PROYECTA
EMPRESA PARA EL DESARROLLO TERRITORIAL

GOBIERNO DEL QUINDÍO

# PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD 2026

## EMPRESA PARA EL DESARROLLO TERRITORIAL

## PROYECTA

## 2026

**Gobernación del Quindío** Calle 20 N° 13-22, piso 16, Armenia, Quindío
PBX **741 77 00** EXT **320** - proyecta@proyecta.gov.co - **www.proyecta.gov.co**

www.**quindio**.gov.co

# 1. Identificación y Valoración de Activos Críticos

Basado en el inventario actual, los activos con mayor nivel de riesgo para 2026 son:

- **Servicios de Red:** Router Mikrotik y Switches TP-Link/3COM (Soporte de protocolos y segmentación).
- **Información Ciudadana:** Datos personales en el portal proyecta.gov.co y aplicativos misionales.
- **Hardware de Usuario:** 16 equipos de escritorio y 2 portatiles con procesadores de 4ta generación (Riesgo de obsolescencia y falta de parches de seguridad modernos).
- **Infraestructura IPv6:** Nuevos servicios de Intranet y Extranet en modalidad *Dual Stack*.

# 2. Matriz de Tratamiento de Riesgos 2026

| Activo / Proceso | Riesgo Identificado | Nivel de Riesgo | Acción de Tratamiento | Control a Implementar | Responsable |
|---|---|---|---|---|---|
| **Infraestructura de Red** | Acceso no autorizado o denegación de servicio por vulnerabilidades en protocolos antiguos. | Alto | **Mitigar** | Instalación de **Switches Capa 2/4 corporativos** con administración CLI/SSH segura. | Área de Sistemas |
| **Transición IPv6** | Brechas de seguridad durante la coexistencia de protocolos IPv4 e IPv6 (*Dual Stack*). | Muy Alto | **Mitigar** | Procesos de **Hardening** y actualización de políticas en el UTM NG Firewall. | Área de sistemas / QSOFTING |

| | | | | | |
|---|---|---|---|---|---|
| **Equipos de Cómputo** | Infección por malware avanzado debido a hardware que no soporta funciones de seguridad de SO modernos. | Medio | **Mitigar** | Actualización de licencias **Kaspersky** y plan de renovación tecnológica gradual. | Gerencia<br>Gestión Adminsitrativa y Área de Sistemas |
| **Privacidad de Datos** | Fuga de información sensible o incumplimiento de la Ley 1581 por falta de controles de acceso. | Alto | **Mitigar** | Implementación de formatos de autorización y base de datos centralizada de terceros. | Gestion Adminsitrativa y Gestion Juridica |
| **Disponibilidad de Datos** | Desincronización de logs que impida la trazabilidad de incidentes o delitos informáticos. | Medio | **Mitigar** | Activación y configuración del **servicio NTP** en toda la infraestructura de red. | Área de Sistemas |

# 3. Acciones Prioritarias de Mitigación (Plan de Acción)

## A. Aseguramiento de la Red (Hardening)

- **Control:** Personalización de cada punto del switch dependiendo del dispositivo conectado (Access Point, etc.) para evitar suplantaciones.
- **Meta 2026:** 100% de los puntos de red caracterizados y asegurados.

## B. Gestión de la Continuidad y Trazabilidad

- **Control:** Implementación de un Sistema de Correlación de Eventos (NMS) integrado con el servicio NTP para identificar rápidamente problemas de desconexión.

La implementación de un **Sistema de Gestión de Red (NMS)** o un **Sistema de Correlación de Eventos** en **PROYECTA** es un paso técnico fundamental para garantizar la trazabilidad y la seguridad digital en la vigencia 2026. Basado en el documento técnico y los estándares de **MinTIC**, el proceso se divide en las siguientes etapas:

**Preparación de la Base: Sincronización NTP**

Antes de correlacionar eventos, todos los dispositivos deben hablar "en el mismo tiempo".

