promueve+

Plan de tratamiento de riesgos de seguridad y privacidad de la información

2026

CONTENIDO

INTRODUCCIÓN

La gestión del plan de tratamiento de riesgos de seguridad y privacidad de la información son aquellos procesos que reducen las pérdidas y brindan protección de la información, permitiendo conocer las debilidades que afectan durante todo el ciclo de vida del servicio.

Todos los servidores públicos en cumplimiento de sus funciones están sometidos a riesgos que pueden hacer fracasar una gestión; por lo tanto, es necesario tomar las medidas, para identificar las causas y consecuencias de la materialización de dichos riesgos.

Cualquier tipo de organización independiente de su tamaño y tipo afronta factores tanto internos como externos que pueden afectar uno de los activos más importante de la entidad que es la información. Todas las actividades de una entidad involucran riesgos y de una forma u otra los gestionan mediante su identificación, análisis y su respectivo tratamiento.

Por esa razón, el presente plan tiene como objetivo orientar y facilitar la implementación y desarrollo de una eficaz, eficiente y efectiva gestión del riesgo, desde la identificación hasta el monitoreo; enfatiza en la importancia de la administración del riesgo, sus fundamentos teóricos y de una orientación para facilitar su identificación, reconocimiento de las causas, efectos, definición de controles y de lineamientos sencillos y claros para su adecuada gestión.

OBJETIVOS

OBJETIVO GENERAL

Definir las actividades y lineamientos que permitan gestionar los riesgos de seguridad y privacidad de la información en PROMUEVE MÁS durante la vigencia 2026.

OBJETIVOS ESPECÍFICOS

- Identificar y clasificar los riesgos que afectan los sistemas de información y la página web institucional
- Definir acciones de mitigación y protocolos de respuesta ante incidentes.
- Evaluar el nivel de riesgo actual y el impacto de los controles implementados.

- Realizar seguimiento y control a la eficacia del plan de tratamiento de riesgos de seguridad de la información.

CONTEXTO ESTRATÉGICO

El plan se articula con la misión y visión institucional, y contribuye al fortalecimiento de los sistemas de información, la optimización de procesos misionales y administrativos, y la implementación de la Política de Gobierno Digital y de Seguridad Digital.

ARTICULACIÓN CON EL CONTEXTO ESTRATÉGICO	
APORTES AL DIRECCIONAMIENTO ESTRATÉGICO	✓ Fortalecer los Sistemas Información ✓ Fortalecer el uso de las tecnologías de la información ✓ Optimizar los procesos misionales ✓ Mejorar los procesos administrativos
GESTIÓN Y DESEMPEÑO INSTITUCIONAL	✓ Política de Gobierno Digital ✓ Política de Seguridad Digital ✓ Política de transparencia, acceso a la información pública y lucha contra la corrupción

La gestión de los riesgos de seguridad de la información son aquellos procesos que reducen

las pérdidas y brindan protección de la información, permitiendo conocer las debilidades que afectan durante todo el ciclo de vida del servicio.

Se define el Plan de Tratamiento de Riesgos de seguridad y privacidad de la información como el proceso mediante el cual se identifica, comprende,evalúa, y mitiga cualquier tipo de riesgo o amenaza en la información de una determinada organización. Dentro de dicho plan, se contempla la identificación de activos informáticos, las vulnerabilidades y amenazas a los que se encuentran expuestos, así como su probabilidad de ocurrencia y el impacto de estas; lo anterior con el fin de determinar los controles adecuados para aceptar, disminuir, transferir o evitar la ocurrencia del riesgo.

ALCANCE

El Plan de Tratamiento de Riesgos de seguridad y privacidad de la información es de estricta aplicabilidad y cumplimiento por parte de todos los servidores públicos, contratistas y otros que presten sus servicios o tengan algún tipo de relación con la Entidad; dicho tratamiento de riesgo debe involucrar a todos los procesos y actividades desarrolladas por Promueve Mas, en especial aquellos que impactan directamente la consecución de los objetivos misionales.

TÉRMINOS Y DEFINICIONES.

