

SERVICIO WIFI CORPORATIVO EN RCJA GUÍA DE USUARIO

Índice

1	Objeto.....	3
2	Alcance.....	4
3	Descripción del servicio	5
3.1	<i>Acceso y tipología de usuarios.....</i>	<i>5</i>
3.2	<i>Protocolos de autenticación</i>	<i>10</i>
4	Configuración de dispositivos.....	11
4.1	<i>SSID RCJA</i>	<i>11</i>
4.1.1	<i>Dispositivos Android.....</i>	<i>11</i>
4.1.2	<i>Dispositivos IOS.....</i>	<i>13</i>
4.1.3	<i>Dispositivos Windows 11.....</i>	<i>14</i>
4.1.4	<i>Dispositivos Windows 10.....</i>	<i>22</i>
4.1.5	<i>Dispositivos Windows 8</i>	<i>28</i>
4.1.6	<i>Dispositivos MAC</i>	<i>33</i>
4.1.7	<i>Dispositivos Linux</i>	<i>35</i>
4.2	<i>SSID IoT.....</i>	<i>36</i>
5	Gestión de Incidencias	38

1 Objeto

El objeto de este documento es **proporcionar a los responsables TIC** de los organismos una guía general sobre la conexión a la red WIFI de la Junta de Andalucía para facilitar a los distintos departamentos de informática la tarea de conexión de usuarios, y ayudarles a elaborar sus propios manuales en función de sus procedimientos o necesidades más específicas. También se tratará como proceder ante incidencias o consultas.

A lo largo del documento se detallan también las **soluciones tecnológicas** de comunicaciones asociadas a cada tipología de escenario WIFI, en función de la sede, en el marco tecnológico de la RCJAv4, para ayudar a entender el servicio.

El conjunto de estos escenarios depende de varios factores, uno de ellos es dependiente de la sede desde la que se conectan los usuarios, pues las arquitecturas tecnológicas que subyacen son diferentes. También depende de factores relacionados con el usuario, concretamente con su ubicación e información recogida en LDAP si se trata de un usuario corporativo.

Asimismo, se definen los **comportamientos esperados según el SSID** empleado en cada caso.

2 Alcance

El servicio se define para los siguientes clientes:

- Dispositivos Android
- Dispositivos IOS
- Dispositivos Windows
- Dispositivos MAC
- Dispositivos Linux

Se tratarán para los diferentes SSIDs.

3 Descripción del servicio

A continuación, a modo de contextualización, se incluyen detalles técnicos que ayuden a entender el servicio.

Según se ha previsto en el proyecto, los APs WIFI desplegarán en todas las sedes 3 SSIDs, cada uno de los cuales debe tener un comportamiento diferente:

SSID	Visibilidad	Capacidad	Uso
RCJA	Visible	Preferente	Para empleados de la Junta de Andalucía, con cuenta LDAP , que puedan conectarse de manera transparente en sedes de su organismo o de manera itinerante en el resto de sedes de la Junta de Andalucía.
IOT	Oculto	Preferente	Para equipamiento IoT como alarmas, sensores inteligentes, impresoras,
ANDALUCIA VUELA	Visible	Best effort	Para ciudadanía.

Nota: En relación al SSID ANDALUCIA VUELA, el servicio aún no estará disponible para la ciudadanía hasta que se realicen los trabajos necesarios para la definición del servicio y cumplimiento de normativa RGPD.

3.1 Acceso y tipología de usuarios

Los escenarios tecnológicos se definen en base a la tipología de usuarios y dependen de tres variables:

- El SSID
- La ubicación del usuario
- La información recogida en LDAP, para usuarios corporativos, concretamente en el atributo JAPERFILACCESO

Se ha considerado a nivel WiFi el escenario **multisede** (compartido o multiVRF), con diferente carácter al de RCJA. En este contexto se considera el edificio como un todo, independientemente del número de accesos y VPNs que tenga, garantizando el servicio a un usuario en su totalidad, independientemente del lugar desde el que se realice la conexión. De esta forma, de cara a la gestión de toda la infraestructura, se define una sede dominante, como

se detallará más adelante, pero en función de la identificación del LDAP cada usuario local se conecta por su acceso.

La identificación y acceso al SSID RCJA se realizará identificando al usuario a través del LDAP que en función del atributo **JAPERFILACCESO** le permitirá unas visibilidades u otras.

