Normas ISO 27006-27007,27008

International Organization for Standardization

BY : Marcelo Rodrigo Duran Mamani

Introducción a la norma ISO 27006

La norma ISO 27006 proporciona directrices para la acreditación de organismos de certificación que auditan y certifican Sistemas de Gestión de Seguridad de la Información (SGSI) según la norma ISO 27001.

Garantiza que las certificaciones ISO 27001 sean válidas y confiables.

¿A quién aplica la norma ISO 27006?

Organismos de certificación que buscan acreditar para la certificación ISO 27001.

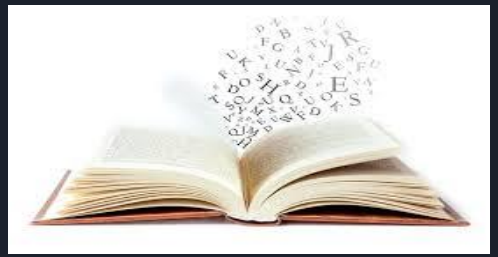
¿Cuáles son los beneficios de la norma ISO 27006?

Mayor confianza en las certificaciones ISO 27001.

Mejora la calidad de las auditorías y evaluaciones del SGSI.

Promueve prácticas consistentes de seguridad de la información en toda la industria.

Estructura y contenido de la norma ISO 27006



La norma ISO 27006 se compone de 10 capítulos y 4 anexos.

Cubre temas como:

- Requisitos de gestión para organismos de certificación.
- Competencia e imparcialidad de los auditores.
- Proceso de auditoría y certificación.
- Vigilancia y control de los organismos de certificación.

Puntos clave de la norma ISO 27006

La norma ISO 27006 no es una norma independiente, sino que complementa a la norma ISO 27001.

Las organizaciones que buscan la certificación ISO 27001 deben trabajar con un organismo de certificación acreditado según la norma ISO 27006.

La norma ISO 27006 se revisa periódicamente para reflejar los cambios en el panorama de las amenazas de seguridad de la información.

Introducción a la norma ISO 27007

La norma ISO 27007 proporciona directrices para la auditoría de Sistemas de Gestión de Seguridad de la Información (SGSI) basados en la norma ISO 27001.

Ayuda a los auditores a evaluar si el SGSI cumple con los requisitos de la norma ISO 27001 y si los controles de seguridad de la información se están implementando de manera adecuada.

La norma ISO 27007 se basa en gran medida en ISO 19011, el estándar para auditar sistemas de gestión.

¿Para qué sirve la norma ISO 27007?

La norma ISO 27007 es útil para:

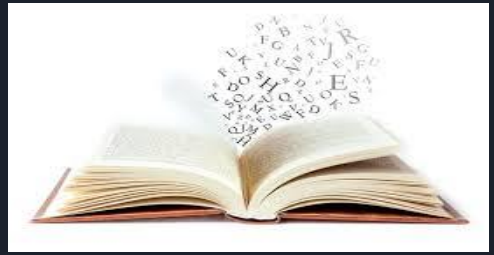
Evaluar la eficacia de un SGSI.

Identificar las áreas de mejora del SGSI.

Demostrar la conformidad con la norma ISO 27001.

Mejorar la confianza en los sistemas de seguridad de la información.

Estructura de la norma ISO 27007



La norma ISO 27007 se compone de las siguientes secciones:

Introducción: Alcance, propósito, referencias normativas.

Términos y definiciones.

Principios de auditoría.

Gestión de un programa de auditoría: Directrices que incluyen planificación, programación y asignación de recursos para auditoría.

Realización de la auditoría: Preparación para la auditoría, recolección de evidencia y realización de pruebas de auditoría.

Competencia y evaluación de auditores: Proporciona requisitos de competencia y directrices sobre la evaluación de los auditores.

Informe de auditoría: Hallazgos, no conformidades y recomendaciones para la mejora del SGSI.

Seguimiento de la auditoría: Verificación de la implementación de las recomendaciones y realización de auditorías de seguimiento.

