TABLA DE CONTENIDO

1. INTRODUCCIÓN

En el contexto de la transformación digital y el incremento de los riesgos asociados al manejo de la información, la entidad implementa el Plan de Sensibilización y Comunicación de Seguridad de la Información como un instrumento estratégico orientado a fortalecer la cultura organizacional en seguridad digital, promover la apropiación tecnológica y asegurar el cumplimiento de los lineamientos definidos en el **Plan Estratégico de Tecnologías de la Información (PETI), el Plan de Seguridad y Privacidad de la Información y el Plan de Tratamiento de Riesgos de Seguridad.**

Este plan de sensibilización en seguridad de la información se formula con el propósito de fortalecer el conocimiento y las competencias de los colaboradores frente al uso adecuado de las tecnologías y la gestión responsable de los activos de información. Su implementación responde al análisis de incidentes, riesgos y situaciones identificadas por la Oficina de Tecnologías de la Información y las Comunicaciones (OTIC), que evidencian la necesidad de promover acciones de sensibilización, educación y apropiación de buenas prácticas. A través de estrategias de comunicación y formación, se busca contribuir a la mitigación de riesgos y a la protección de la **confidencialidad, integridad y disponibilidad** de la información institucional.

Dada la evolución constante de los riesgos y cambios tecnológicos y normativos, el plan será actualizado **anualmente**, con el fin de incorporar mejoras, atender nuevas necesidades institucionales y fortalecer continuamente la cultura de seguridad de la información en la entidad.

2. OBJETIVO

Fortalecer la cultura institucional en materia de seguridad de la información en la Región Metropolitana Bogotá – Cundinamarca (RMBC), mediante el desarrollo de estrategias de sensibilización, comunicación y apropiación dirigidas a servidores públicos, contratistas y colaboradores, con el fin de promover buenas prácticas en el uso de los recursos tecnológicos, prevenir incidentes de seguridad digital y contribuir a la protección de la confidencialidad, integridad y disponibilidad de la información institucional. Se especifica de la siguiente manera:

1. Promover el conocimiento y la apropiación de las políticas, lineamientos y buenas prácticas de seguridad de la información entre los servidores públicos, contratistas y colaboradores de la entidad.
2. Sensibilizar a los usuarios sobre los principales riesgos de seguridad digital, tales como phishing, malware, fuga de información y uso inadecuado de los recursos tecnológicos institucionales.
3. Fomentar comportamientos responsables en el manejo de la información y en el uso de los sistemas y plataformas tecnológicas de la entidad.
4. Difundir periódicamente recomendaciones, alertas y contenidos educativos relacionados con la seguridad de la información y la protección de datos.
5. Contribuir a la prevención de incidentes de seguridad mediante la generación de una cultura organizacional orientada a la protección de los activos de información de la entidad.

3. ALCANCE

Comprende el diseño, implementación y seguimiento de estrategias de sensibilización y comunicación orientadas a fortalecer la cultura de seguridad de la información, mediante el desarrollo de campañas, jornadas de formación, difusión de contenidos y actividades educativas relacionadas con la prevención de riesgos digitales y el uso adecuado de los sistemas de información.

Así mismo, el plan abarca los canales institucionales definidos para la divulgación de información, así como las actividades de monitoreo, evaluación e indicadores de cumplimiento asociados al proceso de sensibilización.

No hace parte del alcance del presente plan la implementación de controles técnicos de seguridad, gestión de infraestructura tecnológica o administración de herramientas de seguridad, los cuales se gestionan a través de otros procesos y políticas institucionales.

