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

VIGENCIA 2026

ENTIDAD: CONCEJO MUNICIPAL DE BUCARAMANGA

PROCESO: GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN

FECHA DE ACTUALIZACIÓN: ENERO DE 2026

---

1. INTRODUCCIÓN

El presente plan define las acciones concretas que el Concejo de Bucaramanga ejecutará para tratar, mitigar, transferir o evitar los riesgos que amenazan la confidencialidad, integridad y disponibilidad de su información. Este documento responde al componente de "Gestión de Riesgos" del Modelo de Seguridad y Privacidad de la Información (MSPI) de MinTIC y la Ley 1581 de 2012.

2. OBJETIVO GENERAL

Implementar controles y acciones efectivas para reducir la probabilidad y el impacto de los riesgos de seguridad digital identificados en el Mapa de Riesgos Institucional, garantizando la continuidad de la operación del Concejo (sesiones, acuerdos, actas) y la protección de datos personales**.**

3. METODOLOGÍA DE TRATAMIENTO

Para cada riesgo identificado, el Concejo de Bucaramanga aplicará una de las siguientes cuatro (4) opciones de tratamiento, basadas en la norma ISO/IEC 27001:

1. Mitigar / Reducir: Implementar controles (software, políticas, hardware) para bajar el nivel de riesgo.
2. Transferir / Compartir: Pasar el riesgo a un tercero (ej. pólizas de seguros, tercerización de almacenamiento en la nube).
3. Evitar: Eliminar la actividad que genera el riesgo (ej. dejar de usar un software obsoleto).

4. Aceptar: Asumir el riesgo si el costo del control es mayor al valor del activo (requiere firma de la Alta Dirección).

---

4. MATRIZ DE TRATAMIENTO DE RIESGOS (PLAN DE ACCIÓN 2026)

Esta sección es el núcleo del documento. Se presentan los riesgos más críticos para un Concejo Municipal y sus respectivos controles sugeridos.

ID	Riesgo Identificado	Nivel de Riesgo	Estrategia de Tratamiento	Acciones / Controles a Implementar (Plan de Acción)	Responsable	Fecha Límite
R-01	Secuestro de información (Ransomware) en equipos de Secretaría General o Jurídica.	EXTREMO	Mitigar	1. Implementación de copias de seguridad (Backups) automatizadas en la nube (ej. Google Drive/OneDrive Corporativo) diarias. 2. Restricción de permisos de instalación de software en equipos misionales.	Ing. de Sistemas / TI	Feb 2026
R-02	Pérdida o daño de grabaciones de sesiones plenarias y comisiones (Audios/Videos).	ALTO	Transferir	1. Almacenamiento redundante en servidores externos o plataformas de streaming (YouTube institucional) como repositorio alterno. 2. Mantenimiento preventivo a equipos de grabación del recinto.	Comunicaciones / TI	Mar 2026
R-03	Alteración no autorizada de Proyectos de Acuerdo o Actas en formato digital.	ALTO	Mitigar	1. Implementación de firma digital certificada para documentos finales.	Secretaria General	Abr 2026

ID	Riesgo Identificado	Nivel de Riesgo	Estrategia de Tratamiento	Acciones / Controles a Implementar (Plan de Acción)	Responsable	Fecha Límite
				2. Control de versiones estricto y bloqueo de edición en carpetas compartidas.		
R-04	Fuga de datos personales de contratistas o ciudadanos (Ley 1581).	MODERADO	Mitigar	1. Cifrado de bases de datos de Talento Humano. 2. Firma de acuerdos de confidencialidad con todo el personal que maneja datos sensibles.	Jurídica / Talento Humano	Feb 2026
R-05	Suplantación de identidad de Concejales en correos electrónicos o redes oficiales.	ALTO	Mitigar	1. Activación obligatoria de autenticación de doble factor (2FA) en cuentas de correo institucional. 2. Campaña de sensibilización sobre Phishing e Ingeniería Social.	TI / Comunicaciones	Jun 2026
R-06	Obsolescencia tecnológica de servidores o equipos de cómputo.	MODERADO	Aceptar / Planear	1. Crear fondo de renovación tecnológica. 2. Realizar mantenimiento correctivo mientras se gestionan recursos para renovación.	Dirección Admin.	Dic 2026

5. SEGUIMIENTO Y MONITOREO

La Oficina de Control Interno o quien haga sus veces realizará el seguimiento a este plan con la siguiente periodicidad:

- Primer Seguimiento: Junio de 2026 (Avance del 50%).
- Segundo Seguimiento: Diciembre de 2026 (Avance del 100%).

6. RECURSOS REQUERIDOS

Para la ejecución de este plan se estiman los siguientes recursos:

- Humanos: Líder de TI, Apoyo Jurídico y Líderes de Proceso.
- Tecnológicos: Renovación de licencias de Antivirus, espacio en Nube y Certificados Digitales.
- Financieros: Presupuesto asignado al rubro de Fortalecimiento Institucional / TIC.

APROBACIÓN:

Presidente del Concejo **Robín Anderson Hernández Reyes**

Secretario(a) General **Wilmar Alfonso Palacio Verano**

Líder de Tecnología / Sistemas **José Luis Carreño Galeano**

Fecha: 28 de Enero de 2026