PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

2025

ALONSO JOSE DEL RIO JIMENEZ
Presidente Asamblea Departamental de Bolívar
Periodo 2025

KATERINE GARCIA MARRUGO
Secretaria General Asamblea Departamental de Bolívar
Periodo 2025

Introducción

La **Asamblea Departamental de Bolívar** reconoce la importancia de proteger la información y los datos personales de todos los ciudadanos y trabajadores; así como, la necesidad de garantizar la seguridad en la gestión de los datos tratados por nuestros mecanismos de información. Este plan tiene como objetivo establecer las directrices del año 2025 para identificar y mitigar los riesgos asociados con la seguridad y privacidad de la información, en cumplimiento de las leyes colombianas relacionadas con la protección de datos personales como la **Ley 1581 de 2012**, la **Ley 1266 de 2008**, y las disposiciones del **Ministerio de Tecnologías de la Información y las Comunicaciones y la Norma ISO 27001.**

Objetivo General

Este Plan tiene como objetivo principal diseñar medidas para identificar y mitigar riesgos asociados con la seguridad de la información y la privacidad de los datos dentro de la **Asamblea Departamental de Bolívar**, asegurando el cumplimiento de la normatividad vigente y creando un entorno seguro para la gestión de la información.

Objetivos Específicos

- Comprender los términos de riesgo
- Identificar los riesgos a los que se expone la información en los medios de información oficiales de la Asamblea Departamental de Bolívar.
- Establecer medidas de control preventivas y correctivas para mitigar los riesgos de seguridad y privacidad.
- Garantizar la protección de los datos personales de los ciudadanos y empleados de la Organización.

Alcance

Este Plan está enfocado en la identificación, tratamiento y seguimiento de riesgos asociados a los medios de información y comunicación de la Asamblea Departamental de Bolívar.

Su finalidad es realizar una eficiente gestión de riesgos de seguridad y privacidad de la información, que permita que la Asamblea Departamental De Bolívar, realice buenas prácticas que contribuyan a la toma de decisiones y prevención de incidentes de seguridad de información que puedan afectar la gestión de la entidad.

Definiciones y conceptos

- **Riesgo:** Posibilidad de que suceda un daño o perjuicio que genere múltiples consecuencias.
- **Gestión de riesgos:** Identificar, evaluar y controlar los riesgos que pueden afectar a la organización. La gestión busca reducir y/o controlar los riesgos y sus efectos.
- **Amenaza:** Es un ente o escenario que hace uso de una vulnerabilidad para generar un perjuicio o impacto negativo en la institución.
- **Vulnerabilidad:** Es una falencia o debilidad que puede está presente en la tecnología, las personas, las políticas y/o procedimientos.
- **Seguridad:** Estar libre de peligro, daño o riesgo. Es también, la capacidad de responder a amenazas, riesgos o vulnerabilidades.
- **Riesgo de Seguridad de la Información**: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información.
- **Impacto:** Consecuencias que puede ocasionar a la organización la materialización del riesgo.
- **Confidencialidad**: Mantener información en secreto y privada. Es un principio fundamental de la seguridad de la información.

Documentos de referencia

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información se basa en los siguientes lineamientos para su estructura y funcionamiento:

- Decreto 612 de 2018, "Por el cual se fijan directrices para integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entindades del Estado", donde se encuentra el presente Plan Estratégico de seguridad de la Información (PESI) como uno de los requisitos a desarrollar para cumplir con esta normativa.
- Resolución 500 de 2021. "Por la cual se establecen los lineaminetos y estándares para la estrategia de seguridad digital y se adopta al modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital"
- Manual de Gobierno Digital – MINTIC.
- Decreto 767 de 2022 "Por el cual se establecen los lienamientos general de la política de gobierno digital.." del Ministerio de las tecnologías de la información y las comunicaciones.
- Ley 1581 de 2012 "Por la cual se dictan disposiciones generales para la protección de datos personales"

Identificación de Riesgos

Algunos de los riesgos identificados que pueden afectar la seguridad y privacidad de la información dentro de la Asamblea Departamental de Bolívar son:

- **Acceso no autorizado a datos sensibles**: Riesgo de que personas no autorizadas, y/o atacantes externos accedan a información sensible.
- **Pérdida de datos**: Riesgo de que los datos sean eliminados accidentalmente o se pierdan por fallas en los sistemas de respaldo.
- **Divulgación no autorizada de datos personales**: Exposición de datos personales de los ciudadanos, empleados o Diputados sin su consentimiento.
- **Ataques informáticos**: Amenazas cibernéticas que pueden comprometer la integridad de los sistemas, los datos y la información.
- **Desactualización de los sistemas de seguridad**: Riesgo asociado con la falta de actualización de las herramientas de seguridad, tales como antivirus y autenticadores.

Evaluación de Riesgos

Cada riesgo identificado se evalúa según la probabilidad de ocurrencia y el impacto potencial en la organización. Esto se resume en la siguiente matriz de evaluación de riesgos:

Riesgo	Probabilidad	Impacto
Acceso no autorizado a datos sensibles	Alta	Alto
Pérdida de datos	Media	Alto
Divulgación no autorizada de datos personales	Baja	Alto
Ataques informáticos	Alta	Medio
Desactualización de sistemas de seguridad	Media	Medio

Estrategias de Tratamiento de Riesgos

1. Prevención

Para mitigar los riesgos antes de que ocurran, se implementarán las siguientes medidas preventivas:

- **Control de acceso**: Implementación de un sistema de autenticación para acceder a sistemas y bases de datos sensibles. Definición de roles y permisos claros para cada usuario.
- **Cifrado de datos**: Implementación de cifrado de datos sensibles tanto en tránsito como en reposo. Esto garantiza que la información no pueda ser leída por personas no autorizadas.
- **Capacitación en seguridad informática**: Desarrollo de programas de capacitación para empleados de la Asamblea, centrados en buenas prácticas de seguridad informática, manejo de contraseñas seguras, detección de correos fraudulentos, y medidas para proteger los datos personales.

2. Detección

La detección temprana de incidentes de seguridad es clave para minimizar su impacto. Las medidas a implementar incluyen:

- **Monitoreo de la infraestructura tecnológica**: Implementación de herramientas de monitoreo que alerten sobre actividades inusuales o intentos de acceso no autorizado.

- **Auditorías de seguridad**: Auditorías internas para evaluar la efectividad de las medidas de seguridad y detectar vulnerabilidades.

3. Respuesta

En caso de que se produzca un incidente de seguridad, la Asamblea debe responder rápidamente. Estas medidas incluyen:

- **Plan de respuesta a incidentes**: Desarrollo de un protocolo de respuesta que detalle los pasos a seguir en caso de una violación de seguridad. Este plan incluye la identificación, contención, erradicación y recuperación de la información afectada.
- **Notificación de incidentes**: En caso de que se vea comprometida la privacidad de los datos personales, se notificará a los afectados y a las autoridades competentes en el tiempo estipulado por la ley.

4. Mitigación

Para reducir el impacto de los riesgos, se implementarán las siguientes medidas:

- **Respaldo de datos**: Implementación de copias de seguridad periódicas para garantizar la recuperación de los datos en caso de pérdida.
- **Mantenimiento y actualización de sistemas**: Asegurar que los sistemas operativos, aplicaciones y herramientas de seguridad estén siempre actualizados con los últimos parches de seguridad.