MANUAL DE PROCEDIMIENTO: ASEGURAMIENTO DE SERVICIOS EN LA RED WISP

MathisTechnology S.A.S. | NIT: 901.560.844

Cumplimiento Normativo: Directrices de Seguridad Digital de MinTIC, Estándar ISO 27001 y Regulaciones de la ANE (Agencia Nacional del Espectro) para Redes Inalámbricas.

---

1. OBJETIVO

Establecer las directrices técnicas y administrativas para proteger la información que circula a través de la infraestructura de red inalámbrica (WISP) de MathisTechnology S.A.S., garantizando la seguridad en los radioenlaces, estaciones base, nodos de distribución y equipos en las premisas del cliente (CPE) en las zonas rurales de Cómbita y municipios cercanos.

2. CONTROL DE ACCESO Y SEGURIDAD INALÁMBRICA (WISP)

- **Cifrado de Radioenlaces: Todo el tráfico que viaja de manera inalámbrica entre los nodos principales (Access Points) y las antenas de los clientes (CPE) debe estar cifrado utilizando protocolos robustos (WPA3-Enterprise o en su defecto WPA2-AES con llaves extensas), prohibiendo redes abiertas o sin cifrar.**
- **Ocultamiento y Aislamiento: Los nombres de red (SSID) de administración de la infraestructura deben estar ocultos. Se debe activar la función de *Client Isolation* (Aislamiento de Clientes) en los nodos para evitar que los usuarios de la red puedan verse o atacarse entre sí.**
- **Autenticación Centralizada: El acceso de los clientes al servicio de internet inalámbrico se debe validar mediante un sistema centralizado (como servidores RADIUS o PPPoE de alta seguridad), asignando credenciales únicas y dinámicas por usuario.**

3. SEGURIDAD DE LA INFRAESTRUCTURA FÍSICA Y LÓGICA

- **Seguridad en Torres y Nodos: Los nodos físicos de distribución (torres de antenas) deben contar con medidas de seguridad física (cerramientos, candados de alta seguridad) para evitar la manipulación física de los cables de red (UTP/FTP) y los dispositivos de radio.**
- **Segmentación de Red (VLANs): Se debe implementar una separación estricta mediante redes virtuales (VLANs) para aislar completamente el tráfico de administración de las antenas y enrutadores, del tráfico de navegación comercial de los clientes.**

4. CIFRADO Y TRANSFERENCIA SEGURA DE INFORMACIÓN

- **Gestión Remota Protegida: Queda prohibido el acceso a las antenas y estaciones base mediante protocolos inseguros (como HTTP o Telnet). Toda gestión remota**

de la red inalámbrica debe realizarse obligatoriamente mediante HTTPS, SSH, o a través de una red VPN corporativa cifrada con autenticación de dos factores (2FA).

5. REGISTROS DE AUDITORÍA Y MONITOREO EN TIEMPO REAL

- Monitoreo del Espectro y Enlaces: Se deben generar y almacenar reportes automáticos de eventos (Syslog) de las estaciones base. Estos registros deben registrar caídas de enlaces, intentos de desasociación forzada (ataques de desautenticación Wi-Fi) e intentos fallidos de acceso a las consolas de administración de las antenas.

6. GESTIÓN DE INCIDENTES ESPECÍFICOS DE REDES INALÁMBRICAS

Siguiendo los lineamientos de MinTIC para la gestión de riesgos tecnológicos, ante incidentes inalámbricos se actuará de la siguiente manera:

1. Detección de Interferencia o Ataque: Monitoreo constante ante ataques de denegación de servicio inalámbrico (DoS), clonación de MAC o presencia de Access Points piratas (*Rogue APs*).
2. Mitigación: Cambio inmediato de frecuencias (canales) coordinado, bloqueo de direcciones MAC sospechosas a nivel de Access Point y actualización remota de llaves de cifrado.
3. Registro: Reporte obligatorio en la bitácora interna de incidentes detallando la afectación del servicio inalámbrico en la zona rural.

7. ROLES Y RESPONSABILIDADES

Rol / Cargo	Responsabilidad en la Red WISP
Responsable de Seguridad Digital	Auditar que las políticas de cifrado inalámbrico se cumplan y liderar la respuesta ante incidentes.
Ingeniero / Administrador WISP	Configurar las frecuencias, asegurar las contraseñas de las antenas, revisar servidores RADIUS/PPPoE y monitorear logs.
Técnico de Instalaciones / Campo	Garantizar el aseguramiento físico de las antenas de los clientes, asignar claves seguras en los routers domésticos y reportar daños.

Fecha de Aprobación: 7 / 10 / 2025
Versión del Documento: 2.0 (Especialidad WISP)