INFORME DE SEGUIMIENTO A LOS PLANES DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN / SEGURIDAD DIGITAL – SECRETARÍA GENERAL DE LA ALCALDÍA MAYOR DE BOGOTÁ

Mayo 2026

Cra 8 No. 10 - 65
Código postal 111711
Tel: 381 3000
www.bogota.gov.co
Info: Linea 195

SECRETARÍA GENERAL

Contenido

1. INTRODUCCIÓN

En el contexto actual, donde la transformación digital y la exposición a amenazas cibernéticas se intensifican, la gestión proactiva de los riesgos de seguridad digital se ha convertido en un pilar fundamental para garantizar la integridad, confidencialidad y disponibilidad de la información institucional. La Secretaría General de la Alcaldía Mayor de Bogotá, tiene la responsabilidad de asegurar que todas las dependencias implementen y mantengan planes efectivos para mitigar estos riesgos, alineados con las políticas públicas y los estándares internacionales de ciberseguridad.

El monitoreo y seguimiento a los planes de tratamiento de riesgos no solo permite evaluar el cumplimiento de las acciones propuestas, sino que también facilita la identificación temprana de brechas, la reorientación de estrategias y la optimización de recursos. Este proceso permite:

1. **Adaptarse al entorno donde los riesgos de seguridad evolucionan rápidamente.**
2. **Garantizar el cumplimiento normativo**
3. **Fortalecer la resiliencia institucional**
4. **Promover la rendición de cuentas**

En cumplimiento del Modelo de Seguridad y Privacidad de la Información (MSPI) y de la Guía Metodológica para la gestión de riesgos de seguridad digital, se presenta el informe de seguimiento correspondiente al II semestre de 2025. El siguiente documento consolida el estado del reporte remitido por las dependencias de la Secretaría General de la Alcaldía Mayor de Bogotá.

2. OBJETIVO

Realizar la verificación de los avances en el desarrollo de las actividades definidas en los planes de tratamiento de riesgos de seguridad de la información / seguridad digital por parte de las dependencias de la Secretaria General de la Alcaldia Mayor de Bogotá para la vigencia I Cuatrimestre 2026, con el fin de identificar brechas, evaluar cumplimiento y realizar las recomendaciones correspondientes.

3. ALCANCE

El presente informe comprende el seguimiento ejecutivo a las **37 dependencias** durante el I cuatrimestre de 2026, equivalentes al 100 % de las dependencias de la entidad. Se aclara que las dependencias OFICINA DE COMUNICACIONES SGAMB, Dirección Distrital de Innovación Pública y Estado Abierto y Subdirección de Innovación Pública – IBO para la vigencia 2026 solo remiten información relacionada con la materialización de riesgos, entendiendo que hasta esta vigencia se están construyendo las matrices de activos de información e identificación de riesgos de seguridad.

4. METODOLOGÍA

1. Para la revisión de los planes de tratamiento de riesgos se dispuso por parte del Oficial de Seguridad de la Información un repositorio para cada dependencia con el fin que se incluyera la información correspondiente en la matriz de riesgos y las evidencias en la carpeta de monitoreo respectiva.

2. Para el proceso de gestión de seguridad y privacidad de la información en la entidad, se definió una estructura como se muestra a continuación:

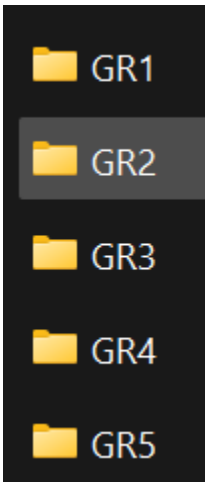

Ilustración 1 Organización Repositorio Seguridad

3. Dentro de la carpeta de Activos de información para la vigencia 2026, se crearon las carpetas de cada dependencia y dentro de esta la carpeta de monitoreo I cuatrimestre 2026.

4. Las dependencias deben realizan la actualización en la matriz correspondiente, detallando los avances en la implementación de las actividades definidas en la hoja de plan de tratamiento – seguimiento al plan de tratamiento de riesgos.

