Tabla de contenido

1. Propósito

El presente documento tiene como objetivo primordial establecer el marco normativo y operativo para la **protección de la infraestructura de red y comunicaciones** del H. Ayuntamiento de Morelia. En un entorno gubernamental donde la interconectividad es vital para el servicio ciudadano, esta política busca garantizar que el intercambio de información ocurra bajo niveles estrictos de confidencialidad, integridad y disponibilidad.

A través de esta política, se persiguen los siguientes objetivos estratégicos:

- **Blindaje de la Infraestructura Crítica:** Establecer los controles necesarios para proteger el perímetro de la red institucional contra accesos no autorizados, intrusiones y ataques de denegación de servicio (DoS) que pudieran paralizar la operación municipal.
- **Aislamiento y Segmentación (Zero Trust):** Implementar una arquitectura de red que evite el movimiento lateral de amenazas, asegurando que los sistemas sensibles (como Tesorería, Catastro y Nómina) operen en entornos lógicamente separados de las redes de uso público o administrativo general.
- **Garantía de la Triada de Seguridad en Tránsito:** Asegurar que cualquier dato que viaje a través de las redes locales, enlaces inalámbricos o conexiones remotas (VPN) esté protegido contra interceptación o modificación malintencionada mediante protocolos de cifrado robustos.
- **Regulación del Uso de Internet y Mitigación de Riesgos Web:** Definir los criterios de filtrado web para prevenir la descarga accidental de malware, el acceso a sitios de phishing y el uso indebido del ancho de banda institucional, alineando el comportamiento digital del colaborador con los objetivos de productividad y seguridad.
- **Cumplimiento Normativo y Legal:** Alinearse con los requisitos de la norma ISO/IEC 27001:2022 (específicamente los controles 8.20 al 8.23) y con las disposiciones de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados, garantizando la custodia segura de la información de los ciudadanos de Morelia durante su transmisión.
- **Resiliencia en las Comunicaciones:** Establecer las bases para un monitoreo continuo que permita detectar anomalías en tiempo real, facilitando una respuesta rápida y coordinada ante cualquier evento de red que ponga en riesgo la continuidad del gobierno digital.

2. Alcance

Esta política es de **cumplimiento obligatorio y aplicación transversal** para toda la estructura organizativa del H. Ayuntamiento de Morelia. Su cobertura se extiende sobre los siguientes dominios:

2.1. Alcance Humano y Organizacional

- **Personal Interno:** Todos los servidores públicos, empleados de confianza, base y personal por honorarios que utilicen los recursos de red institucionales.
- **Terceros y Proveedores:** Prestadores de servicios, consultores externos y proveedores de soporte técnico que requieran acceso a la red (local o remoto) para labores de mantenimiento o implementación.
- **Usuarios Visitantes:** Ciudadanos o externos que hagan uso de los puntos de acceso inalámbricos (Wi-Fi) proporcionados en las áreas de atención pública.

2.2. Alcance Tecnológico e Infraestructura de Comunicaciones

La política rige sobre todos los activos físicos y lógicos que componen el ecosistema de comunicaciones, incluyendo de forma enunciativa mas no limitativa:

- **Capa Perimetral:** Firewalls de nueva generación (NGFW), Firewalls de Aplicaciones Web (WAF), Sistemas de Detección y Prevención de Intrusiones (IDS/IPS) y Balanceadores de Carga.
- **Capa de Conmutación y Ruteo:** Todos los switches (core, distribución y acceso) y routers que gestionan el tráfico de datos.
- **Redes Inalámbricas (WLAN):** Puntos de acceso (APs) y controladores inalámbricos dentro de las dependencias municipales y plazas públicas conectadas.
- **Enlaces de Datos:** Conexiones de fibra óptica, radioenlaces y servicios de internet provistos por terceros (ISPs).
- **Servicios de Red:** Protocolos de resolución de nombres (DNS), asignación de direcciones (DHCP), servicios de directorio (Active Directory) y servidores de archivos.

