



## SIFI WSS

### Records capturados del Assessment:

- ID : 1
- BSSID : 0C-B9-37-4A-F8-CC
- ESSID : NETBEDROOM
- Agente SIFI : 100.64.0.4
- El handshake capturado es :
- Contraseña del AP :
- Tipo de test realizado: WPA/WPA2 Advance



**Valoracion:**  
**SIFI WSS**

Estado	Descripcion
Seguro	Todos los pentest con resultados positivos y ninguna vulnerabilidad detectada
Estable	Al menos un resultado negativo en cualquiera de las funciones principales
Vulnerable	Al menos dos resultados negativos en cualquiera de las funciones principales
Critico	Todos los pentest con resultados negativos en las funciones principales

**Según la tabla de valoración SIFI, el estado de seguridad es:**

**Seguro. Todos los pentest con resultados positivos y ninguna vulnerabilidad detectada.**

## **Políticas de seguridad (Generales)**

### **- Política corporativa:**

Un apéndice adicional a las recomendaciones de seguridad podrían ser las recomendaciones de políticas WLAN corporativas. El auditor puede ayudar al cliente a redactar una política de seguridad de la red inalámbrica si aún no tiene una.

### **- Seguridad física:**

La instalación de unidades de cerramiento para proteger contra el robo y el acceso físico no autorizado a los puntos de acceso puede ser una recomendación. Estas también se utilizan a menudo con fines estéticos.

### **- Declaracion de autoridad:**

Define quien implemento la politica WLAN y la direccion ejecutiva que respalda la politica

### **- Audiencia aplicable:**

Define el publico al que se le aplica la politica, ya sea, empleados, visitantes o contratistas

### **- Evaluacion de riesgos y analisis de amenazas:**

Define los posibles riesgos y amenazas de seguridad inalámbrica y cuál será el impacto financiero en la empresa si se produce un ataque con éxito.

## **Advanced Wireless Security Information:**

- Channel : 9
- Privacy : WPA2
- Cipher : CCMP
- Authentication : PSK

## Recomendaciones para AWSI:

Best practices para PSK:

- Se debera cambiar la contraseña por defecto a una nueva
- Generar una contraseña nueva/diferente para cada tunel VPN
- Usar un generador de contraseñas aleatorias
- Generar una contraseña de 13 o mas caracteres para evitar ataques de fuerza bruta
- Usar una combinacion de caracteres especiales y letras mayusculas en la generacion de la contraseña
- Generar una contraseña nueva/diferente para cada tunel VPN