Para efectos del presente Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, se adoptan las siguientes definiciones:

- **Activo de Información**: Elementos físicos o digitales que contienen datos relevantes para la entidad, incluyendo aplicaciones, servicios web, redes, hardware, documentos y recurso humano.
- **Administración de Riesgo**: Conjunto de actividades orientadas a identificar, valorar, evaluar, manejar y monitorear los riesgos que afectan la entidad.
- **Análisis de Riesgo:** Determinación del impacto en función de la consecuencia o efecto y de la probabilidad de ocurrencia del riesgo.
- **Apetito de Riesgo:** Nivel de riesgo que la entidad está dispuesta a aceptar en función de sus objetivos estratégicos y normativos.
- **Capacidad de Riesgo:** Máximo nivel de riesgo que la entidad puede soportar antes de comprometer el logro de sus objetivos.
- **Causas:** Circunstancias, situaciones o agentes generadores del evento de riesgo.
- Causa Inmediata: Condiciones bajo las cuales se presenta el riesgo, sin constituir la causa principal.
- **Causa Raíz**: Razón principal por la cual se puede presentar el riesgo.
- **Confidencialidad:** Propiedad de la información que garantiza que solo sea accesible por personas, procesos o entidades autorizadas.
- **Consecuencia:** Hechos o resultados derivados de la ocurrencia de un riesgo.
- **Control:** Acciones encaminadas a reducir la probabilidad de ocurrencia o el impacto de un riesgo.
- **Disponibilidad:** Condición que asegura que la información esté accesible y utilizable cuando se requiera.
- **Evento:** Situación que afecta el logro de objetivos institucionales, derivada de la materialización de un riesgo.
- **Factores de Riesgo**: Fuentes generadoras de riesgos.

- **Frecuencia:** Periodicidad con que ocurre un evento de riesgo.
- **Gestor del Riesgo:** Funcionario líder de la dependencia que apoya al responsable del riesgo.
- **Identificación del Riesgo:** Descripción de la situación no deseada que puede afectar la entidad.
- **Impacto:** Magnitud de las consecuencias que puede ocasionar la materialización de un riesgo.
- **Integridad:** Propiedad que asegura exactitud y completitud de la información.
- **Mapa de Riesgos:** Herramienta metodológica que permite inventariar riesgos por proceso, describiendo causas, consecuencias y tratamientos.
- **Nivel de Riesgo:** Valor que resulta de combinar la probabilidad de ocurrencia y el impacto de un evento.
- **Plan Anticorrupción y de Atención al Ciudadano:** Estrategia de lucha contra la corrupción que debe ser implementada por todas las entidades públicas.
- **Políticas de Administración del Riesgo:** Criterios que orientan la toma de decisiones para minimizar los riesgos de la entidad.
- **Probabilidad:** Medida que estima la posibilidad de ocurrencia de un evento.
- **Responsable del Riesgo:** Encargado de identificar, valorar y definir el plan de contingencia y monitoreo de riesgos.
- **Riesgo:** Posibilidad de ocurrencia de un evento que afecta el cumplimiento de objetivos institucionales.
- **Riesgo Residual:** Riesgo que permanece después de aplicar controles de mitigación.
- **Riesgo Inherente:** Riesgo puro, sin controles aplicados.
- **Riesgo de Seguridad de la Información:** Posibilidad de que una amenaza explote una vulnerabilidad y cause pérdida o daño en un activo de información.
- **Riesgo de Corrupción:** Posibilidad de que, por acción u omisión, se desvíe la gestión pública hacia un beneficio privado.

- **Tratamiento:** Opciones que determinan las acciones para administrar un riesgo.
- Tratamiento del Riesgo: Valor máximo de desviación admisible respecto al apetito de riesgo definido por la entidad.
- **Valoración:** Grado de exposición al riesgo según probabilidad e impacto, aplicando controles existentes.
- **Vulnerabilidad:** Debilidad de un activo o control que puede ser explotada por una amenaza.

MARCO NORMATIVO

El presente Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información se fundamenta en las siguientes disposiciones legales y normativas vigentes en Colombia, que orientan la gestión de la información, la protección de datos personales y la seguridad digital:

- Ley 44 de 1993: Por la cual se modifica y adiciona la Ley 23 de 1982 y la Ley 29 de 1944 en materia de derechos de autor. Esta norma establece la protección de las obras intelectuales y garantiza que la información generada por la entidad tenga un marco legal de propiedad y uso adecuado.

- Ley 527 de 1999: Define y reglamenta el acceso y uso de los mensajes de datos, el comercio electrónico y las firmas digitales. Además, establece las entidades de certificación y dicta disposiciones que permiten a PROMUEVE MÁS utilizar medios electrónicos con validez jurídica, asegurando la autenticidad y confiabilidad de la información transmitida digitalmente.

