COMIPOL
COOPERATIVA MULTIACTIVA, MILITAR Y POLICIAL
Honestidad - Lealtad - Dignidad

COOPERATIVA MULTIACTIVA MILITAR Y POLICIAL COMIPOL
NIT. 900052579-1

La **COOPERATIVA MULTIACTIVA MILITAR Y POLICIAL COMIPOL**, presenta su **POLÍTICA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI)** en virtud de lo consagrado en la Ley 1266 de 2008, Ley 1581 de 2012 y su Decreto reglamentario 1377 de 2013, aplicable a todo dato personal que haya sido suministrados o que se suministre a **COMIPOL**, y tiene como objetivo principal dar a conocer a sus Asociados, clientes, usuarios, empleados, proveedores, contratistas y público en general, la regulación interna adoptada por **COMIPOL** sobre esta materia.

1. INTRODUCCIÓN

COMIPOL, determina la importancia de la Política de Gestión de la Información, la cual permite el desarrollo continuo de la misión y el cumplimiento del objetivo de la misma, implementando reglas que permitan proteger los tres pilares importantes como son: la confidencialidad, integridad y disponibilidad en el ciclo de vida de la información.

Las políticas que integran el Sistema de Gestión de Seguridad de la Información SGSI, las cuales deben ser adoptadas por los asociados, funcionarios, contratistas, visitantes y terceros que presten sus servicios o tengan algún tipo de relación con la Cooperativa Multiactiva Militar y Policial Comipol; estas se encuentran enfocadas al cumplimiento de la normatividad legal Colombiana vigente y a las buenas prácticas de seguridad de la información, basadas en el modelo de seguridad y privacidad de la información de la estrategia Gobierno en Línea (GEL) del Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia.

El Modelo de Seguridad y Privacidad será actualizado periódicamente para estar acorde con las buenas prácticas de seguridad, así mismo recoge además de los cambios técnicos de la norma, legislación de Protección de Datos Personales, Transparencia y Acceso a la Información Pública, entre otras, las cuales se deben tener en cuenta para la gestión de la información.

2. OBJETIVO

Establecer las políticas que regulan la seguridad de la información en la Cooperativa Multiactiva Militar y Policial Comipol, que deben conocer, acatar y cumplir todos los asociados, funcionarios, contratistas, visitantes y terceros que presten sus servicios o tengan algún tipo de relación con COMIPOL, bajo la dirección y liderazgo de la Dirección Administrativa de la cooperativa.

3. ALCANCE

Las políticas de seguridad y privacidad de la Información son aplicables en todos los procesos y aspectos administrativos y de control que deben ser cumplidos por asociados, funcionarios, contratistas y terceros que presten sus servicios o tengan algún tipo de relación con COMIPOL, para el cumplimiento de sus funciones y para obtener un adecuado nivel de protección de la seguridad de la información, participando en la toma de medidas preventivas y correctivas, para el logro del objetivo y finalidad de las políticas.

Los usuarios tienen la obligación de dar cumplimiento a las políticas emitidas y aprobadas por la Gerencia y Auditoria del (PGSI) de la Cooperativa.

4. APLICABILIDAD

Las políticas de Seguridad y Privacidad de la información, contenidas en el Sistema de Gestión de Seguridad de la Información – SGSI, son de obligatorio cumplimiento y aplican a los asociados, directivos, funcionarios, contratistas, terceros y en general a todos los usuarios de la información que permitan el cumplimiento de los propósitos generales de **COMIPOL.**

5. TERMINOS Y DEFINICIONES

- **Aplicaciones**: Es todo el software que se utiliza para la gestión de la información. Ejemplo: SICOOPWEB.

Es un software completo de exportación de datos de los sistemas de información producidos por JORJWEB LTDA. a internet, tales como: SICOOP++, TRANSPSOFT++, SICOM++, SIEP++, Y SIEP++.; donde los usuarios pueden conocer estados de cuentas y saldos de aportes, créditos, ahorros, Intereses y valor de cuotas de los asociados, empleados y proveedores.

