



# ANÁLISIS E IMPLEMENTACIÓN DE LA NORMA ISO 27001:2013

## INTRODUCCIÓN

Un Sistema de Gestión de Seguridad de la Información, garantiza que una organización tiene confidencialidad e integridad de los datos que almacena, mediante buenas prácticas. En especial, establecer, implementar, monitorear y mejorar el Sistema de Gestión de Seguridad de la Información que se relaciona con aspectos financieros, legales o confidenciales, puede demostrar un mayor nivel de compromiso con los clientes, socios, proveedores e interesados que se encuentran involucrados. También, permite garantizar que la información no se divulgará con otros fines que no son establecidos por la organización o de fácil acceso para los colaboradores no correspondientes.

## OBJETIVOS GENERALES

- Analizar los requisitos establecidos en la norma ISO 27001:2013 para asegurar la confidencialidad de la información que se tiene dentro de la organización.
- Implementar los controles de seguridad adecuados para establecer, implementar y monitorear un Sistema de Gestión de Seguridad de la información dentro de la organización.

## OBJETIVOS ESPECÍFICOS

**Al final el curso, los participantes:**

- Comprenderán los riesgos para la información, en distintas áreas de la organización.
- Identificarán los requisitos y elementos para asegurar la confidencialidad de la información.
- Implementarán un proceso de mejora continua para garantizar a los involucrados con la organización, que la fiabilidad y compromiso es uno de los principales principios de la organización.

## TEMARIO

### 1. INTRODUCCIÓN

- 1.1 Antecedentes
- 1.2 Concepto clave

### 2. CONTEXTO DE LA ORGANIZACIÓN

- 2.1 Comprensión de la organización y de su contexto
- 2.2 Comprensión de las necesidades y expectativas de las partes interesadas
- 2.3 Determinación del alcance del sistema de gestión
- 2.4 Sistema de la seguridad de la información

### 3. LIDERAZGO

- 3.1 Liderazgo y compromiso
- 3.2 Política
- 3.3 Roles, responsabilidades y autoridades en la organización

### 4. PLANIFICACIÓN

- 4.1 Acciones para tratar los riesgos y oportunidades
- 4.2 Objetivos de seguridad de la Información y planificación para su consecución

### 5. SOPORTE

- 5.1 Recurso
- 5.2 Competencia
- 5.3 Concienciación
- 5.4 Comunicación
- 5.5 Información documentada

### 6. OPERACIÓN

- 6.1 Planificación y control operacional
- 6.2 Apreciación de los riesgos de seguridad de la información
- 6.3 Tratamiento de los riesgos de seguridad de la información

### 7. EVALUACIÓN DE DESEMPEÑO

- 7.1 Seguimiento, medición, análisis y evaluación
- 7.2 Auditoría interna
- 7.3 Revisión por la dirección

### 8. MEJORA

- 8.1 No conformidad y acciones correctivas
- 8.2 Mejora continua

## DIRIGIDO A

- Directores
- Gerentes o Jefes de TI
- Responsables de sistemas y técnicos que tengan responsabilidad con la seguridad de la información, y profesionales que serán formados como auditores internos en la organización

## MODALIDAD



### *In company*

Impartido en las instalaciones del cliente



### *Online*

Consulte catálogo, de clic [aquí](#).

## INFORMES E INSCRIPCIONES

- 📞 CDMX 55 4000 1324
- MTY. 81 2474 9959
- QRO. 442 167 1450
- GDL. 33 1580 8051

- ✉ [informes@cursosnormasiso.com](mailto:informes@cursosnormasiso.com)
- [informes@sgmconsultores.com.mx](mailto:informes@sgmconsultores.com.mx)

## DURACIÓN

8 HRS

## ¿POR QUÉ SOMOS TU MEJOR OPCIÓN?

- Constancia con valor curricular, registrada ante la STPS.
- Cursos asesorados por profesionales.
- Tutoría y seguimiento con auditores y asesores.
- Realización de actividades durante el curso.
- Óptimos resultados con una mínima inversión.

## OTROS CURSOS RELACIONADOS

Consultar

## ¿BUSCA ASESORÍA PARA IMPLEMENTAR?

Solicite visita diagnóstico

SÍGUENOS



SGM Consultores México