Actividad de repaso

Recursos para el aprendizaje – Retos – Eje 3

Reto 1 – Parte 1

Los dispositivos router Wi-Fi o dispositivos multipropósito traen por defecto una configuración básica, la cual permite conexión automática a cualquier dispositivo inalámbrico, asignándole una dirección IP y acceso a la red sin ningún tipo de restricción, generando vulnerabilidad a la misma.

El control de acceso a las redes inalámbricas se puede generar por filtrado Mac, SSID Broadcast, y control por DHCP, es importante aclarar que estos tipos de controles no generan seguridad en la red, solamente controlan el acceso a la misma.

El reto 1 consiste en cambiar la configuración que trae por defecto el router Wi-Fi y generar control de acceso de los dispositivos terminales ha dicho medio.

Requisitos:

Simulador Packet tracer

1 router Wi-Fi WRT300

2 equipos portátiles

2 equipos de escritorio

Actividad de repaso

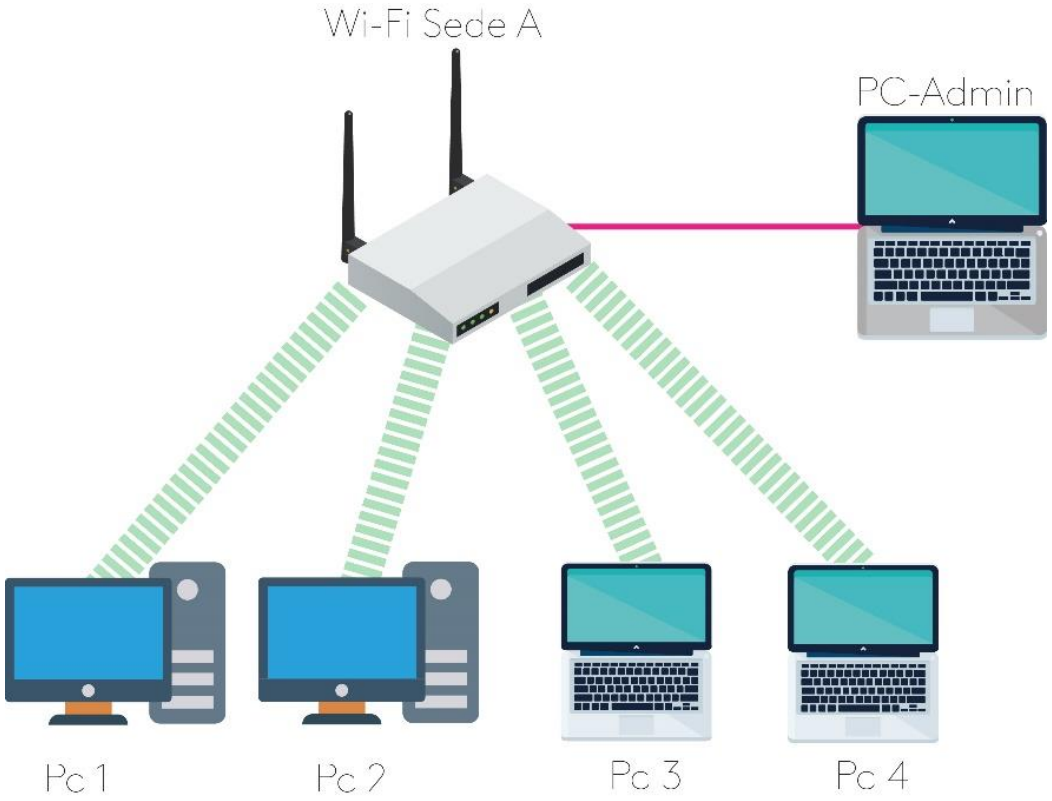

Figura 1. Topología reto 1
Fuente: propia

Recuerde que se debe agregar tarjeta de red inalámbrica a los equipos terminales cuando estos no la traen por defecto.

Desarrollo

1. Elaborar el montaje según la imagen mostrada.

2. Verificar la conectividad entre las máquinas y el router Wi-Fi (si alguna maquina no conecta, se debe revisar la tarjeta de red).

Actividad de repaso

3. Emita el comando IPCONFIG en cada máquina y determine la dirección IP que le ha asignado el router Wi-Fi. Observe la imagen como referencia.

