MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN "MIPG"

POLITICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

IPIALES, ENERO DE 2026

ALCALDÍA MUNICIPAL DE Ipiales

Dirección: Carrera 5 No.12-04 Ipiales, Nariño, Colombia
Teléfono: (+57) 6027732333, Celular 3218598556
Email: unimos@unimosesp.com.co
Página web: www.unimosesp.com.co

POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN		
ELABORÓ	**REVISÓ**	**APROBÓ**
Luis Carlos Salazar Araujo	Carmenza M. Belalcázar R.	Comité Institucional de Gestión y Desempeño
Jefe Oficina de Operaciones Digitales	Jefe Oficina Asesora de Planeación	UNIMOS S.A. E.S.P.
FECHA	**FECHA**	**FECHA**
30/01/2026	30/01/2026	12/02/2026

REGISTRO DE MODIFICACIONES
Reestructuración de Políticas de acuerdo a los lineamientos y Gestión de el Plan de Gobierno Municipal “Ipiales, gobierno del pueblo”.
Actualización de la Política vigencia 2026.

1 TABLA DE CONTENIDO

CONTENIDO

1. INTRODUCCIÓN

La Empresa Municipal de Telecomunicaciones de Ipiales UNIMOS S.A. E.S.P. con el fin de lograr el cumplimiento normativo en los temas relacionados con la administración y protección de la información en cada una de sus dimensiones como la disponibilidad, integridad y confidencialidad, ha elaborado una serie de acciones para la implantación de un Subsistema de Gestión de Seguridad de la Información (SGSI) alineado con los objetivos estratégicos de la Entidad.

En el marco del Modelo Integrado de Planeación y Gestión (MIPG), UNIMOS S.A. E.S.P. reconoce que la información es uno de sus activos más valiosos. Para la vigencia 2025, esta política busca consolidar la protección de la infraestructura que soporta los servicios de telecomunicaciones en Ipiales, garantizando que el tratamiento de datos se realice bajo estándares de seguridad digital que generen confianza en la ciudadanía y den cumplimiento a los requerimientos del Departamento Administrativo de la Función Pública.

2. DEFINICIONES

- **MSPI:** Modelo de Seguridad y Privacidad de la Información.
- **S.I.G:** Sistema de Información Geográfica.
- **SGSI:** Sistema de Gestión de Seguridad de la Información.
- **Sistema de información:** Cualquier equipo de cómputo o telecomunicaciones, sistema o subsistema interconectado o no conectado usado para la adquisición, almacenamiento, manipulación, gestión, movimiento, control, despliegue, conmutación, intercambio, transmisión o recepción de voz, datos, vídeo en formas análogas o digitales, así como el software, firmware o hardware que forme parte del sistema.
- **Integridad:** Hace referencia a la fidelidad de la información o recursos, y normalmente se expresa en lo referente a prevenir el cambio impropio o desautorizado.
- **Confidencialidad:** Es la necesidad de ocultar o mantener secreto sobre determinada información o recursos.
- **Disponibilidad:** Hace referencia a que la información debe permanecer accesible a elementos autorizados.
- **Código malicioso:** un gusano informático usa archivos compartidos para contaminar cientos de estaciones dentro de la entidad. La entidad recibe un reporte del vendedor de sus antivirus en donde alerta de un virus que se dispersa a gran velocidad mediante correo electrónico por Internet. El virus aprovecha una vulnerabilidad presente en los servidores de la entidad, basado en la experiencia de la entidad en otros incidentes se estima que el virus podría afectar a los equipos en un lapso de tres horas
- **Acceso no autorizado:** un atacante utiliza una herramienta de explotación de vulnerabilidades para tener acceso al archivo de password de usuarios. Un perpetrador obtiene acceso no autorizado a nivel de administrador a un servidor y a la información confidencial que

contiene y luego intimida a la víctima amenazando la de divulgar a la prensa a la información si no realiza el pago de un dinero.

