**Política de Seguridad Perimetral y Firewall Institucional**

1. **Objetivo:**

El objetivo de esta política es establecer directrices claras para el uso, configuración y mantenimiento de los firewalls institucionales con el fin de garantizar la seguridad de la red de la delegación y protegerla contra amenazas cibernéticas.

1. **Responsabilidades**:

El equipo de tecnología de la información será responsable de administrar, configurar y mantener los firewalls institucionales.

Los usuarios y departamentos de la organización deberán cumplir con las políticas y directrices establecidas por el equipo de tecnología de la información.

1. **Configuración del Firewall**:

El firewall se configurará para permitir el tráfico esencial necesario para las operaciones de la organización y bloquear todo el tráfico no autorizado.

El acceso a los servicios y puertos se limitará para realizar tareas laborales.

Se establecerán políticas de filtrado basadas en listas blancas y negras para permitir o bloquear tráfico específico.

1. **Actualizaciones y Parches**:

El firewall se mantendrá actualizado con las últimas actualizaciones y parches de seguridad.

1. **Registros y Auditoría**:

Se registrarán todos los eventos de firewall, incluyendo intentos de acceso no autorizado.

Se revisarán periódicamente los registros del firewall para identificar posibles amenazas o incidentes de seguridad.

1. **Política de Uso**:

Los usuarios no podrán deshabilitar, eludir o modificar la configuración del firewall sin la aprobación del equipo de seguridad de la información.

No se permitirá el uso no autorizado de túneles VPN o conexiones cifradas que eviten el escrutinio del firewall.

1. **Cumplimiento y Auditorías**:

La organización realizará auditorías periódicas de seguridad para garantizar el cumplimiento de esta política.

1. **Sanciones**:

El incumplimiento de esta política puede dar lugar a medidas disciplinarias, que pueden incluir la suspensión o terminación del acceso a la red de la organización.