**RESUMEN DE LA NORMA ISO 27001 Y SEGURIDAD POR NIVELES**

**JOSE LUIS TAMARA MARTINEZ**

**AUDITORIA DE SISTEMAS**

**WILLIAM MONTOYA DIAZ**

**I. UNIVERSITARIA PASCUA BRAVO**

**TECNOLOGIA DESARROLLO DE SOFTWARE**

**2024-1**

**Introducción:**

En el panorama digital actual, la información se ha convertido en el alma de las organizaciones, impulsando su éxito y determinando su futuro. Sin embargo, este tesoro invaluable también se ha convertido en un blanco atractivo para las amenazas cibernéticas, los ataques de malware, las filtraciones de datos y otras vulnerabilidades que pueden poner en riesgo la continuidad del negocio, la reputación y el cumplimiento legal.

Ante este panorama desafiante, surge la necesidad imperiosa de implementar estrategias robustas y sistemáticas para proteger la información, donde la norma ISO 27001 y la seguridad por niveles se posicionan como herramientas indispensables.

**Norma ISO 27001: Sistema de Gestión de la Seguridad de la Información (SGSI)**

* **La norma ISO 27001 es un estándar internacionalmente reconocido que establece los requisitos para implementar un SGSI. Este sistema ayuda a las organizaciones a:**

**1**. Identificar y evaluar sus riesgos de seguridad de la información.

**2.** Implementar controles de seguridad adecuados para mitigar esos riesgos.

**3.** Mejorar continuamente la eficacia de su programa de seguridad de la información.

* **Principios fundamentales de la ISO 27001:**

1. **Confidencialidad:** La información solo debe ser accesible para las personas autorizadas.

2. **Integridad:** La información debe ser precisa y completa.

3. **Disponibilidad:** La información debe estar disponible cuando se necesite.

* **Componentes clave de un SGSI:**

1. **Política de seguridad de la información:** Define el compromiso de la organización con la seguridad de la información.

**2. Objetivos de control de seguridad de la información:** Establecen metas específicas para proteger la información.

**Anexo A:** Contiene 114 controles de seguridad recomendados para abordar diversos riesgos.

* **Plan de tratamiento de riesgos:** Describe las acciones para mitigar los riesgos identificados.
* **Procedimientos y registros:** Documentan las prácticas de seguridad de la organización.
* **Auditorías y revisiones:** Evalúan la eficacia del SGSI
* **Beneficios de implementar la ISO 27001:**

**1. Mejora la protección de la información:** Reduce el riesgo de filtraciones de datos, robos cibernéticos y otras amenazas.

**2. Aumenta la confianza de los clientes y socios:** Demuestra el compromiso de la organización con la seguridad.

**3. Optimiza los procesos de negocio:** Fortalece la eficiencia y la continuidad operativa.

**4. Cumple con los requisitos legales y regulatorios:** Se adhiere a las leyes y regulaciones aplicables a la protección de datos.

* **Implementación de la ISO 27001:**

La implementación de la ISO 27001 implica un proceso estructurado que comprende las siguientes etapas:

**1. Establecimiento del contexto:** Definir el alcance del SGSI, identificar las partes interesadas y comprender las necesidades y expectativas de la organización.

**2. Evaluación de riesgos:** Identificar y analizar los riesgos de seguridad de la información que enfrenta la organización.

**3. Tratamiento de riesgos:** Seleccionar e implementar controles de seguridad adecuados para mitigar los riesgos identificados.

**4. Implementación y operación:** Implementar los controles de seguridad seleccionados, documentar los procesos y procedimientos, y capacitar al personal.

**5. Supervisión y revisión:** Monitorear el desempeño del SGSI, realizar auditorías internas y revisiones periódicas, y tomar medidas correctivas cuando sea necesario.

**6. Mejora continua:** Identificar oportunidades para mejorar el SGSI mediante auditorías internas, revisiones por la dirección y retroalimentación de las partes interesadas.

* **Seguridad por Niveles:**

La seguridad por niveles es un enfoque para clasificar la información y aplicar controles de seguridad adecuados según su sensibilidad. Implica establecer diferentes niveles de seguridad para proteger la información en función de su valor e impacto potencial en caso de pérdida o divulgación.

* **Categorías de seguridad por niveles:**

**Nivel 1: Información de bajo impacto:** Información que no tiene un impacto significativo en la organización si se pierde o divulga.

**Nivel 2: Información de impacto moderado:** Información que puede tener un impacto moderado en la organización si se pierde o divulga.

**Nivel 3: Información de alto impacto:** Información que puede tener un impacto significativo en la organización si se pierde o divulga.

**Nivel 4: Información crítica:** Información que es esencial para la operación del negocio y que tendría un impacto grave en la organización si se pierde o divulga.

* **Controles de seguridad por niveles:**

Para cada nivel de seguridad, se deben aplicar controles de seguridad específicos. Algunos ejemplos de controles de seguridad incluyen:

**1. La sensibilidad de la información:** Cuanto más sensible sea la información, más controles de seguridad estrictos se requieren.

**2. El impacto potencial de una pérdida o divulgación:** Si la pérdida o divulgación de la información podría tener un impacto significativo en la organización, se deben implementar controles de seguridad más robustos.

**3. Los requisitos legales y regulatorios:** La organización debe cumplir con todas las leyes y regulaciones aplicables a la protección de la información, lo que puede requerir la implementación de controles de seguridad específicos.

**4. Los recursos disponibles:** La organización debe considerar los recursos disponibles para implementar y mantener los controles de seguridad.

**5. La evaluación de riesgos:** La organización debe realizar una evaluación de riesgos para identificar y evaluar los riesgos específicos de seguridad de la información que enfrenta, y luego seleccionar controles de seguridad adecuados para mitigar esos riesgos.

**Sin embargo, en general, se pueden observar las siguientes tendencias:**

**Nivel 1 (Información de bajo impacto):** Se pueden implementar controles de seguridad básicos, como:

* Control de acceso físico básico
* Sensibilización sobre seguridad de la información para empleados
* Protección con contraseña

**Nivel 2 (Información de impacto moderado):** Se pueden implementar controles de seguridad más robustos, como:

* Control de acceso físico más estricto
* Firewalls
* Antivirus
* Copias de seguridad regulares

**Nivel 3 (Información de alto impacto):** Se deben implementar controles de seguridad muy estrictos, como:

* Cifrado de datos
* Control de acceso lógico granular
* Monitoreo continuo de la seguridad
* Auditorías de seguridad regulares

**Nivel 4 (Información crítica):** Se deben implementar los controles de seguridad más estrictos posibles, como:

* Salas seguras
* Controles biométricos
* Planes de recuperación ante desastres
* Pruebas de penetración regulares