- **Acceso a la Información Pública:** Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4).

- **Alerta**: Una notificación formal de que se ha producido un incidente relacionado con la seguridad de la información.

- **Almacenamiento en servidor:** Equipo de Cómputo, destinado para

almacenamiento de la toda la información, mediante enlaces de red compartida, con todos los equipos de propiedad de la entidad.

- **Amenaza:** causa potencial de un incidente no deseado, el cual, de no ser detectado a tiempo, puede causar daño al sistema operativo de la entidad.

- **Auditor**: Persona encargada de verificar, la calidad e integridad del trabajo que se ha realizado en un área particular.

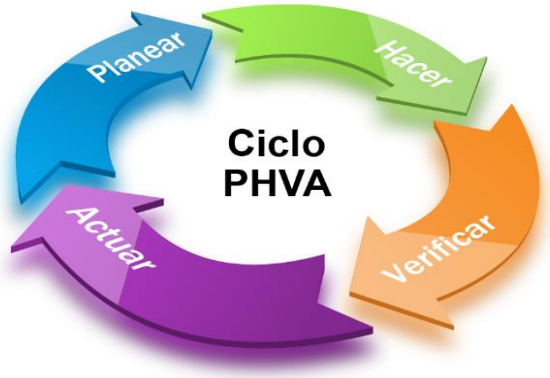
- **Auditoría**: Proceso planificado y sistemático en el cual un auditor obtiene evidencias objetivas que le permitan emitir un juicio informado sobre el estado y efectividad del SGSI de una organización.

- **Autenticación**: Proceso que tiene por objetivo asegurar la identificación de una persona o sistema.

- **Bases de Datos Personales:** Conjunto organizado de datos personales que es objeto de Tratamiento (Ley 1581 de 2012, art 3).

- **Ciclo PHVA:** Herramienta de mejora continua, utilizada por Comipol, en la implementación de sistemas de gestión, basada en 4 pasos: Planear, Hacer, Verificar y Actuar.

Ciclo **PHVA del SGSI**: Planeación del Sistema de Gestión (Planear)