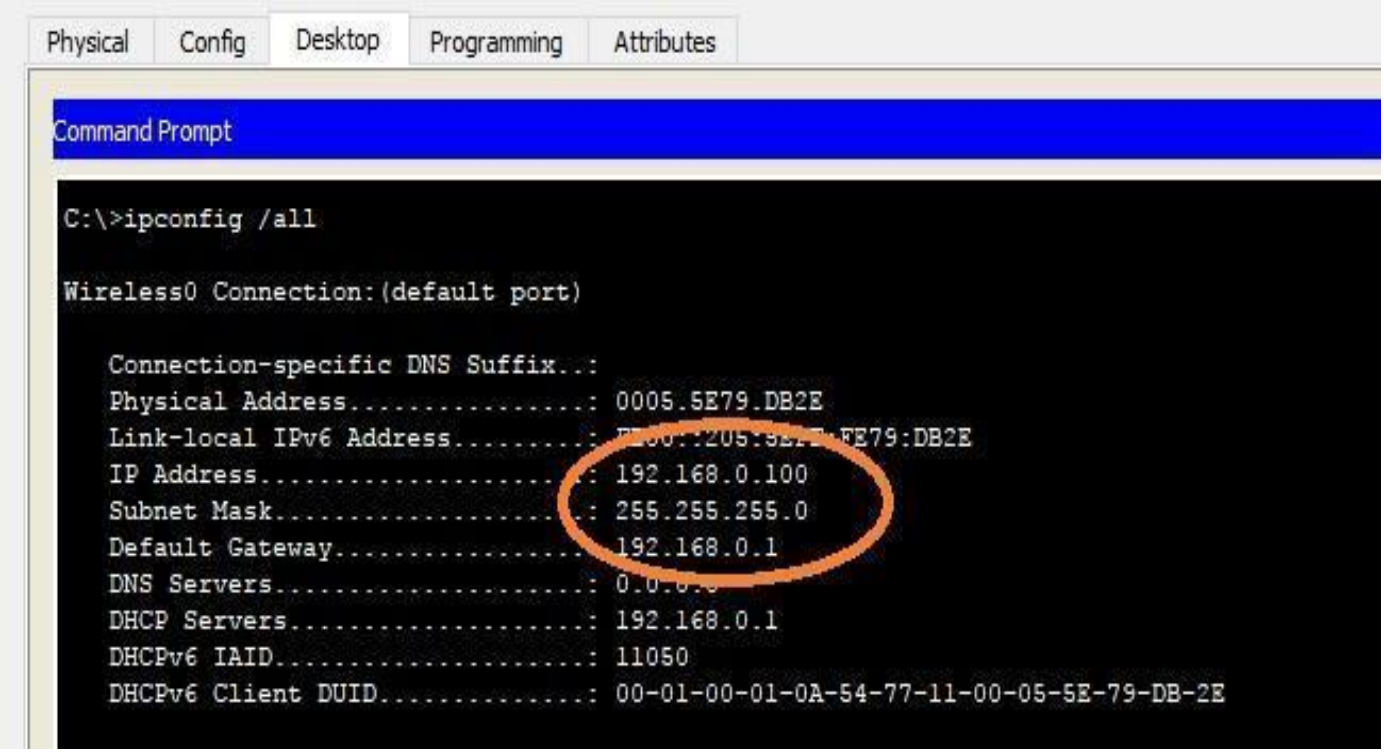

Figura 2. Resultado de emitir IPconfig en el PC1
Fuente: propia

Actividad de repaso

4. Una vez determinada la dirección IP de cada máquina, compruebe conectividad entre las maquinas por medio del comando PING, como se muestra en la imagen siguiente.

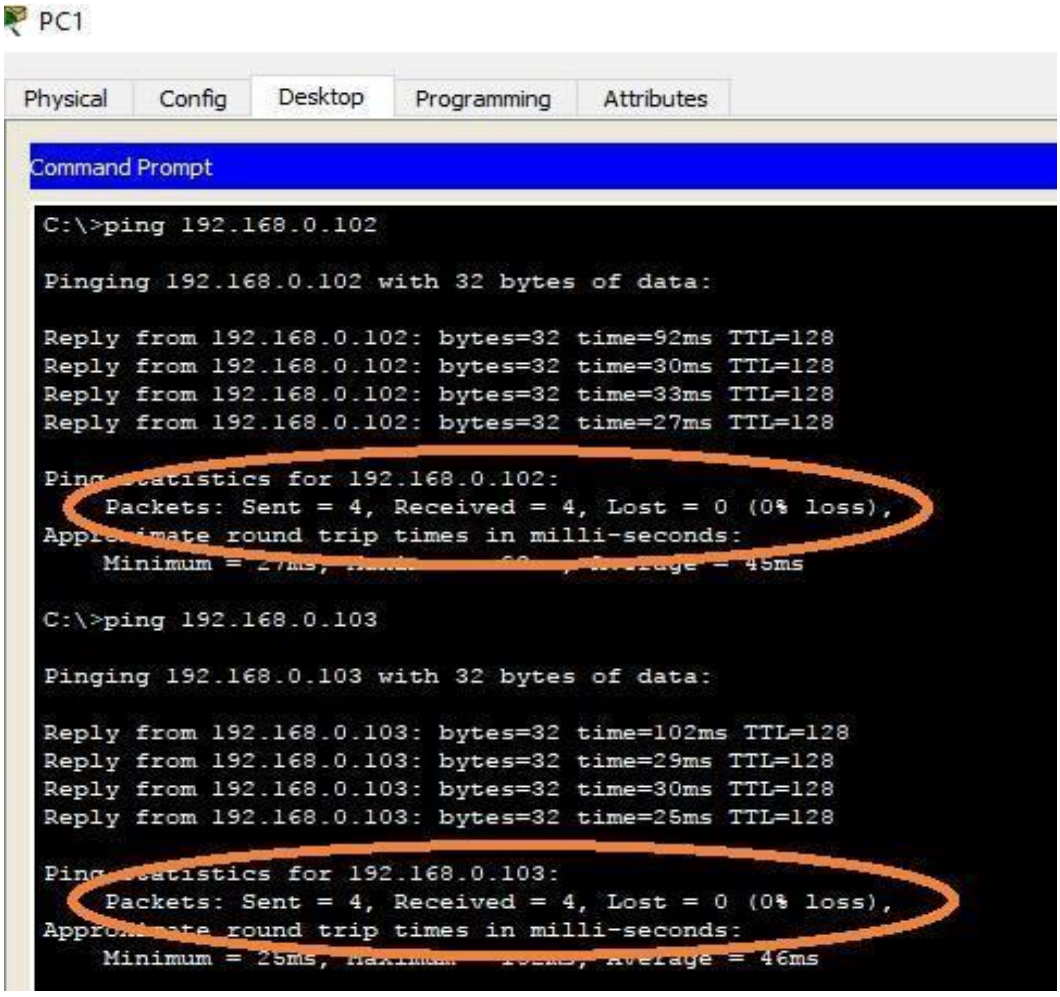

Figura 3. Resultado comando ping
Fuente: propia

Actividad de repaso

5. Acceda a la configuración del router Wi-Fi desde el navegador Web del equipo conectado por cable al router, digitando la dirección IP 192.168.0.1 del router en la URL del navegador, con las credenciales user: "admin" password: "admin", (para acceder a la configuración del router Wi-Fi se recomienda conectarse por cable ya que cada vez que se realice un cambio este se reiniciará).