- **Uso inapropiado:** un usuario entrega copias de software de la entidad a personas no autorizadas. Una persona amenaza a otra vía correo electrónico.
- **Seguridad de la Información:** Preservación de la confidencialidad, disponibilidad e integridad de la información (ISO/IEC 27000) independiente de su medio de conservación, transmisión o formato.

3. MARCO LEGAL

NORMA	DESCRIPCIÓN
Ley 527 de 1999	Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.
Ley 679 de 2011	Por medio de la cual se expide un estatuto para prevenir y contrarrestar la explotación,la pornografía y el turismo sexual con menores, en desarrollo del artículo 44 de la Constitución
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.
Ley 1266 de 2008	Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejode la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.
Decreto 886 de 2014	Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012, relativo al Registro Nacional de Bases de Datos.
Ley 1581 de 2012	Por la cual se dictan disposiciones generales para la protección de datos personales.
Ley 1221 de 2007,Ley 2088 de 2021 , Ley 2121 de 202	Por la cual se establecen normas para promover y regular el Teletrabajo y se dictan otras disposiciones, Trabajo Remoto, Trabajo en casa
Ley 1341 de 2009	Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones.
Ley 1403 de 2010	Por la cual se adiciona la Ley 23 de 1982, sobre Derechos de Autor, se establece una remuneración por comunicación pública a los artistas intérpretes o ejecutantes de obras y grabaciones audiovisuales o "Ley Fanny Mikey"
Ley 1712 de 2014	Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.
Decreto 1078 de 2015	Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
Decreto 105 de 2015	Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.
Decreto 415 de 2016	Por el cual se adiciona el Decreto Único Reglamentario del sector de la Función Pública, Decreto Numero 1083 de 2015, en lo relacionado con la definición de los lineamientos para el fortalecimiento institucional en materia de tecnologías de la información y las comunicaciones.

Decreto 728 de 2017	Por el cual se adiciona el capítulo 2 al título 9 de la parte 2 del libro 2 del Decreto Único Reglamentario del sector TIC, Decreto 1078 de 2015, para fortalecer el modelo de Gobierno Digital en las entidades del orden nacional del Estado colombiano, a través de la implementación de zonas de acceso público a Internet inalámbrico.
Resolución 793 de 2019 de la ANE	Por la cual se adopta la Política del Sistema de Gestión de Seguridad y Privacidad de la información, Seguridad Digital y se definen lineamientos frente al uso de la información
Resolución 500 DE 2021	Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital.
CONPES 3995 de 2020	Política Nacional de Seguridad Nacional que tiene como objetivo fortalecer las capacidades de las múltiples Partes interesadas para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital, en el marco de cooperación, colaboración y asistencia, con el fin de contribuir al crecimiento de la economía digital nacional, lo que a su vez impulsará una mayor prosperidad económica y social.
Norma técnica colombiana 27001de 2022	TECNOLOGÍA DE LA INFORMACIÓN. TÉCNICAS DE SEGURIDAD. SISTEMAS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI). REQUISITOS
Norma técnica colombiana 27002 de 2022	Estándar para la seguridad de la información. Código de buenas prácticas para la gestión de la seguridad de la información.
olución 02277 de 2025 (Min	Actualiza el Modelo de Seguridad y Privacidad de la Información (MSPI), alineándolo con prácticas internacionales modernas.
Decreto 472 de 2024	Establece el Modelo de Gobernanza de Seguridad Digital, definiendo roles para la protección de la Infraestructura Crítica Cibernética.
Ley 2416 de 2024	Declara las telecomunicaciones como un servicio de utilidad pública e interés social, elevando la prioridad de la continuidad del servicio ante incidentes.
Decreto 767 de 2022	Define los nuevos lineamientos de la Política de Gobierno Digital y el concepto de Resiliencia Tecnológica.
Ley 2108 de 2021	Reconoce el internet como servicio público esencial y universal.

4. OBJETIVOS

4.1 *OBJETIVO GENERAL.*

Establecer y formalizar el marco de gobernanza para el Sistema de Gestión de Seguridad de la Información (SGSI) en UNIMOS S.A. E.S.P., mediante la definición de lineamientos, roles y responsabilidades que aseguren la protección de los activos de información, el cumplimiento normativo de protección de datos personales y la continuidad operativa del servicio de telecomunicaciones.