SEGUIMIENTO AL PLAN DE TRATAMIENTO DE RIESGOS						
DESCRIPCIÓN DE ACTIVIDADES	SOPORTES (indicar por cada actividad)	% DE AVANCE (ACUMULADO)		MATERIALIZACIÓN DEL RIESGO		
		I SEMESTRE	II SEMESTRE	EVENTO QUE EVIDENCIA LA MATERIALIZACION DEL RIESGO	FECHA DE OCURRENCIA	ACCIONES DE TRATAMIENTO IMPLEMENTADAS

Ilustración 2 Seguimiento Plan de tratamiento de riesgos

5. Una vez actualizada la matriz y cargadas las evidencias por parte del enlace de seguridad de la información delegado, se realiza el reporte por medio de correo electrónico o memorando enviado a la Oficina de tecnologías de la Información y las Comunicaciones, indicando lo siguiente:

   - Reporte de la actualización de la matriz y evidencias.
   - Reporte de la materialización o no de riesgos de seguridad en el periodo.
   - Reporte del monitoreo de riesgos de seguridad indicando si estos continúan o no en los mismos niveles.

6. Por último, el oficial de seguridad, realiza la revisión correspondiente y en caso de tener observaciones lo informa al enlace para su respectiva actualización.

Nota. Durante todo el proceso de monitoreo se realiza el seguimiento por parte del Oficial de seguridad de la información con el fin que las dependencias entreguen la información dentro de los tiempos establecidos conforme como esta descrito en el documento Guía Metodológica para la gestión de riesgos de seguridad digital - 4204000-GS-096.

"...Los dueños de los activos de información deberán reportar el resultado del seguimiento a los riesgos de seguridad de la información / seguridad digital los primeros diez días hábiles siguientes al corte del cuatrimestre. En los casos que se requiera, este plazo puede ser ampliado con aprobación del jefe de la Oficina de Tecnologías de la Información y las Comunicaciones sin exceder los plazos establecidos para publicación y envío de información a la Oficina de Control Interno."

5. DESARROLLO

Como se muestra en la siguiente imagen, al corte del I cuatrimestre del 2026, el total de riesgos de seguridad de la información / seguridad digital fue de 514 riesgos, de los cuales 7 riesgos están en nivel alto y corresponden al 1% y 120 riesgos en nivel moderado que corresponden al 23%, a estos riesgos se les definió plan de tratamiento por parte de las dependencias.

El 75% que corresponde a 387 riesgos se encuentran en nivel bajo, los cuales son monitoreados por parte de las dependencias sin tener que generar plan de tratamiento.

TIPO DE ACTIVOS	NIVEL DE RIESGO RESIDUAL			
	Alto	Moderado	Bajo	Total general
Datos / Información	3	30	98	131
Servicios	1	20	80	101
Hardware / Infraestructura	0	15	67	82
Recurso Humano	2	23	40	65
Instalaciones	0	7	40	47
Base de Datos	0	12	35	47
Software / Aplicaciones Informáticas	1	13	25	39
Soportes de Información / Dispositivos móviles	0	0	2	2
Total general	**7**	**120**	**387**	**514**
%	**1%**	**23%**	**75%**	**100%**

Ilustración 3 Riesgos de seguridad de la información / seguridad digital I cuatrimestre 2026

Teniendo en cuenta que la mayoría de los riesgos identificados se asociaban a la pérdida de confidencialidad / integridad de la información digital, riesgos asociados a la pérdida de confidencialidad o disponibilidad del personal, dentro de las principales actividades definidas en los planes de tratamiento por parte de las dependencias se definieron las siguientes:

- ✓ Fortalecimiento de la cultura de seguridad para evitar la materialización de riesgos de seguridad.
- ✓ Seguimiento al cumplimiento de políticas de seguridad (ej. Gestión de copias de respaldo, gestión de contraseñas)
- ✓ Implementación de repositorios de SharePoint en las dependencias.