¿Dónde se aplica la norma ISO 27007?

La norma ISO 27007 se puede aplicar a cualquier tipo de organización, ya sea del sector público o privado, pequeñas o grandes, y en cualquier sector o industria.

Puede ser aplicada por auditores internos y externos que estén encargados de realizar auditorías de un SGSI basado en la norma ISO 27001.

Es de gran utilidad para los consultores que asesoran a las organizaciones sobre cómo implementar y mantener un SGSI y para los responsables de la seguridad de la información en las organizaciones que buscan mejorar su sistema de seguridad de la información y demostrar su conformidad con la norma ISO 27001.

Caso práctico: Empresa de Servicios Financieros

Situación: La empresa contrata a un equipo de auditores internos o externos para realizar una auditoría del SGSI y asegurarse de que cumple con los requisitos de la norma.

Aplicación de la norma ISO 27007:

La norma ISO 27007 proporciona directrices sobre cómo planificar y realizar la auditoría, recopilar evidencia y evaluar los hallazgos.

La norma también ayuda

Introducción a la norma ISO 27008

La norma ISO 27008 proporciona directrices para la implementación y operación de controles de seguridad de la información.

Es aplicable a cualquier tipo y tamaño de empresa, tanto pública como privada.

Sirve como complemento a las normas ISO 27001 e ISO 27002.

¿Para qué sirve la norma ISO 27008?

Mejorar la seguridad de la información de una organización.

Garantizar que los controles de seguridad de la información se implementen y operen de manera efectiva.

Demostrar el cumplimiento de las regulaciones de seguridad de la información.

Reducir el riesgo de pérdidas por ciberataques y otras amenazas de seguridad de la información.

Relación con otras normas

La norma ISO 27008 es compatible con otras normas de la serie ISO 27000, como ISO 27001 e ISO 27002.

La norma ISO 27001 proporciona un marco para la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI).

La norma ISO 27002 proporciona una lista de controles de seguridad de la información que se pueden implementar para cumplir con los requisitos de la norma ISO 27001.

La norma ISO 27008 complementa estas normas al proporcionar directrices para la implementación y operación de los controles de seguridad de la información.

Caso práctico: Empresa minorista

situación: La empresa está preocupada por el creciente riesgo de ciberataques.

Solución: La empresa implementa la norma ISO 27008 para ayudar a mejorar su seguridad de la información.

Beneficios:

La empresa pudo identificar y evaluar sus riesgos de seguridad de la información.

La empresa implementó controles de seguridad de la información efectivos para mitigar sus riesgos.

La empresa pudo demostrar su cumplimiento de las regulaciones de seguridad de la información.

La empresa redujo el riesgo de pérdidas por ciberataques y otras amenazas de seguridad de la información.

Conclusión

La norma ISO 27008 es una herramienta valiosa para las organizaciones que buscan mejorar su seguridad de la información.

La norma proporciona directrices para la implementación y operación de controles de seguridad de la información efectivos.

La norma es compatible con otras normas de la serie ISO 27000.

La norma puede ayudar a las organizaciones a reducir el riesgo de pérdidas por ciberataques y otras amenazas de seguridad de la información.

Conclusión General de la Normas 27006-7-8

Las normas ISO 27006, 27007 y 27008 son herramientas valiosas para las organizaciones que buscan mejorar su seguridad de la información.

- **ISO 27006:** Garantiza la validez de las certificaciones ISO 27001.
- **ISO 27007:** Mejora las auditorías del SGSI y demuestra el cumplimiento.
- **ISO 27008:** Implementa controles de seguridad efectivos para proteger la información.

Al implementar estas normas, las organizaciones pueden:

- Proteger su información confidencial.
- Reducir el riesgo de ciberataques y otras amenazas de seguridad de la información.
- Aumentar la confianza de clientes, socios y otras partes interesadas en la seguridad de la información de la organización.

En resumen, las normas ISO 27006, 27007 y 27008 son una inversión valiosa para cualquier organización que se tome en serio la seguridad de su información.

GRACIAS POR SU ATENCION ……..