# Implementación de Navegación Segura en Codearts Solutions

## 🔹 Fase 1: Configuración de Proxy y Filtrado de Contenido

```
# Instalar Squid

sudo apt update && sudo apt install squid -y


# Editar configuración principal

sudo nano /etc/squid/squid.conf


# Crear lista negra

echo "badsite.com" | sudo tee /etc/squid/blacklist.txt


# Agregar reglas de acceso en squid.conf

acl blacklist dstdomain "/etc/squid/blacklist.txt"

http_access deny blacklist


# Usar DNS seguro (ejemplo con Cloudflare)

sudo nano /etc/systemd/resolved.conf

# Cambiar DNS=1.1.1.1

sudo systemctl restart systemd-resolved
```

## 🔹 Fase 2: Seguridad en Navegadores y Protección contra Phishing

# Política para bloquear descargas peligrosas (en Windows por GPO o en Linux por configuración de navegador)

# Simulación de phishing (crear HTML falso en Apache)

sudo apt install apache2 -y

sudo nano /var/www/html/phishing.html

# Monitoreo de clics con acceso a logs

sudo tail -f /var/log/apache2/access.log

## 🔹 Fase 3: Monitoreo y Detección de Tráfico Sospechoso

# Instalar Snort (modo IDS)

sudo apt install snort -y

sudo snort -A console -i eth0 -c /etc/snort/snort.conf

# Ver logs de Squid

sudo tail -f /var/log/squid/access.log

# Análisis en tiempo real con Wireshark (modo GUI) o tshark (modo CLI)

sudo tshark -i eth0

# Integración SIEM (ejemplo básico con Wazuh)

curl -sO https://packages.wazuh.com/4.x/wazuh-install.sh

sudo bash wazuh-install.sh -a

## 🔹 Fase 4: Implementación de Políticas y Restricciones en la Red

```
# Bloqueo de puertos no autorizados con UFW
sudo ufw default deny outgoing
sudo ufw allow out 443
sudo ufw allow out 53
sudo ufw enable

# Crear política por departamento (ejemplo con iptables + MAC)
sudo iptables -A INPUT -m mac --mac-source AA:BB:CC:DD:EE:FF -j ACCEPT
sudo iptables -A INPUT -j DROP

# VPN corporativa (ejemplo con OpenVPN)
sudo apt install openvpn -y
sudo systemctl enable openvpn@server
```