4.2 *OBJETIVOS ESPECÍFICOS.*

Para alcanzar el objetivo general, la entidad se traza los siguientes hitos operativos:

- ✓ Institucionalizar la Gobernanza: Formalizar la estructura de roles asegurando que cada dependencia de la empresa identifique y asuma sus responsabilidades específicas en la custodia de la información.
- ✓ Fortalecer la Protección de Datos: Garantizar el cumplimiento del 100% de los requisitos de la Ley 1581 de 2012, implementando avisos de privacidad y autorizaciones de tratamiento de datos en todos los puntos de contacto con el suscriptor.
- ✓ Gestionar el Riesgo de Información: Realizar el primer inventario de activos de información institucional y su respectiva valoración de riesgos, priorizando la protección de las bases de datos de facturación y los sistemas de gestión de red.
- ✓ Asegurar la Disponibilidad Técnica: Implementar protocolos básicos de seguridad perimetral (Firewalls y Antivirus) y un esquema de copias de seguridad (Backups) que garantice la recuperación de la información ante fallos técnicos o errores humanos.

✓ Promover la Cultura Digital: Capacitar al personal administrativo y operativo en buenas prácticas de seguridad de la información, enfocándose en la protección de contraseñas y el manejo seguro del correo institucional.

5. ALCANCE

La presente Política General de Seguridad y Privacidad de la Información es de cumplimiento obligatorio y define el marco de actuación para la protección de los activos de información en todos los niveles de UNIMOS S.A. E.S.P.

5.1.1 Sujetos Obligados

El alcance de esta política vincula a:

- Talento Humano: Todos los servidores públicos, trabajadores oficiales y pasantes de la entidad.
- Colaboradores Externos: Contratistas de prestación de servicios y personal de outsourcing.
- Terceros: Proveedores, aliados estratégicos y cualquier entidad externa que, por razón de sus funciones, tenga acceso a la infraestructura tecnológica o trate datos personales bajo la responsabilidad de UNIMOS S.A. E.S.P.

5.1.2 Ámbito Físico y Geográfico

La política aplica en:

- Instalaciones Físicas: Sede administrativa, centros de atención al usuario y puntos de venta.
- Infraestructura de Red: Nodos de telecomunicaciones, centros de cableado, cuartos de servidores y toda la extensión de la red de fibra óptica en el municipio de Ipiales.
- Entornos de Movilidad: Dispositivos móviles corporativos y accesos remotos autorizados para el desarrollo de funciones institucionales.

5.1.3 Ámbito Tecnológico y de Información

El alcance cubre la protección de:

- Información Digital: Bases de datos de suscriptores, sistemas de facturación (ERP), sistemas de gestión de red (NMS), correo electrónico institucional y archivos en servidores compartidos.
- Información Física: Documentación técnica de la red, expedientes de talento humano, contratos y archivos físicos bajo custodia de la entidad.
- Activos de Soporte: Hardware (computadores, servidores, equipos de red), software (licencias, aplicativos propios) y canales de comunicación.

5.1.4 Procesos Institucionales

En concordancia con el Modelo Integrado de Planeación y Gestión (MIPG), esta política impacta la totalidad del mapa de procesos de UNIMOS S.A. E.S.P.:

- Procesos Estratégicos: Planeación y toma de decisiones basadas en datos seguros.
- Procesos Misionales: Prestación de servicios de internet y televisión, garantizando la continuidad.
- Procesos de Apoyo: Gestión administrativa, financiera, jurídica y de talento humano.
- Procesos de Evaluación: Auditoría y control interno para la verificación del cumplimiento.