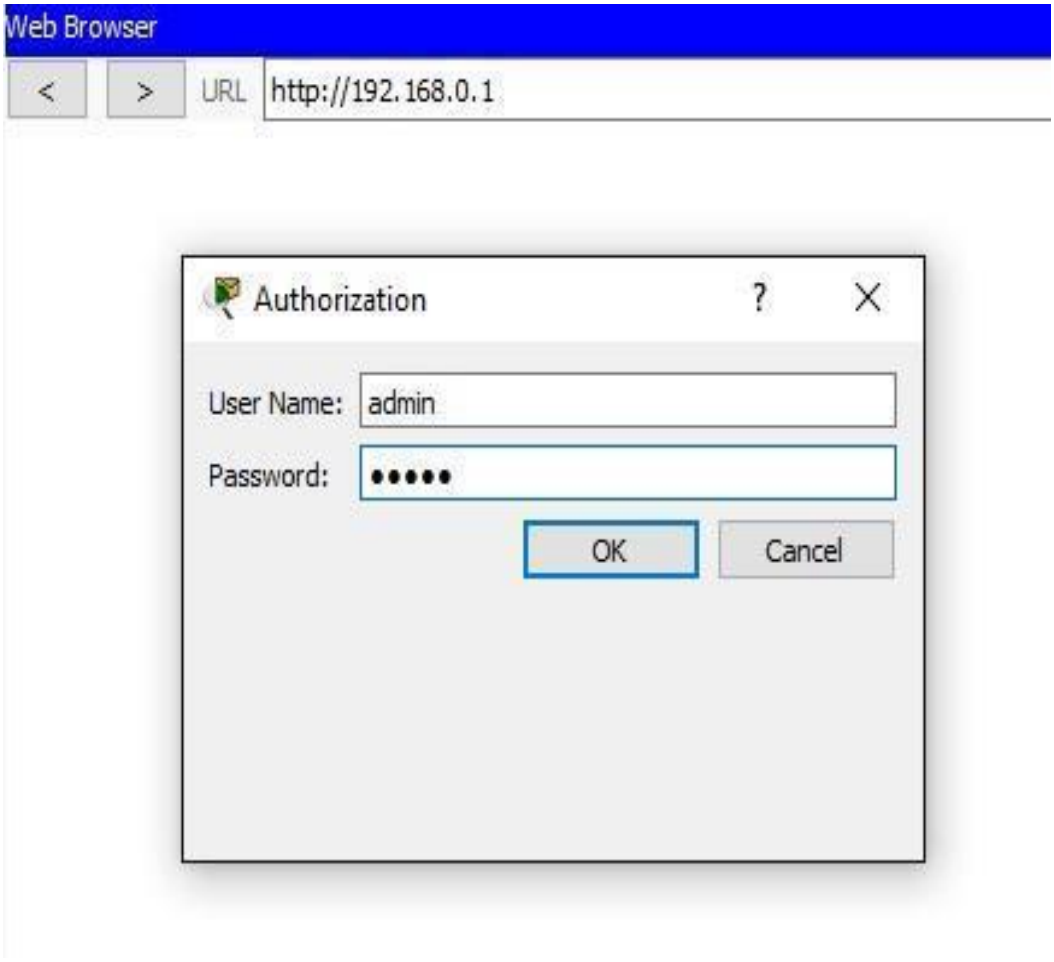

Figura 4. Acceso a router Wi-Fi por navegador Web
Fuente: propia

Actividad de repaso

6. Una vez en la GUI del router Wi-Fi nos ubicamos en la pestaña Wireless – Network Name (SSID) (por defecto trae como SSID "Default"), lo cambiamos por "SEGURIDAD", desactivamos el SSID broadcast y guardamos los cambios realizados.

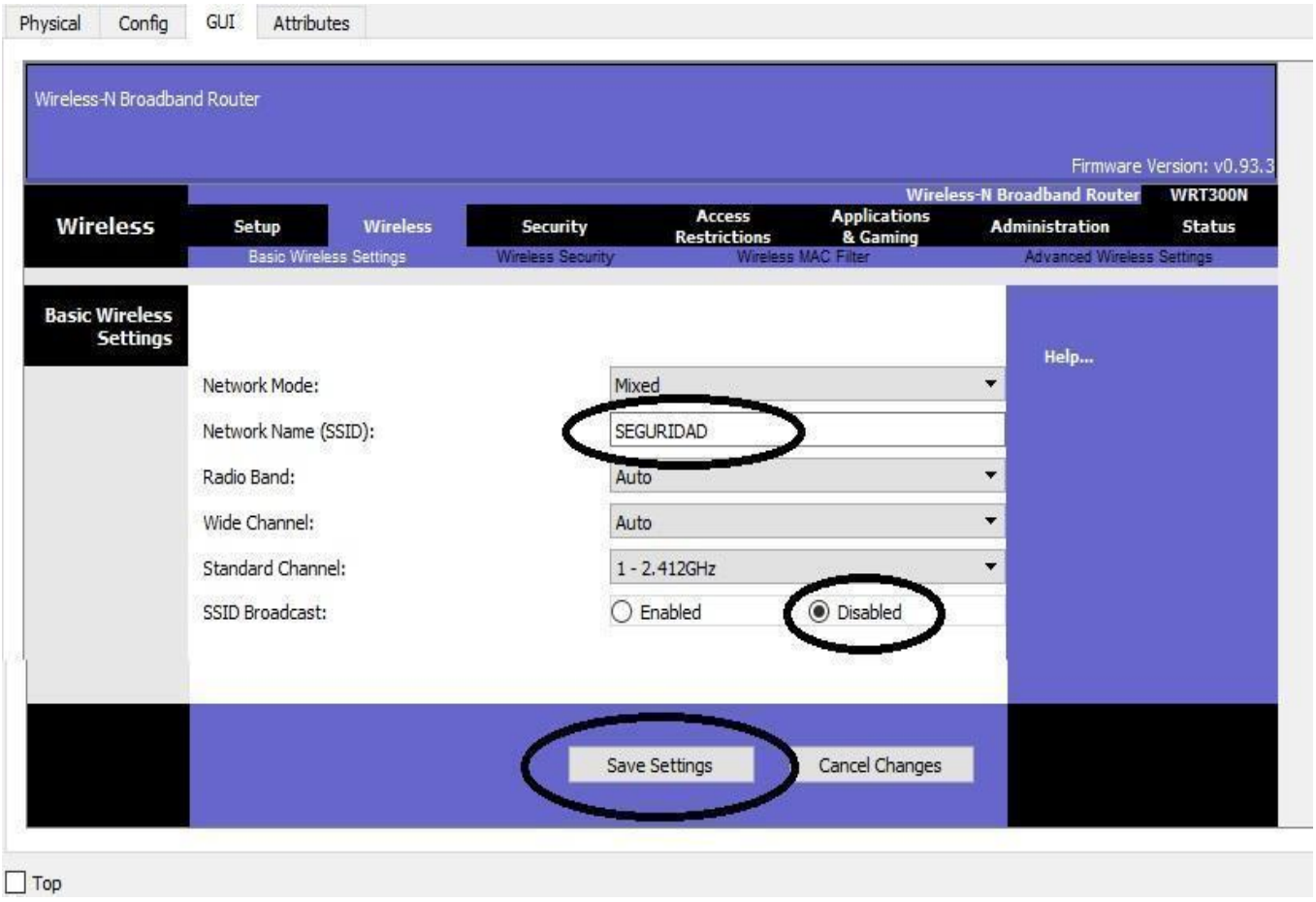

Figura 5. SSID Broadcast
Fuente: propia

Actividad de repaso

Ahora analice: al cambiar el SSID y desactivar el broadcast ¿Qué sucede con las máquinas? ¿Por qué?

