PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

1. POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La Política de Seguridad y Privacidad de la Información es la declaración general que representa la posición de PROMUEVE MÁS con respecto a la protección de los activos de información (los funcionarios, contratistas, terceros, la información, los procesos, las tecnologías de información incluido el hardware y el software), que soportan los procesos de la Entidad y apoyan la implementación del Sistema de Gestión de Seguridad de la Información, por medio de la generación y publicación de sus políticas, procedimientos e instructivos, así como de la asignación de responsabilidades generales y específicas para la gestión de la seguridad de la información.

PROMUEVE MÁS, para asegurar el direccionamiento estratégico de la Entidad, establece la compatibilidad de la política y de los objetivos de seguridad de la información, estos últimos correspondientes a:

a) Mitigar los riesgos de la entidad.
b) Cumplir con los principios de seguridad de la información.
c) Cumplir con los principios de la función administrativa.
d) Mantener la confianza de los funcionarios, contratistas y terceros.
e) Apoyar la innovación tecnológica.
f) Implementar el sistema de gestión de seguridad de la información.
g) Proteger los activos de información.
h) Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
i) Fortalecer la cultura de seguridad de la información en los funcionarios y clientes externos de PROMUEVE MÁS.
j) Garantizar la continuidad del servicio frente a incidentes.

1.1 Alcance

Esta política aplica a toda la entidad, sus funcionarios, contratistas y terceros de PROMUEVE MÁS y la ciudadanía en general.

1.2 Nivel de cumplimiento

Todas las personas cubiertas por el alcance y aplicabilidad deberán dar cumplimiento a esta política. A continuación, se establecen las políticas que soportan el plan de seguridad y privacidad de la información de PROMUEVE MÁS.

a) PROMUEVE MÁS ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, amparado en lineamientos claros alineados a las necesidades de la entidad, y a los requerimientos regulatorios que le aplican a su naturaleza.

b) Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, contratistas o terceros.

c) PROMUEVE MÁS protege la información generada, procesada o resguardada por los procesos de la entidad y activos de información que hacen parte de los mismos.

d) PROMUEVE MÁS protege la información creada, procesada, transmitida o resguardada por los procesos de la entidad, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.

e) PROMUEVE MÁS protege su información de las amenazas originadas por parte del personal.

f) PROMUEVE MÁS controla la operación de sus procesos de la entidad garantizando la seguridad de los recursos tecnológicos y las redes de datos.

g) PROMUEVE MÁS garantiza a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.

h) PROMUEVE MÁS garantiza la disponibilidad de sus procesos de la entidad y la continuidad de su operación basado en el impacto que pueden generar los eventos.

i) PROMUEVE MÁS garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

El incumplimiento a la política de Seguridad y Privacidad de la Información, traerá consigo, las consecuencias legales que apliquen a la normativa de la Entidad, incluyendo lo establecido en las normas que competen al Gobierno nacional y territorial en cuanto a Seguridad y Privacidad de la Información se refiere.

2. IMPLEMENTACIÓN DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

2.1 Justificación:

PROMUEVE MÁS con el propósito de salvaguardar la información de la entidad en todos sus aspectos, garantizando la seguridad de los datos y el cumplimiento de las normas legales, ha establecido realizar un Plan de Seguridad y Privacidad de la información con el ánimo de que no se presenten pérdidas, robos, accesos no autorizados y duplicación de la misma, igualmente promueve una política de seguridad de la información física y digital de acuerdo a la caracterización de los usuarios tanto internos como externos.

La seguridad de la información se entiende como la preservación de las siguientes características:

a. **Confidencialidad:** se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.
b. **Integridad:** se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.
c. **Disponibilidad:** se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.

Adicionalmente, debe considerarse los conceptos de:

a) Auditabilidad: define que todos los eventos de un sistema deben poder ser registrados para su control posterior.

b) Protección a la duplicación: consiste en asegurar que una transacción sólo se realiza una vez, a menos que se especifique lo contrario. Impedir que se grabe una transacción para luego reproducirla, con el objeto de simular múltiples peticiones del mismo remitente original.

c) No repudio: se refiere a evitar que una entidad que haya enviado o recibido información alegue ante terceros que no la envió o recibió.

d) Legalidad: referido al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeto el Organismo.

e) Confiabilidad de la Información: es decir, que la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.

A los efectos de una correcta interpretación del presente Plan, se realizan las siguientes definiciones:

a) Información: se refiere a toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro.

b) Sistema de Información: se refiere a un conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión

y difusión de información según determinados procedimientos, tanto automatizados como manuales.

c) Tecnología de la Información: se refiere al hardware y software operados la entidad o por un tercero que procese información en su nombre, para llevar a cabo una función propia del Organismo, sin tener en cuenta la tecnología utilizada, ya se trate de computación de datos, telecomunicaciones u otro tipo.