- Ley 1273 de 2009: Modifica el Código Penal y crea un nuevo bien jurídico tutelado denominado "protección de la información y de los datos". Esta ley preserva integralmente los sistemas que utilizan las tecnologías de la información y las comunicaciones, estableciendo sanciones frente a delitos informáticos y garantizando la seguridad de los activos digitales de la entidad.

- Ley 1581 de 2012: Dicta disposiciones generales para la protección de datos personales. PROMUEVE MÁS debe cumplir con esta norma para asegurar que la recolección, almacenamiento, uso y circulación de datos personales se realice bajo principios de legalidad, finalidad, libertad, veracidad, transparencia y seguridad.

- Decreto 19 de 2012: Establece normas para suprimir o reformar regulaciones, procedimientos y trámites innecesarios en la Administración Pública. En el contexto de la gestión de riesgos, este decreto promueve la simplificación y eficiencia en los procesos de control y tratamiento de la información.

- Decreto 1377 de 2013: Reglamenta parcialmente la Ley 1581 de 2012 sobre protección de datos personales. Define lineamientos para la autorización del tratamiento de datos y la responsabilidad de las entidades en la protección de la información de los ciudadanos.

- Ley 1712 de 2014: Crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional. Esta norma obliga a PROMUEVE MÁS a garantizar el acceso a la información pública, fortaleciendo la confianza ciudadana y la rendición de cuentas, en equilibrio con la protección de datos sensibles.

- Decreto 1081 de 2015: Expide el Decreto Reglamentario Único del Sector Presidencia de la República. Incluye disposiciones sobre transparencia, acceso a la información y gestión pública, que deben ser

aplicadas en la administración de riesgos de seguridad digital.

- Decreto 1078 de 2015: Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones. Establece los lineamientos generales para la implementación de la política de Gobierno Digital, la gestión de TIC y la seguridad de la información en entidades públicas.

- Decreto 1499 de 2017: Modifica el Decreto 1083 de 2015 en lo relacionado con el Modelo Integrado de Planeación y Gestión (MIPG). Este modelo articula la gestión de riesgos con la planeación institucional, asegurando que los riesgos de seguridad y privacidad sean tratados como parte integral de la gestión pública.

- Decreto 1008 de 2018: Establece los lineamientos generales de la política de Gobierno Digital y subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015. Este decreto refuerza la necesidad de implementar estrategias de seguridad digital y gestión de riesgos en las entidades públicas.

- Guía para la administración del riesgo y diseño de controles en entidades públicas (Función Pública, 2020): Documento técnico que orienta a las entidades en la identificación, valoración y tratamiento de riesgos, incluyendo los relacionados con la seguridad y privacidad de la información. PROMUEVE MÁS adopta esta guía como referencia metodológica para la gestión de riesgos tecnológicos.

DESARROLLO DEL PLAN DE TRATAMIENTO DE RIESGOS Y PRIVACIDAD DE LA INFORMACION

El desarrollo el Plan de Tratamiento de Riesgos de seguridad y privacidad de la información, tiene como propósito es la identificación, estimación y evaluación de los riesgos de Promueve Mas, para definir un plan de tratamiento que se ajuste a los objetivos de cada uno de los procesos. La Gestión de Riesgos de Promueve Mas, incluyendo los Riesgos de Seguridad y Privacidad se lleva a cabo por los Líderes de cada proceso y lo gestionan para el cumplimiento de la misión, visión y objetivos misionales, con el fin de determinar el tratamiento del riesgo aceptable sobre cada uno de los riesgos identificados, teniendo en cuenta el siguiente esquema:

El plan contempla las siguientes fases:

IDENTIFICACION DE RIESGOS

Se realizará un inventario de los activos de información y tecnológicos de la entidad, identificando

las vulnerabilidades y amenazas a las que están expuestos. Ejemplo: pérdida de datos por falta de respaldo en nube, ataques informáticos a la página web, manipulación de sistemas de información.

EVALUACIÓN DE RIESGOS

Cada riesgo será evaluado en función de su **probabilidad de ocurrencia** y **nivel de impacto** sobre los procesos institucionales. Esta evaluación permitirá clasificar los riesgos en zonas (alta, media, baja) y definir prioridades de tratamiento.

