

# EVALUACIÓN DE CUMPLIMIENTO ISO 27001

La Seguridad de la información es lo más importante para cada organización que empieza en los niveles más altos. Las organizaciones deben garantizar la confidencialidad, integridad y disponibilidad (CIA) de su información digital para evitar cualquier interrupción en las operaciones comerciales. Incrementar los riesgos de seguridad de información de los actores de amenaza, tanto interna como externa, agregar los desafíos de los requerimientos reglamentarios que siempre están evolucionando. Las organizaciones deben monitorear continuamente a las personas, procesos y tecnología para regular y administrar los riesgos de seguridad.

Sin los marcos de trabajo de control y administración adecuados, un incumplimiento a los datos puede tener impacto a largo plazo, incluso la pérdida de ganancias, pérdida de reputación y potencialmente, la pérdida de empleados, clientes y confianza de los interesados.

ISO 27001 es un marco de trabajo de seguridad de la información editado por la Organización Internacional de Normalización (ISO, por sus siglas en inglés) para ayudar a las organizaciones a identificar, analizar y abordar los riesgos de seguridad de la información. Una evaluación de cumplimiento ISO 27001 ayuda a las organizaciones a revisar y comprender las políticas y procedimientos adecuados necesarios para cumplir con los requerimientos del Sistema de Administración de Seguridad de la Información (ISMS, por sus siglas en inglés). Es el primer paso para garantizar la CIA de la información digital de una compañía y garantizar las operaciones comerciales continuas.

## EVALUACIÓN DE CUMPLIMIENTO ISO 27001

La Evaluación de Cumplimiento de ISO 27001 de SoftwareONE ayuda a los clientes a evaluar rápidamente su disposición e identificar las áreas de incumplimiento. Los consultores de seguridad de SoftwareONE trabajan estrechamente con los clientes para comprender la estructura de la organización, los procesos comerciales y el alcance de su cumplimiento con ISO 27001. Los interesados clave responsables de los controles ISO 27001 serán entrevistados para que comprendan las políticas, procedimientos y prácticas de seguridad de la información. Con base en las entrevistas, documentos de apoyo y la efectividad de los controles existentes, SoftwareONE evaluará el cumplimiento y postura de riesgo con todos los requerimientos ISO 27001 y proporcionará un informe detallado con los siguientes pasos que se recomiendan.

### 1. Alcance



Identificar el alcance del cumplimiento de ISO 27001, las unidades comerciales and operations involved

### 2. Preparar



Entrevista y revisión para comprender las políticas procesos y controles de ISO 27001

### 3. Evaluar



Evaluar y analizar los controles y resumir las áreas de cumplimiento e incumplimiento

### 4. Informar



Informe ejecutivo detallado resaltando las áreas de incumplimiento para cada control y siguientes pasos recomendados

## GRUPOS DE CONTROL Y CONTROLES ISO 27001

La Evaluación de Cumplimiento de ISO 27001 de SoftwareONE ayuda a los clientes a comprender su postura de riesgo contra 14 grupos de control y 114 controles distintos.

Grupo de Control	N.º de Controles
Políticas de seguridad de información	2
Organización de la seguridad de la información	7
Seguridad del recurso humano	6
Administración de activos	10
Control de acceso	14
Criptografía	2
PSeguridad física y ambiental	15
Seguridad de operaciones	14
Seguridad de comunicaciones	7
Adquisición, desarrollo y mantenimiento del sistema	13
Relaciones del proveedor	5
Administración de incidentes de seguridad de la información	7
Aspectos de seguridad de la información de la administración de continuidad comercial	4
Cumplimiento de los requerimientos; es decir, políticas, requerimientos y normativas externos	8

## INFORME DE CUMPLIMIENTO ISO 27001

Cada Cliente de la Evaluación del Cumplimiento ISO 27001 recibe un informe integral que identifica las áreas de incumplimiento. Los clientes pueden usar el informe para priorizar los siguientes pasos hacia la certificación ISO 27001. SoftwareONE también puede ayudar a planificar y priorizar la estrategia y mapa de ruta para cerrar los vacíos identificados.

### RESUMEN DE CUMPLIMIENTO ISO 27001 CONTRA LOS CONTROLES