2.2 Objetivo

Definir los mecanismos y todas las medidas necesarias por parte de PROMUEVE MAS, tanto técnica, lógica, física, legal y ambiental para la protección de los activos de información, los recursos y la tecnología de la entidad, con el propósito de evitar accesos no autorizados, divulgación, duplicación, interrupción de sistemas, modificación, destrucción, pérdida, robo, o mal uso, que se pueda producir de forma intencional o accidental, frente a amenazas internas o externas, asegurando el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información.

2.3 Alcance

Este Plan de Seguridad y Privacidad de la Información y su política, son aplicables a todos los funcionarios de PROMUEVE MÁS, a sus recursos, procesos y procedimientos tanto internos como externos, así mismo al personal vinculado a la entidad y terceras partes, que usen activos de información que sean propiedad de la entidad.

2.4 Cumplimiento

El cumplimiento de la Política de Seguridad y Privacidad de la Información es obligatorio. Si los funcionarios de la entidad o terceros violan este plan, PROMUEVE MÁS se reserva el derecho de tomar las medidas correspondientes.

2.5 Comunicación

Mediante socialización a todos los funcionarios de Promueve+ se dará a conocer el contenido del documento de las políticas de seguridad, así mismo se deberá informar a los contratistas y/o terceros en el momento que se requiera con el propósito de realizar los ajustes y la retroalimentación necesaria para dar cumplimiento efectivo al plan.

3. DESCRIPCIÓN DE LAS POLÍTICAS

Los usuarios deben acatar los lineamientos guía de clasificación de la información para el acceso, divulgación, almacenamiento, copia, transmisión, etiquetado y eliminación de la información contenida en los recursos tecnológicos, así como de la información física de la

entidad.

La información física y digital de PROMUEVE MAS debe tener un periodo de almacenamiento que puede ser dictaminado por requerimientos legales o misionales; este período debe ser indicado en las tablas de retención documental y cuando se cumpla el periodo de conservación, se le debe dar el tratamiento de acuerdo a la disposición final definida por la entidad.

Los usuarios deben tener en cuenta estas consideraciones cuando impriman, escaneen, saquen copias y envíen faxes: verificar las áreas adyacentes a impresoras, escáneres, fotocopiadoras y máquinas de fax para asegurarse que no quedaron documentos relacionados o adicionales; asimismo, recoger de las impresoras, escáneres, fotocopiadoras y máquinas de fax, inmediatamente los documentos confidenciales para evitar su divulgación no autorizada o mal intencionada.

El personal provisto por terceras partes debe asegurarse que, en el momento de ausentarse de su puesto de trabajo, sus escritorios se encuentren libres de documentos y medios de almacenamiento, utilizados para el desempeño de sus labores; estos deben contar con las protecciones de seguridad necesarias de acuerdo con su nivel de clasificación.

La información que se encuentra en documentos físicos debe ser protegida, a través de controles de acceso físico y las condiciones adecuadas de almacenamiento y resguardo.

Los equipos de cómputo de usuario final que se conecten o deseen conectarse a las redes de datos de PROMUEVE MAS deben cumplir con todos los requisitos o controles para autenticarse en ellas y únicamente podrán realizar las tareas para las que fueron autorizados.

PROMUEVE MAS velará porque los funcionarios y el personal provisto por terceras partes tengan acceso únicamente a la información necesaria para el desarrollo de sus labores y porque la asignación de los derechos de acceso esté regulada por normas establecidas para tal fin.

Todas las áreas destinadas al procesamiento o almacenamiento de información sensible, así como aquellas en las que se encuentren los equipos y demás infraestructura de soporte a los sistemas de información y comunicaciones, se considera áreas de acceso restringido.

4. PRIVACIDAD Y CONFIDENCIALIDAD

Las Unidades de Gestión que procesan datos personales de beneficiarios, funcionarios, proveedores u otras terceras partes deben obtener la autorización para el tratamiento de estos datos con el fin de recolectar, transferir, almacenar, usar, circular, suprimir, compartir, actualizar y transmitir dichos datos personales en el desarrollo de las actividades de la entidad.

Las Unidades de Gestión que procesan datos personales de beneficiarios, funcionarios, proveedores u otras terceras partes deben asegurar que solo aquellas personas que tengan una necesidad laboral legítima puedan tener acceso a dichos datos.

Las Unidades de Gestión que procesan datos personales de beneficiarios, funcionarios, proveedores u otras terceras partes deben establecer condiciones contractuales y de seguridad a las entidades vinculadas o aliadas delegadas para el tratamiento de dichos datos personales.

Las Unidades de Gestión que procesan datos personales de beneficiarios, funcionarios, proveedores u otras terceras partes deben acoger las directrices técnicas y procedimientos establecidos para el intercambio de estos datos con los terceros delegados para el tratamiento de dichos datos personales.

Copias de Seguridad

Toda información que pertenezca a la matriz de activos de información institucional o que sea de interés para un proceso operativo o de misión crítica debe ser respaldada por copias de seguridad.

Dicho procedimiento debe incluir las actividades de almacenamiento de las copias en sitios seguros.

La creación de copias de seguridad de archivos usados, custodiados o producidos por usuarios individuales es responsabilidad exclusiva de dichos usuarios.