2.3. Alcance de la Información y Tránsito de Datos

- **Datos en Movimiento:** Todo flujo de información que transite a través de la infraestructura del Ayuntamiento, ya sea de forma interna (LAN) o externa (WAN/Internet).
- **Conectividad Remota:** Sesiones de trabajo a través de túneles cifrados (VPN) y protocolos de escritorio remoto autorizados.
- **Voz y Video:** Tráfico generado por sistemas de Telefonía IP (VoIP), sistemas de videoconferencia institucional y redes de videovigilancia (CCTV).

2.4. Alcance Geográfico y Ambiental

- **Oficinas Centrales y Desconcentradas:** Todas las dependencias físicas pertenecientes al Ayuntamiento, incluyendo Palacios Municipales, delegaciones, módulos de tesorería y centros de mando.
- **Entornos de Teletrabajo:** Cualquier ubicación externa desde la cual un colaborador acceda a la red institucional mediante dispositivos autorizados.

3. Políticas de Seguridad en Redes y Filtrado Web

3.1. Gestión y Control de Infraestructura de Red (Control 8.20)

La Dirección de TI debe asegurar que todos los dispositivos de red operen bajo un estado de máxima seguridad.

- **Configuración Segura (Hardening):** Queda prohibido el uso de configuraciones por defecto. Todo equipo (switch, router, firewall) debe tener contraseñas robustas, servicios innecesarios deshabilitados y protocolos de gestión cifrados (SSH v2, HTTPS, SNMP v3).
- **Control de Puertos Físicos:** Los puertos de red en áreas de acceso público o común deben permanecer desactivados administrativamente. Solo se activarán bajo solicitud formal y para dispositivos previamente registrados en el inventario.
- **Protección contra Intrusiones:** Es obligatorio el uso de sistemas de detección y prevención de intrusiones (IDS/IPS) configurados para bloquear automáticamente patrones de ataque conocidos.

3.2. Seguridad en los Servicios de Red (Control 8.21)

Se debe garantizar que los servicios proporcionados por terceros (ISPs) y los servicios internos de red mantengan la integridad institucional.

- **Acuerdos de Nivel de Servicio (SLA):** Todo contrato con proveedores de internet debe incluir cláusulas de seguridad y disponibilidad mínima del 99.9%.
- **Protocolos Seguros:** Se prohíbe el tránsito de información sensible a través de protocolos claros (HTTP, FTP, Telnet). Es mandatorio el uso de versiones cifradas (HTTPS, SFTP, SSH).

- **Integridad del DNS:** Se deben implementar mecanismos de protección para el servicio de nombres de dominio institucional, evitando el envenenamiento de caché o redirecciones maliciosas.
- **Firewall de software libre:** se deben implementar políticas de evaluación y ponderación del uso de software libre para control de tráfico y acceso a redes.

3.3. Segregación de Redes y Segmentación Lógica (Control 8.22)

El Ayuntamiento adopta una arquitectura de **"Defensa en Profundidad"** mediante la segregación lógica de entornos.

- **Arquitectura de VLANs:** La red debe estar segmentada por funciones. Como mínimo, se establecerán VLANs independientes para: **Tesorería/Pagos, Servidores Críticos, Administración General, Telefonía IP y Videovigilancia.**
- **Zona Desmilitarizada (DMZ):** Los servicios expuestos a internet (como el Portal de Trámites de Morelia) deben residir en una DMZ aislada, de modo que un compromiso en la web no permita el acceso directo a la red interna de bases de datos.
- **Aislamiento de Wi-Fi:** La red inalámbrica para invitados/ciudadanos debe estar físicamente o lógicamente separada de la red operativa, sin visibilidad alguna hacia los recursos internos del Ayuntamiento.

3.4. Conectividad Remota y Redes Privadas Virtuales (VPN)

El acceso a la red interna desde el exterior debe ser considerado un riesgo de alta criticidad.

- **Túneles Cifrados:** Todo acceso remoto debe realizarse a través de una VPN con cifrado **AES-256**.
- **Doble Factor de Autenticación (MFA):** Es requisito indispensable el uso de MFA para establecer una conexión VPN. No se autorizarán accesos basados únicamente en usuario y contraseña.
- **Postura de Seguridad del Endpoint:** El sistema de VPN debe validar que el equipo remoto cumpla con requisitos mínimos (antivirus activo y parches al día) antes de permitir la conexión.