4. DEFINICIONES

- **Activo de Información:** Recurso que tiene valor para la entidad y que soporta los procesos institucionales, incluyendo información, sistemas de información, servicios tecnológicos, infraestructura, documentos físicos o digitales y el conocimiento de las personas.
- **Amenaza:** Causa potencial de un incidente no deseado que puede explotar una vulnerabilidad y generar afectaciones a los activos de información, comprometiendo la seguridad de la información.
- **Colaborador:** Persona que, en el desarrollo de sus funciones o actividades dentro de la entidad, tiene acceso autorizado a información o recursos tecnológicos, incluyendo servidores públicos, contratistas y terceros.
- **Confidencialidad:** Propiedad de la información que asegura que esta no sea puesta a disposición ni revelada a individuos, entidades o procesos no autorizados.
- **Contratista:** Persona natural o jurídica vinculada a la entidad mediante un contrato, que ejecuta actividades específicas y que, en el marco de sus obligaciones, puede acceder a información o recursos tecnológicos institucionales.
- **Control de Seguridad:** Medida de tipo administrativo, técnico, físico o legal implementada para gestionar riesgos de seguridad de la información, ya sea previniendo, detectando, corrigiendo o mitigando su materialización.
- **Disponibilidad:** Propiedad de la información y de los sistemas que la procesan, que garantiza su acceso y uso oportuno por parte de usuarios autorizados cuando sea requerido.
- **Incidente de Seguridad de la Información:** Evento único o serie de eventos de seguridad de la información que tienen una probabilidad significativa de comprometer las operaciones institucionales o amenazar la confidencialidad, integridad o disponibilidad de la información.
- **Ingeniería: Social:** Técnica utilizada para manipular a las personas con el fin de obtener información confidencial, acceso a sistemas o la ejecución de acciones que comprometan la seguridad de la información.

- **Integridad:** Propiedad de la información que salvaguarda la exactitud y completitud de los activos de información y de sus métodos de procesamiento.
- **Malware:** Software diseñado con fines maliciosos para infiltrarse, dañar, alterar o interrumpir el funcionamiento de sistemas de información, afectar la disponibilidad de los servicios o comprometer la información institucional.
- **Phishing:** Modalidad de ataque basada en ingeniería social mediante la cual se intenta obtener información sensible de los usuarios a través de comunicaciones fraudulentas que simulan provenir de fuentes confiables.
- **Riesgo de Seguridad de la Información:** Efecto de la incertidumbre sobre los objetivos de la entidad relacionado con la posibilidad de que una amenaza explote una vulnerabilidad y genere impactos negativos en los activos de información.
- **Seguridad de la Información:** Preservación de la confidencialidad, integridad y disponibilidad de la información, así como de otras propiedades como autenticidad, responsabilidad, no repudio y fiabilidad.
- **Sensibilización en Seguridad de la Información:** Proceso planificado y continúo orientado a fortalecer la cultura de seguridad digital en la entidad mediante actividades de formación, comunicación y apropiación de buenas prácticas.
- **Servidor Público (Funcionario Público):** Persona vinculada legal y reglamentariamente a la entidad para ejercer funciones públicas y que, en el desarrollo de sus responsabilidades, puede acceder o gestionar activos de información institucionales.
- **Vulnerabilidad:**
  Debilidad de un activo o control que puede ser explotada por una o más amenazas y comprometer la seguridad de la información.

5. SIGLAS

- **MinTIC:** Ministerio de Tecnologías de la Información y las Comunicaciones
- **MSPI:** Modelo de Seguridad y Privacidad de la Información
- **OTIC:** Oficina de Tecnologías de la Información y las Comunicaciones
- **RMBC:** Región Metropolitana Bogotá – Cundinamarca
- **SGSI:** Sistema de Gestión de Seguridad de la Información
- **TIC:** Tecnologías de la Información y las Comunicaciones

6. MARCO NORMATIVO

Resolución No. 065 de 2025 – RMBC: Adopta la Política de Seguridad Digital y Privacidad de la Información de la entidad, estableciendo lineamientos para la gestión de riesgos y la protección de los datos personales.

Decreto 338 de 2022: Fortalece la gobernanza de la seguridad digital en las entidades públicas y define el modelo institucional para su gestión.