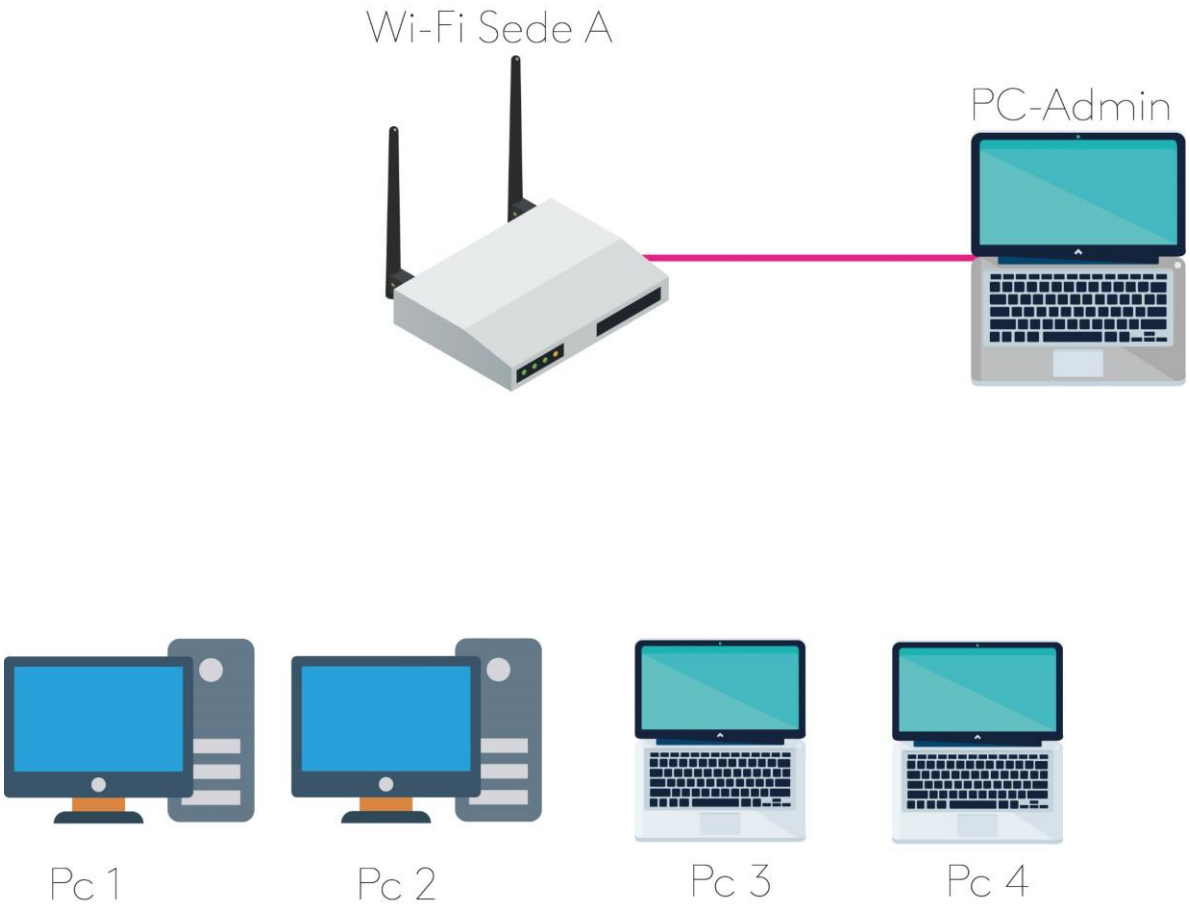

Figura 6. SSID desactivado
Fuente: propia

Si observamos al cambiar el SSID y desactivar el SSID Broadcast, las máquinas se desconectan, porque cada máquina está buscando la red DEFAULT, como no la encuentra no se puede conectar.

Pero, ¿El router Wi-Fi sigue emitiendo señal?

SI. El router sigue emitiendo señal, pero no genera broadcast del nombre, por consiguiente, sólo quien conozca el ID (por tenerlo configurado de antemano) y/o lo configure de forma manual podrá conectarse.

Actividad de repaso

7. Configurar de forma manual el SSID.

   Para configurar el SSID ingrese al equipo, pestaña Config, seleccione Interface Wireless, y coloque en el SSID "SEGURIDAD".

