MATHIS TECHNOLOGY S.A.S.

# GUÍA DE SEGURIDAD DE LA RED Y PREVENCIÓN DE RIESGOS

**ALINEACIÓN ESTRATÉGICA CON EL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN (MSPI) - MINTIC**

---

## 1. GOBIERNO DIGITAL Y OBJETIVOS EN MATHIS TECHNOLOGY

La presente guía establece las directrices de obligatorio cumplimiento para el personal, contratistas y administradores de tecnología de **Mathis Technology S.A.S.**, adoptando los tres principios del Modelo de Gobierno Digital de MinTIC:

- **Confidencialidad:** Asegurar que los datos de la compañía y de nuestros clientes sean accesibles únicamente por credenciales explícitamente autorizadas.
- **Integridad:** Proteger la exactitud de los desarrollos, bases de datos y configuraciones lógicas frente a modificaciones maliciosas o accidentales.
- **Disponibilidad:** Garantizar la continuidad operativa de los servicios de red y almacenamiento digital frente a cualquier contingencia interna o externa.

## 2. MATRIZ DE RIESGOS DIGITALES IDENTIFICADOS

Bajo los criterios de monitoreo de MinTIC, se han catalogado los vectores de ataque más críticos a los que se expone la infraestructura tecnológica de la organización:

### A. Amenazas de Infraestructura Tecnológica (Prioridad Crítica)

- **Ransomware corporativo:** Secuestro y cifrado de código fuente o repositorios de datos institucionales exigiendo un rescate financiero.
- **Intrusiones en la Capa de Red:** Explotación de puertos abiertos o firmware desactualizado en routers, switches y firewalls corporativos.
- **Fuga de Información Privada:** Brechas de seguridad que comprometan datos de terceros, infringiendo la Ley 1581 de Protección de Datos Personales en Colombia.

### B. Vectores de Ingeniería Social (Prioridad Alta)

- **Phishing dirigido:** Correos o comunicaciones engañosas dirigidas a colaboradores con el fin de extraer llaves criptográficas o credenciales administrativas.
- **Suplantación del Entorno Web:** Páginas falsas que imitan portales institucionales de Mathis Technology S.A.S. para engañar a usuarios o clientes.

### C. Riesgos Humanos y de Convivencia Digital

- **Ciberacoso y Filtraciones Internas:** Compromiso del clima organizacional mediante dinámicas digitales nocivas o mal uso de la información confidencial.
- **Exposición de Credenciales:** Compartición indebida de accesos mediante canales de mensajería no cifrados.

## 3. PROTOCOLOS DE PREVENCIÓN DE MATHIS TECHNOLOGY S.A.S.

Aplicando el enfoque del ciclo de mejora continua PHVA (Planear, Hacer, Verificar, Actuar) exigido por MinTIC, se implementan los siguientes controles preventivos de manera estricta:

### Seguridad Lógica y de Red (Controles Técnicos)

- **Túneles Seguros:** Uso obligatorio de conexiones VPN empresariales y protocolos HTTPS estrictos para el acceso a cualquier entorno operativo.
- **Autenticación Multifactor (MFA):** Implementación de autenticación de doble factor sin excepción para correos corporativos y accesos root.
- **Gestión de Parches:** Ventanas de mantenimiento obligatorias para la actualización del sistema operativo y parches de seguridad en toda la red de terminales.
- **Defensa Perimetral activa:** Firewalls perimetrales con políticas de denegación por defecto y sistemas antivirus con análisis en tiempo real.

### Políticas de Uso Seguro (Controles de Usuario)

- **Aislamiento de Redes Públicas:** Prohibición absoluta de conectar estaciones de trabajo de Mathis Technology S.A.S. a redes Wi-Fi abiertas o públicas.
- **Higiene y Verificación:** Obligatoriedad de inspección de dominios y remitentes antes de ejecutar descargas o responder a requerimientos externos.

1. Mapeo de Activos ➔ 2. Análisis de Vulnerabilidades

# GUÍA DE SEGURIDAD DE LA RED Y PREVENCIÓN DE RIESGOS DIGITALES

**ALINEADO CON EL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN (MSPI) - MINTIC COLOMBIA**

---

## 1. PRINCIPIOS FUNDAMENTALES DEL MINTIC

Esta guía adopta los tres pilares del Modelo de Gobierno Digital de MinTIC con el fin de salvaguardar y proteger la infraestructura tecnológica y los activos de información institucionales:

- **Confidencialidad:** Garantizar que la información sea accesible únicamente para el personal debidamente autorizado.
- **Integridad:** Salvaguardar la exactitud y totalidad de la información, evitando alteraciones no autorizadas.
- **Disponibilidad:** Asegurar que los usuarios autorizados tengan acceso a la información y recursos de red siempre que lo requieran.