Decreto 767 de 2022: Establece lineamientos de la Política de Gobierno Digital orientados al uso estratégico y seguro de las tecnologías.

Resolución 746 de 2022: Actualiza y fortalece el Modelo de Seguridad y Privacidad de la Información (MSPI) en las entidades del Estado.

Resolución 500 de 2021: Adopta el MSPI como instrumento para la gestión de la seguridad digital en el marco de Gobierno Digital.

Resolución 1519 de 2020: Define estándares para el acceso a la información pública, seguridad digital, accesibilidad web y datos abiertos.

Documento CONPES 3995 de 2020: Establece la Política Nacional de Confianza y Seguridad Digital para fortalecer la gestión del riesgo digital.

Documento CONPES 3854 de 2016: Define lineamientos para el fortalecimiento de las capacidades del país en seguridad digital.

Decreto 612 de 2018: Establece directrices para la articulación de los planes institucionales, incluyendo los relacionados con tecnologías y seguridad digital.

Ley 1712 de 2014: Regula el derecho de acceso a la información pública y promueve la transparencia en las entidades del Estado.

Decreto 886 de 2014: Reglamenta el Registro Nacional de Bases de Datos para la protección de la información personal.

Decreto 1377 de 2013: Reglamenta aspectos del tratamiento y protección de datos personales.

Ley 1581 de 2012: Establece el régimen general de protección de datos personales en Colombia.

7. PÚBLICO OBJETIVO

Para la implementación del Plan de Sensibilización y Comunicación en Seguridad de la Información de la Región Metropolitana Bogotá – Cundinamarca (RMBC), se identifican los siguientes grupos de interés, los cuales tienen relación directa o indirecta con el uso, manejo y protección de la información institucional.

Estos actores participan en los procesos organizacionales y utilizan los recursos tecnológicos de la entidad, por lo cual es fundamental promover en ellos una cultura de seguridad de la información orientada a la prevención de riesgos digitales y al cumplimiento de las políticas institucionales.

Servidores Públicos: Funcionarios vinculados a la entidad mediante relación legal y reglamentaria, quienes en el ejercicio de sus funciones utilizan sistemas de información, herramientas tecnológicas y acceden a información institucional.

Contratistas: Personas naturales o jurídicas vinculadas mediante contratos de prestación de servicios u otros tipos de contratación, que desarrollan actividades en apoyo a la gestión institucional y que pueden tener acceso a información o recursos tecnológicos de la entidad.

Colaboradores: Personas que participan en actividades institucionales o que, en el desarrollo de sus funciones, interactúan con los sistemas de información y recursos tecnológicos de la entidad, incluyendo servidores públicos, contratistas y terceros autorizados.

Alta Dirección: Directivos y responsables de la toma de decisiones estratégicas en la entidad, quienes tienen la responsabilidad de promover el cumplimiento de las políticas institucionales, incluyendo las relacionadas con la seguridad de la información.

Área de Tecnologías de la Información y las Comunicaciones – OTIC: Dependencia responsable de liderar la implementación de controles, lineamientos y estrategias relacionadas con la seguridad digital, así como de coordinar acciones de prevención, gestión y respuesta ante incidentes de seguridad de la información.

Ciudadanía y usuarios externos: Personas naturales o jurídicas que interactúan con los servicios digitales o plataformas de la entidad y que pueden suministrar o consultar información a través de los canales institucionales.

8. DESCRIPCIÓN METODOLÓGICA DEL TEMA A DESARROLLAR

La ejecución del Plan de Sensibilización y Comunicación en Seguridad de la Información de la Región Metropolitana Bogotá – Cundinamarca (RMBC) se desarrollará mediante una metodología estructurada basada en **la planificación, ejecución, seguimiento y mejora continua** de las actividades definidas, en concordancia con los objetivos institucionales y los lineamientos del **Modelo de Seguridad y Privacidad de la Información (MSPI).**

