NORMAS ISO 27000

MSc. Sergio Granizo

Explicado Fácilmente

Contenido

TABLA DE CONTENIDOS

NORMAS ISO 27000

Familia ISO 27000

Contiene un conjunto de buenas prácticas para el establecimiento, implementación, mantenimiento y mejora de **Sistemas de Gestión de la Seguridad de la Información.**

NORMAS ISO 27000

Norma ISO 27000

Contiene el vocabulario en el que se apoyan el resto de normas, de forma similar a una guía o diccionario que describe los términos de todas las normas de la familia.

En esta norma los términos se clasifican las siguientes categorías:

- Términos relativos a la seguridad de la información
- Términos relativos a la gestión
- Términos relativos a los riesgos de seguridad de la información
- Términos relativos a la documentación

Norma ISO 27001

Especifica los requisitos para la implantación del **Sistemas de Gestión de la Seguridad de la Información.**
Es la norma más importante de la familia ISO 27000.
Las organizaciones pueden obtener la certificación ISO 27001.

En esta norma los términos se clasifican las siguientes categorías:

- Adopta un enfoque de gestión de riesgos.
- Promueve la mejora continua de los procesos.

NORMAS ISO 27000

Norma ISO 27002

Proporciona recomendaciones de las mejores prácticas para la gestión de seguridad de la información.

Dominios principales de las Normas ISO 27002

- Políticas de Seguridad
- Organización de la Seguridad de la Información
- Seguridad de los Recursos Humanos
- Gestión de los Activos
- Control de Accesos
- Cifrado
- Seguridad Física y Ambiental

Norma ISO 27003

Es la guía para la implementación de un SGSI, se complementa con la norma ISO 27001

NORMAS ISO 27000

Norma ISO 27004

Métricas para la gestión de seguridad de la información. Es la que proporciona recomendaciones de **quién, cuándo y cómo** realizar mediciones de seguridad de la información.

1. Elegir los objetivos y procesos de medición.
2. Describir las líneas principales.
3. Elegir los datos.
4. Desarrollo del sistema de medición.
5. Interpretar los valores medidos.
6. Notificar dichos valores.

La norma ISO 27004 establece:

- El monitoreo y medición del rendimiento de la seguridad de la información.
- El monitoreo y medición de la efectividad de un Sistema de Gestión de la Seguridad de la Información (SGSI), incluidos procesos y controles.
- Análisis y evaluación de los resultados de monitorización y medición.

NORMAS ISO 27000

Norma ISO 27005

Suministra las directrices para gestionar los riesgos que puede sufrir la información de una empresa

- Prefacio.
- Introducción.
- Referencias normativas.
- Términos y definiciones.
- Estructura.
- Fondo.
- Descripción del proceso de ISRM.
- Establecimiento Contexto.
- Información sobre la evaluación de riesgos de seguridad (ISRA).
- Tratamiento de Riesgos Seguridad de la Información.
- Admisión de Riesgos Seguridad de la información.
- Comunicación de riesgos de seguridad de información.
- Información de seguridad Seguimiento de Riesgos y Revisión.
- Anexos

NORMAS ISO 27000

Norma ISO 27006

Es un conjunto de requisitos formales de acreditación para las organizaciones certificadoras.

ISO 27006: 2015 establece estándares para la demostración de la competencia de los auditores del SGSI. El SGSI de auditoría del organismo de certificación es necesario para verificar que cada auditor del equipo de auditoría tenga conocimiento de:

- Monitoreo, medición, análisis y evaluación del SGSI
- Seguridad de la información
- Sistemas de gestión
- Principios de auditoría
- Conocimiento técnico de los sistemas a auditar.

NORMAS ISO 27000

Norma ISO 27007

Es una guía para auditar SGSIs. Establece qué auditar y cuando, cómo asignar los auditores adecuados, la planificación y ejecución de la auditoría, las actividades claves, etc.

El estándar cubre todas las partes específicas de un SGSI (Sistema de Gestión de la Seguridad de la Información):

- Controlar el programa de auditoría del SGSI (determinar los puntos de la auditoría, cómo y cuándo hacer la auditoría, encontrar los riesgos de la auditoría, decidir quién debe hacerla, etc.), esto se debe a que este estándar se alinea con los requisitos de la cláusula 9.2 de ISO/IEC 27001:2013.
- Ejecutar un sistema de gestión de la auditoría (realización de una planificación y posterior implementación con los respectivos informes y resultados).
- Gestionar los auditores (competencias, habilidades, atributos, evaluación).

CONCLUSIONES

Gracias

"La Seguridad es un hábito…"

MSc. Sergio Granizo
Magister en Software
Cel: 0997009187
sergio_granizo@yahoo.com