- ✓ Seguimiento a la entrega y cargue de información en repositorios.
- ✓ Realizar seguimiento a las de firmas de acuerdos de confidencialidad.
- ✓ Solicitar respaldo de información proveedores externos.
- ✓ Realizar seguimiento a las actas de entrega de cargos/contratos de funcionarios / contratistas.

Al cierre del seguimiento del I cuatrimestre de 2026 se realizó la revisión de la información reportada por **37 dependencias**. La distribución por grupos muestra mayor concentración de pendientes en el **Grupo 1**, mientras que los **Grupos 2, 3, 4 y 5** presentan un comportamiento mayoritariamente de reporte remitido. Asimismo, se identificaron dos dependencias nuevas ubicadas en el **Grupo 3**, las cuales deberán ser incorporadas formalmente al siguiente ciclo semestral de seguimiento.

Categoría	Cantidad	Porcentaje
Dependencias obligadas a reportar y nuevas	37	100,0 %
Dependencias Nuevas que realizan reporte	3	8,11%
Dependencias obligadas a reportar que realizaron reporte	27	72,97%
Dependencias obligadas a reportar que no realizaron reporte	7	18,92%

6. HALLAZGOS CLAVE

- **Cumplimiento parcial del proceso de monitoreo.** De las 34 dependencias obligadas a presentar el seguimiento al Plan de Tratamiento de Riesgos, únicamente **27 (72,97 %)** remitieron el reporte, mientras que **7 dependencias (18,92 %)** no lo hicieron. Esta situación limita la capacidad institucional para verificar el avance de las acciones de tratamiento y evaluar la efectividad de los controles implementados.
- **Incorporación de nuevas dependencias al proceso.** Se evidencia la participación de **3 dependencias nuevas**, lo que representa un avance en la cobertura institucional del proceso de gestión de riesgos y en la apropiación del Modelo de Seguridad y Privacidad de la Información (MSPI).
- **Necesidad de fortalecer el seguimiento por parte de la primera línea de defensa.** El monitoreo de los planes de tratamiento depende de los responsables de cada proceso y de los dueños de los activos de información. La ausencia de reportes evidencia diferencias en el nivel de apropiación de las responsabilidades asociadas a la gestión de riesgos entre las dependencias.

- **Avance en el acompañamiento institucional.** Durante el proceso se desarrollaron mesas de trabajo, jornadas de aclaración de dudas, actualización de enlaces de seguridad y acompañamiento técnico para facilitar el reporte del primer cuatrimestre, evidenciando un esfuerzo institucional por fortalecer la gestión de riesgos.

7. PRINCIPALES RIESGOS EVIDENCIADOS

Desde la perspectiva de seguridad de la información, el principal riesgo no es únicamente el incumplimiento del reporte, sino las consecuencias que este genera sobre la capacidad de gestión de la entidad:

- Falta de visibilidad sobre el estado real de los riesgos residuales, impidiendo determinar si las acciones de tratamiento están siendo ejecutadas y si los niveles de riesgo se mantienen dentro del apetito definido por la Entidad.

- Posible materialización de riesgos no controlados, debido a retrasos o ausencia en la implementación de actividades de mitigación definidas en los planes de tratamiento.

- Debilitamiento del proceso de mejora continua del MSPI, al no contar con información completa para realizar el seguimiento, análisis de tendencias y toma de decisiones por parte de la OTIC y del Comité Institucional de Gestión y Desempeño.

- Riesgo de incumplimiento de los lineamientos institucionales y de la metodología de gestión de riesgos, la cual establece que todos los riesgos residuales moderados, altos o extremos deben contar con planes de tratamiento, seguimiento periódico y evidencia de su ejecución.

- Incremento del riesgo operativo y reputacional, al no poder demostrar la gestión efectiva de los riesgos asociados a los activos de información críticos de la Entidad.

8. RECOMENDACIONES ESTRATÉGICAS

Se recomienda a nivel institucional:

- Continuar fortaleciendo el compromiso de los líderes de proceso respecto a la ejecución y seguimiento de los planes de tratamiento de riesgos, recordando que

constituyen la primera línea de defensa del Sistema de Gestión de Seguridad de la Información.

