SafeWork HomeOffice

Prototipo de Seguridad para Teletrabajo en Windows 10/11

7 de abril de 2025

Resumen

Prototipo funcional para Windows 10/11 que automatiza seguridad básica en equipos de home office usando herramientas gratuitas: OpenVPN (VPN), Squid (proxy), Firewall de Windows (PowerShell) y generación de logs con Python. Diseñado para demostrar conceptos de ciberseguridad en un proyecto escolar de 1 mes, sin costos de licencias.

1. Objetivos

1.1. Objetivo General

Implementar un sistema que restrinja el uso no laboral de equipos corporativos mediante:

- Conexión VPN obligatoria (OpenVPN).
- Filtrado de tráfico web (Squid).
- Bloqueo de aplicaciones (Firewall vía PowerShell).
- Registro de actividad (Python + Event Viewer).

1.2. Objetivos Específicos

1. Automatizar la configuración de OpenVPN con servidores gratuitos.
2. Bloquear 5 sitios web no laborales (ej. redes sociales) con Squid.
3. Restringir aplicaciones peligrosas (ej. Torrent) con PowerShell.
4. Generar un reporte diario de actividad en CSV.

2. Alcance

- **SO**: Windows 10/11 Pro (64-bit).
- **Herramientas**: OpenVPN, Squid Portable, Python 3.12, PowerShell.
- **Límites**: No requiere servidor externo (solo demostración local).

3. Justificación

Este proyecto se justifica por:

- **Necesidad empresarial**: 68 % de las PYMEs en México no supervisan equipos en home office (AMIPCI, 2023).
- **Ahorro de costos**: Soluciones comerciales similares cuestan desde $15,000 MXN anuales (ej. Cisco AnyConnect).

- **Impacto académico**: Demuestra la aplicación práctica de:
  - Redes privadas virtuales (VPN).
  - Filtrado de contenido.
  - Seguridad perimetral.
- **Viabilidad técnica**: Todas las herramientas son gratuitas y compatibles con Windows.

4. Marco Teórico

4.1. Seguridad en Teletrabajo

Basado en el modelo **Zero Trust** (NIST SP 800-207), se implementan:

- **Autenticación obligatoria**: VPN con certificados.
- **Principio de mínimo privilegio**: Firewall por aplicación.
- **Monitoreo continuo**: Registro de eventos.

4.2. Herramientas Utilizadas

- **OpenVPN**: Protocolo TLS/SSL con cifrado AES-256.
- **Squid**: Proxy con ACLs (Listas de Control de Acceso).
- **Windows Firewall**: Filtrado de tráfico por reglas.
- **Event Viewer**: Fuente centralizada de logs en Windows.

5. Costos

Cuadro 1: **Desglose de costos (MXN)**

Concepto	**Costo**	**Notas**
OpenVPN	$0	Software open-source
Squid para Windows	$0	Versión portable
Python 3.12	$0	Intérprete gratuito
PowerShell	$0	Incluido en Windows
Servidor VPN gratuito (VPNBook)	$0	Para pruebas
Total	**$0**	

Conclusión

Este prototipo demuestra que es posible implementar controles básicos de seguridad para teletrabajo sin costos, usando herramientas gratuitas y enfocándose en Windows 10/11. Ideal para proyectos académicos con tiempo limitado.