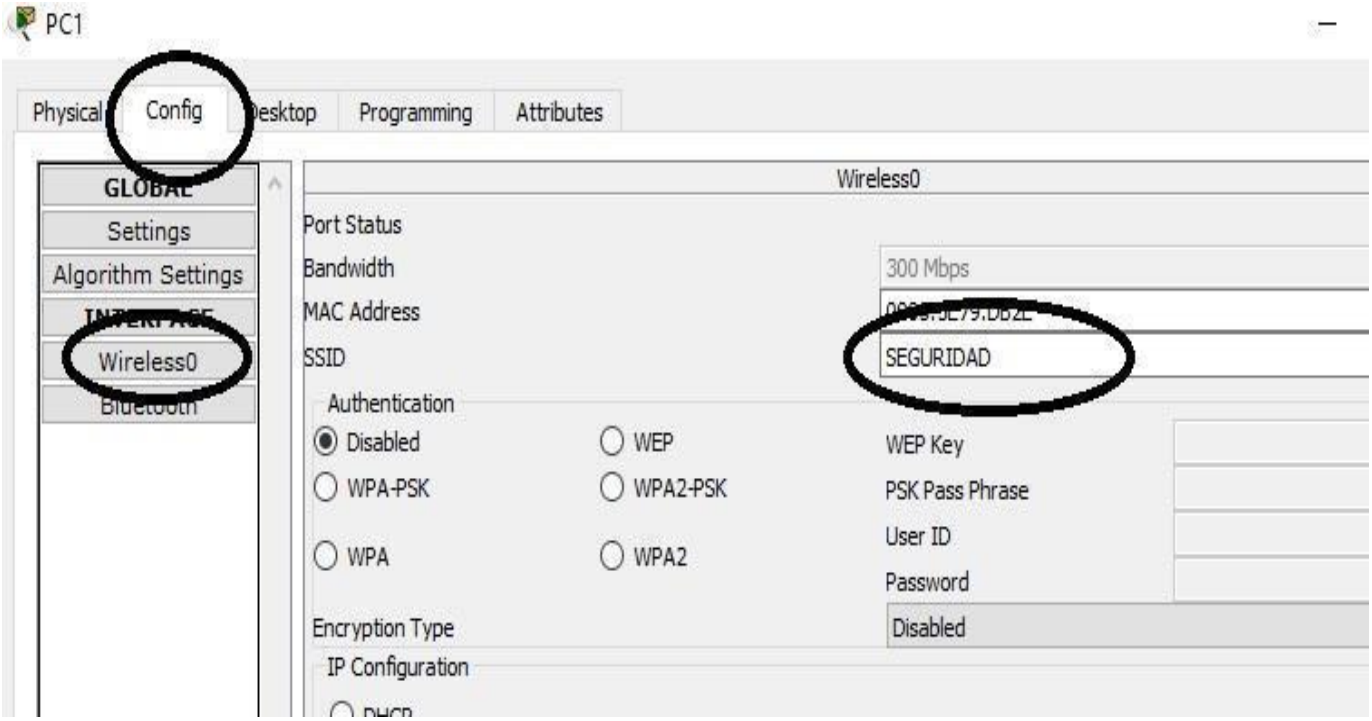

Figura 7. Configuración del SSID en el PC
Fuente: propia

Actividad de repaso

¿Qué sucede cuando se le asigna el SSID al PC1?

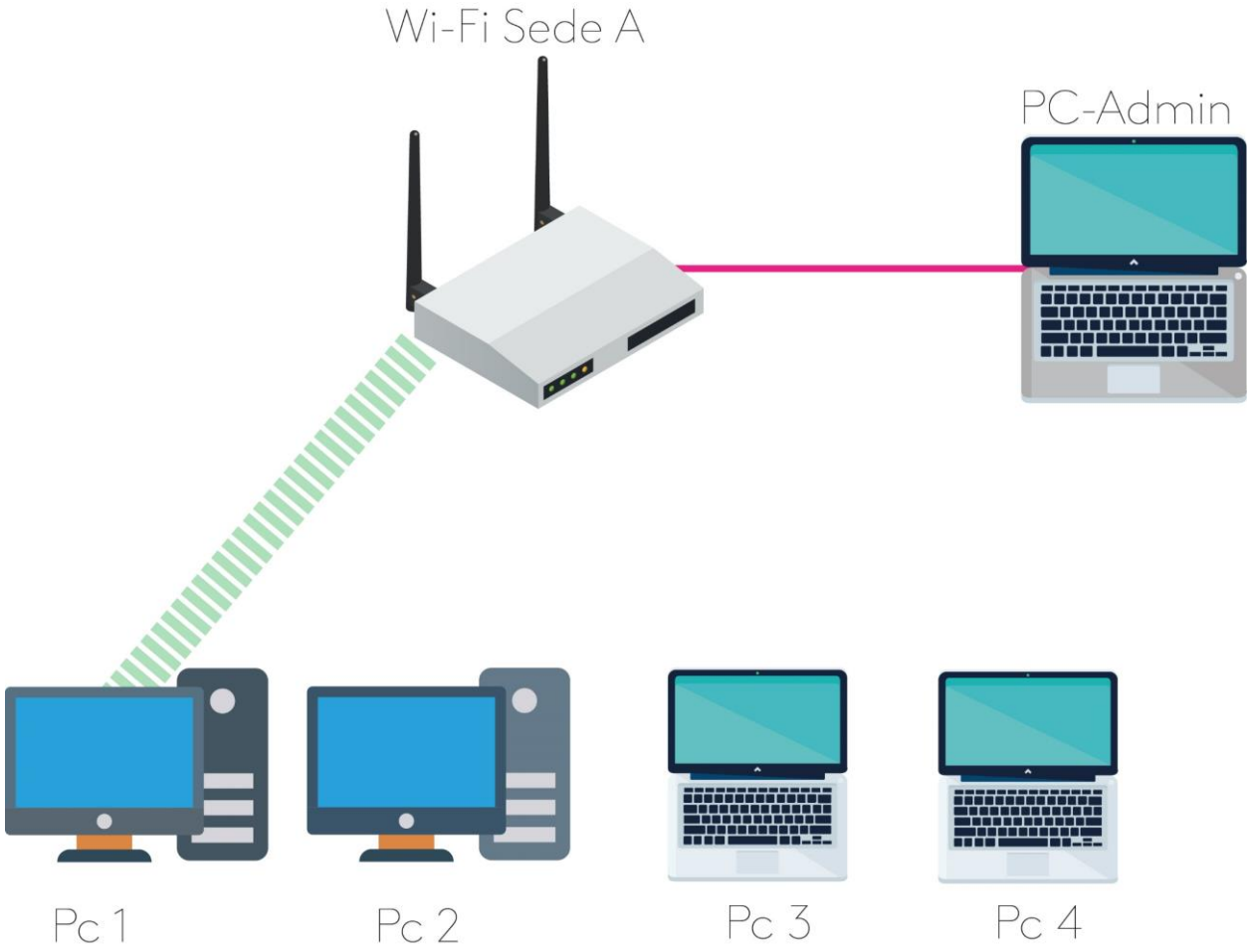

Figura 8. Pc1 con configuración manual de SSID
Fuente: propia

Si observamos, al asignar o configurar el SSID de forma manual en el equipo, este se conecta de inmediato.

8. Configurar el SSID en las demás máquinas para que todas accedan al dispositivo inalámbrico.

Actividad de repaso

Reto 1- parte 2

MAC
Identificador único del dispositivo de red.

Ahora generamos control de acceso por medio del filtrado MAC.

La MAC es el identificador único o dirección física del dispositivo de red o NIC, está formado por 48 bit agrupados en 12 dígitos hexadecimales.

Se obtiene al emitir el comando ipconfig /all en la consola de CMD de windows, con el nombre dirección física.