PLANEAR

1)Definir el alcance del SGSI

2) Definir la política de seguridad de la información para la entidad

3) Realizar el análisis de riesgos

4) Seleccionar los controles a implementar

5) Definir el plan de tratamiento del riesgo

6) Ejecutar la accion de aplicabilidad

HACER

1) Ejecutar el plan de tratamiento del riesgo

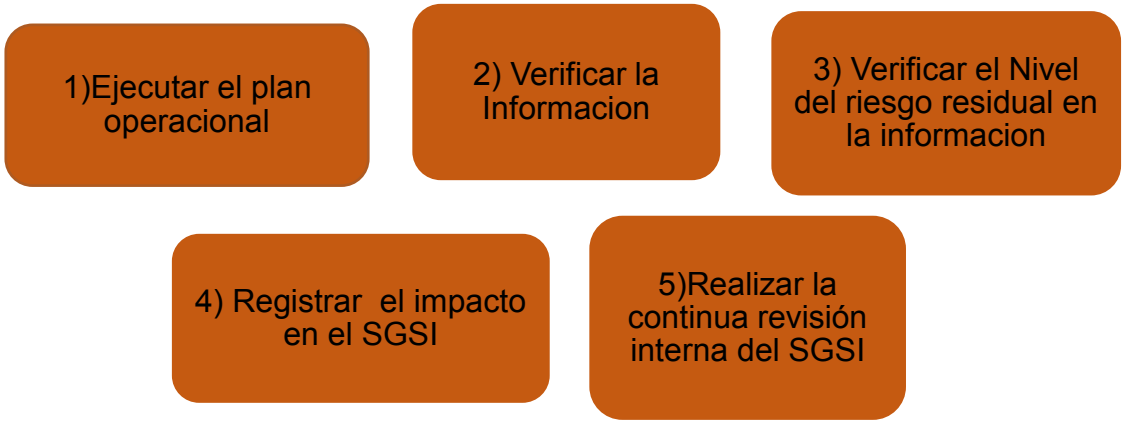
2) Documentar los procesos

3) Implementar las políticas

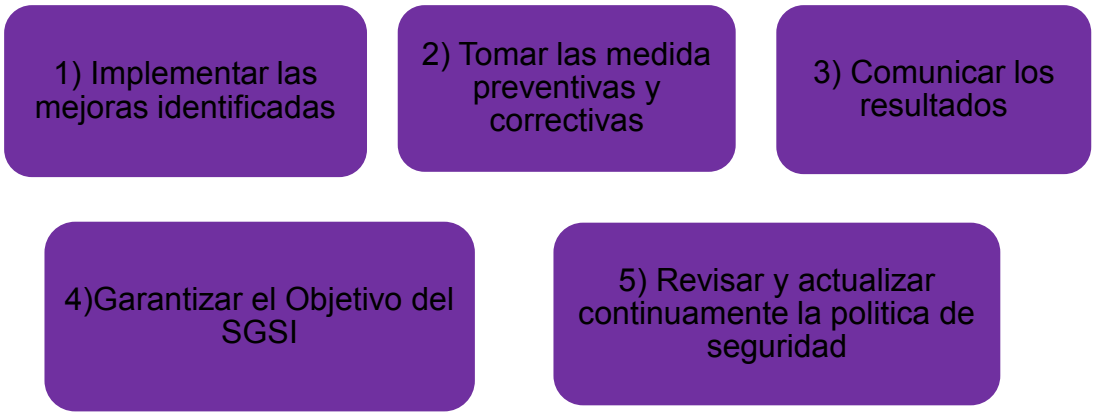
4) Gestionar la operación y los recursos

5)Implementar las respuestas a los posibles incidentes

VERIFICAR



ACTUAR



- **Ciberespacio**: Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).

- **Control:** Las políticas, los procedimientos, las prácticas y las estructuras organizativas implementadas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido.

- **Confiabilidad:** La integridad de la información dependerá de los hardware y software, utilizados para el almacenamiento y procesamiento de la información.
- **Confidencialidad:** Acceso a la información por parte únicamente de quienes estén autorizados, la cual define que la información no está disponible ni deberá ser revelada a individuos, entidades, o procesos no autorizados.

- **Datos Abiertos:** Todos aquellos datos, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos (Ley 1712 de 2014, art 6).

- **Datos Personales:** son cualquier información relativa a una persona física viva identificada o identificable. Las distintas informaciones, que recopiladas pueden llevar a la identificación de una determinada persona, también constituyen datos de carácter personal.

- **Datos Personales Públicos:** Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público.

  Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva. (Decreto 1377 de 2013, art 3).

- **Datos Personales Privados:** Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular. (Ley 1581 de 2012, art 3 literal h).

- **Datos Personales Mixtos:** Para efectos de esta guía es la información que contiene datos personales públicos junto con datos privados o sensibles.

- **Datos Personales Sensibles:** Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a

sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos. (Decreto 1377 de 2013, art 3).

- **Declaración de aplicabilidad:** Documento que enumera los controles aplicados por el SGSI de COMIPOL, tras el resultado de los procesos de evaluación y tratamiento de riesgos.

- **Desastre:** Cualquier evento accidental, natural o malintencionado que interrumpe las operaciones o servicios habituales de una organización durante el tiempo suficiente como para verse afectada de manera significativa.

- **Derecho a la Intimidad:** Derecho fundamental cuyo núcleo esencial lo constituye la existencia que le permite a dicho individuo el pleno desarrollo de su vida personal, espiritual y cultural (Constitución Política de Colombia).

