MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN

"MIPG"

PLAN DE TRATAMIENTO DE RIESGO DE SEGURIDAD DE LA INFORMACION 2026

"UNIMOS" EMPRESA MUNICIPAL DE TELECOMUNICACIONES DE IPIALES

S.A. E.S.P.

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

PLAN TRATAMIENTO DE RIESGO DE SEGURIDAD DE LA INFORMACION 2026		
ELABORÓ	**REVISÓ**	**APROBÓ**
Luis Carlos Salazar Araujo	Carmenza M. Belalcázar R.	Comité Institucional de Gestión y Desempeño
Jefe Oficina Operaciones Digitales	Jefe Oficina Asesora de Planeación	UNIMOS S.A. E.S.P.
FECHA	**FECHA**	**FECHA**
16/01/2026	20/01/2026	12/02/2026

REGISTRO DE MODIFICACIONES
Actualización vigencia de gestión 2024-2027
Actualización del formato fecha y logo

Tabla de contenido

1. INTRODUCCIÓN

El presente **Plan de Tratamiento de Riesgos de Seguridad de la Información (PTR)** constituye el componente operativo y táctico del Sistema de Gestión de Seguridad de UNIMOS S.A. E.S.P. para la vigencia 2026. A diferencia de años anteriores, este plan adopta un enfoque de **Defensa Activa**, diseñado para proteger la infraestructura crítica de telecomunicaciones en un entorno donde el acceso a Internet es un **Servicio Público Esencial** (Ley 2108 de 2021) y las amenazas han evolucionado hacia ataques automatizados mediante Inteligencia Artificial y Ransomware de quinta generación.

El PTR 2026 no es un inventario estático de problemas, sino una hoja de ruta de **controles de mitigación**. Su ejecución garantiza que los riesgos identificados en la matriz institucional sean abordados mediante la implementación de salvaguardas técnicas (como la arquitectura Zero Trust y el cifrado de datos) y administrativas, reduciendo la exposición de los activos críticos —tales como Nodos, OLTs y bases de datos de suscriptores— a niveles de riesgo residual aceptables para la alta dirección.

Bajo los lineamientos de la **ISO/IEC 27005:2022** y el **MIPG**, este documento articula las acciones de respuesta necesarias para preservar la **confidencialidad, integridad y disponibilidad** de la información. El éxito de este plan radica en la corresponsabilidad de los líderes de proceso de UNIMOS, quienes actúan como dueños del riesgo, asegurando que la seguridad digital sea el pilar fundamental que soporte la continuidad del negocio y la confianza de la ciudadanía de Ipiales.

2. OBJETIVOS

2.1. Objetivo General

Ejecutar y monitorear el tratamiento técnico de los riesgos de seguridad digital en UNIMOS S.A. E.S.P., mediante la implementación de controles proporcionales al nivel de amenaza, con el fin de garantizar la **resiliencia operativa** de la infraestructura de telecomunicaciones y la protección de los datos personales de los ciudadanos de Ipiales.

2.2. Objetivos Específicos

- **Mitigación de Riesgos Críticos:** Implementar el 100% de las acciones de tratamiento definidas para los riesgos calificados como "Extremos" y "Altos".
- **Aseguramiento de Infraestructura Esencial (Ley 2108):** Desplegar controles de endurecimiento y autenticación multifactor (MFA) en el acceso administrativo a OLTs, Nodos y sistemas de gestión de red (NMS) para prevenir interrupciones del servicio por accesos no autorizados.
- **Eficiencia en la Recuperación (Resiliencia):** Garantizar que las acciones de tratamiento (backups inmutables y sitios de réplica) permitan un Tiempo de Objetivo de Recuperación (**RTO**) menor a 4 **horas** ante un incidente de Ransomware en servicios críticos de internet y facturación.
- **Control de Riesgos de Terceros:** Establecer controles de seguridad técnica y cláusulas de cumplimiento en el 100% de los contratos con proveedores de nube y soporte técnico externo, asegurando la **Soberanía de Datos** en territorio nacional.
- **Gestión de Amenazas por IA:** Actualizar la matriz de controles para incluir la detección y respuesta ante incidentes de ingeniería social avanzada (Deepfakes y Phishing automatizado) que afecten los procesos financieros y comerciales.
- **Cultura Basada en Riesgo:** Lograr que el 100% de los líderes de proceso de UNIMOS realicen al menos un ejercicio de autoevaluación de sus riesgos operativos, fomentando la descentralización de la seguridad.

