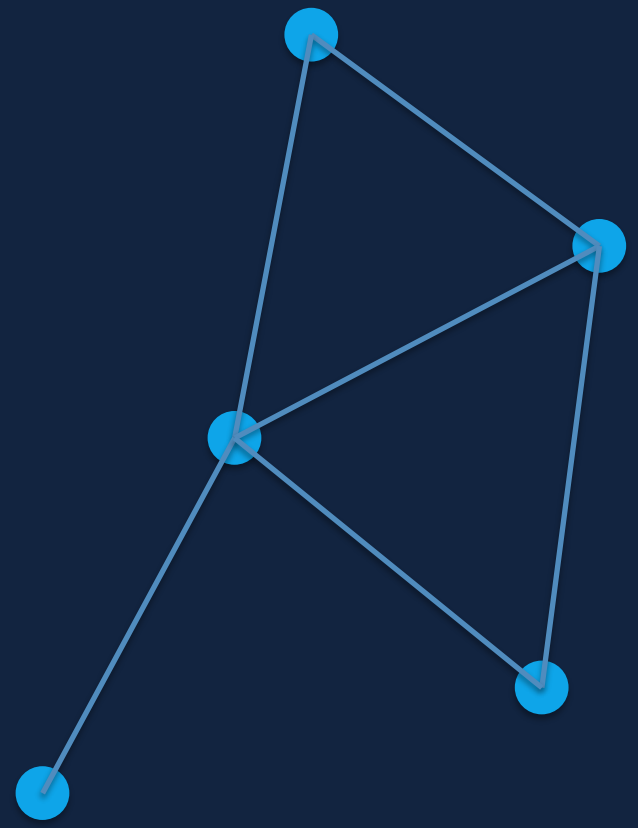
POLÍTICAS PARA LA GESTIÓN DE REDES

Seguridad • disponibilidad • rendimiento • control



¿Qué es la gestión de redes?

1 Supervisar

Observar disponibilidad, rendimiento, capacidad y eventos.

2 Configurar

Administrar routers, switches, AP, firewalls y servicios.

3 Proteger

Reducir riesgos, controlar accesos y responder a incidentes.

4 Optimizar

Detectar cuellos de botella y mejorar el uso de recursos.

5 Documentar

Registrar configuraciones, cambios, inventario y procedimientos.

¿Qué es una política de gestión de redes?

✓ **Definición**

Conjunto de reglas, criterios y procedimientos que orientan cómo se utiliza, administra, protege y supervisa una red.

✓ **¿Para qué sirve?**

Establece qué está permitido, quién puede realizar acciones, qué controles deben aplicarse y cómo actuar ante riesgos.

Debe alinearse con los objetivos de la organización.

Debe ser conocida por las personas a quienes aplica.

Debe poder verificarse mediante controles, registros o auditorías.

Debe revisarse cuando cambian tecnologías, riesgos o requisitos.

Objetivos de las políticas de red

1 Seguridad

Confidencialidad, integridad y protección.

2 Disponibilidad

Mantener servicios accesibles y operativos.

3 Rendimiento

Usar recursos de red eficientemente.

4 Control

Definir permisos, responsabilidades y cambios.

5 Continuidad

Reducir impacto de fallas e incidentes.

6 Cumplimiento

Atender normas y requisitos internos.

Las políticas deben equilibrar seguridad y productividad: controlar sin obstaculizar innecesariamente el trabajo.

Principales tipos de políticas

1 Acceso y autenticación

Usuarios, contraseñas, MFA, privilegios y acceso remoto.

2 Uso aceptable

Navegación, aplicaciones, descargas y BYOD.

3 Seguridad

Firewall, segmentación, actualizaciones y protección.

4 Dispositivos de red

Configuración segura, inventario, respaldos y cambios.

5 Monitoreo y registros

Logs, alertas, métricas, retención y revisión.

6 Continuidad

Redundancia, respaldos, recuperación y pruebas.

