Caso de Auditoría de Seguridad de la Información basada en ISO/IEC 27001

Introducción

SoftNova Solutions S.A.C. es una empresa peruana dedicada al desarrollo de software y consultoría tecnológica, con clientes en sectores sensibles como banca, salud y logística, la empresa gestiona información crítica, tanto propia como de terceros.

Ante la creciente necesidad de garantizar la seguridad de la información y cumplir con estándares internacionales, se ha decidido realizar una **Auditoría Interna de Seguridad de la Información**, alineada con la norma **ISO/IEC 27001:2022**.

Motivo para la Auditoría

La auditoría tiene como finalidad evaluar el grado de implementación y eficacia del **Sistema de Gestión de Seguridad de la Información (SGSI)** de la empresa, identificar brechas y generar recomendaciones que preparen a la organización para una futura certificación.

Descripción de la Organización

- **Nombre:** SoftNova Solutions S.A.C.
- **Sector:** Desarrollo de software y servicios de TI
- **Ubicación:** Lima, Perú
- **Tamaño:** 120 colaboradores
- **Servicios:** Desarrollo web y móvil, DevOps, integración de APIs, soporte TI
- **Clientes:** Entidades financieras, clínicas, operadores logísticos

Situación Actual

SoftNova ha avanzado en la implementación de su SGSI, incluyendo la definición de políticas, clasificación de activos y asignación de responsables. Sin embargo, el cumplimiento aún es parcial y existen riesgos detectados durante la fase preparatoria de auditoría.

Sin embargo, mediante análisis preliminares pasivos se han detectado posibles debilidades:

1. **Gestión de accesos:**
    - Cuentas compartidas en entornos de desarrollo.
    - Autenticación sin factores adicionales en sistemas críticos.
2. **Inventario de activos incompleto:**
    - Equipos personales utilizados sin autorización ni cifrado.
    - Datos sensibles no registrados formalmente.
3. **Políticas de seguridad no difundidas:**
    - Documentos firmados solo por la alta dirección.

- Ausencia de capacitaciones al personal operativo.

4. **Entorno de desarrollo inseguro:**
    - Procesos DevOps sin revisión de seguridad.
    - Ausencia de pruebas de vulnerabilidades antes del despliegue.
5. **Monitoreo y respuesta a incidentes limitado:**
    - Falta de un sistema de registro de eventos de seguridad (SIEM).
    - No se han realizado simulacros de respuesta a incidentes.

Justificación para la Auditoría

La auditoría interna de seguridad de la información tiene como finalidad identificar vulnerabilidades en los procesos y controles implementados en la empresa, verificar el cumplimiento con los requisitos de la norma ISO/IEC 27001 y evaluar la madurez del Sistema de Gestión de Seguridad de la Información (SGSI), con el objetivo de anticiparse a posibles brechas de seguridad y fortalecer la protección de los activos de información.

Producto Académico

Plan de Auditoría de Seguridad de la Información según ISO/IEC 27001:2022.