FASE	CONCEPTO
PLANIFICACIÓN	Se definen los temas a socializar, el público objetivo, los canales de comunicación, los responsables y el cronograma de actividades, tomando como base la identificación de riesgos de seguridad de la información, las necesidades institucionales y las prioridades estratégicas de la entidad.
EJECUCION	Se desarrollan las actividades de sensibilización a través de charlas presenciales o virtuales, campañas de comunicación, difusión de piezas informativas y espacios de formación, orientados a promover buenas prácticas en el uso de los recursos tecnológicos, la identificación de amenazas como phishing y malware, y el fortalecimiento de hábitos de seguridad digital en los usuarios.
SEGUIMIENTO Y MONITOREO	Contempla el registro de las actividades realizadas, el control de asistencia, la consolidación de evidencias y la medición de resultados mediante indicadores de cumplimiento. Así mismo, se aplican encuestas de percepción de seguridad de la información con el fin de evaluar el nivel de apropiación de los contenidos y detectar oportunidades de mejora.
MEJORA CONTINUA	Se analizan los resultados obtenidos a partir de los indicadores y las encuestas, permitiendo ajustar las estrategias de sensibilización, fortalecer los contenidos y optimizar las actividades futuras, garantizando la evolución del programa y su alineación con las necesidades institucionales y los riesgos emergentes en materia de seguridad digital.

8.1. Fase de planificación:

Inicia con la identificación de necesidades de sensibilización, la cual se realiza a partir del análisis de riesgos de seguridad de la información, incidentes reportados, buenas prácticas institucionales y comportamientos observados en los usuarios de la entidad.
Se reconoce que una parte significativa de las vulnerabilidades en seguridad de la información se originan en el factor humano, derivadas de desconocimiento, prácticas inadecuadas o falta de apropiación de las políticas institucionales.

En este sentido, se identifican las siguientes necesidades:

<u>Problemas y necesidades identificadas:</u>

- Uso inadecuado de contraseñas en equipos, correos electrónicos y sistemas institucionales, incluyendo contraseñas débiles o compartidas.
- Mal uso del correo electrónico institucional, incluyendo apertura de enlaces sospechosos, descarga de archivos maliciosos y uso para fines no institucionales.
- Falta de conocimiento en la identificación y reporte de incidentes de seguridad de la información.
- Riesgo asociado a la ejecución de archivos maliciosos, uso inadecuado de dispositivos externos (USB) y manejo inseguro de información digital.
- Manejo inadecuado de la información institucional, incluyendo almacenamiento inseguro, compartición indebida y falta de criterios de clasificación.
- Ausencia de hábitos de seguridad digital en el entorno laboral, como dejar sesiones abiertas, compartir credenciales o descuidar el entorno físico de trabajo.
- Uso emergente de herramientas de inteligencia artificial sin criterios de seguridad, lo que puede generar riesgos de fuga de información o uso indebido de datos institucionales.
- Falta de preparación frente a la gestión de crisis digitales y manejo de información en canales oficiales.

Canales de sensibilización y comunicación:

Estos canales permitirán difundir periódicamente recomendaciones de seguridad digital, alertas sobre amenazas y buenas prácticas en el uso de los recursos tecnológicos institucionales, conforme a las políticas de seguridad de la información de la entidad. Con ello se busca fortalecer la apropiación de la seguridad digital, promover el manejo responsable de la información y prevenir incidentes que puedan afectar los activos institucionales.

Los canales definidos para la ejecución del plan son los siguientes:

- Charlas presenciales y/o virtuales: En estos escenarios, y en coordinación con el Grupo de Talento Humano, el equipo de Seguridad de la Información brindará sesiones de sensibilización dirigidas a los servidores públicos, contratistas y colaboradores, las cuales podrán desarrollarse de manera presencial o virtual según las necesidades de la entidad.

- Correos institucionales: Envío de comunicaciones periódicas a los usuarios con recomendaciones de seguridad, alertas sobre amenazas activas, campañas de prevención y recordatorios de buenas prácticas en el uso de los recursos tecnológicos.