3. MARCO LEGAL

El presente Plan se fundamenta en el bloque de legalidad colombiano y los estándares internacionales de seguridad digital vigentes, asegurando que **UNIMOS S.A. E.S.P.** cumpla con sus obligaciones como prestador de servicios esenciales:

3.1. Normatividad Nacional

- **Constitución Política de Colombia:** Artículo 15 (Derecho a la intimidad y Habeas Data).
- **Ley 2108 de 2021:** Por la cual se garantiza el acceso a Internet como un **servicio público esencial y universal**, obligando a la protección de la infraestructura que soporta dicha conectividad.
- **Ley 1581 de 2012:** Régimen General de Protección de Datos Personales (Tratamiento de información de suscriptores).
- **Ley 1273 de 2009:** Ley de Delitos Informáticos (Protección de los activos de información y sistemas).
- **Decreto 1078 de 2015:** Decreto Único Reglamentario del Sector TIC, que establece los lineamientos para el Modelo de Seguridad y Privacidad de la Información (MSPI).
- **Ley 1437 de 2011 (CPACA):** Obligaciones de las entidades en la gestión de documentos y archivos digitales.
- **Directiva Presidencial 03 de 2021:** Fortalecimiento de la ciberseguridad y confianza digital en las entidades del Estado.

3.2. Referentes Internacionales y Estándares

- **ISO/IEC 27001:2022:** Estándar internacional para Sistemas de Gestión de Seguridad de la Información (SGSI).
- **ISO/IEC 27005:2022:** Directrices para la gestión de riesgos de seguridad de la información.
- **NIST Cybersecurity Framework (v2.0):** Marco de referencia para la gestión de ciberseguridad en infraestructuras críticas.

3.3. Lineamientos Institucionales (MIPG)

- **Manual Operativo del MIPG (Función Pública):** Dimensión de Gestión con Valores para el Resultado, específicamente la política de Gobierno Digital.
- **Guía para la Administración de Riesgos y el Diseño de Controles (DAFP, 2020):** Metodología oficial para la valoración y tratamiento de riesgos en entidades públicas.

4. ALCANCE

El presente plan define el marco de actuación para la mitigación de riesgos de seguridad y privacidad en toda la estructura de UNIMOS S.A. E.S.P., abarcando los siguientes frentes durante la vigencia 2026:

4.1. Alcance Organizacional y Humano

El tratamiento de riesgos es de aplicación obligatoria para:

- Todos los procesos institucionales (Estratégicos, Misionales, de Apoyo y de Evaluación).
- El 100% de los funcionarios, trabajadores oficiales y contratistas, incluyendo aquellos que realizan funciones bajo modalidades de Teletrabajo o Trabajo Remoto.
- Terceros y proveedores con acceso a la infraestructura crítica o que realicen tratamiento de datos personales por cuenta de la entidad.

4.2. Alcance Tecnológico e Infraestructura

Se priorizará el tratamiento de riesgos sobre los activos que garantizan la continuidad del servicio esencial:

- Infraestructura de Red (Core): Nodos de fibra óptica, equipos de cabecera (OLTs), routers de borde y sistemas de gestión de red (NMS).
- Sistemas Misionales: Plataformas de facturación, bases de datos de suscriptores, CRM y sistemas de soporte técnico.
- Entornos de Nube y Emergentes: Servicios alojados en la nube (SaaS, PaaS, IaaS) y herramientas de Inteligencia Artificial utilizadas en procesos administrativos o de analítica de datos.