- **Evaluación de riesgos** es un proceso en el cual la entidad debe identificar los riesgos de seguridad de su información y determinar la probabilidad de ocurrencia y su impacto (ISO27000)

- **Gestión de claves:** La Cooperativa **COMIPOL** tiene definidos los lineamientos mínimos en cuanto a calidad que deben tener las contraseñas para ser utilizadas como mecanismo de autenticación en los accesos a la red, aplicaciones y/o sistemas de información de la entidad y son de pleno conocimiento de sus funcionarios, administradores y contratistas y cumplen con los parámetros mínimos para que una contraseña sea considera como fuerte, gestión de cambio de contraseña, así mismo determinan los accesos a la red, las aplicaciones y sistemas de información que requirieren los usuarios para el acceso a la información de forma segura.

- **Gestión de riesgos:** Proceso de identificación, control y minimización o eliminación, de los riesgos que afecten a la información de la entidad.

- **Hardware**: Son todos aquellos Equipos electrónicos donde se procesa la información. Ejemplo: Equipos de cómputo, Discos duros externos.

- **Información - Datos**: Son todos aquellos elementos básicos de la información (en cualquier formato) que se generan, recogen, gestionan, transmiten y destruyen en COMIPOL, siendo requeridos para el cumplimiento de los objetivos.

- **Instalaciones**: Son todos los lugares en los que se alojan los sistemas de información, Infraestructura física que soporta el funcionamiento de la entidad cubriendo los aspectos relacionados con documentos, títulos valor, muebles, equipos y demás elementos de propiedad de la cooperativa.

- **Personal**: Es todo el personal vinculado a la Cooperativa, los asociados, proveedores, usuarios, administradores y en general, todos aquellos que tengan acceso de una manera u otra a los activos de información de COMIPOL.

- **Redes de Comunicaciones**: Los dispositivos y su interacción que habilitan el servicio de comunicaciones de red en la entidad.

- **Servicios**: Son tanto los servicios internos, aquellos que una parte de la organización suministra a otra, como los externos, aquellos que la organización suministra a clientes, usuarios y proveedores.

- **Software**: Las aplicaciones y sistemas de información que atienden los procesos informáticos de la entidad.

- **Tecnología**: Son todos los equipos utilizados para desarrollar y generar la información. Ejemplo: equipo de cómputo, teléfonos, impresoras.

6. POLITICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La Política de Gestión de Seguridad y Privacidad de la Información es la declaración general que representa la posición de la administración para asegurar la dirección estratégica de la entidad, establece la compatibilidad de la política de seguridad de la información y los objetivos de seguridad de la información, estos últimos correspondientes a:

- Cumplir con los principios de la función administrativa.
- Minimizar el riesgo de los procesos misionales de la entidad.
- Cumplir con los principios de seguridad de la información.
- Mantener la confianza de los asociados, administradores, funcionarios, contratistas, terceros y público en general.
- Apoyar la innovación tecnológica. Evitar la obsolescencia.
- Implementar el sistema de gestión de seguridad de la información.
- Proteger los activos de información.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad

de la información.
- Fortalecer la cultura de seguridad de la información.
- Garantizar la continuidad del negocio frente a incidentes.

7. PRINCIPIOS DE SEGURIDAD QUE SOPORTAN EL SGSI DE COMIPOL

Comipol define, implementa, opera y mejorara de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos específicos, de acuerdo a las necesidades de la cooperativa y a los requerimientos regulatorios que le aplican a su naturaleza.

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

COMIPOL protegerá la información generada, procesada o resguardada por los procesos de negocio y activos de información que hacen parte de los mismos.

COMIPOL protegerá la información creada, procesada, transmitida o resguardada por sus procesos de negocio, 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.

COMIPOL protegerá su información de las amenazas originadas por parte del personal.

COMIPOL protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.

COMIPOL controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.

COMIPOL implementará control de acceso a la información, sistemas y recursos de red.

COMIPOL garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.

COMIPOL garantizará 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.

COMIPOL garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

El incumplimiento a la Política de Gestión de Seguridad 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.

