TEMA8. ESTANDARES SOBRE SEGURIDAD DE LA INFORMACION: UNE-ISO/IEC 27000

Jaime Lorenzo Sánchez

11 de febrero de 2022

Capítulo 1

Estructura del documento del estándar

1.1. Listar las secciones del estándar

1. Introducción
2. Objeto y campo de aplicación.
3. Términos y definiciones
4. Sistemas de Gestión de Seguridad de la Información
5. Familia de normas SGSI

1.2. ¿Sigue algún orden? ¿Cuál es?

Sigue un orden lógico, desde los preliminares hasta el material más específico y avanzado (introducción ->alcance ->términos ->definiciones).

Capítulo 2

¿Qué organizaciones han participado en el desarrollo de este estándar?

ISO e IEC

Capítulo 3

Diferencias y similitudes entre los términos: suceso, suceso de seguridad de la información, incidencia de seguridad de la información, riesgo, amenaza.

1. **Suceso**: Ocurrencia de un conjunto particular de circunstancias.

2. **Suceso de seguridad de la información**: Ocurrencia detectada en un estado del sistema, servicio o red que indica una posible violación de la política de seguridad de la información, un fallo de seguridad o una situación desconocida hasta el momento y que puede ser relevante para la seguridad.

3. **Incidencia de seguridad de la información**: Un único evento o un conjunto de eventos de seguridad de la información, inesperados o no deseados, con una probabilidad significativa de comprometer las operaciones empresariales y de amenazar la seguridad de la información.

4. **Riesgo**: Combinación de la probabilidad de ocurrencia de un daño y de la severidad del mismo.

5. **Amenaza**: Posible causa de un incidente no deseado, el cual puede causar daño a un sistema u organización.

Capítulo 4

¿Por qué es importante la seguridad de la información?

Porque es esencial para permitir que una organización logre sus objetivos, y mantenga y mejore el cumplimiento de la legislación y su imagen.

Capítulo 5

¿Qué es un Sistema para la Gestión de la Seguridad de la Información (SGSI)?

Es un sistema que proporciona un modelo para establecer, implementar, operar, monitorizar, revisar, mantener y mejorar la protección de los activos de información para alcanzar los objetivos de negocio, basado en una apreciación del riesgo y en los niveles de aceptación del riesgo de la organización diseñados para tratar y gestionar con eficacia los riesgos.

Capítulo 6

¿Cuáles son los principios que contribuyen a la implementación de un SGSI?

1. Conciencia de la necesidad de seguridad de la información.
2. Asignación de responsabilidades en seguridad de la información.
3. Incorporación del compromiso de la Dirección y los intereses de las partes interesadas.
4. Mejora de los valores sociales.
5. Apreciaciones de riesgos para determinar los controles adecuados para alcanzar niveles aceptables de riesgo.
6. Seguridad incorporada como un elemento esencial en los sistemas y redes de información.
7. Prevención y detección activas de incidentes de seguridad de la información.
8. Garantizar una aproximación exhaustiva a la gestión de la seguridad de la información.

9. Evaluación continua de la seguridad de la información y la realización de modificaciones cuando corresponda.

Capítulo 7

¿Cuáles son las dimensiones de la seguridad de la información?

Confidencialidad, disponibilidad e integridad.

Capítulo 8

¿Por qué es importante un SGSI?

Porque un SGSI es un elemento facilitador que apoya el comercio electrónico y es esencial para las actividades de gestión de riesgos.

Capítulo 9

¿Qué factores son críticos para el éxito de un SGSI?

1. Política, objetivos y actividades de seguridad de la información estén alineados con los objetivos.

2. Un enfoque y un marco para el diseño, ejecución, seguimiento, mantenimiento y mejora de la seguridad de la información en consonancia con la cultura de la organización.

3. Apoyo visible y compromiso de todos los niveles de la Dirección, especialmente de la alta Dirección.

4. Conocimiento y entendimiento de los requisitos de protección de los activos de información obtenido mediante la aplicación de la gestión del riesgo de la seguridad de la información.

5. Programa efectivo de concienciación, formación y educación sobre seguridad de la información, informando a todos los empleados y otras partes pertinentes de sus obligaciones en seguridad de la información establecidas en las políticas de seguridad de la información, normas, etc., y motivarlos a actuar en consecuencia.

6. Proceso eficaz de gestión de incidentes de seguridad de la información.

7. Enfoque efectivo de gestión de la continuidad del negocio.

8. Sistema de medición utilizado para evaluar el desempeño en la gestión de la seguridad de la información y sugerencias de mejora.

Capítulo 10

¿Qué estándares principales que componen la familia 27000? ¿Cuáles de ellos son normativos?

1. ISO/IEC 27000: Visión general y vocabulario.
2. ISO/IEC 27001: Requisitos del SGSI.
3. ISO/IEC 27006: Requisitos para organismos de certificación de SGSI.
4. ISO/IEC 17021: Requisitos para organismos de certificación de SG.
5. ISO/IEC 27002: Código de buenas prácticas.
6. ISO/IEC 27007: Guía de auditoría.
7. ISO/IEC 27004: Métricas
8. ISO/IEC 27005: Gestión de riesgos.
9. ISO/IEC 27003: Guía de implementación.
10. ISO/IEC 27011: Telecomunicaciones.
11. ISO/IEC 27799: Sanidad.

Son normativos ISO/IEC 27001, ISO/IEC 27006 e ISO/IEC 17021.