**Evaluación de la Situación Actual**

**Alcance de la Red Actual**

1. **Dispositivos:** La red actual consta de un router, un switch y cuatro dispositivos finales.
2. **Topología:** La red parece tener una topología en estrella simple, con el router en el centro y el switch conectado a este para distribuir la conexión a los dispositivos finales.

**Problemas Potenciales**

1. **Rendimiento:**
   * **Congestión de Red:** A medida que se conecten más dispositivos, es probable que la red actual experimente cuellos de botella y congestión, especialmente con solo un switch gestionando todas las conexiones.
   * **Baja Velocidad de Transmisión:** Los dispositivos podrían experimentar velocidades de transmisión reducidas debido a la falta de segmentación y recursos insuficientes.
2. **Seguridad:**
   * **Falta de Segmentación:** Sin subredes, es más fácil para un atacante moverse lateralmente una vez que haya comprometido un dispositivo.
   * **Falta de Políticas de Seguridad:** La ausencia de políticas y medidas de seguridad específicas deja la red vulnerable a ataques.

**Topología de Red**

**Propuesta de Topología**

1. **Topología Jerárquica:** Utilizar una topología de red jerárquica que incluya un router central, switches de distribución y switches de acceso para cada subred.
2. **Conexiones:**
   * **Router Central:** Conectar un router central al switch principal.
   * **Switches de Distribución:** Conectar switches de distribución al router central para cada departamento.
   * **Switches de Acceso:** Conectar switches de acceso a los switches de distribución para distribuir la conexión a los dispositivos en cada departamento.

**Equipos de Red**

**Dispositivos Necesarios**

1. **Router:**
   * Capacidad para gestionar múltiples subredes.
   * Soporte para VLANs (Virtual LANs).
   * Soporte para QoS (Quality of Service) para priorizar el tráfico.
2. **Switches:**
   * Switches de distribución y de acceso con soporte para VLANs.
   * Switches gestionables para permitir la configuración de seguridad y QoS.
3. **Firewalls:**
   * Firewall dedicado para proteger la red contra amenazas externas.
4. **Servidores:**
   * Un servidor privado para cada subred.
   * Un servidor adicional en el departamento de Tecnología accesible desde todas las subredes.
5. **Access Points:** Si se requiere conectividad inalámbrica, instalar access points con soporte para WPA3 y configuración de SSID por departamento.

**Especificaciones Técnicas**

* **Router:** Capacidad de procesamiento alta, múltiples interfaces gigabit, soporte para IPv6.
* **Switches:** Switches gestionables con al menos 48 puertos gigabit, soporte para PoE si se usan dispositivos que lo requieran.
* **Firewall:** Firewall con capacidad para inspección de paquetes profunda (DPI), gestión de amenazas unificada (UTM).

**Seguridad de la Red**

**Medidas de Seguridad**

1. **Segmentación de Red:**
   * Crear VLANs para cada subred: Marketing, Tecnología y Contabilidad.
2. **Políticas de Seguridad:**
   * Implementar políticas de acceso basado en roles (RBAC).
   * Políticas de contraseña fuertes y autenticación multifactor (MFA).
3. **Configuración de Firewall:**
   * Reglas de firewall para permitir solo el tráfico necesario entre subredes.
   * Configuración de VPN para acceso remoto seguro.
   * Monitoreo de tráfico y alertas de actividad sospechosa.

**Políticas de Personal**

1. **Capacitación:** Capacitar al personal sobre buenas prácticas de seguridad, phishing y manejo de información sensible.
2. **Acceso:** Limitar el acceso a áreas críticas de la red basado en roles y necesidades.

**Gestión de la Red**

**Herramientas de Gestión**

1. **Sistema de Gestión de Red (NMS):** Implementar un NMS como SolarWinds, PRTG o Nagios para monitorear el rendimiento de la red, alertas y gestión de configuración.
2. **Herramientas de Monitoreo:**
   * Monitoreo de tráfico en tiempo real.
   * Análisis de logs y auditorías de seguridad.

**Plan de Implementación**

**Cronograma**

1. **Fase 1: Evaluación y Planificación**
   * Duración: 1 semana
   * Actividades: Auditoría de red, compra de equipos, planificación de la implementación.
2. **Fase 2: Instalación de Equipos**
   * Duración: 2 semanas
   * Actividades: Instalación de routers, switches, firewalls y servidores.
3. **Fase 3: Configuración y Pruebas**
   * Duración: 1 semana
   * Actividades: Configuración de VLANs, políticas de seguridad, reglas de firewall, pruebas de conectividad.
4. **Fase 4: Implementación Final y Capacitación**
   * Duración: 1 semana
   * Actividades: Implementación de cambios, capacitación al personal, pruebas de estrés.

**Comunicación de Cambios**

* **Reuniones Informativas:** Reuniones con los departamentos para explicar los cambios.
* **Documentación:** Proporcionar manuales y guías de usuario para los nuevos sistemas.

**Mantenimiento Continuo**

**Medidas de Mantenimiento**

1. **Actualizaciones:** Mantener los dispositivos y software actualizados con los últimos parches de seguridad.
2. **Monitoreo:** Monitoreo continuo de la red para detectar y responder a problemas rápidamente.
3. **Auditorías de Seguridad:** Realizar auditorías de seguridad periódicas.

**Políticas de Seguridad y Respuesta a Incidentes**

* **Políticas de Seguridad:** Implementar políticas claras de uso aceptable, gestión de contraseñas y acceso remoto.
* **Procedimientos de Respuesta:** Establecer procedimientos claros para la respuesta a incidentes de seguridad, incluyendo planes de contingencia.

**Evaluación del Éxito**

**Métricas de Evaluación**

1. **Rendimiento:**
   * Velocidad de transmisión.
   * Latencia.
   * Disponibilidad de la red.
2. **Seguridad:**
   * Número de incidentes de seguridad reportados.
   * Eficacia de las políticas de seguridad implementadas.
3. **Satisfacción del Usuario:**
   * Encuestas de satisfacción a los empleados.
   * Reducción de quejas relacionadas con la red.