8. POLÍTICA DE SEGURIDAD DEL AREA DE RECURSOS HUMANOS

INTEGRIDAD La política de integridad es conocida y aceptada por todos los funcionarios y contratistas que hacen parte de la cooperativa Comipol, la cual se refiere al manejo íntegro e integral de la información tanto interna como externa, conocida o administradas por los mismos.

De esta manera, toda información verbal, física y electrónica, es adoptada, procesada y entregada o transmitida integralmente, coherentemente, exclusivamente a las personas correspondientes y a través de los medios correspondientes, sin modificaciones ni alteraciones.

En proceso de vinculación contractual, el Compromiso de administración y manejo integro e integral de la información interna y externa hace parte de las cláusulas del respectivo contrato laboral, bajo la denominación de **Acuerdo De Confidencialidad** de la información y establece la vigencia del mismo acorde al tipo de vinculación del personal al cual aplica el cumplimiento.

9. POLÍTICA DE MANEJO, DISPOSICIÓN DE INFORMACIÓN, MEDIOS Y EQUIPOS

Los medios y equipos donde se almacena, procesan o comunica la información, deben mantenerse con las medidas de protección físicas y lógicas, que permitan su monitoreo y correcto estado de funcionamiento, para ello se debe realizar los mantenimientos preventivos y correctivos que se requieran de manera periódica.

El servicio de acceso a Internet, Intranet, sistemas de información, medio de almacenamiento, aplicaciones (Software), cuentas de red, navegadores y equipos de cómputo son propiedad de la cooperativa y deben ser usados únicamente para el cumplimiento de la misión de la entidad.

Una vez se termina un contrato laboral, de acuerdo a lo definido por la administración, se realiza una copia de seguridad de la información que se ubica en un disco extraíble de propiedad de la entidad y posteriormente se realiza el borrado de la información del equipo de cómputo correspondiente.

9.1. Copia de Respaldo

Comipol, proporciona medios de respaldo adecuados para asegurar que toda la información esencial y el software, se pueda recuperar después de una falla, garantizando que la información y la infraestructura de software crítica de la entidad, sean respaldadas y puedan ser restauradas en caso de una falla y/o desastre.

9.2. Backup: Ha sido el medio tradicional utilizado para las copias de respaldo y actualmente es la tecnología más utilizada para este propósito.

10 REGISTRO DE LA TRANSFERENCIA DE DATOS

Las transferencias de información realizadas en COMIPOL, deben ser registradas en los servidores correspondientes almacenando los siguientes datos referentes al evento:

- Fecha
- Hora
- Dirección IP origen
- Dirección IP Destino
- Usuario que envía
- Transmisión exitosa / fallida
- Tamaño de los datos transmitidos
- Algoritmo de cifrado o firmado

11. POLÍTICA DE USO DE CORREO ELECTRÓNICO

- La adecuada protección de la información de Comipol, en el uso del servicio de correo electrónico por parte de los usuarios autorizados.

- La cuenta de correo electrónico es personal e intransferible, no existe justificación para que una cuenta de correo sea usada por otra persona ya que esto se cataloga como una suplantación.

- Ningún funcionario está autorizado para utilizar una cuenta diferente a la asignada.

- La cuenta de correo asignado es para uso exclusivo de temas laborales concernientes al objetivo de la entidad.

- La cuenta de correo de una persona desvinculada de la entidad, podrá ser consultada por un funcionario formalmente autorizado por la gerencia, pero no podrá enviar correos desde la misma.

- Se deben borrar sin abrir los correos de los cuales no se tenga certeza del origen y propósito.

- Se deben clasificar como spam las cuentas de correo que lo ameriten.

- No utilizar el correo asignado por Comipol, para propósitos diferentes al laboral.

- La información clasificada como confidencial solo puede ser enviada en forma cifrada.

