Plan de Tratamiento de Riesgos 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 tiene la responsabilidad de proteger la información pública y privada que maneja en el marco de sus actividades legislativas y administrativas, tanto en formato físico como digital. El tratamiento de la información debe ser realizado con estricto cumplimiento de las leyes de protección de datos y de los principios de seguridad informática.

Este Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información tiene como objetivo identificar, evaluar, controlar y tratar los riesgos asociados con la gestión de la información, asegurando que se implemente un enfoque adecuado para proteger la confidencialidad, integridad y disponibilidad de los datos, minimizando los impactos que puedan surgir por incidentes de seguridad.

2. OBJETIVOS DEL PLAN DE TRATAMIENTO DE RIESGOS

Objetivo General:

Establecer un plan integral de tratamiento de riesgos de seguridad y privacidad de la información, que permita al Concejo Municipal de Galapa proteger los datos personales y la información institucional, garantizando el cumplimiento de las normativas vigentes y asegurando la confianza del público en el manejo de sus datos.

Objetivos Específicos:

1. Identificar y evaluar los riesgos que puedan afectar la seguridad y privacidad de la información en el Concejo Municipal.
2. Implementar controles de seguridad adecuados para mitigar los riesgos identificados, tanto a nivel tecnológico como organizacional.
3. Asegurar el cumplimiento de las normativas de privacidad y protección de datos personales, de acuerdo con la Ley 1581 de 2012 y la Ley 1266 de 2008.
4. Capacitar al personal del Concejo sobre buenas prácticas en seguridad de la información y protección de datos.
5. Establecer procedimientos claros para la gestión de incidentes de seguridad relacionados con la información.

3. IDENTIFICACIÓN Y EVALUACIÓN DE RIESGOS

3.1. Identificación de Activos de Información

- ✓ Datos personales: Información sensible de los empleados, concejales, contratistas y ciudadanos que interactúan con el Concejo Municipal, tales como nombres,

documentos de identidad, direcciones, datos financieros, entre otros.

- ✓ Documentos oficiales: Actas de sesiones, proyectos legislativos, informes, resoluciones y demás documentos generados por el Concejo.
- ✓ Sistemas informáticos: Infraestructura tecnológica utilizada para gestionar la información (servidores, bases de datos, aplicaciones, correos electrónicos, etc.).
- ✓ Redes de comunicación: La red interna y externa del Concejo, que incluye Internet, servidores de correos electrónicos, plataformas de videoconferencia, entre otros.

3.2. Identificación de Riesgos

Riesgos Técnicos:

- ✓ Ciberataques (phishing, malware, ransomware, etc.) que puedan comprometer la confidencialidad e integridad de los datos.
- ✓ Accesos no autorizados a los sistemas informáticos y bases de datos debido a fallas en los controles de acceso.
- ✓ Pérdida de datos por fallas en los sistemas de respaldo, corrupción de archivos o destrucción accidental.
- ✓ Fugas de información debido a la falta de cifrado de comunicaciones y datos almacenados.

Riesgos Organizacionales:

- ✓ Uso indebido de la información por parte de los empleados o terceros autorizados.
- ✓ Errores humanos en la manipulación o el almacenamiento de datos sensibles.
- ✓ Falta de capacitación y sensibilización en cuanto a las políticas de privacidad y seguridad de la información.

Riesgos Legales y Regulatorios:

- ✓ No cumplimiento de las leyes de protección de datos personales (Ley 1581 de 2012 y Ley 1266 de 2008).
- ✓ Reclamaciones por violación de la privacidad de los datos personales de los ciudadanos, empleados y concejales.

3.3. Evaluación de Riesgos

Una vez identificados los riesgos, se debe evaluar la probabilidad y el impacto de cada uno. Esto se puede hacer utilizando una escala de evaluación de riesgos que clasifique los riesgos en bajo, medio o alto según su gravedad.

4. Tratamiento de los Riesgos

4.1. Controles y Medidas de Mitigación

Controles Técnicos:

- ✓ Implementar medidas de seguridad para la protección de redes y sistemas informáticos, como firewalls, antivirus y cifrado de datos.
- ✓ Control de acceso: Establecer políticas de control de acceso basadas en roles para garantizar que solo el personal autorizado tenga acceso a la información sensible.
- ✓ Copia de seguridad: Implementar un sistema de respaldo de datos de forma regular, tanto en servidores locales como en la nube, para evitar la pérdida de información.
- ✓ Autenticación de múltiples factores (MFA): Implementar la autenticación de dos factores para el acceso a sistemas críticos.
- ✓ Cifrado de datos: Asegurar que todos los datos sensibles sean cifrados tanto en tránsito como en reposo.

Controles Organizacionales:

- ✓ Política de privacidad y seguridad de la información: Establecer políticas claras sobre el tratamiento y uso de la información, las cuales deben ser revisadas y aprobadas por la alta dirección del Concejo.
- ✓ Capacitación continua: Desarrollar e implementar un programa de capacitación en seguridad de la información y protección de datos para todo el personal.
- ✓ Sensibilización: Crear campañas de concientización para sensibilizar a los empleados sobre la importancia de la seguridad de la información y la privacidad de los datos.

Controles Legales y Regulatorios:

- ✓ Cumplimiento de normativas: Asegurar el cumplimiento de las leyes y regulaciones nacionales e internacionales sobre privacidad y protección de datos, como la Ley 1581 de 2012 y la Ley 1266 de 2008.
- ✓ Auditorías y monitoreo: Realizar auditorías periódicas para verificar el cumplimiento de las políticas de seguridad y privacidad de la información.
- ✓ Gestión de incidentes de seguridad: Establecer un protocolo para gestionar incidentes de seguridad, que incluya la notificación a las autoridades competentes en caso de violación de la privacidad.

4.2. Plan de Acción para la Implementación

Acción	Responsable	Plazo
Actualización de políticas de seguridad y privacidad	Comité de Seguridad y Privacidad	Febrero 2025
Implementación de cifrado de datos en sistemas críticos	Equipo de TI	Abril 2025
Capacitación sobre seguridad de la información	Recursos Humanos y TI	Marzo - Julio 2025
Implementación de medidas de control de acceso	Equipo de TI	Junio 2025
Creación de protocolo de gestión de incidentes de seguridad	Seguridad Informática	Mayo 2025
Auditoría de seguridad y privacidad de la información	Auditoría Interna	Noviembre 2025

5. Monitoreo y Evaluación

Es necesario realizar un monitoreo continuo de la implementación del plan y de la eficacia de las medidas de mitigación. Esto puede incluir:

1. Revisión periódica de los controles implementados y actualización de los protocolos de seguridad según sea necesario.
2. Auditorías internas para evaluar el cumplimiento de las políticas y la efectividad de las medidas de protección de la información.
3. Análisis de incidentes de seguridad para determinar las causas y aplicar mejoras a los controles existentes.

6. Conclusión

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información tiene como propósito garantizar que el Concejo Municipal de Galapa proteja adecuadamente la información pública y privada, mitigando los riesgos que puedan comprometer su confidencialidad, integridad y disponibilidad. La implementación de este plan contribuirá a la mejora continua de las prácticas de seguridad de la información, fortaleciendo la confianza de los ciudadanos y empleados en el manejo de sus datos personales.