TRATAMIENTO DE RIESGOS

Se establecerán acciones específicas para cada riesgo identificado, que pueden incluir:

- **Reducir:** implementación de copias de seguridad en nube, controles de acceso y autenticación segura.
- **Mitigar:** instalación de firewalls, monitoreo continuo de la página web, protocolos de respuesta ante incidentes.
- **Transferir:** contratación de servicios especializados (ej. soporte técnico con Computar, ERP con Solution System).
- **Evitar:** eliminación de prácticas inseguras y fortalecimiento de políticas institucionales.

MONITOREO Y SEGUIMIENTO

El plan será monitoreado de manera **semestral**, verificando la eficacia de los controles implementados y ajustando las acciones según la evolución de los riesgos. Se generarán informes de seguimiento que serán presentados al Comité Institucional de Gestión y Desempeño.

CULTURA DE SEGURIDAD

Se promoverá la sensibilización y capacitación del personal en temas de seguridad digital, uso responsable de la información y cumplimiento de las políticas de privacidad. La cultura de seguridad será un eje transversal para garantizar la sostenibilidad del plan

BENEFICIOS DE LA ADMINISTRACIÓN EN LA GESTIÓN DE RIESGOS

La administración de riesgos de seguridad y privacidad de la información en PROMUEVE

MÁS constituye un proceso integral que involucra a la alta dirección, líderes de procesos y servidores públicos. Su implementación aporta beneficios estratégicos, operativos y culturales que fortalecen la gestión institucional y garantizan la protección de los activos de información.

Entre los principales beneficios se destacan:

- **Apoyo a la toma de decisiones:** La identificación y valoración de riesgos proporciona información confiable que permite a la alta dirección tomar decisiones oportunas y fundamentadas en evidencia.
- **Garantía de la operación normal de la organización:** La gestión de riesgos asegura la continuidad de los procesos misionales y administrativos, minimizando interrupciones derivadas de incidentes tecnológicos o de seguridad.
- **Minimización de la probabilidad e impacto de los riesgos:** La implementación de controles adecuados reduce significativamente la posibilidad de ocurrencia de eventos adversos y mitiga sus consecuencias en caso de materialización.
- **Mejoramiento en la calidad de procesos y servicios:** La administración de riesgos fortalece la eficiencia y eficacia de los procesos institucionales, generando confianza en los grupos de interés y en la ciudadanía.
- **Fortalecimiento de la cultura de control:** La gestión de riesgos fomenta la responsabilidad compartida en la protección de la información, promoviendo prácticas seguras y transparentes en todos los niveles de la entidad.
- **Incremento de la capacidad institucional para alcanzar objetivos:** Al reducir vulnerabilidades y amenazas, la entidad mejora su capacidad de cumplir metas estratégicas y operativas.
- **Disponibilidad de herramientas y controles efectivos:** La administración de riesgos dota a PROMUEVE MÁS de metodologías, protocolos y mecanismos que permiten una gestión más eficaz y eficiente de la seguridad digital.
- **Generación de confianza institucional:** La adecuada gestión de riesgos fortalece la relación entre la entidad y sus grupos de interés, consolidando la transparencia y la

credibilidad de PROMUEVE MÁS.

Promueve Mas, sigue los lineamientos trazados por el Gobierno Nacional en cumplimiento de la Ley de Transparencia y acceso a la información y en la Política de Gobierno Digital, buscando fortalecer la relación Ciudadano - Estado, mejorando la prestación de servicios por parte de las entidades, y generando confianza en las instituciones que conforman la administración pública y el Estado en general, a través del uso y aprovechamiento de las TIC, las cuales se integran al Modelo Integrado de Planeación y Gestión - MIPG y a las políticas de Gestión y Desempeño Institucional.

CLASIFICACIÓN DE LOS RIESGOS SOBRE LOS ACTIVOS DE TECNOLOGIA DE INFORMACIÓN.

Todas las organizaciones deben implementar planes para gestionar los riesgos que afectan a sus sistemas de información, tecnologías de la información y activos informáticos. PROMUEVE MÁS reconoce que los riesgos más comunes provienen de ataques informáticos, fallas en la infraestructura tecnológica y ausencia de políticas robustas de respaldo, lo cual puede comprometer la confidencialidad, integridad y disponibilidad de la información institucional.

