Implementación de Navegación Segura en Codearts Solutions

🔹 Fase 1: Configuración de Proxy y Filtrado de Contenido

- Se instala y configura **Squid** como proxy para controlar el tráfico HTTP/HTTPS.
- Se aplican listas negras/blancas para restringir o permitir el acceso a sitios web.
- Se bloquea contenido malicioso mediante reglas de filtrado.
- Se integran DNS seguros como **Cloudflare (1.1.1.1)** o **Google DNS (8.8.8.8)**.

Error común:
Squid no bloquea páginas HTTPS correctamente.
Solución:
Habilitar el filtrado de tráfico HTTPS mediante **SSL Bump** en la configuración.

🔹 Fase 2: Seguridad en Navegadores y Protección contra Phishing

- Se instalan extensiones como **uBlock Origin** y **HTTPS Everywhere**.
- Se restringen scripts y rastreadores maliciosos.
- Se aplican políticas que impiden descargas no autorizadas.
- Se simula un ataque de phishing como prueba de concienciación.

Error común:
Extensiones no instaladas correctamente por políticas corporativas.
Solución:
Aplicar configuración mediante **GPOs (en Windows)** o scripts automatizados en entornos Linux.

🔹 Fase 3: Monitoreo y Detección de Tráfico Sospechoso

- Se implementa **Snort o Suricata** como NIDS.
- Se revisan logs de Squid y herramientas SIEM (como Wazuh).
- Se usa **Wireshark** para analizar tráfico en tiempo real.

Error común:
Demasiadas alertas falsas (false positives).
Solución:
Ajustar las reglas de Snort/Suricata y aplicar listas de exclusión (whitelisting).

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

- Se configura el firewall para bloquear tráfico a sitios no permitidos.
- Se implementa una **VPN corporativa** para navegación segura.
- Se definen políticas por departamento para limitar accesos web.

Error común:
El firewall bloquea sitios legítimos por error.
Solución:
Actualizar y revisar las reglas del firewall, agregando excepciones necesarias.