- Boletines de seguridad digital: Publicación de boletines informativos que recopilan alertas, tendencias de ciberseguridad, incidentes relevantes y recomendaciones prácticas para fortalecer la cultura de seguridad de la información.

- Piezas gráficas y material visual: Difusión de afiches, infografías y contenidos visuales a través de canales internos, orientados a reforzar mensajes clave de seguridad de manera clara y accesible para los usuarios.

8.2. Fase de ejecución:

La fase de ejecución del Plan de Sensibilización y Comunicación en Seguridad de la Información comprende el desarrollo de las actividades definidas en la etapa de planificación, orientadas a atender los riesgos asociados al factor humano. Su implementación se realiza mediante campañas de sensibilización que abordan temáticas clave de seguridad digital, a través de canales institucionales como charlas, correos electrónicos, boletines, piezas gráficas e intranet.

Para su adecuada ejecución se definen:

- Campaña
- Tema por socializar
- Público objetivo
- Canal de comunicación
- Responsable
- Fecha

El siguiente cuadro presenta la programación de las campañas de sensibilización en seguridad de la información definidas para la vigencia 2026.

Debido al nivel de detalle requerido, la información se organiza mediante el uso combinado de texto descriptivo y cuadro, facilitando su consulta, control y comprensión.

Campaña 1 – Prevención de amenazas digitales:
Campaña orientada a fortalecer la capacidad de los usuarios para identificar, prevenir y reportar amenazas como phishing y malware. Promueve el análisis seguro de correos, enlaces y archivos adjuntos, el uso adecuado de dispositivos externos y el reporte oportuno de incidentes, con el fin de reducir los riesgos y el impacto de eventos de seguridad en la entidad.

Campaña 2 – Protección de la información y accesos:
Campaña orientada a fortalecer las buenas prácticas para la protección de la información institucional y el control de accesos a los sistemas. Promueve el uso de contraseñas seguras, la autenticación multifactor, el bloqueo de sesiones y el cumplimiento de políticas como escritorio y pantalla limpia, así como el manejo adecuado de la información para prevenir accesos o divulgaciones no autorizadas.

Campaña 3 – Seguridad en entornos digitales y comunicación:
Campaña orientada a sensibilizar sobre los riesgos asociados al uso de tecnologías digitales y la comunicación institucional en medios digitales. Promueve el uso seguro de herramientas como la inteligencia artificial, la protección de la información institucional, el manejo responsable de los canales oficiales y la adecuada gestión de la información durante incidentes, con el fin de prevenir fugas de datos y mitigar impactos reputacionales para la entidad.

Luego de la descripción de cada campaña, se presenta el cuadro con la programación de las actividades de sensibilización para el año 2026:

CAMPAÑA	TEMA A SOCIALIZAR	PÚBLICO OBJETIVO	CANAL DE COMUNICACIÓN	RESPONSABLE	FECHA
Campaña 1	Reporte y gestión de incidentes de seguridad de la información. Phishing y correos maliciosos	Funcionarios contratistas colaboradores	*Charlas presenciales/virtuales *Correos institucionales *Piezas gráficas *Intranet	Equipo de Seguridad de la Información de TI	Abril 2026
	Prevención de malware y uso seguro de dispositivos y archivos	Funcionarios contratistas colaboradores	*Charlas presenciales/virtuales *Boletines de seguridad digital *Piezas informativas	Equipo de Seguridad de la Información de TI	Mayo 2026
Campaña 2	Buenas prácticas en el manejo de la información institucional	Funcionarios contratistas colaboradores	*Charlas presenciales/virtuales *Correos institucionales *Intranet	Equipo de Seguridad de la Información de TI	Junio 2026
	Uso seguro de contraseñas y autenticación multifactor (MFA)	Funcionarios contratistas colaboradores	*Correos institucionales *Piezas gráficas *Boletines de seguridad digital	Equipo de Seguridad de la Información de TI	Julio 2026
	Hábitos de seguridad digital	Funcionarios contratistas colaboradores	*Charlas presenciales/virtuales *Piezas visuales *Intranet	Equipo de Seguridad de la Información de TI	Agosto 2026
Campaña 3	Inteligencia Artificial: cómo usarla de manera segura	Funcionarios contratistas colaboradores	*Charlas presenciales/virtuales *Boletines de seguridad digital *Correos institucionales	Equipo de Seguridad de la Información de TI	Sept. 2026
	Rol de Community Manager en situaciones de crisis cibernéticas	Funcionarios, contratistas, colaboradores	*Charlas presenciales/virtuales *Correos institucionales *Material informativo	Equipo de Seguridad de la Información de TI	Sept. 2026