Figura 9. Dirección MAC
Fuente: propia

En el router Wi-Fi se puede generar control de acceso por medio de la dirección MAC, permitiendo o denegando el listado de direcciones MAC que se registren.

Desarrollar esta acción en redes productivas se considera una buena práctica, pero al igual que el SSID no brindan seguridad a la información.

Ahora:

1. Compruebe que todos los equipos estén conectados al router Wi-Fi.

Actividad de repaso

2. Acceda al router Wi-Fi por medio de navegador web.
3. Ubíquese en la pestaña Wireless – Filter MAC.
4. Seleccione el botón "enable", el cual activará el servicio de filtrado MAC.
5. Registre las MAC de los Pc1 y Pc2.
6. Seleccione la opción "Permit Pcs" (permitir que la lista de PCs con Mac registrada accedan a la red), y salvar (save settings).

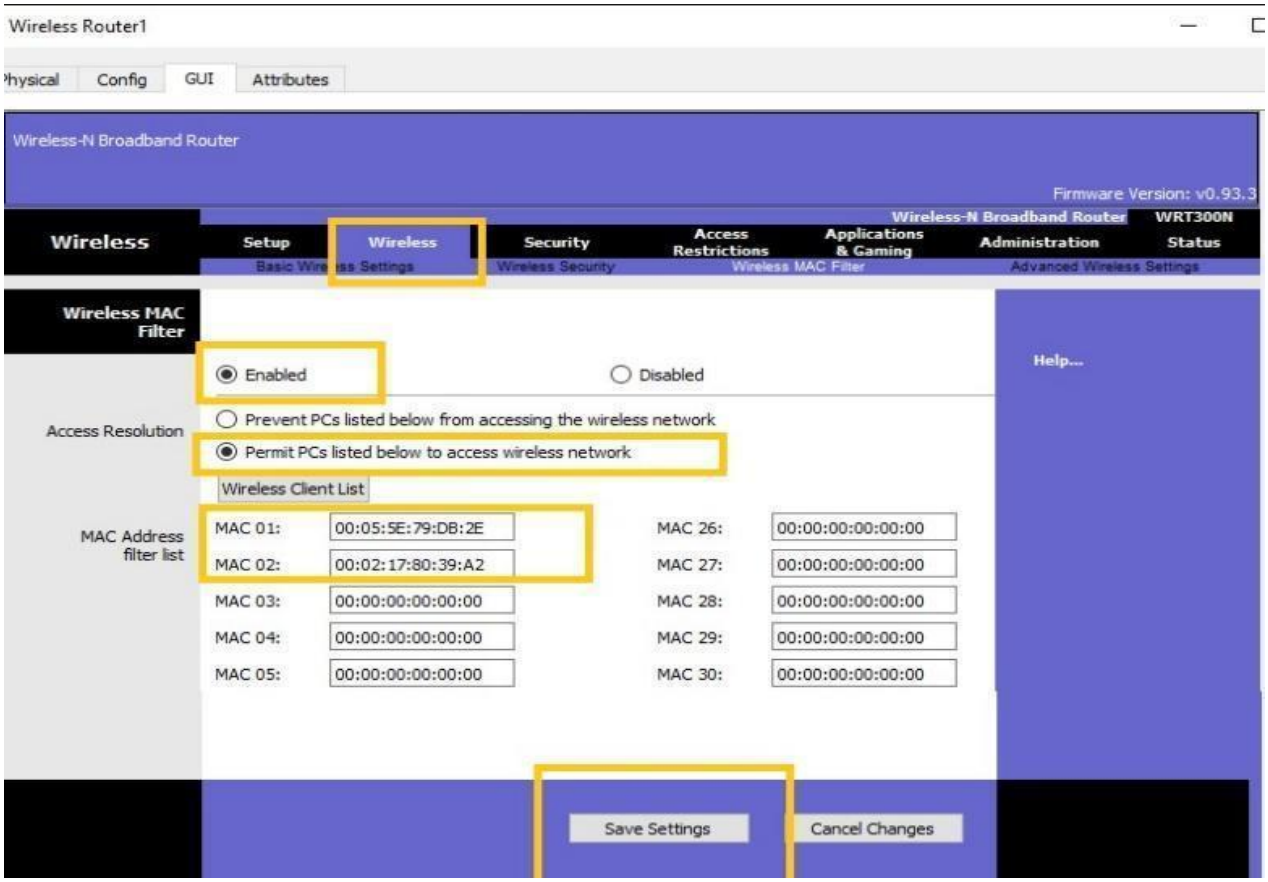

Figura 10. Filtrado MAC en router Wi-Fi
Fuente: propia

7. Analice, ¿Qué pasa con los equipos que registraron las MAC?

Como la opción seleccionada es permitir que las MAC registradas se conecten a la red, estos equipos permanecerán conectados, los equipos de MAC no registradas se desconectarán.

Actividad de repaso

Reto 2

Este reto consiste en configurar una red Wi-Fi segura.

La preocupación por la seguridad de la información se extiende cada día más, ya que la información se ha convertido en uno de los activos más valiosos de las compañías.Pero, ¿A qué está expuesta dicha información?

La información está expuesta al robo, alteración, modificación, divulgación, denegación de acceso, secuestro, entre otros muchos factores que la ponen en riesgo.

Las redes son un factor de vulnerabilidad para la información porque son propensas a ser chuzadas, en los últimos años nos hemos enfrentado a escándalos de divulgación de información (caso Wikileaks), acceso abusivo a información personal (caso Sepúlveda), secuestro de información (caso ransomware wanna cry), entre otros muchos casos.

Chuzada
Palabra comúnmente utilizada para significar la interpretación de una red sea telefónica o de datos.

En la búsqueda de seguridad de la información se han desarrollado algoritmos y protocolos de seguridad que se encargan de encriptar los medios por donde viaja la información.

En los dispositivos router Wi-Fi se han desarrollado los protocolos WEP, WPA y WPA2 los cuales además de generar control de acceso brindan niveles de seguridad al encriptar los canales por donde viaja dicha información.

Protocolo de seguridad WEP (seguridad equivalente a cableado): este protocolo utiliza el algoritmo RC4 (cifrado de flujo obsoleto), por lo cual en el año 2004 WEP fue abandonado por la alianza Wi-Fi como protocolo de seguridad.

Protocolo de seguridad WPA surge como mejora del protocolo WEP.