4.3. Alcance Geográfico y Físico

Las acciones de tratamiento se ejecutarán en:

- La sede administrativa y centros de atención al cliente en el municipio de Ipiales.
- La totalidad de los nodos y redes de distribución de servicios de telecomunicaciones.
- Los activos de información que se encuentren fuera de las instalaciones físicas bajo custodia de empleados autorizados.

4.4. Alcance Normativo y de Privacidad

El plan aborda los riesgos que impacten el cumplimiento de:

- La Ley 1581 de 2012 (Protección de Datos Personales).
- La Ley 2108 de 2021 (Acceso a Internet como Servicio Público Esencial).
- Los estándares de la ISO/IEC 27001:2022, asegurando la resiliencia institucional ante ataques cibernéticos.

5. TERMINOLOGÍA Y CONCEPTOS CLAVE

Para la correcta interpretación del presente plan, se definen los siguientes términos bajo los estándares de seguridad digital y resiliencia operativa:

- **Activo de Información Crítica:** Cualquier sistema, dato o infraestructura (como las OLTs y Nodos de red) cuya pérdida de disponibilidad o integridad afecte directamente la prestación del servicio esencial de telecomunicaciones en Ipiales.
- **Amenaza Emergente:** Nuevas formas de ataque que aprovechan tecnologías como la Inteligencia Artificial Generativa para realizar *phishing* automatizado o crear contenidos sintéticos (*deepfakes*) con el fin de suplantar identidades institucionales.
- **Arquitectura de Confianza Cero (Zero Trust):** Modelo de seguridad que asume que la red institucional puede estar comprometida y, por lo tanto, exige una verificación continua de identidad y dispositivo para cada solicitud de acceso.
- **Ciberresiliencia:** Capacidad de UNIMOS S.A. E.S.P. para anticipar, resistir, recuperarse y adaptarse a incidentes cibernéticos, garantizando que el servicio de internet no sufra interrupciones prolongadas.
- **Control de Seguridad:** Medida técnica, administrativa u organizacional (como el MFA - Autenticación de Múltiple Factor) que se implementa para modificar o mitigar un riesgo identificado.
- **Impacto de Negocio (BIA):** Evaluación técnica de las consecuencias que tendría para la empresa y la comunidad la caída de un servicio o el compromiso de una base de datos de suscriptores.
- **Infraestructura Crítica de Telecomunicaciones:** Conjunto de activos físicos y lógicos indispensables para la conectividad del municipio, protegidos bajo la Ley 2108 de 2021.
- **Riesgo Residual:** El nivel de riesgo que permanece después de haber implementado los controles de seguridad definidos en este plan.

- **Soberanía de Datos:** Concepto que asegura que la información de los usuarios de UNIMOS, aun cuando esté alojada en nubes internacionales, se mantenga protegida bajo la jurisdicción y leyes de protección de datos de Colombia.
- **Vulnerabilidad Técnica:** Debilidad presente en el software de los equipos de red, servidores o aplicaciones que puede ser explotada por un atacante para ganar acceso no autorizado.
- **Riesgo Estratégico:** Se asocia con la forma en que se administra la Entidad, su manejo se enfoca a asuntos globales relacionados con la misión y el cumplimiento de los objetivos estratégicos, la clara definición de políticas, diseño y conceptualización de la entidad por parte de la alta gerencia.
- **Riesgos de Imagen**: Están relacionados con la percepción y la confianza por parte de la ciudadanía hacia la institución
- **Riesgos Operativos:** Comprenden riesgos provenientes del funcionamiento y operatividad de los sistemas de información institucional, de la definición de los procesos, de la estructura de la entidad, de la articulación entre dependencias.
- **Riesgos Financieros:** Se relacionan con el manejo de los recursos de la entidad que incluyen la ejecución presupuestal, la elaboración de los estados financieros, los pagos, manejos de excedentes de tesorería y el manejo sobre los bienes.
- **Riesgos de Cumplimiento:** Se asocian con la capacidad de la entidad para cumplir con los requisitos legales, contractuales, de ética pública y en general con su compromiso ante la comunidad.
- **Riesgos de Tecnología:** Están relacionados con la capacidad tecnológica de la Entidad para satisfacer sus necesidades actuales y futuras y el cumplimiento de la misión.
- **Riesgos de Corrupción:** Relacionados con acciones, omisiones, uso indebido del poder, de los recursos o de la información para la obtención de un beneficio particular o de un tercero.
- **Reducción del Riesgo:** Acciones que se toman para disminuir la probabilidad las consecuencias negativas, o ambas, asociadas con un riesgo.
- **Retención del Riesgo:** Aceptación de la pérdida o ganancia proveniente de un riesgo particular. Seguridad de la información: Preservación de la confidencialidad, integridad y disponibilidad de la información.
- **Seguimiento:** Mesa de trabajo semestral, en el cual se revisa el cumplimiento del plan de acción, indicadores y metas de riesgo y se valida la aplicación n de los controles de seguridad de la información sobre cada uno de los procesos.
- **Tratamiento del Riesgo:** Proceso para modificar el riesgo" (Icontec Internacional, 2011).

