certificación reconocida en la gestión de la protección de la privacidad con ISO / IEC 27701. Demuestra su compromiso con la protección y confidencialidad de los datos personales en la continuidad de sus acciones realizadas para asegurar su sistema de información.

El estándar ISO 27701, publicado en agosto de 2019, se basa en dos estándares de seguridad de la información ISO y los amplía para incluir la protección de datos personales: ISO 27001, que certifica un sistema de gestión de seguridad de TI; ISO 27002, que detalla buenas prácticas para implementar las medidas de seguridad necesarias.

¿En qué consiste esta certificación?

La ISO / IEC 27701 es una certificación que permite el reconocimiento de un sistema de gestión para la protección de la privacidad en el marco de la gestión de riesgos relacionados con el tratamiento de datos personales. Es una extensión de las normas 27001 y 27002.

Esto significa que para acceder a la certificación ISO / IEC 27701, es necesario cumplir con los requisitos relacionados con el sistema de gestión de seguridad de la información. Al final de la auditoría, si es favorable, se le emiten dos certificados: ISO / IEC 27001 e ISO / IEC 27701.

Desarrollado originalmente como ISO / IEC 27552, ISO 27701 proporciona requisitos específicos y orientación para establecer, implementar, mantener y mejorar continuamente un Sistema de Gestión de la Información de Privacidad (PIMS) como una extensión del Sistema de Gestión de Seguridad de la Información (SGSI) flexible definido en ISO 27001, para que tenga en cuenta las protecciones de privacidad necesarias para procesar PII además de la seguridad de la información.

Al igual que la norma ISO 27001, ISO 27701 no espera que las organizaciones adopten todos y cada uno de los controles en todas las situaciones. En cambio, requiere que las organizaciones comprendan el contexto particular en el que procesan la PII y ajusten el conjunto particular de controles y la implementación relacionada de esos controles de una manera que sea apropiada para sus actividades de procesamiento.

Desglosando conceptos

Para comprender mejor el nuevo estándar, deben entenderse dos términos clave: controladores y procesadores. Estos términos

se encuentran en muchas leyes y regulaciones de privacidad, incluido el GDPR.

Por lo general, un «controlador» es la entidad que dirige la razón por la que se recopila y procesa la PII en primer lugar, y el «procesador» es una entidad legal separada (es decir, no un empleado) responsable de procesar dichos datos en nombre de ese controlador. El estándar recientemente publicado se aplica tanto a los controladores como a los procesadores de PII, independientemente de las jurisdicciones y los sectores en los que operan, y también incluye asignaciones al GDPR y a la ISO / IEC. 29100, marcos de seguridad ISO / IEC 27018 e ISO / IEC 29151.

Ventajas y beneficios

- Demostrar la implementación de una política de datos controlados.
- Certificar un alto nivel de confidencialidad y protección de la privacidad
- Proteger los datos personales controlando los riesgos
- Beneficiarse de la certificación facilitada por su complementariedad con ISO / IEC 27001
- Fortalecer los lazos de confianza con sus clientes con certificación reconocida
- Estar en línea con las leyes y regulaciones relacionadas con la protección de datos personales.

¿Cuáles empresas y organizaciones se ven afectadas por esta norma?

La certificación ISO / IEC 27701 está dirigida tanto a organismos que ya cuentan con la certificación ISO / IEC 27001 como a todos aquellos que deseen que se reconozcan sus medidas a favor de la protección de datos, ya sean responsables del tratamiento y / o sub- procesadores, de acuerdo con las leyes

y regulaciones existentes.

Los requisitos de ISO 27701

Para estandarizar y fortalecer la protección de datos personales, ISO 27701, extiende el sistema de gestión de seguridad de la información para incluir las particularidades del tratamiento de datos personales como:

- Determinación del papel del organismo a certificar (controlador de datos , subcontratista);
- Gestión unificada de los riesgos de TI para la organización y riesgos para la privacidad de las personas interesadas,
- Designación de una persona responsable de la protección de la privacidad;
- Conciencia del personal, clasificación de datos, protección de medios extraíbles, gestión de acceso y cifrado de datos, copia de seguridad de datos, registro de eventos;
- Condiciones de transferencia de datos, protección de la privacidad por diseño y por defecto, gestión de incidentes; cumplimiento de requisitos legales y reglamentarios, etc.
- Aporta medidas específicas para el tratamiento de datos personales, teniendo en cuenta el papel del organismo (responsable del tratamiento, subcontratista, subcontratista o subcontratista): principios fundamentales: propósito del procesamiento , base legal , obtención y retiro del consentimiento, inventario de las operaciones de procesamiento, evaluación del impacto en la privacidad ; derechos de las personas: información, acceso, rectificación, supresión, toma de decisiones automatizada; protección de la privacidad por diseño y por defecto (privacidad por diseño y por defecto): minimización, des-identificación y eliminación de datos, período de retención; contratos de

subcontratación, transferencias e intercambio de datos.

De manera similar a los estándares ISO existentes, los suplementos ISO 27701, este nuevo estándar ISO puede convertirse en el estándar de facto de atención para que las organizaciones protejan la información de identificación personal (PII) y puede usarse para demostrar el cumplimiento de las regulaciones de privacidad en todo el mundo, incluidos los Datos generales Reglamento de protección (UE) 2016/679 (GDPR).

Requisitos aplicables a controladores y procesadores

Confidencialidad

Las personas autorizadas para acceder a la PII deben firmar un acuerdo de confidencialidad.

Análisis de riesgo

Se debe realizar una evaluación de riesgos de privacidad para identificar los riesgos de procesamiento de PII.

Supervisión

Las organizaciones deben designar a una persona que sea responsable de desarrollar, implementar, mantener y monitorear su programa de gobierno y privacidad.

Entrenamiento

Se requiere capacitación en conciencia de privacidad para el personal que tiene acceso a PII.

Procesos internos

Las organizaciones deben adoptar varias políticas y procedimientos, como planes de respuesta a incidentes por violaciones de PII.

Mantenimiento de registros

ISO 27701 requiere que las organizaciones mantengan un registro de todas las actividades de procesamiento de PII, incluidas las transferencias de PII entre jurisdicciones y las divulgaciones a terceros.

Leer también: HostDime con certificación SOC 2 Tipos I y II: seguridad, disponibilidad, integridad, confidencialidad, privacidad ; Data Center Tier IV, qué es, en qué consiste, cuáles son sus características y funcionalidades ; Construcción del data center