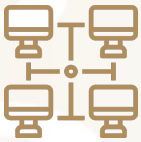
Acciones para aplicar en el Firewall Perimetral

Política de seguridad

Definir una política de seguridad detallada. **Documentar las reglas** específicas para el **firewall**, proporcionando una guía clara para su administración y mejorando la seguridad.



Segmentación de Redes

Dividir la red en segmentos lógicos según la función y la sensibilidad. Configurar zonas de seguridad en el firewall **para controlar el tráfico**, limitando así el impacto potencial de posibles ataques.

Reglas por Principio de Menor Privilegio

Aplicar el **principio de "menor privilegio"** en las reglas del firewall. **Permitir solo el tráfico necesario** para funciones específicas, reduciendo la superficie de ataque y minimizando el riesgo.

Actualizaciones

Mantener **actualizado el firmware y las reglas del firewall**. Aplicar **parches y actualizaciones** para abordar vulnerabilidades y reforzar las defensas contra amenazas emergentes.

Monitoreo

Monitorear eventos de seguridad y **configurar alertas** para identificar intrusiones o comportamientos anómalos, permitiendo una respuesta rápida.

VPN para Acceso Remoto

Implementar VPN para cifrar la comunicación entre dispositivos remotos y la red interna. Proteger las comunicaciones y **evitar accesos no autorizados** a través de **conexiones remotas**. Se deberá **utilizar VPN** para acceder a los **sistemas internos** de la institución. **Evitar exponer** los sistemas a **internet.**

Registro Detallado de Acceso

Mantener **registros detallados de acceso**, incluyendo todas las actividades del firewall. Facilitar la auditoría, la investigación forense y el seguimiento de eventos de seguridad. Activar el **almacenamiento de los logs en un syslog**.

Aplicar el Bloqueo Geográfico

Configurar el bloqueo geográfico en sistemas de uso nacional, que permitan tráfico solo desde direcciones IP asociadas a México. **Bloquear el tráfico entrante de los demás países** en aquellos sistemas que no lo requieran. Esta medida refuerza las defensas, porque limita el acceso a direcciones geográficas específicas, reduciendo así la exposición a amenazas externas.