12. POLÍTICA DE REVISIONES DE SEGURIDAD DE LA INFORMACIÓN.

La cooperativa Comipol, se compromete a garantizar el funcionamiento del sistema de gestión de seguridad de la información de acuerdo a las políticas y procedimientos implementados, con el firme propósito de mantener protegida la entidad y sus asociados.

La administración de la cooperativa, se compromete a verificar y supervisar el cumplimiento de las políticas de seguridad de la información.

13. POLÍTICA DE SEGURIDAD DE PROVEEDORES.

Las empresas contratadas para los diferentes servicios requeridos por Comipol, mediante firma de contratos o convenios, deberán comprometerse a cumplir con los acuerdos de confidencialidad y a mantener resguardada la seguridad de la información y los servicios de procesamiento de información de la cooperativa, a los cuales tienen acceso.

13.1. Protección de Datos Personales con Proveedores

Se debe incluir dentro del Contrato una cláusula que haga referencia al cumplimiento de la Política de protección de Datos Personales de Comipol y el compromiso de la empresa prestadora del servicio de no divulgar ni compartir información de la empresa con terceros ni personas no autorizadas, este documento debe ser entregado al

proveedor para su entendimiento y aceptación.

14. POLÍTICA DE DATOS PERSONALES

Legalidad en materia de tratamiento de datos: COMIPOL adoptara de forma permanente el tratamiento a que se refiere la ley 1581 de 2012 y las disposiciones que la desarrollen.

• **COMIPOL**, protegerá la información generada, procesada o resguardada por los procesos de negocio, su infraestructura tecnológica y activos del riesgo que se genera de los accesos otorgados a terceros (ej.: proveedores o asociados).

15. DERECHOS DEL TITULAR DE LA INFORMACIÓN PERSONAL

EL TITULAR en calidad de propietario de la Información Personal suministrada a la cooperativa Comipol, tendrá los siguientes derechos:

- Conocer, actualizar y rectificar su Información Personal gratuitamente;
- Solicitar prueba de la existencia de la autorización otorgada a **COMIPOL.**
- Ser informado respecto al uso que se le ha dado a su Información Personal.
- Revocar la autorización y solicitar la supresión del dato cuando no se haga un uso conforme a los usos y finalidades autorizados.
- Presentar consultas y reclamos referentes a la Información Personal.

16. CONECTIVIDAD Y REDES SOCIALES:

Sin perjuicio del estricto cumplimiento de la **Cooperativa,** con las normas sobre seguridad de la información que, como entidad vigilada por la Superintendencia de la Economía Solidaria, se deja expresa constancia que **COMIPOL** no posee, vínculos, enlaces, fan page, cuentas con diferentes redes sociales, incluyendo, pero sin limitarse, Facebook, Twitter, Instagram, etc. En este orden de ideas, si alguna persona o entidad hace contacto por estos medios con **COMIPOL**, no será veraz y deberá abstenerse de brindar información personal.

En consecuencia, no será responsabilidad de **COMIPOL** la recolección, transmisión y, en general, el tratamiento que le sea proporcionado a la Información Personal de la persona o entidad en los eventos descritos en este numeral.

En esta medida, la persona o entidad que ingrese simultáneamente a la página web de **COMIPOL**, se compromete expresamente a conocer y a someterse a sus políticas de privacidad.

17. CUMPLIMIENTO

La Cooperativa Multiactiva Militar y Policial - COMIPOL, declara que todos sus funcionarios y contratistas son responsables de ejecutar la presente política en el desarrollo de sus actividades y están altamente comprometidos a realizar las gestiones tendientes a su puesta en marcha.

En caso de violación de las políticas de seguridad y privacidad, ya sea de forma intencional o por negligencia, la Cooperativa COMIPOL, tomará las acciones disciplinarias y legales correspondientes.

Nivel de cumplimiento

Todas las personas cubiertas por el alcance y aplicabilidad deberán dar cumplimiento un 100% de la política.