Las aplicaciones WPA modernas usan un clave previamente compartido (PSK), conocida como WPA personal, y el protocolo de integridad de clave temporal o TKIP para encriptación. Mientras que WPA Enterprise o empresarial utiliza un servidor de autenticación RADIUS para la generación de claves y certificados.

Protocolo de seguridad WPA2 en una mejora de seguridad del protocolo WPA ya que integra el estándar de cifrado avanzado AES, el cual se considera de alto nivel de seguridad.

Configuración de seguridad en router Wi-Fi

1. Con base en la misma topología del reto 1, acceder al dispositivo inalámbrico por medio del navegador Web del equipo que está conectado por cable.
2. Acceder a la pestaña Wireless- menú Wilreless security.

Actividad de repaso

3. Seleccionar el tipo de seguridad que quiere configurar (para el ejemplo WPA2)

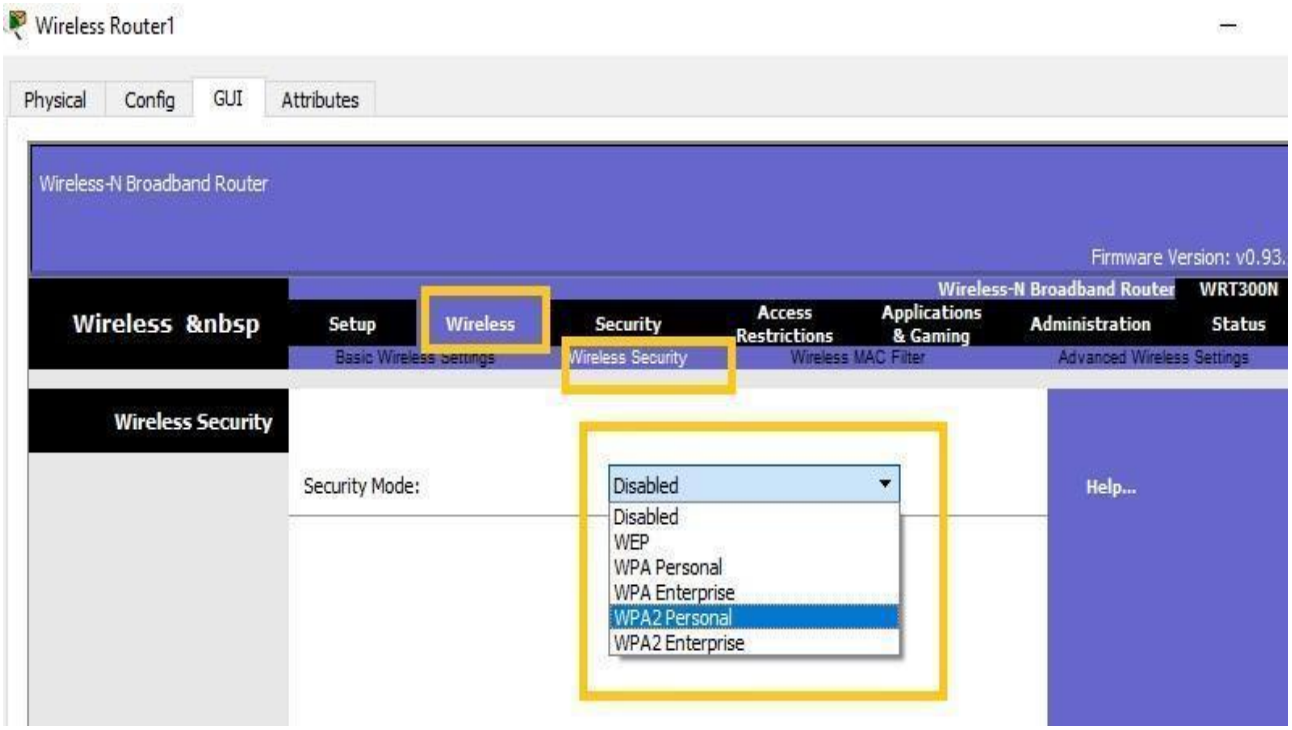

Figura 11. Protocolos de seguridad Wi-Fi
Fuente: propia

Actividad de repaso

4. Configurar clave de acceso WPA 2 “AREANDINA” y salvar los cambios.