6. NIVEL DE CUMPLIMIENTO

Todas las personas cubiertas por el alcance y aplicabilidad de este documento deberán dar cumplimiento al **100%** de las directrices aquí establecidas. El SGSI-P de **UNIMOS S.A. E.S.P.** se sustenta en los siguientes doce (12) pilares operativos:

1. **Mejora Continua del SGSI-P:** UNIMOS S.A. E.S.P. se compromete a definir, implementar, operar y mejorar de forma continua su Sistema de Gestión de Seguridad de la Información y Privacidad, alineado estrictamente a las necesidades de la prestación del servicio de telecomunicaciones y a los requerimientos regulatorios vigentes.
2. **Responsabilidades Definidas y Transversales:** Las responsabilidades frente a la seguridad de la información son obligatorias y serán definidas, publicadas y aceptadas formalmente por cada uno de los empleados, contratistas o terceros, quienes asumen tareas específicas de custodia según su rol.
3. **Protección de Activos de Información:** La entidad protegerá la información generada, procesada o resguardada, asegurando que cada proceso de negocio cuente con un inventario de activos debidamente valorado y protegido.
4. **Clasificación y Manejo de la Información:** UNIMOS S.A. E.S.P. aplicará controles de seguridad proporcionales a la clasificación de la información (Pública, Interna o Confidencial), con el fin de minimizar impactos financieros, operativos o legales derivados de un uso incorrecto.

5. **Seguridad ligada al Talento Humano:** La entidad implementará controles para proteger la información de amenazas originadas por el factor humano, garantizando que el personal conozca sus deberes antes, durante y después de su vinculación laboral o contractual.

6. **Seguridad Física y Ambiental:** Se protegerán las instalaciones de procesamiento, nodos de red y la infraestructura tecnológica crítica que soporta la operación de fibra óptica, restringiendo el acceso físico solo a personal autorizado.

7. **Seguridad en la Operación y Redes:** UNIMOS S.A. E.S.P. garantizará la seguridad en la operación de sus procesos de negocio mediante el endurecimiento de los recursos tecnológicos y el monitoreo constante de las redes de datos.

8. **Control de Acceso Lógico:** Se implementarán controles de acceso robustos y perfiles de usuario basados en el principio de "necesidad de saber", limitando el acceso a sistemas y recursos de red exclusivamente a lo requerido para el cumplimiento de funciones.

9. **Seguridad en el Ciclo de Vida de los Sistemas:** La entidad garantizará que los requisitos de seguridad y privacidad sean parte integral del diseño, desarrollo y mantenimiento de sus sistemas de información y aplicaciones.

10. **Gestión de Incidentes y Debilidades:** UNIMOS S.A. E.S.P. asegura una mejora efectiva de su modelo mediante la gestión proactiva de eventos de seguridad, la identificación de vulnerabilidades y la documentación de lecciones aprendidas ante incidentes.

11. **Continuidad del Negocio y Resiliencia:** Se garantizará la disponibilidad de los procesos críticos y la continuidad de la operación de telecomunicaciones, basándose en análisis de impacto que permitan una recuperación ágil ante eventos disruptivos.

12. Cumplimiento Legal y Normativo: La entidad garantiza el cumplimiento estricto de las obligaciones legales (Ley 1581 de 2012, Ley 1273 de 2009, Ley 2108 de 2021), regulatorias y contractuales vigentes en materia de seguridad digital.

6.1 CONSECUENCIAS DEL INCUMPLIMIENTO

El incumplimiento de la Política General de Seguridad y Privacidad de la Información traerá consigo las consecuencias legales y administrativas que apliquen según la normativa de la Entidad. Esto incluye lo establecido en el **Código General Disciplinario**, las cláusulas penales contractuales y las normas del Gobierno Nacional y territorial vigentes en materia de Seguridad y Privacidad de la Información.

7. DESARROLLO DE LA POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

UNIMOS S.A. E.S.P. desarrolla su estrategia de seguridad basándose en el control de los riesgos operativos y la protección de la información de sus suscriptores, estructurada en los siguientes dominios:

7.1 Principios de Seguridad en UNIMOS

Toda acción administrativa y técnica en la empresa debe regirse por:

- **Responsabilidad Integral:** La seguridad es un compromiso de todas las oficinas, no solo de TI.
- **Legalidad (Habeas Data):** El respeto absoluto por la privacidad de los ciudadanos de Ipiales.
- **Continuidad:** La información debe estar disponible para garantizar que el servicio esencial de internet no se interrumpa.