- **Valoración del Riesgo:** Proceso global de identificación del riesgo, análisis del riesgo y evaluación de los riesgos.
- **Vulnerabilidad:** Debilidad de un activo o control que puede ser explotada por una o más amenazas.

6. INTEGRACIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN (MSPI)

En UNIMOS S.A. E.S.P., el Modelo de Seguridad y Privacidad de la Información (MSPI) no opera de manera aislada; se integra directamente con el Modelo Integrado de Planeación y Gestión (MIPG) para asegurar que la seguridad digital sea una capacidad institucional y no solo un requerimiento técnico.

6.1. Articulación con la Gestión de Riesgos Institucionales

El Plan de Tratamiento de Riesgos 2026 se integra con la política de administración de riesgos de la entidad bajo los siguientes lineamientos:

Armonización con el Mapa de Riesgos de Corrupción y Gestión: Los riesgos de seguridad digital que tengan impacto en la transparencia o la legalidad se reportarán de manera consolidada en el Mapa de Riesgos Institucional. Enfoque Basado en Procesos: Cada líder de proceso (Comercial, Técnico, Financiero, Jurídico) es el "dueño del riesgo". La Oficina de Operaciones Digitales y el OSPI actúan como facilitadores técnicos, pero la ejecución de los controles es responsabilidad de cada dependencia.

6.2. Componentes de la Integración para 2026

La integración del MSPI en esta vigencia se soporta en cuatro pilares estratégicos:

a) Gobernanza y Liderazgo: El Comité Institucional de Gestión y Desempeño supervisa el avance del tratamiento de riesgos, asegurando la asignación de recursos presupuestales para la mitigación de amenazas críticas.
b) Cultura Organizacional: Integración del componente humano mediante programas de sensibilización que transforman la política en hábitos operativos (ej. gestión de contraseñas, reporte de incidentes, protección de datos de suscriptores).
c) Gestión del Cambio Tecnológico: Integración de la seguridad desde el diseño en la adquisición de nuevas tecnologías, servicios en la nube o herramientas de Inteligencia Artificial.
d) Cumplimiento Normativo Transversal: Sincronización de las auditorías de Control Interno con los requisitos del FURAG, asegurando que las evidencias de tratamiento de riesgos se generen de manera continua y no solo al cierre de la vigencia.

6.3. Relación con la Continuidad del Servicio

Como prestadores de un servicio público esencial (Ley 2108 de 2021), la integración del MSPI garantiza que el Plan de Tratamiento de Riesgos soporte directamente el Plan de Continuidad del Negocio. Esto asegura que, ante un desastre digital, la entidad sepa cómo responder para restablecer la conectividad de los habitantes de Ipiales en el menor tiempo posible.

