

Plan de Seguridad y Privacidad de la Información

Concejo Municipal de Galapa Atlántico

Enero de 2025

Mesa Directiva

ROBERTO CUAO ZUÑIGA
Presidente

CECIL CANTILLO PEREZ
Vicepresidente

MARLON MARRIAGA ARIZA
Segundo Vicepresidente

SHARON PERALTA MENDEZ
Secretaria General

1. INTRODUCCIÓN

El Concejo Municipal de Galapa es responsable de la gestión y protección de una amplia variedad de datos e información que son esenciales para sus actividades administrativas y legislativas. Estos incluyen datos personales de empleados, concejales y ciudadanos, así como información institucional sensible. La seguridad y privacidad de la información son pilares fundamentales para la transparencia, la eficiencia operativa y la confianza pública.

Este Plan de Seguridad y Privacidad de la Información tiene como objetivo establecer un conjunto de medidas y políticas para proteger los datos gestionados por el Concejo Municipal, asegurando su confidencialidad, integridad y disponibilidad, así como el cumplimiento de las normativas legales aplicables.

2. OBJETIVOS DEL PLAN

Objetivo General:

Desarrollar y ejecutar un plan integral de seguridad y privacidad de la información que permita al Concejo Municipal de Galapa proteger la información sensible, cumplir con las normativas legales vigentes y promover una cultura organizacional que valore la seguridad de los datos.

Objetivos Específicos:

- ✓ Proteger la información sensible y los datos personales de los ciudadanos, empleados y concejales.
- ✓ Cumplir con las normativas legales sobre la protección de datos, como la Ley 1581 de 2012 y la Ley 1266 de 2008.
- ✓ Establecer medidas de seguridad informática para prevenir accesos no autorizados, ataques cibernéticos y pérdida de datos.
- ✓ Garantizar la confidencialidad, integridad y disponibilidad de la información almacenada y gestionada por el Concejo Municipal.
- ✓ Capacitar al personal en buenas prácticas de seguridad y privacidad de la información.

3. MARCO NORMATIVO

Este Plan se encuentra alineado con las siguientes leyes y regulaciones:

- ✓ Ley 1581 de 2012: Establece disposiciones generales para la protección de datos personales en Colombia.
- ✓ Ley 1266 de 2008: Regula el manejo de la información financiera y crediticia de las personas.

- ✓ Resolución 0312 de 2019: Establece los lineamientos para la implementación de un Sistema de Gestión de Seguridad y Salud en el Trabajo (SG-SST), que también afecta a la gestión de la información y protección de los trabajadores.
- ✓ Normas internacionales de ciberseguridad (ISO/IEC 27001, NIST, etc.): Para la implementación de controles y auditorías en la seguridad de la información.

4. IDENTIFICACIÓN DE LA INFORMACIÓN Y ACTIVOS CRÍTICOS

4.1. Tipos de Información a Proteger

Datos Personales:

- ✓ Nombre, documentos de identidad, direcciones, números de teléfono, correos electrónicos.
- ✓ Información laboral de los empleados y contratistas (números de seguridad social, información bancaria).

Información Institucional:

- ✓ Actas de sesiones del Concejo, informes, proyectos legislativos.
- ✓ Contratos, resoluciones y demás documentos oficiales.
- ✓ Bases de datos internas del Concejo, incluyendo presupuestos, proyectos y archivos históricos.

Sistemas y Plataformas:

- ✓ Servidores, bases de datos, correos electrónicos, sistemas de gestión administrativa.
- ✓ Plataformas de participación ciudadana (portal web, redes sociales, aplicaciones móviles).

Datos Sensibles:

- ✓ Información sobre salud, antecedentes penales, o cualquier otro dato clasificado como sensible que sea recopilado para cumplir con la legislación vigente.

4.2. Evaluación de los Riesgos

Los principales riesgos identificados que pueden afectar la seguridad y privacidad de la información incluyen:

- ✓ Ciberataques: Phishing, malware, ransomware, etc.
- ✓ Accesos no autorizados: Personal no autorizado con acceso a bases de datos o sistemas sensibles.

- ✓ Pérdida o daño de información: Por fallas en sistemas de respaldo, errores humanos o fallos tecnológicos.
- ✓ Fugas de información: Por falta de cifrado o mala gestión en el acceso a datos.
- ✓ Cumplimiento inadecuado de las leyes de protección de datos personales.