3.5. Filtrado de Contenido Web y Control de Navegación (Control 8.23)

El acceso a internet debe ser gestionado para mitigar riesgos de malware y optimizar los recursos institucionales.

- **Bloqueo por Reputación y Categoría:** Se bloqueará el acceso a sitios categorizados como: Phishing, Malware, Juegos de azar, Contenido adulto y servicios de anonimización (Proxies/VPNs comerciales).
- **Listas Negras Dinámicas:** El sistema de filtrado web debe actualizarse diariamente mediante fuentes de inteligencia de amenazas para bloquear dominios maliciosos de reciente aparición.
- **Inspección de Tráfico Cifrado:** El Firewall perimetral deberá realizar la inspección de tráfico SSL/TLS (siempre que la capacidad técnica lo permita) para detectar amenazas ocultas en sitios HTTPS, exceptuando categorías sensibles (Banca y Salud) para proteger la privacidad del usuario.
- **Acceso libre a internet:** el acceso sin restricción a internet cuando sea necesario deberá ser autorizado por el titular de la dependencia, previa evaluación de la Dirección de Tecnologías.

3.6. Monitoreo, Registro y Alertas de Red

La red debe ser "auditable" en todo momento.

- **Recolección de Logs:** Se deben capturar los registros de tráfico, intentos de conexión fallidos y cambios en las tablas de ruteo. Estos logs deben centralizarse y protegerse contra alteración.
- **Análisis de Tráfico:** Se realizarán análisis periódicos de flujo (NetFlow) para identificar comportamientos anómalos que pudieran indicar una fuga de información o la presencia de una botnet dentro de la red municipal.

4. Procedimientos

4.1. Gestión de Reglas en Dispositivos Perimetrales (Firewall/WAF)

Cualquier modificación en las reglas de acceso debe seguir el principio de **"Mínimo Privilegio"**.

1. **Solicitud:** El área interesada debe llenar el formato **F-RED-01**, justificando la necesidad técnica de apertura (Puerto, IP origen, IP destino y protocolo).
2. **Análisis de Riesgo:** El administrador de red evalúa si la apertura compromete la seguridad de la zona (VLAN). Se prioriza siempre el uso de puertos estándar y seguros.
3. **Implementación Temporal:** De ser posible, las reglas se habilitarán con una fecha de expiración para evitar la acumulación de "puertas abiertas" innecesarias.

4. **Registro:** Se guarda el log del cambio en la bitácora de administración del equipo.

4.2. Aprovisionamiento y Mantenimiento de VLANs

Para asegurar la segregación efectiva:

1. **Mapeo de Puerto:** Antes de conectar un equipo en una oficina, el técnico de TI debe identificar a qué departamento pertenece y asignar el puerto del switch a la VLAN correspondiente (ej. VLAN 10 para Tesorería, VLAN 20 para Administración).
2. **Hardening Pre-conexión:** Ningún dispositivo de red nuevo entrará en producción sin haber cambiado la contraseña de fábrica y actualizado el firmware a la versión estable recomendada por el fabricante.
3. **Revisión de Puertos:** Mensualmente, se realizará un escaneo de los switches para identificar puertos activos que no tengan un dispositivo registrado en el inventario, procediendo a su desactivación inmediata.

4.3. Gestión de Accesos Remotos (VPN)

1. **Solicitud y Validación:** El colaborador solicita el acceso remoto. TI verifica que el dispositivo desde el que se conectará (laptop institucional) cuente con el antivirus **Bitdefender** actualizado y los parches de seguridad al día.
2. **Configuración de MFA:** Se enrola al usuario en la plataforma de autenticación de doble factor. El usuario no podrá establecer la conexión sin el código dinámico (token) generado en su dispositivo autorizado.
3. **Monitoreo de Sesión:** El sistema de VPN registrará la hora de inicio, fin y la dirección IP de origen. Las sesiones inactivas por más de 30 minutos se cerrarán automáticamente.

