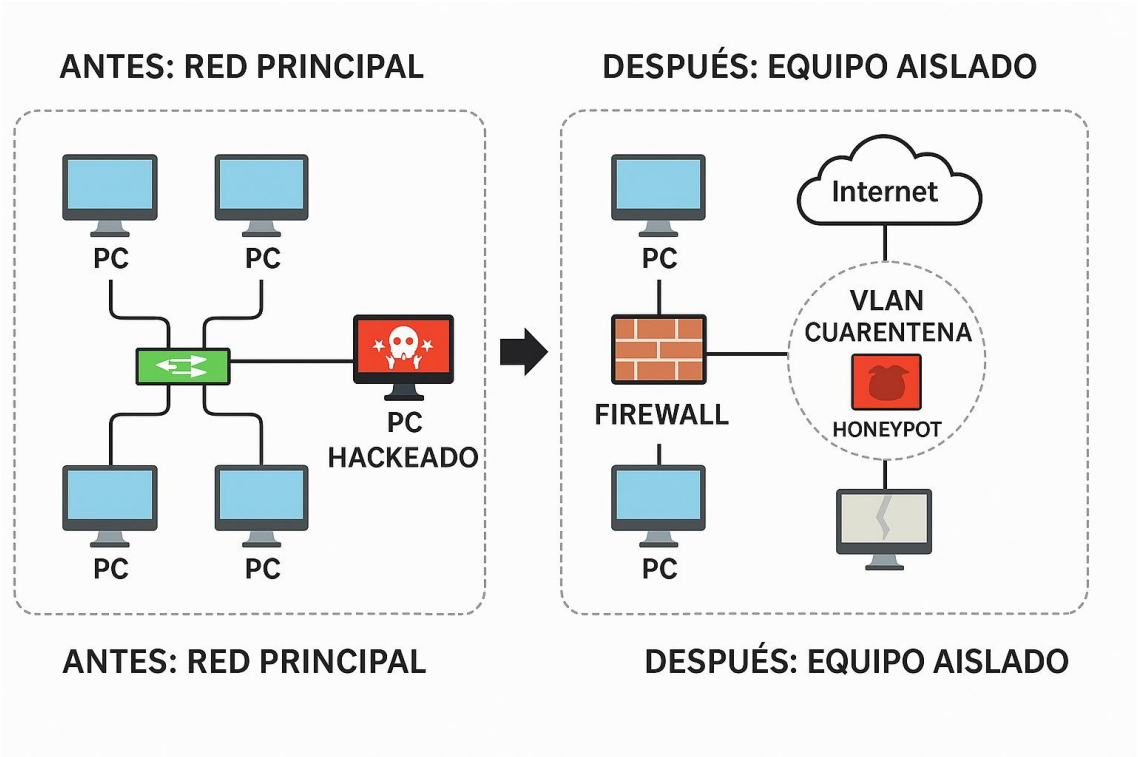
PROYECTO FINAL: DIAGRAMA DE RED



Informe sobre la Tipología de Aislamiento de Equipos en Redes

1. Introducción En el presente informe se describe la metodología utilizada para mejorar la seguridad de una red tras la detección de un equipo comprometido. Se ha optado por una estrategia de aislamiento del equipo mediante la implementación de VLAN de cuarentena, firewalls y honeypots.

2. Tipología de Red Elegida La solución implementada se basa en el aislamiento del equipo comprometido en una VLAN de cuarentena. Se han realizado las siguientes acciones:

- **Antes:** Todos los equipos estaban conectados a la red principal sin ningún mecanismo de contención, permitiendo que un equipo hackeado tuviera acceso a otros dispositivos.
- **Después:** Se implementó un firewall para regular el tráfico y un sistema de VLAN de cuarentena donde el equipo sospechoso es aislado, impidiendo su comunicación con la red principal. Adicionalmente, se integró un honeypot para monitorear actividades maliciosas.

3. Propósito de la Implementación El objetivo principal de esta tipología es contener y mitigar amenazas provenientes del equipo comprometido, evitando la propagación de malware o ataques dentro de la infraestructura de la red. Además, permite la investigación de ataques a través del honeypot sin poner en riesgo los recursos principales.

4. Medidas de Seguridad Implementadas

- **Firewall:** Se instaló para restringir el tráfico entre la red principal y la VLAN de cuarentena, permitiendo solo conexiones seguras y previamente autorizadas.
- **VLAN de Cuarentena:** Aislamiento automático del equipo sospechoso para evitar la propagación de amenazas.
- **Honeypot:** Implementación de un señuelo de seguridad para analizar ciberataques sin comprometer la infraestructura.
- **Segmentación de Red:** Reducción de la superficie de ataque al separar el tráfico de los dispositivos comprometidos.
- **Monitoreo Activo:** Inspección continua del tráfico para detectar comportamientos anómalos.

5. Conclusión Esta metodología mejora significativamente la seguridad de la red, minimizando riesgos y permitiendo una mejor gestión de incidentes. Gracias a la implementación de firewalls, VLAN de cuarentena y honeypots, se garantiza una protección efectiva contra amenazas cibernéticas, asegurando la integridad de la infraestructura TI.