## 2. DIAGNÓSTICO: PRINCIPALES RIESGOS EN INTERNET

Con base en las alertas tempranas de ciberseguridad nacional, los riesgos se clasifican en tres categorías críticas:

### A. Amenazas Técnicas y de Infraestructura (Riesgo Alto)

- **Malware y Ransomware:** Software malicioso diseñado para infiltrarse en la red corporativa, cifrar bases de datos y exigir un rescate económico.
- **Ataques a la Capa de Red:** Intrusiones en enrutadores, firewalls o servidores aprovechando vulnerabilidades técnicas no corregidas.
- **Fuga de Datos:** Exposición o pérdida de datos confidenciales, violando las directrices de la Ley 1581 de Protección de Datos Personales.

### B. Amenazas por Ingeniería Social (Riesgo Medio-Alto)

- **Phishing:** Uso de correos, mensajes o enlaces fraudulentos que suplantan a entidades de confianza para robar credenciales.
- **Suplantación de Sitios Web:** Clonación de portales web institucionales o financieros para capturar datos de transacciones de forma ilícita.

### C. Riesgos de Interacción Humana y Convivencia Digital

- **Ciberacoso y Grooming:** Acoso en entornos digitales y manipulación de usuarios vulnerables o menores de edad.
- **Sexting y Sexpreading:** Difusión no consentida de contenido íntimo, comprometiendo la integridad y el entorno seguro de la organización.

## 3. PROTOCOLOS DE PREVENCIÓN SEGÚN EL MINTIC

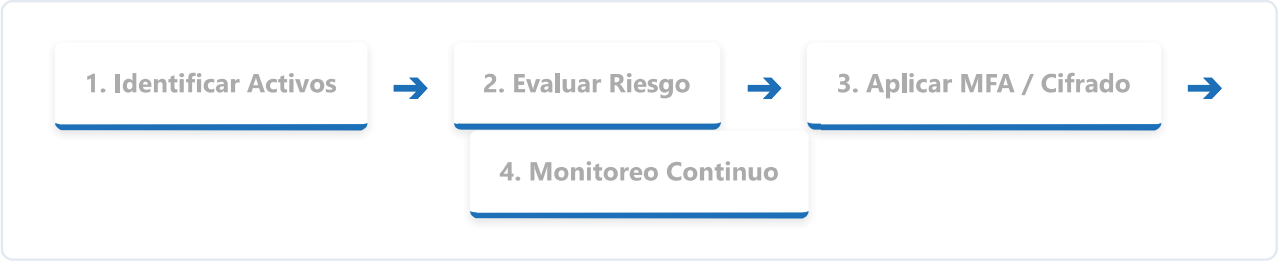
Bajo el enfoque de gestión de riesgos basado en el ciclo PHVA (Planear, Hacer, Verificar, Actuar) del MSPI, se establecen los siguientes controles preventivos de adopción obligatoria:

### Controles Técnicos en la Infraestructura

- **Cifrado y VPN:** Implementación obligatoria de certificados HTTPS y túneles VPN cifrados para todo el tráfico de la red local y remota.
- **Autenticación Multifactor (MFA):** Activación de doble factor de verificación en todas las cuentas corporativas y accesos de administración.
- **Actualización de Parches:** Automatización semanal de parches críticos en firmware de red, servidores y sistemas operativos de escritorio.
- **Seguridad Perimetral:** Configuración estricta de Firewalls y sistemas de detección de intrusos (IDS/IPS) en los nodos de la red.

### Controles de Comportamiento del Usuario

- **Redes Wi-Fi Públicas:** Prohibición estricta de conexiones a redes públicas abiertas para ejecutar tareas de la organización.
- **Gestión de Privacidad:** Restricción estricta de la sobreexposición de datos logísticos, ubicaciones o software interno en redes sociales.
- **Higiene Digital:** Verificación estricta de dominios antes de interactuar con archivos adjuntos o enlaces externos recibidos.




## 4. PROTOCOLO DE REACCIÓN ANTE INCIDENTES DE SEGURIDAD

Acorde a la Guía de Gestión de Incidentes del MinTIC (alineada con la norma ISO/IEC 27035), ante la materialización de un ataque se debe ejecutar el siguiente procedimiento secuencial:

| Fase | Acción Requerida | Responsable / Herramienta |
|---|---|---|
| **1. Identificación** | Detección y registro de anomalías en el tráfico de red, bloqueos o alertas de antivirus. | Administrador de Red / SOC |