4.4. Operación del Filtrado Web y Gestión de Excepciones

1. **Actualización de Firmas:** El sistema de filtrado (FortiGuard, Cisco Umbrella, etc.) debe estar configurado para descargar actualizaciones de reputación de sitios cada 24 horas como máximo.
2. **Solicitud de Excepción:** Si un área requiere acceso a un sitio bloqueado (ej. Comunicación Social a plataformas de video), deberá tramitar el formato **F-RED-03**.
3. **Auditoría de Excepciones:** Trimestralmente, se revisará la lista de sitios permitidos por excepción. Si la necesidad laboral ha cesado, el acceso será revocado para mantener la higiene de la red.

4.5. Monitoreo de Tráfico y Respuesta a Anomalías de Red

1. **Dashboard de Red:** Se mantendrá una pantalla de monitoreo activo (NOC) que muestre el consumo de ancho de banda y la salud de los nodos principales.
2. **Detección de Patrones:** Ante picos inusuales de tráfico hacia el exterior (posible exfiltración) o intentos masivos de conexión interna (posible movimiento lateral de un virus), el sistema disparará una alerta al equipo de respuesta.
3. **Aislamiento Preventivo:** Si se detecta un comportamiento anómalo crítico en un nodo, el técnico de guardia tiene la facultad de aislar esa boca de red o VLAN de forma preventiva mientras se realiza la investigación bajo el procedimiento de **Gestión de Incidentes**.

5. Definiciones

- **DMZ (Zona Desmilitarizada):** Segmento de red aislado que contiene los servicios del Ayuntamiento que deben ser accesibles desde internet (ej. el portal de trámites), evitando que un atacante salte directamente a la red interna.
- **Firewall de Nueva Generación (NGFW):** Dispositivo de seguridad que, además de filtrar puertos e IPs, tiene la capacidad de inspeccionar el contenido de los paquetes (Deep Packet Inspection) para detectar malware o intrusiones.
- **IDS/IPS (Sistema de Detección y Prevención de Intrusiones):** Herramientas que monitorean el tráfico de red en busca de actividades maliciosas o violaciones de políticas, bloqueándolas en tiempo real.
- **MFA (Autenticación Multi-factor):** Control que requiere que el usuario presente dos o más evidencias para validar su identidad (algo que sabe: contraseña; y algo que tiene: un token digital).
- **Segmentación de Red:** Práctica de dividir una red de computadoras en subredes (VLANs), cada una con sus propios controles de seguridad, para reducir la superficie de ataque.
- **VPN (Red Privada Virtual):** Tecnología que crea un túnel cifrado y seguro a través de una red pública (internet), permitiendo que un colaborador trabaje de forma remota como si estuviera dentro del Ayuntamiento.

6. Formatos

Para que la gestión de redes sea auditable y ordenada, se deben utilizar los siguientes registros:

- **F-RED-01: Solicitud de Cambios en Reglas de Firewall y Puertos.**

- *Uso:* Documentar quién pidió un cambio, por qué motivo técnico y quién lo autorizó.

- **F-RED-02: Matriz de Direccionamiento IP y Mapa de VLANs.**
  - *Uso:* El inventario técnico que describe qué dependencias están en qué segmento de red.
- **F-RED-03: Solicitud de Excepción de Filtrado Web.**
  - *Uso:* Registro de usuarios que requieren acceso a categorías bloqueadas por razones laborales específicas.
- **F-RED-04: Bitácora de Monitoreo y Alertas de Red.**
  - *Uso:* Historial de incidencias detectadas por el sistema de monitoreo y las acciones tomadas.

7. Relación Normativa (ISO 27001:2022)

Este documento asegura el cumplimiento de los controles de red más exigentes de la norma internacional:

Control	Título	Justificación del Cumplimiento
8.20	**Seguridad en redes**	Se cumple mediante el endurecimiento (hardening) de dispositivos y el uso de protocolos cifrados.
8.21	**Servicios de red**	Se garantiza a través de la gestión de SLAs con proveedores de internet y la seguridad en servicios DNS/DHCP.
8.22	**Segregación de redes**	Se materializa con la arquitectura de VLANs y el aislamiento de la red Wi-Fi ciudadana de la administrativa.
8.23	**Filtrado web**	Se cumple con la política de bloqueo por categorías y la inspección de tráfico malicioso en la web.