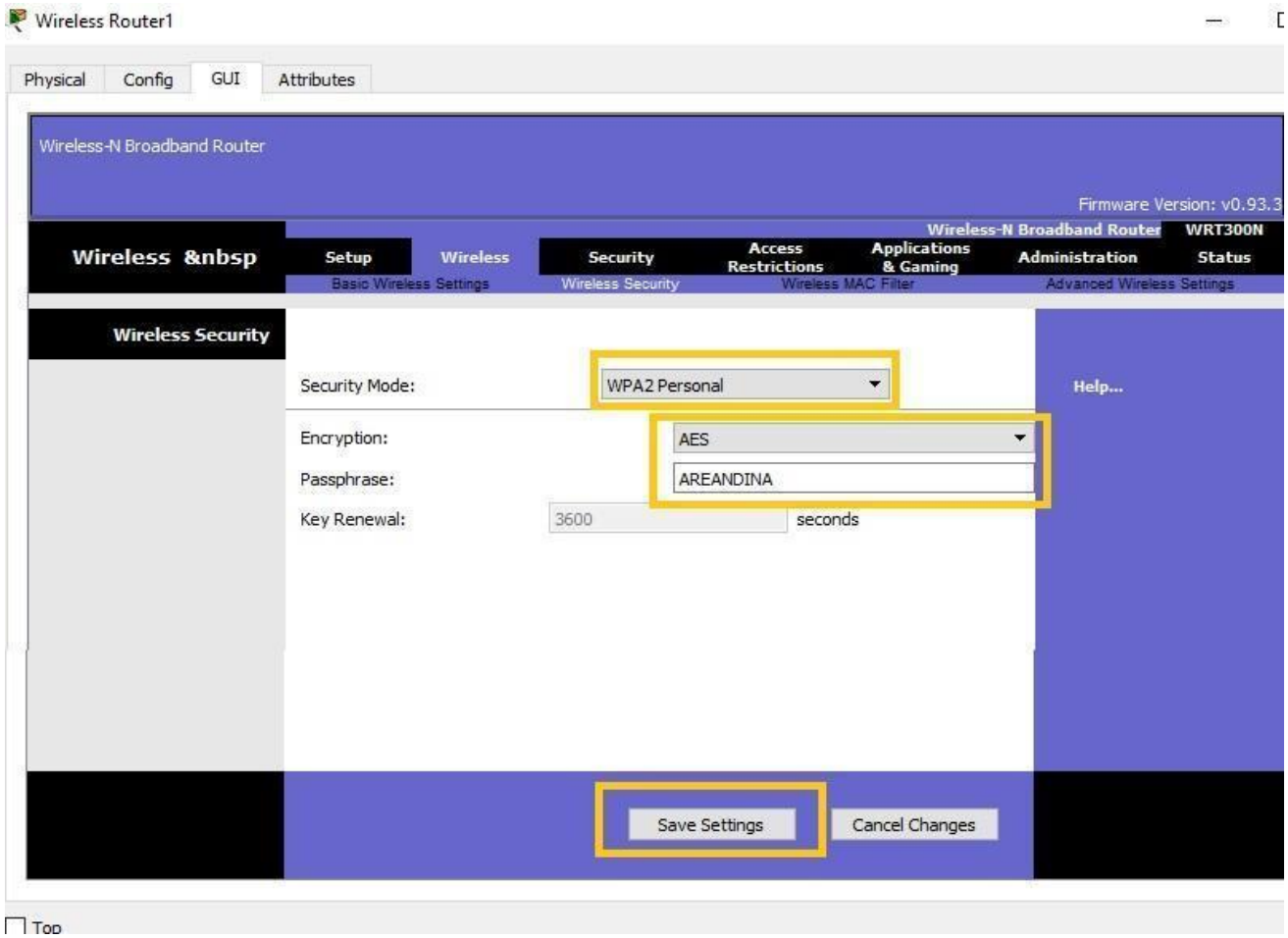

Figura 12 Configuración WPA en router c Wi-Fi
Fuente: propia

5. ¿Qué efecto tiene sobre la red aplicar el protocolo WPA2?

   Las máquinas se desconectan de la red, y se requerirá que cada equipo se registre con el protocolo y contraseña apropiado.

Actividad de repaso

6. Para configurar el PC1 con protocolo WPA2 y la contraseña, acceda a la pestaña Config, menú Wireless, seleccione WPA2 PSK y agregue la contraseña de acceso “AREANDINA”.

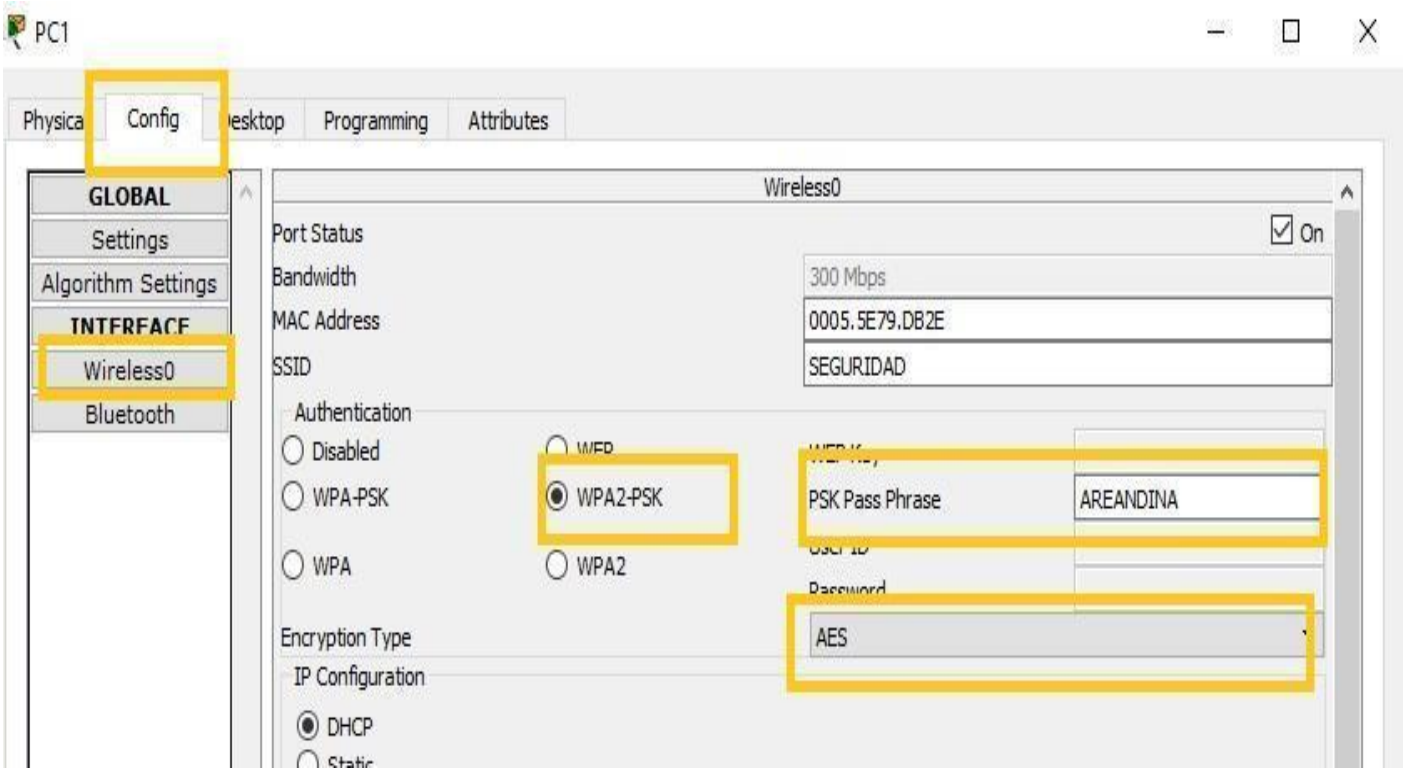

Figura 13. Configuración WPA2 en PC1
Fuente: propia

7. Realice el mismo procedimiento en los demás Pc y compruebe conectividad entre ellos.

Las vulnerabilidades generan riesgos en la información y en la red por tal motivo es importante como departamento de TI tomar las medidas necesarias para minimizar dichas vulnerabilidades y ofrecer una mejor seguridad a compañía, así mismo, generar políticas de seguridad y planes de mitigación en caso de un evento o incidente de seguridad.

TI
Tecnologías de la Información