GUIA

ISO 27018:2023

Sistemas de gestión de protección de la información de protección personal (PII) en servicios de nube pública— Requisitos.

La norma ISO/IEC 27018 es el código de prácticas internacional diseñado específicamente para la protección de datos personales (PII) en nubes públicas.

Funciona como una extensión sectorial de ISO/IEC 27001 y proporciona directrices detalladas para los proveedores de servicios en la nube (CSP) que actúan como encargados del tratamiento de datos (*data processors*).

Estructura y Funcionamiento Técnico

El estándar optimiza la gobernanza de datos en la nube dividiéndose en dos grandes pilares normativos:

Ampliación de Controles Existentes:

Añade directrices específicas de privacidad en la nube a los controles estándar heredados de ISO/IEC 27002.

Anexo A (Controles de Privacidad Nativos):

Incorpora un conjunto de principios específicos alineados con el marco de privacidad global ISO/IEC 29100.

Objetivos y Principios Clave de Privacidad

Cualquier organización que adopte o se certifique bajo este estándar debe cumplir con las siguientes obligaciones técnicas:

Consentimiento y Elección:

Garantizar que los datos solo se procesen siguiendo instrucciones explícitas del cliente (controlador de los datos).

Propósito de Uso:

Prohibir estrictamente el uso de los datos personales para fines comerciales o de marketing sin autorización expresa.

Transparencia de Ubicación:

Informar de manera clara y accesible en qué regiones geográficas se almacenan y procesan físicamente los datos personales.

Notificación de Brechas:

Establecer un protocolo automatizado para registrar y notificar de inmediato cualquier incidente o violación de seguridad a los clientes afectados.

Destrucción Definitiva:

Garantizar el borrado seguro y completo de la información tras la finalización de los contratos de servicio.

Contexto de Versiones y Transición Activa

La evolución tecnológica y la publicación de la última actualización de ISO/IEC 27001:2022 (que reestructuró y redujo los controles de seguridad de 114 a 93) obligaron a modernizar este código de prácticas.

La nueva versión ISO/IEC 27018:2025 ha reemplazado formalmente a las ediciones previas (como la de 2019) para lograr una alineación técnica exacta con la estructura de controles actual de la familia de seguridad de la información.

Las empresas tecnológicas que operan plataformas de infraestructura o software en la nube integran esta certificación junto a ISO/IEC 27017 (seguridad en la nube) para respaldar legalmente su cumplimiento normativo frente a regulaciones estrictas como el RGPD de la Unión Europea.

Para ver el contenido completo de información específica contáctanos, la Norma ISO 27018:2023 se incluye en Gap Analysis.

Atención a Clientes
Lic. Alejandra Morales / Ing Gerardo García
Dirección Comercial WST / Dirección Operaciones WST
55 6581 0662 / 55 6581 0123
licmorales@iso-irca.com / inggarcia@iso-irca.com