**Implementación del Servicio NTP**: Configurar un modelo cliente-servidor para sincronizar los relojes internos de los routers Mikrotik, switches TP-Link y estaciones de trabajo.

**Beneficio Directo**: Esto permite ordenar los eventos y transacciones en orden cronológico exacto, facilitando la identificación de problemas de desconexión.

**Configuración de la Recolección de Datos (Protocolos)**
Para que el NMS reciba información, los activos de red deben ser configurados para enviar datos:

**SNMP (Simple Network Management Protocol)**: Habilitar este protocolo en los switches de nivel corporativo y routers para monitorear el rendimiento (uso de ancho de banda, CPU, estado de puertos).

**Syslog**: Configurar los dispositivos para que envíen sus bitácoras de eventos ("Logs") hacia un servidor centralizado.

**NetFlow/IPFIX**: Útil para analizar el tráfico de red, especialmente en la modalidad dual stack IPv4/IPv6.

**Selección y Despliegue de la Plataforma NMS/SIEM**

Considerando que **PROYECTA** cuenta con equipos Mikrotik y diversos switches, se debe elegir una herramienta que soporte estos fabricantes:

- **Plataformas Sugeridas**: Herramientas como *Zabbix*, *PRTG* o *The Dude* (específico para Mikrotik) para el monitoreo de red, o un SIEM (*Security Information and Event Management*) como *Wazuh* para la seguridad.
- **Instalación**: El software debe residir en un servidor con alta disponibilidad dentro de la infraestructura tecnológica de la empresa.

# 4. Definición de Reglas de Correlación

La "correlación" es lo que convierte datos aislados en alertas inteligentes. En **PROYECTA**, se deben configurar reglas como:

- **Alerta de Intrusión**: Si se detecta un fallo de inicio de sesión en el router Mikrotik seguido de un cambio de configuración en un switch corporativo en menos de 5 minutos.
- **Falla en Cascada**: Si varios Access Points se desconectan simultáneamente, el sistema debe identificar si el problema es el switch de distribución o el proveedor de internet.
- **Seguridad Digital**: Localización cronológica de problemas relacionados con delitos informáticos sobre la infraestructura de networking.

# 5. Visualización y Alistamiento Operativo

- **Tableros de Control (Dashboards)**: Crear mapas de red en tiempo real que muestren el estado de los 65 Access Points y los enlaces de fibra óptica.
- **Hardening**: Como parte del proceso de implementación, se deben disminuir las vulnerabilidades o brechas de seguridad de las aplicaciones de los dispositivos de red antes de conectarlos al NMS.

**Resumen de Beneficios para el PESPI 2026:**

1. **Trazabilidad**: Bitácora de eventos sincronizada para auditorías de Control Interno.
2. **Seguridad**: Contribuye a la localización de problemas en procesos de delitos informáticos.
3. **Eficiencia**: Identificación más rápida de desconexiones de puntos de datos.

- **Meta 2026:** Bitácora de eventos "Log" local sincronizada cronológicamente para procesos de auditoría.

## C. Seguridad en el protocolo IPv6

**Control:** Realizar informes de implementación bajo la **Resolución 1126 de 2021** y capacitar al personal de TI en configuraciones seguras de IPv6.

**Meta 2026:** Certificación de cumplimiento de MinTIC para entidades territoriales.

4. Seguimiento y Evaluación

Para garantizar que el tratamiento sea efectivo, se establecen las siguientes herramientas de monitoreo:

- **Auditorías de Control Interno:** Verificación bimestral de la aplicación de protocolos de seguridad en el cuarto de telecomunicaciones.
- **Evaluación de Proveedores:** Seguimiento estricto a los compromisos de seguridad de los proveedores de software (QSOFTING) y conectividad (Claro).
- **Reporte FURAG:** Medición anual del avance en la política de Seguridad Digital y Privacidad de la Información.

**LINA MARCELA ROLDAN PRIETO**
**GERENTE GENERAL**
**ENERO 29 DE 2026**