8.3. Fase de seguimiento y monitoreo:

Como parte del proceso de control y trazabilidad, se conformará un expediente virtual en la herramienta institucional **SIGMA**, en el cual se almacenarán de manera organizada todas las evidencias asociadas al desarrollo del Plan de Sensibilización en Seguridad de la Información.

El monitoreo y seguimiento al cumplimiento del plan se realizará mediante el indicador **"Porcentaje de cumplimiento del Plan de Sensibilización del SGSI"**, cuyo responsable será el Jefe de la Oficina de Tecnologías de la Información y las Comunicaciones. Este indicador permitirá medir el No. de sensibilizaciones realizadas / (No. Total, de sensibilizaciones programadas) * 100.

8.4. Fase de mejora continua:

Con base en la evaluación de la eficacia de las actividades de sensibilización, el análisis de incidentes de seguridad de la información y la identificación de nuevos riesgos, la entidad definirá e implementará acciones de mejora continua orientadas a fortalecer la cultura de seguridad digital y optimizar las estrategias de comunicación y formación.

Estas acciones permitirán actualizar el plan, ajustar los controles asociados al factor humano y asegurar su alineación con el contexto organizacional, los riesgos emergentes y los objetivos del Sistema de Gestión de Seguridad de la Información.

9. DOCUMENTOS INTERNOS ASOCIADOS

Proceso	Nombre del documento	Repositorio
Gestión de las Tecnologías de la Información y las Comunicaciones	Política de Seguridad y Privacidad de la Información de la RMBC	Página Web
Gestión de las Tecnologías de la Información y las Comunicaciones	Política de Gobierno Digital de la RMBC	Página Web
Gestión de las Tecnologías de la Información y las Comunicaciones	Plan de seguridad y privacidad de la información	Página Web
Gestión de las Tecnologías de la Información y las Comunicaciones	Plan de tratamiento de riesgo	Página Web

10. PRODUCTO O SERVICIO GENERADO

Producto / Servicio Generado	Descripción del Producto / Servicio
Ejecución de campañas de sensibilización y comunicación en seguridad de la información.	Desarrollo y difusión de piezas comunicativas, jornadas de sensibilizacion, material pedagógico y reportes de seguimiento orientados a fortalecer la cultura de seguridad de la información, promover buenas prácticas en el uso de los recursos tecnológicos institucionales y prevenir incidentes asociados al factor humano, conforme a lo establecido en el Plan de Sensibilización del SGSI.

11. CONTROL DE DOCUMENTOS

Versión	Fecha de aprobación	Descripción de la modificación
1	26-06-2026	Creación del documento

ELABORÓ	Brahiam Alirio Cruz Aleman Martha Lucia González Maldonado	Contratistas	Oficina de las Tecnologías de la Información y las comunicaciones
REVISÓ	Silvana Lorena Chaves Patiño	Contratista	Oficina Asesora de Planeación Institucional
APROBÓ	LILIANA MORALES	Jefe	Oficina de las Tecnologías de la Información y las comunicaciones
FECHA DE APROBACIÓN	***COMITÉ INTITUCIONAL DE GESTIÓN Y DESEMPEÑO*** 26-06-2026		