7.2 Lineamientos Estratégicos por Dominios

A. Organización de la Seguridad y Talento Humano

- Cada nuevo empleado o contratista debe firmar un **Acuerdo de Confidencialidad** antes de acceder a los sistemas.
- Al retiro de un colaborador, la oficina de Talento Humano debe notificar a TI en un plazo máximo de 2 horas para la cancelación inmediata de todos los accesos.

B. Gestión de Activos de Información

- Cada dependencia debe mantener un inventario de sus archivos críticos (físicos y digitales).

- La información se clasificará en: **Pública, Interna y Confidencial**. Los datos de facturación y planos de red se consideran **Confidencial**.

C. Seguridad Física y de la Infraestructura de Red

- Los nodos de fibra óptica, OLTs y centros de cableado deben permanecer bajo llave y con acceso restringido.
- Se prohíbe el ingreso de personal ajeno a la empresa a los cuartos técnicos sin supervisión del área de TI.

D. Control de Acceso y Gestión de Contraseñas

- Las contraseñas deben ser personales e intransferibles.
- Se establece un estándar de complejidad (mínimo 8 caracteres, mayúsculas, números y símbolos) con cambio obligatorio cada 90 días para el año 2025.

E. Seguridad en las Operaciones (Copias de Seguridad)

- La oficina de TI ejecutará un plan de respaldos (backups) diarios para las bases de datos misionales.
- Se realizarán pruebas de restauración mensuales para garantizar que la información se puede recuperar en caso de un fallo del sistema.

7.3 Fases de Implementación (Cronograma 2025)

La entidad ejecutará la política en tres fases durante la vigencia:

1. **Fase de Formalización (Trimestre 1):** Socialización de la política y firma de compromisos por parte de los jefes de área.
2. **Fase de Control (Trimestre 2 y 3):** Implementación de antivirus, firewalls y actualización del inventario de activos.
3. **Fase de Evaluación (Trimestre 4):** Auditoría interna de cumplimiento para preparar la transición a los estándares de 2026.

- **7.4. Importancia de la Seguridad para el Servicio Público**

En cumplimiento de la **Ley 2108 de 2021**, UNIMOS S.A. E.S.P. entiende que proteger la información técnica de su red de fibra óptica es proteger el derecho de los ciudadanos a estar conectados. Un fallo en la seguridad de la información es un fallo en la prestación de un servicio esencial.

8. BIBLIOGRAFIA

El desarrollo y actualización de esta política se fundamenta en las siguientes fuentes normativas, estándares internacionales y lineamientos gubernamentales:

- **ISO/IEC 27001:2013/2022:** Sistemas de Gestión de Seguridad de la Información (SGSI) - Requisitos. (Referente principal para la estructuración del ciclo PHVA).
- **ISO/IEC 27002:2022:** Seguridad de la información, ciberseguridad y protección de la privacidad — Controles de seguridad de la información.
- **NIST Cybersecurity Framework (v1.1):** Marco de referencia para la gestión de riesgos de ciberseguridad en infraestructuras críticas.
- **Constitución Política de Colombia:** Artículo 15 (Protección de datos y Habeas Data).
- **Ley 1273 de 2009:** Por medio de la cual se modifica el Código Penal y se crea un nuevo bien jurídico tutelado - denominado “de la protección de la información y de los datos”.
- **Ley 1581 de 2012:** Ley General de Protección de Datos Personales.

- **Ley 2108 de 2021:** Por la cual se establece el acceso a Internet como un servicio público esencial y universal.
- **Decreto 1078 de 2015:** Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
- **Manual de Gobierno Digital (MinTIC):** Lineamientos para el cumplimiento de la política de Seguridad y Privacidad de la Información bajo el Modelo Integrado de Planeación y Gestión (MIPG).