5. ESTRATEGIAS Y CONTROLES DE SEGURIDAD Y PRIVACIDAD

5.1. Seguridad Física y Lógica de la Información

Accesos físicos restringidos:

- ✓ Control de acceso a las áreas donde se gestionan datos sensibles, como servidores y oficinas.
- ✓ Uso de sistemas de seguridad (tarjetas de acceso, cámaras de vigilancia) para evitar el acceso no autorizado.

Control de acceso lógico:

- ✓ Implementación de políticas de control de acceso (autenticación y autorización) para sistemas y aplicaciones internas.
- ✓ Autenticación multifactor (MFA) para usuarios con acceso a información sensible o sistemas críticos.

Cifrado de la información:

- ✓ Todos los datos sensibles deben ser cifrados tanto en reposo (almacenados) como en tránsito (cuando se transmiten por redes).

Protección contra malware y ciberataques:

- ✓ Instalar y mantener actualizado un sistema de protección antivirus y firewall para prevenir accesos no autorizados y ataques cibernéticos.
- ✓ Implementación de un sistema de detección de intrusiones (IDS) para identificar actividades sospechosas en tiempo real.

Sistema de respaldo y recuperación:

- ✓ Implementar copia de seguridad diaria de los datos más críticos y almacenar los respaldos en ubicaciones seguras (servidores locales y nube).
- ✓ Establecer un plan de recuperación ante desastres, que permita restaurar la información rápidamente en caso de pérdida o daño.

5.2. Cumplimiento Legal y Privacidad de Datos

Política de protección de datos:

- ✓ Elaboración de una política de privacidad y seguridad de la información que esté alineada con la Ley 1581 de 2012 sobre protección de datos personales.
- ✓ Implementación de procedimientos claros sobre el manejo de información confidencial y datos sensibles de los ciudadanos, empleados y concejales.

Consentimiento informado:

- ✓ Asegurar que se obtenga el consentimiento explícito de los ciudadanos y empleados para el tratamiento de sus datos personales, según lo estipulado en la legislación vigente.

Auditorías periódicas:

- ✓ Realización de auditorías internas y externas para verificar el cumplimiento con las normativas de privacidad y seguridad de la información.

5.3. Capacitación y Sensibilización

Programa de capacitación:

Establecer un programa de capacitación anual sobre seguridad de la información y protección de datos personales dirigido a todo el personal del Concejo, incluyendo concejales, administrativos y contratistas.

La capacitación debe incluir:

- ✓ Buenas prácticas en el manejo de contraseñas.
- ✓ Detección de correos fraudulentos (phishing).
- ✓ Manejo seguro de dispositivos móviles.

Sensibilización constante:

Campañas de sensibilización sobre la importancia de la privacidad y seguridad de la información, enfocándose en los riesgos de negligencia o descuidos que podrían poner en peligro la integridad de los datos.

5.4. Gestión de Incidentes

Protocolo de gestión de incidentes:

- ✓ Establecer un protocolo de respuesta ante incidentes de seguridad que contemple la notificación inmediata de cualquier brecha de seguridad o violación de la privacidad de la información.
- ✓ El protocolo debe incluir la evaluación del incidente, la mitigación de daños y la notificación a las autoridades competentes si corresponde.

Informe de incidentes:

Toda brecha o incidente de seguridad debe ser documentado y evaluado para determinar las causas y aplicar medidas correctivas, evitando la repetición del problema.

6. EVALUACIÓN Y SEGUIMIENTO

6.1. Monitoreo Continuo

El Concejo Municipal de Galapa debe implementar un sistema de monitoreo continuo de los sistemas de seguridad, así como de las políticas de privacidad y protección de datos. Esto incluye:

- ✓ Revisión periódica de accesos a sistemas y bases de datos.
- ✓ Monitoreo de amenazas y vulnerabilidades externas.
- ✓ Evaluación de la efectividad de las medidas de protección.

6.2. Auditorías y Revisión Anual

Se recomienda realizar auditorías internas y revisiones anuales del plan para asegurar su efectividad y alineación con las regulaciones actuales. En caso de cambios legislativos, el plan debe ser actualizado.

7. CONCLUSIÓN

El Plan de Seguridad y Privacidad de la Información del Concejo Municipal de Galapa tiene como objetivo proteger los datos e información crítica que maneja la institución, garantizando su confidencialidad, integridad y disponibilidad. La implementación de este plan no solo asegura el cumplimiento de las normativas legales, sino que también promueve una cultura organizacional responsable en la gestión de la información, fomentando la confianza de los ciudadanos y empleados.