Auditoría y Fortalecimiento de la Seguridad Wi-Fi en Codearts Solutions

🔹 Fase 1: Análisis de vulnerabilidades en la red Wi-Fi

```
# Instalar herramientas necesarias
sudo apt update && sudo apt install kismet aircrack-ng wireshark -y

# Escanear la red con Kismet (modo monitor)
sudo kismet

# Escanear con airodump-ng en interfaz monitor (ejemplo wlan0mon)
sudo airmon-ng start wlan0
sudo airodump-ng wlan0mon

# Capturar tráfico con Wireshark (modo GUI)
sudo wireshark

# Usar Aircrack-ng para detectar ataques de fuerza bruta
sudo aircrack-ng -a2 -b <BSSID> -w /path/to/wordlist.txt capturefile.cap
```

🔹 Fase 2: Implementación de medidas de seguridad avanzadas

```
# Configurar WPA3/WPA2 en el punto de acceso (ejemplo hostapd.conf)

sudo nano /etc/hostapd/hostapd.conf

# En el archivo hostapd.conf, ajustar:

# wpa=2

# wpa_key_mgmt=SAE WPA-PSK

# rsn_pairwise=CCMP


# Configurar autenticación RADIUS

sudo apt install freeradius -y

sudo nano /etc/freeradius/3.0/clients.conf

# Añadir clientes autorizados (APs)

sudo systemctl restart freeradius


# Filtrado MAC con hostapd.conf

# macaddr_acl=1

# accept_mac_file=/etc/hostapd/accept

sudo nano /etc/hostapd/accept


# Crear lista con MAC autorizadas

echo "AA:BB:CC:DD:EE:FF" | sudo tee -a /etc/hostapd/accept


# Configurar firewall UFW con reglas básicas

sudo ufw enable

sudo ufw deny from <IP no autorizada>
```

🔹 Fase 3: Simulación de ataques y pruebas de seguridad

```
# Simular ataque de de-authentication
sudo aireplay-ng --deauth 10 -a <BSSID> -c <Client MAC> wlan0mon

# Capturar tráfico durante el ataque con Wireshark o tshark
sudo tshark -i wlan0mon -w captura.pcap

# Analizar tráfico para verificar cifrado
sudo tshark -r captura.pcap

# Ejecutar Wifiphisher para ataque de phishing Wi-Fi
sudo apt install wifiphisher -y
sudo wifiphisher
```

🔹 Fase 4: Monitoreo y detección de accesos no autorizados

```
# Instalar y configurar WIDS con Kismet o Snort
sudo apt install kismet snort -y

# Ejecutar Kismet para detección en tiempo real
sudo kismet

# Configurar alertas en firewall (UFW)
sudo ufw logging on
sudo ufw status verbose
```

```
# Monitorear logs de conexiones Wi-Fi
sudo tail -f /var/log/syslog | grep wlan0

# Ajustar reglas para minimizar falsas alertas
# Modificar configuración de Snort o Kismet según documentación
```