7. METODOLOGÍA PARA LA ADMINISTRACIÓN DE RIESGOS

UNIMOS S.A. E.S.P. adopta una metodología basada en el estándar ISO/IEC 27005 y la Guía para la Administración de Riesgos de Función Pública (2020), estructurada en cinco fases cíclicas que garantizan la mejora continua:

7.1. Identificación del Riesgo

En esta fase, cada dependencia debe identificar los eventos que pueden comprometer la información. Para 2026, se incluyen tres categorías de análisis obligatorio:

a) Riesgos de Infraestructura: Relacionados con OLTs, nodos y fibra óptica.
b) Riesgos de Privacidad: Asociados a la Ley 1581 y datos de suscriptores.
c) Riesgos Emergentes: Derivados del uso de nubes públicas e Inteligencia Artificial.

7.2. Análisis y Valoración del Riesgo

El nivel de riesgo se calcula mediante la evaluación de dos variables:

1. **Probabilidad (P):** Frecuencia de ocurrencia basada en el histórico de incidentes de red de UNIMOS y la inteligencia de amenazas del sector. (Escala 1 a 5).
2. **Impacto (I):** Severidad del daño, medida en tres dimensiones:
    - **Operativo:** ¿Afecta el servicio esencial de internet?
    - **Legal:** ¿Incumple con la SIC o Función Pública?
    - **Reputacional:** ¿Afecta la confianza del ciudadano de Ipiales?

Riesgo = Probabilidad (P) X Impacto (I)

7.3. Evaluación del Riesgo (Mapa de Calor)

Los riesgos se ubican en una matriz de 5x5 para determinar su prioridad:

Nivel de Riesgo	Zona	Acción Requerida
Extremo (20-25)	Roja	Tratamiento inmediato. Requiere monitoreo en tiempo real y reporte a Gerencia.
Alto (12-16)	Naranja	Controles técnicos obligatorios (Ej. MFA, Cifrado).
Moderado (6-10)	Amarilla	Procedimientos operativos y monitoreo trimestral.
Bajo (1-5)	Verde	Asumir con controles existentes y revisión anual.

7.4. Tratamiento del Riesgo

Para cada riesgo identificado, los líderes de proceso deben seleccionar una de las siguientes cuatro opciones:

a) Evitar: Eliminar la actividad que genera el riesgo.

b) Reducir (Mitigar): Implementar controles (ej. Autenticación de Múltiple Factor - MFA).

c) Compartir/Transferir: Contratar pólizas de ciberseguridad o tercerizar con proveedores certificados.

d) Asumir: Aceptar el riesgo residual cuando el costo del control supera el impacto potencial.

7.5. Monitoreo y Comunicación

A diferencia de 2025, el monitoreo en 2026 será trimestral. Los líderes de cada área deben reportar a la Oficina Asesora de Planeación y a la Oficina de Jefatura operaciones digitales la efectividad de los controles implementados, generando las evidencias necesarias para la auditoría FURAG 2026.

8. CRONOGRAMA

El cronograma se divide en cuatro fases clave para garantizar que UNIMOS S.A. E.S.P. mantenga su ciber resiliencia durante todo el año:

Fase	Actividad	Responsables	Inicio	Fin
I. Planeación y Diagnóstico	Actualización de la Matriz de Riesgos (incluyendo IA y Nube) y levantamiento de activos.	Oficina de Sistemas / Oficina de Planeación	Enero	Febrero
II. Tratamiento y Mitigación	Implementación de controles técnicos (Cifrado, MFA, Fortalecimiento de Nodos/OLTs).	Subgerencia Técnica / Sistemas	Febrero	Agosto
III. Seguimiento y Verificación	Auditorías internas de cumplimiento de controles y reporte de evidencias para FURAG.	Oficina de Control Interno / OSPI	Marzo	Diciembre
IV. Evaluación y Mejora	Evaluación de Riesgos Residuales y actualización del plan de continuidad.	Comité de Gestión y Desempeño	Junio	Diciembre