La clasificación de riesgos se realiza considerando la probabilidad de ocurrencia y el impacto potencial, lo que permite determinar la zona de riesgo y definir el tratamiento más adecuado. A continuación, se presenta la matriz de riesgos identificados para la vigencia 2026:

REFERENCIA	NOMBRE	CALIFICACION			TRATAMIENTO DEL RIESGO
		PROBABILIDAD INHERENTE	IMPACTO INHERENTE (1-	ZONA DE RIESGO	

Promueve Más S.A.S. – Calle 18 # 7C - 47 – Tel: 3104191960 – operaciones@promuevemas.com

	DEL RIESGO	(1-5)	5)	INHERENTE	
R1	Pérdida, fuga y/o borrado de datos por falta de respaldo en nube	**5**	**4**	**ZONA RIESGO ALTA**	Reducir (implementación de copias en nube y protocolos de recuperación)
R2	Ataques informáticos a aplicativos y página web institucional	**5**	**4**	**ZONA RIESGO ALTA**	Mitigar (firewalls, monitoreo continuo, protocolos de respuesta ante incidentes)
R3	Sistema de información susceptibles de manipulación o adulteración	**5**	**3**	**ZONA RIESGO ALTA**	Reducir (controles de acceso, autenticación segura, auditorías internas)
R4	Interrupción de operaciones por fallas de hardware o servicios tercerizados	**4**	**3**	**Media**	Transferir (contrato con Computar y plan de contingencia)
R5	Riesgos de corrupción en el manejo de información	**3**	**3**	**Media**	Evitar (protocolos de transparencia, auditorías y control interno)

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

A continuación, se presenta el cronograma propuesto para la ejecución de las actividades del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información en PROMUEVE MÁS durante la vigencia 2026:

ACTIVIDADES	META	INDICADOR	RESPONSABLE	ENE				FEB				MAR				ABR				MAY				JUN				JUL				AGO				SEP				OCT				NOV				DIC			
				1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
Actualizar el plan de tratamientos de riesgos de la informacion para la vigencia 2026	Actualizar el plan de tratamiento de riesgos de la informacion para la vigencia 2026	Acto administrativo de aprobacion del plan de seguidad y privacidad de la informacion para la vigencia 2026	DIRECCIÓN ADMINISTRATIVA Y FINANCIERA					P																																								
Definir la matriz de riesgos informaticos y establecer los respectivos controles	Implementacion y seguimiento trimestral del la matiz de riesgo	Nº de seguimientos apartir de la implementación de la matriz de riesgos	DIRECCIÓN ADMINISTRATIVA Y FINANCIERA																								P																						
Monitoreo de ataques cibemeticos a la pagina institucional	Monitoreo Trimestral 2026	Nº de Monitoreos realizados	DIRECCIÓN ADMINISTRATIVA Y FINANCIERA												P												P											P										P
Capacitacion en gestion de riesgos y seguridad digital	Realizar una capacitacion semestral	Nº de capacitaciones realizadas en vigencia 2026	DIRECCIÓN ADMINISTRATIVA Y FINANCIERA																				P																									P
Seguimiento al cumplimiento del plan anual de tratamientos de riesgos de seguridad y privacidad de la informacion	Realizar seguimiento semestral en vigencia 2026	Nº de seguimientos realizados en vigencia 2026	DIRECCIÓN ADMINISTRATIVA Y FINANCIERA																								P																						P

INDICADOR

El cumplimiento del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información será medido mediante el siguiente indicador de gestión:

Fórmula:

Numero de actividades desarrolladas/numero de total de actividades programadas * 100

Periodicidad: Semestral y Trimestral

Este indicador permite evaluar el grado de avance en la ejecución del plan, identificar desviaciones y establecer acciones correctivas oportunas. Su aplicación asegura que la entidad mantenga un control permanente sobre la gestión de riesgos y la efectividad de los controles implementados.

VIGENCIA

El presente **Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información** entra en vigencia a partir de su adopción y publicación por la Dirección Administrativa y Financiera de PROMUEVE MÁS, y tendrá una duración de un (1) año, correspondiente a la vigencia 2026.

La revisión y actualización del plan se realizará de manera anual, o antes si las condiciones

tecnológicas, normativas o institucionales lo requieren, con el fin de asegurar su pertinencia y efectividad.

Manizales, vigencia 2026.