18. PROCEDIMIENTO DE CONSULTA, RECTIFICACIÓN Y RECLAMOS:

Las consultas y solicitudes deben ser dirigidas por el solicitante a través de cualquier medio y a cualquiera de los contactos que se señalan más adelante, y serán atendidas en un término máximo de diez (10) días hábiles, contados a partir de la fecha de recibo de las mismas por cualquier medio de comunicación.

En caso de que no sea posible resolver la solicitud dentro de este término, el solicitante será informado de dicha situación en la dirección de notificación que haya incluido en la respectiva consulta, y el término de respuesta se podrá extender hasta por cinco (5) días hábiles adicionales.

Rectificaciones y Reclamos: Cuando solicitante en su calidad o sus causahabientes consideren que su información debe ser corregida, actualizada o suprimida, o cuando adviertan un presunto incumplimiento por parte de COMIPOL de sus deberes en materia de Protección de Datos Personales o seguridad de la información, contenidos en la legislación aplicable y en la presente política, podrán presentar un reclamo de la siguiente manera:

Presentar solicitud escrita frente al requerimiento específico;

Si el reclamo resulta incompleto, COMIPOL requerirá solicitante dentro de los cinco (5) días siguientes a la recepción de la solicitud para que complete y subsane su petición.

Si transcurren diez (10) días, desde la fecha del requerimiento sin que solicitante haya dado respuesta o subsanada la solicitud, se entenderá desistida la pretensión.

19. **MODIFICACIONES A LA POLÍTICA**

COMIPOL se encuentra plenamente facultada para modificar la presente **POLÍTICA DE SEGURIDAD DE LA INFORMACION**. Cualquier cambio será debidamente publicado en la página web de la cooperativa COMIPOL **www.comipol.com**

El ingreso y registro en la Página Web de COMIPOL, será entendido como manifestación expresa de la aceptación de la presente Política de Privacidad y de otorgar la correspondiente autorización para que COMIPOL obtenga y de tratamiento a los datos personales de los visitantes de la misma.

20. ALCANCE/APLICABILIDAD

La presente, **POLÍTICA DE GESTION DE SEGURIDAD DE LA INFORMACION**, aplica a toda la entidad, sus Asociados, administradores, funcionarios, contratistas, terceros y la ciudadanía en general.

21. CONTACTOS

En el evento de alguna duda o inquietud sobre la presente **POLÍTICA DE GESTION DE SEGURIDAD DE LA INFORMACION** o el tratamiento y uso de la Información Personal favor dirigir sus consultas, peticiones, quejas o reclamos así:

- Mediante correo electrónico, al e-mail: **recepcion@comipol.com**
- Solicitud por escrito, en la dirección: Calle 12 No 7-32 Oficina 802, de Bogotá D.C.,
- Llamando a nuestras líneas de contacto al teléfono (1)7042444, Cel.3102753917-3132857731.

22. VIGENCIA:

La presente versión de la **POLÍTICA DE GESTION DE SEGURIDAD DE LA INFORMACION** de la Cooperativa Comipol, se encuentra vigente a partir del día 15 de marzo del año 2022, y podrá ser consultada en la página de internet www.comipol.com.

23. MARCO LEGAL

- **Ley 1581 de 2012**, "Protección de Datos personales".
- **Ley 1266 de 2008**, por la cual se dictan disposiciones generales del Habeas Data y se regula el manejo de la información contenida en base de datos personales.
- **Ley 1273 de 2009**, por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado 'de la protección de la información y de los datos'- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.
- **Decreto 1377 de 2013**, Por el cual se reglamenta parcialmente la Ley 1581 de 2012.
- **Decreto 2573 De 2014**, Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones.
- **Ley 1712 de 2014**, Por medio del cual se crea la ley de transparencia y del derecho de acceso a la información pública nacional."
- **Norma Técnica ISO 27001** La cual define buenas prácticas que se encuentran asociadas a la seguridad de la información.

Elaboro: PAOLA ARIAS DIAZ

Aprobó: CARLOS SANCHEZ MONTENEGRO
Representante Legal Comipol