- Continuar con la implementación de esquema de seguimiento periódico a las dependencias que no presentan los reportes dentro de los plazos establecidos, incluyendo alertas tempranas y acompañamiento focalizado.

- Continuar realizando mesas de trabajo y asistencia técnica, especialmente con aquellas dependencias que presentan mayores dificultades en la elaboración o seguimiento de sus planes de tratamiento.

- Fortalecer la capacitación de los enlaces de seguridad de la información, orientándola a la definición de actividades de tratamiento, establecimiento de indicadores, recopilación de evidencias y monitoreo del avance de los planes.

- Presentar periódicamente al Comité Institucional de Gestión y Desempeño el estado de cumplimiento de los planes de tratamiento, identificando dependencias con mayores rezagos y promoviendo acciones de mejora.

- Integrar el seguimiento de los planes de tratamiento con el proceso de actualización de activos de información y el análisis de vulnerabilidades, con el fin de asegurar que los riesgos emergentes, las nuevas amenazas y los cambios tecnológicos sean incorporados oportunamente en la gestión del riesgo.

- Promover una cultura de gestión del riesgo basada en la mejora continua, asegurando que el monitoreo de los planes no sea entendido como un requisito documental, sino como un mecanismo para reducir la probabilidad de materialización de riesgos que afecten la confidencialidad, integridad y disponibilidad de la información institucional, en concordancia con el Modelo de Seguridad y Privacidad de la Información (MSPI) y la ISO/IEC 27001:2022.

9. CONCLUSIÓN

Los resultados del seguimiento al primer cuatrimestre de 2026 evidencian un nivel de cumplimiento aceptable del 76,5 % por parte de las dependencias obligadas a reportar el avance de sus planes de tratamiento de riesgos de seguridad de la información, lo que refleja un grado importante de apropiación institucional del proceso. No obstante, persiste un

porcentaje de dependencias que no remitieron la información requerida, situación que limita la capacidad de la Entidad para realizar un monitoreo integral del estado de los riesgos, verificar la implementación efectiva de los controles definidos y evaluar la eficacia de las acciones de tratamiento adoptadas.

De conformidad con la Política de Seguridad de la Información y la Estrategia de Seguridad Digital de la Entidad, la gestión de riesgos constituye uno de los pilares fundamentales para preservar la confidencialidad, integridad, disponibilidad y resiliencia de la información y de los servicios institucionales. En este contexto, el seguimiento oportuno a los planes de tratamiento representa un mecanismo esencial de mejora continua, que permite identificar desviaciones, adoptar acciones preventivas y correctivas, fortalecer la toma de decisiones basada en riesgos y asegurar el cumplimiento de los objetivos institucionales en materia de seguridad digital.

En consecuencia, se hace necesario continuar fortaleciendo la corresponsabilidad de los líderes de proceso, propietarios de activos de información y enlaces de seguridad, promoviendo una participación activa y oportuna en las actividades de monitoreo y reporte.

Así mismo, se recomienda continuar consolidando una cultura organizacional orientada a la gestión integral del riesgo, incrementando el acompañamiento técnico, el seguimiento periódico y la rendición de cuentas sobre el cumplimiento de los planes de tratamiento, con el propósito de alcanzar una cobertura del 100 % y mantener un nivel de madurez acorde con los lineamientos del Modelo de Seguridad y Privacidad de la Información (MSPI), la Política de Gobierno Digital y la Estrategia de Seguridad Digital de la Entidad.

10. ELABORACIÓN

	NOMBRE	CARGO	FECHA
ELABORÓ	Lourdes María Acuña Acuña	Contratista	15/05/2026

11. CONTROL DE CAMBIOS

ASPECTOS QUE CAMBIARON EN EL DOCUMENTO	DETALLE DE LOS CAMBIOS EFECTUADOS	FECHA DEL CAMBIO	VERSIÓN
N/A	Creación del documento	15/02/2026	1.0

Cra 8 No. 10 - 65
Código postal 111711
Tel: 381 3000
www.bogota.gov.co
Info: Linea 195