

# Implementación de un Sistema de Gestión de Seguridad de la Información basado en **ISO 27001:2013**

2020 [contacto@grcbit.com](mailto:contacto@grcbit.com)

---

## Introducción

La norma ISO 27001:2013 ayuda a las organizaciones a implementar un Sistema de Gestión de Seguridad de la Información (SGSI) para proteger sus datos, aunque el enfoque de la norma considera cualquier medio (físico, electrónico, analógico) donde residen los datos, la realidad es que hoy en día estos son almacenados, procesados o transmitidos principalmente a través de sistemas de información, por lo que es necesario implementar controles de seguridad para mitigar los riesgos asociados al uso de tecnologías para proteger adecuadamente los datos.

---


## Desarrollo


Uno de los activos más importantes para las organizaciones son los datos, ya que una afectación a los mismos puede causar impactos negativos como: afectación a la reputación de la marca, incumplimiento con leyes y regulaciones, fuga de información, robo de identidad, fraudes, entre otros.

Por lo cual es necesario implementar un Sistema de Gestión de Seguridad de la Información (SGSI) que nos permita mitigar los riesgos que puedan poner en peligro la información de la organización.

Una de las normas internacionales más aceptadas para la implementación de un SGSI es ISO 27001:2013, dicha norma es aplicable a cualquier tipo de organización sin importar su tipo o tamaño, la implementación del SGSI se debe realizar de una manera sistemática, documentada y estructurada

De manera general esta norma nos indica que se deben llevar a cabo las siguientes actividades para implementar un adecuado sistema de protección de datos.



- 
- Definir una política de seguridad de la información.
  - Analizar el contexto de la Organización.
  - Identificar requerimientos internos y externos de seguridad.
  - Implementar y documentar una metodología de análisis de riesgos.
  - Definir roles y responsabilidades.
  - Diseñar controles de seguridad adecuados para la mitigación de riesgos.
  - Definir un tratamiento de riesgos.
  - Revisar periódicamente el SGSI para su mejora continua.
  - Definir métricas e indicadores de riesgo.
  - Establecer acciones correctivas y de mejora.
  - Definir una matriz de aplicabilidad para definir el alcance del SGSI y establecer los controles necesarios para una adecuada gestión de riesgos.
- 

---

## ¿Cómo podemos ayudarle?

- Asesorar para implementar un SGSI basado en ISO 27001:2013.
- Realizar una auditoría sobre su SGSI actual para evaluar su nivel de madurez y conformidad a la norma ISO 27001:2013.
- Definir un plan de acción que esté enfocado a presentar una auditoría de certificación.
- Diseñar controles de acuerdo al “Anexo A” (114 controles) de ISO 27001:2013.