Promueve Más S.A.S. – Calle 18 # 7C - 47 – Tel: 3104191960 – operaciones@promuevemas.com

RESOLUCION No. 018 DE 2026
30 de enero de 2026

"POR MEDIO DE LA CUAL SE ADOPTA EL PLAN DE TRATAMIENTO DE RIESGOS Y PRIVACIDAD DE LA INFORMACIÓN DE PROMUEVE MAS PARA LA VIGENCIA DE 2026"

El Gerente General de PROMUEVE MÁS S.A.S., En ejercicio de las facultades legales y estatutarias, y

CONSIDERANDO

Que la Constitución Política de Colombia, señala en su artículo 2º que: "Son fines esenciales del Estado servir a la comunidad, promover la prosperidad general y garantizar la efectividad de los principios, derechos y deberes consagrados en la Constitución".

Que el inciso segundo del artículo 209 de la Constitución Política, señala que las autoridades administrativas deben coordinar sus actuaciones para el adecuado cumplimiento de los fines del Estado.

Que de conformidad con el artículo 69 de los Estatutos, le corresponde al Gerente de PROMUEVE MÁS S.A.S., dirigir la empresa manteniendo la unidad de interés en torno a la misión, visión y objetivos de acuerdo con una planificación definida; de la misma forma, le implica realizar la gestión necesaria para lograr el desarrollo de la Entidad de acuerdo con los planes y programas establecidos, teniendo en cuenta las características del entorno y las internas de la Empresa.

Que el artículo 1° del Decreto 612 de 2018 consagra: "Artículo 1. Adicionar al Capítulo 3 del Título 22 de la Parte 2 del Libro 2 del Decreto 1083 de 2015, Único Reglamentario del Sector de Función Pública", los siguientes artículos: "2.2.22.3.14. Integración de los planes institucionales y estratégicos al Plan de Acción. Las entidades del Estado, de acuerdo con el ámbito de aplicación del Modelo Integrado de Planeación y Gestión, al Plan de Acción de que trata el artículo 74 de la Ley 1474 de 2011, deberán integrar los planes institucionales y estratégicos

Que mediante Decreto 415 del 7 de marzo de 2016, se adiciono al Decreto 1083 de 2015, todo lo relacionado con la definición de los lineamientos para el fortalecimiento institucional en materia de Tecnologías de la Información y las Comunicaciones.

Que el Decreto 1078 de 2015 contempló en el artículo 2.2.9.1.2.2, los instrumentos para implementar la Estrategia de Gobierno en Línea, dentro de los cuales se exige la elaboración por parte de cada entidad de un Plan de Seguridad y Privacidad de la información.

Que mediante el Plan de Tratamiento de Riesgo de Seguridad y Privacidad de la Información se busca proteger la integridad y garantizar la disponibilidad y confidencialidad de todos los archivos de información de la entidad.

Promueve Más S.A.S. – Calle 18 # 7C - 47 – Tel: 3104191960 – operaciones@promuevemas.com

RESOLUCION No. 018 DE 2026
30 de enero de 2026

"POR MEDIO DE LA CUAL SE ADOPTA EL PLAN DE TRATAMIENTO DE RIESGOS Y PRIVACIDAD DE LA INFORMACIÓN DE PROMUEVE MAS PARA LA VIGENCIA DE 2026"

Que, para dar cumplimiento a las disposiciones legales anteriormente mencionadas, se formuló el plan de Tratamiento de Riesgos y Privacidad de la información para la vigencia 2026.

Que el día 20 enero de 2026 se realizó reunión del Comité de Gestión y Desempeño, donde se aprobaron los diferentes planes según Decreto 612 de 2018, entre ellos el plan de Tratamiento de Riesgos y Privacidad de la información para la vigencia fiscal de 2026.

Que es necesario adoptar el plan de Tratamiento de Riesgos y Privacidad de la información alineado a la Planeación Estratégica de PROMUEVE MAS.

En mérito de lo expuesto,

RESUELVE

ARTICULO PRIMERO. Adoptar el plan de Tratamiento de Riesgos y Privacidad de la información de PROMUEVE MAS para la vigencia 2026, el cual se encuentra establecido en documento anexo, que hace parte integral del presente acto administrativo.

ARTICULO SEGUNDO. La presente resolución rige a partir de la fecha de publicación.

COMUNIQUESE, NOTIFIQUESE, PUBLIQUESE, Y CUMPLASE

Dado en la ciudad de Manizales - Caldas a los treinta (30) días del mes de diciembre del año 2026.

HUGO FERNANDO MONCADA CUERVO
Gerente
PROMUEVE MÁS S.A.S.

Proyectó: Daniela López Betancur
Abogada Contratista

Promueve Más S.A.S. – Calle 18 # 7C - 47 – Tel: 3104191960 – operaciones@promuevemas.com