Seguridad perimetral informatica

Emilio Cabo Gomis

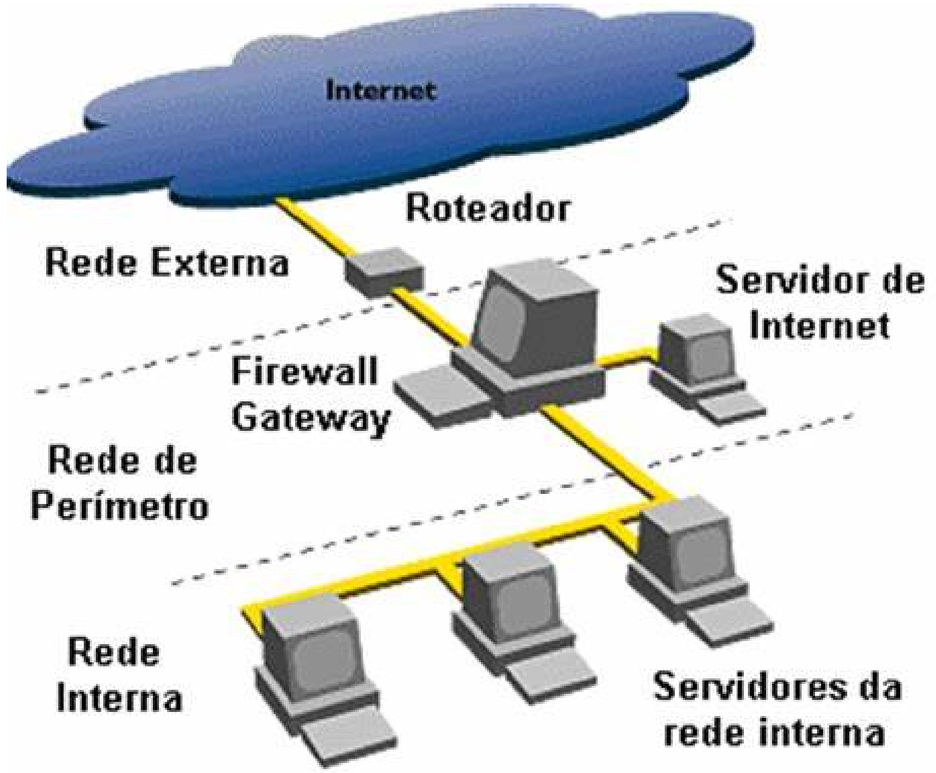
Definición

La seguridad perimetral informática es el proceso de proteger el perímetro de una red mediante una combinación de software, dispositivos y técnicas. Este concepto es crucial para proteger los activos de una organización frente a amenazas externas.

perímetro de red

- El perímetro de red separa la intranet privada de una empresa del mundo público (Internet).

- Es esencial para mantener la información confidencial fuera del alcance de personas maliciosas.



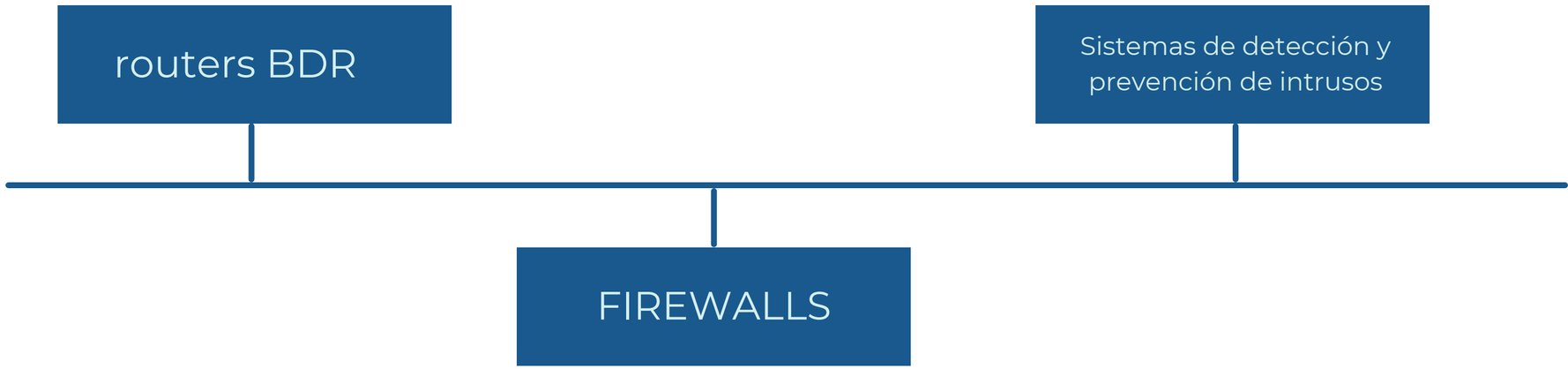
el avance de la teconologia como las tecnologias cloud hace que el contepto del perímetro de red varíe.
Es necesario adaptarse

importancia

- Protege contra hackers, malware y violaciones de datos.

- Es fundamental para la seguridad en entornos de trabajo modernos, especialmente con el aumento del trabajo remoto.

herramientas



buenas practicas

diseño de red

Configurar un diseño seguro que incorpore todos los sistemas y hardware necesarios.

Monitoreo Pasivo y Activo

Utilizar herramientas para rastrear vulnerabilidades y patrones de comunicación.

Zonificación de la Red

Segmentar la red en zonas de seguridad con diferentes niveles de restricción.

Amenazas para la seguridad del permimetro

amenaza1: Malware (virus, spyware, ransomware, worms).
amenaza2: empleados maliciosos

phishing

Aplicaciones y dispositivos móviles.

ataques con contraeña

sofware de seguridad obsoleto

monitoreo

pasivo:
- Utiliza dispositivos de seguridad, routers, computadoras, servidores remotos y firewalls para rastrear vulnerabilidades.
- Herramientas de monitoreo pasivo se activan o programan a horas determinadas para rastrear actividades sospechosas.

activo:
- Proporciona una mirada más rigurosa y cubre todas las posibles vulnerabilidades de la red.
- Herramientas de monitoreo activo envían alertas en tiempo real sobre patrones irregulares de tráfico, intentos fallidos de inicio de sesión, etc.

¿Cómo podemos medir la seguridad informática

- Comparar informes y registros de ciberamenazas con los estándares del sector.
- Realizar evaluaciones y análisis frecuentes de sucesos medibles.
- Identificar vulnerabilidades mediante herramientas de gestión de activos.