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

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

- Escanear la red con Kismet y airodump-ng para identificar dispositivos conectados y puntos de acceso no autorizados.
- Detectar SSID ocultos y redes no autorizadas (Rogue AP).
- Capturar tráfico con Wireshark para verificar intentos de ataque MITM o sniffing.
- Identificar ataques de fuerza bruta en la red con Aircrack-ng.

Error común: No detectar todos los dispositivos ocultos o Rogue AP.
Solución: Usar escaneo prolongado y activar modos promiscuos para captar tráfico pasivo.

🔹 Fase 2: Implementación de medidas de seguridad avanzadas

- Configurar cifrado WPA3 o WPA2-AES para proteger la comunicación inalámbrica.
- Activar autenticación basada en RADIUS para dispositivos empresariales.
- Implementar filtrado MAC y segmentación de red para dispositivos críticos.
- Configurar firewalls y listas de control de acceso (ACLs) para limitar accesos sospechosos.

Error común: Dispositivos no compatibles con WPA3 o RADIUS.
Solución: Planificar actualización de hardware o habilitar compatibilidad mixta temporalmente.

🔹 Fase 3: Simulación de ataques y pruebas de seguridad

- Simular un ataque de de-authentication y evaluar la resistencia de la red.
- Intentar interceptar tráfico con Wireshark y comprobar si los datos están cifrados correctamente.
- Evaluar la seguridad de la red con herramientas de auditoría Wi-Fi como Wifiphisher.

Error común: Fallar al detectar ataques de de-authentication.
Solución: Monitorizar logs del AP y usar alertas automáticas para detectar patrones de ataque.

🔹 Fase 4: Monitoreo y detección de accesos no autorizados

- Configurar un Sistema de Detección de Intrusos Wi-Fi (WIDS) para alertar sobre dispositivos no autorizados.
- Implementar reglas de alerta en el firewall para detectar accesos sospechosos.
- Activar logs y monitoreo en tiempo real de conexiones Wi-Fi.

Error común: Sobrecarga de alertas falsas que dificultan la detección real.
Solución: Ajustar sensibilidad del WIDS y filtrar alertas mediante listas blancas.