INFORMACIÓN GENERAL

Nombre del Proyecto:
Implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) basado en riesgos para PYME que procesa, almacena o transmite datos de tarjeta.

Patrocinador del Proyecto:
Gerencia General / Alta Dirección

Director del Proyecto:
Oficial de Seguridad de la Información / Consultor SGSI

Fecha de inicio estimada:
[Definir]

Duración estimada:
6 a 9 meses (según tamaño y madurez)

JUSTIFICACIÓN DEL PROYECTO

La organización procesa, almacena o transmite datos de tarjetas de crédito, lo que la obliga al cumplimiento del estándar PCI DSS v4.0.1 y de la normativa colombiana vigente en materia de protección de datos personales.

Actualmente:

- No existe un SGSI formal estructurado.
- La gestión de riesgos es parcial o reactiva.
- No hay proceso formal de gestión de incidentes alineado a estándares.
- Existen brechas frente a los requisitos PCI.
- El incumplimiento puede generar:
    - Multas impuestas por el banco adquirente.
    - Suspensión de la capacidad de procesar pagos con tarjeta.
    - Sanciones por incumplimiento de la Ley 1581 de 2012.
    - Pérdida reputacional y financiera.

Este proyecto establece una base estructurada para el cumplimiento sostenible de PCI DSS mediante un enfoque basado en riesgos.

OBJETIVO DEL PROYECTO

Objetivo General

Implementar un Sistema de Gestión de Seguridad de la Información (SGSI) basado en riesgos que permita a la organización cumplir de manera obligatoria con el estándar PCI DSS vigente para la protección de datos de tarjetas de crédito y con la normativa colombiana aplicable en materia de protección de datos y seguridad de la información, tomando como referencia

complementaria las mejores prácticas internacionales para fortalecer la gestión de riesgos y los controles de seguridad.

Objetivos Específicos

1. Delimitar y proteger el entorno de datos de tarjeta (CDE).
2. Identificar y clasificar los activos críticos asociados al procesamiento de datos.
3. Realizar análisis y tratamiento de riesgos alineado a las mejores prácticas (ISO 27005-ISO31000).
4. Implementar los controles obligatorios establecidos por PCI DSS.
5. Establecer un proceso formal de gestión de incidentes.
6. Asegurar el cumplimiento de la Ley 1581 de 2012 y demás normativa colombiana aplicable.
7. Definir métricas e indicadores de seguimiento del cumplimiento PCI.

ALCANCE DEL PROYECTO

4.1 Incluye

- Identificación y delimitación del CDE
- Inventario y clasificación de activos
- Análisis de brechas frente a PCI DSS
- Gestión de riesgos del entorno CDE
- Implementación de controles PCI prioritarios
- Documentación de políticas y procedimientos
- Diseño del procedimiento de gestión de incidentes
- Capacitación al personal involucrado
- Preparación para evaluación PCI (SAQ o auditoría)

4.2 Excluye

- Certificación ISO 27001 formal
- Implementación de SOC 24/7
- Transformaciones tecnológicas fuera del alcance del CDE
- Auditoría QSA externa (podrá contratarse separadamente)