Dependiendo del contexto de la empresa, la gestión de redes se divide en tres enfoques principales:

1. Políticas de Seguridad de la Red (Ciberseguridad)

Establecen los lineamientos para monitorear, gestionar y proteger la infraestructura frente a accesos no autorizados o amenazas externas: Control de acceso, cifrado de datos, uso de cortafuegos, respuesta a incidentes

2. Políticas de Gestión de Tráfico y Administración Técnica

Se enfocan en el rendimiento del sistema y las buenas prácticas del área de TI para que la red funcione de forma continua y veloz: Optimización en caso de saturación, Monitoreo constante, Control de cambios y configuraciones.

3. Políticas de Uso Aceptable (Para Empleados)

Regulan la interacción humana con los recursos de conectividad de la compañía: Restricción de contenidos, Medidas disciplinarias, Uso profesional.

Política de acceso a la red

Crear cuentas individuales; evitar cuentas compartidas.

Aplicar mínimo privilegio: cada usuario recibe solo los permisos necesarios.

Usar contraseñas robustas y, cuando sea posible, autenticación multifactor (MFA).

Definir condiciones para acceso remoto: dispositivos autorizados, cifrado y autenticación.

Revisar periódicamente cuentas, privilegios y accesos de personas que cambian de función.

i Ejemplo de regla

El acceso administrativo a dispositivos de red deberá realizarse mediante cuentas personales, autenticación fuerte y canales seguros.

Pregunta: ¿qué podría ocurrir si un administrador comparte su contraseña con otra persona?

Política de seguridad de la red

A Segmentación

Separar redes por funciones o niveles de confianza.

B Firewall

Definir y revisar reglas de tráfico según necesidad y riesgo.

C Actualizaciones

Aplicar parches y actualizaciones de seguridad.

D Protección

Desactivar servicios innecesarios y proteger endpoints.

E Cifrado

Proteger información sensible en tránsito.

F Vulnerabilidades

Identificar, priorizar, corregir y verificar.

Política de uso aceptable

✓ Uso permitido

Utilizar los recursos de red para actividades académicas o laborales autorizadas, respetando las normas internas.

! Uso restringido

Evitar actividades que introduzcan malware, comprometan la seguridad, saturen recursos o infrinjan derechos.

Definir reglas para instalación de software y extensiones.

Regular USB y dispositivos personales (BYOD).

Establecer criterios para redes Wi-Fi de invitados.

Comunicar consecuencias del incumplimiento y proceso de reporte.

Monitoreo, registros y métricas

Disponibilidad: porcentaje de tiempo operativo de los servicios.

Rendimiento: latencia, pérdida de paquetes, utilización de enlaces y capacidad.

Seguridad: intentos de acceso, eventos sospechosos, bloqueos y alertas.

Configuración: cambios, errores y desviaciones respecto a la línea base.

Logs: conservarlos durante el periodo definido y protegerlos contra alteraciones.

M Ejemplo de indicador

Disponibilidad mensual

99.9%

No basta con medir: deben existir umbrales, responsables y acciones ante desviaciones.

Checklist de una buena política

- ✓ ¿Tiene un objetivo claro?
- ✓ ¿Define a quién aplica?
- ✓ ¿Es específica y comprensible?
- ✓ ¿Indica responsabilidades?
- ✓ ¿Puede verificarse?
- ✓ ¿Considera excepciones y escalamiento?
- ✓ ¿Se revisa periódicamente?
- ✓ ¿Está alineada con los riesgos de la organización?

Una política útil no es un documento decorativo: orienta decisiones y se traduce en controles y acciones concretas.

Caso práctico: “Red sin reglas”

APLICACIÓN

! Situación

Una empresa de 80 personas presenta:

- Usuarios comparten contraseñas.
- Equipos de red con configuraciones antiguas.
- Nadie registra los cambios.
- Wi-Fi de invitados comparte segmentos con sistemas internos.
- Incidentes reportados informalmente.
- No existen respaldos periódicos de configuraciones.

? Reto

Propongan al menos 6 políticas para reducir los riesgos.

Para cada política indiquen:

1. Nombre.
2. Regla principal.
3. Responsable.
4. Cómo se verificará.
5. Riesgo que reduce.