Los valores definidos para JAPERFILACCESO son los siguientes:

- Denegado:** No se permite el acceso WIFI al usuario
- WIFI:** El usuario puede hacer uso del WIFI y acceder a diferentes recursos según su ubicación:
 - Sede de su organismo: Accede a todos los recursos locales y direccionamiento dentro de la sede donde se encuentre
 - Sede de otro organismo: Conmutación centralizada en la sede de itinerancia de su organismo, Acceso a su VPN de RCJA y navegación por Internet.
- Itinerante:** Los usuarios que dispongan de este valor en el atributo siempre salen a través de la infraestructura central sin pasar por los servicios propios de su sede. El objetivo es dotar de seguridad las conexiones de sedes que no disponen de FWs, obligándoles a usar la infraestructura de seguridad del NIXA.
- Atributo no existe o está vacío:** el usuario navega y accede a SSHH pero NO a la VPN de ningún organismo.

Inicialmente el atributo **no existe** y será el administrador del LDAP el que lo cree y asigne uno de los valores actuales a cada cuenta. Si desea un despliegue masivo tendrá que solicitarlo por los mecanismos establecidos para correo corporativo.

En la siguiente tabla se explica de manera más detallada el comportamiento esperado del servicio en cada caso (se señalan en color azul los escenarios en los que se establece un túnel entre el AP y el CORE WIFI, mientras que se marcan en color verde los escenarios en los que el tráfico se conmuta en local, esto es relevante en relación a las opciones de establecimiento de garantías de caudal):

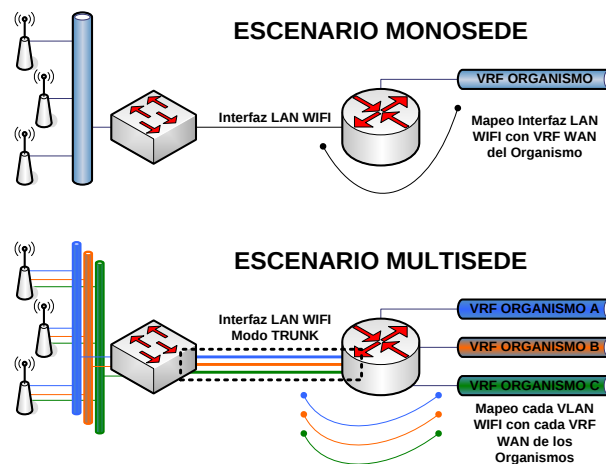
Política de acceso WIFI				
Tipo de usuario	Atributo LDAP	Ubicación Usuario		Comportamiento
		En sedes de su Organismo	En sedes de otro Organismo	
RCJA	No Existe	Política Itinerante	Política Itinerante	Se establece un túnel entre el AP y el CORE WIFI correspondiente, que

Política de acceso WIFI				
Tipo de usuario	Atributo LDAP	Ubicación Usuario		Comportamiento
		En sedes de su Organismo	En sedes de otro Organismo	
	Vacío	Política Itinerante	Política Itinerante	encapsula y encamina el tráfico del usuario hasta el CORE WIFI, donde se le da conectividad a Internet y servicios horizontales de RCJA, a través de la VRF de Itinerancia (VPNIP_VRF_ITINERANCIA_204). No accede a la VPN de SU Organismo, pero si puede levanta Cliente VPN.
	Denegado	Sin Acceso	Sin Acceso	Sin Acceso
	WIFI	Política Local	Política Itinerante VRF Propia	En caso de que se trate de un usuario local al Organismo, su tráfico lo saca el AP por la conexión local de RCJA y VRF del Organismo, a través de la que tendrá acceso a Internet, servicios horizontales de RCJA, visibilidades específicas entre su Organismo y otros Organismos, así como a las redes y servicios propios de su Organismo*. En caso de que se trate de un usuario en itinerancia, su tráfico lo tuneliza el AP hasta el CORE WIFI correspondiente, donde se le da conectividad al usuario directamente con la VRF de su Organismo, a través de la que tendrá acceso a Internet, servicios horizontales de RCJA, visibilidades específicas entre su Organismo y otros Organismos, así como a las redes y servicios propios de su Organismo.
	Itinerante	Política Itinerante VRF Propia	Política Itinerante VRF Propia	Su tráfico lo tuneliza el AP hasta el CORE WIFI correspondiente, donde se le da conectividad al usuario directamente con la VRF de su Organismo , a través de la que tendrá acceso a Internet, servicios

Política de acceso WIFI				
Tipo de usuario	Atributo LDAP	Ubicación Usuario		Comportamiento
		En sedes de su Organismo	En sedes de otro Organismo	
				horizontales de RCJA, visibilidades específicas entre su Organismo y otros Organismos, así como a las redes y servicios propios de su Organismo.
IoT	N/A	N/A	N/A	Su tráfico lo saca el AP por la conexión local de RCJA y VRF del Organismo, a través de la que tendrá acceso a Internet, servicios horizontales de RCJA, visibilidades específicas entre su Organismo y otros Organismos, así como a las redes y servicios propios de su Organismo*.
Vuela	N/A	N/A	N/A	En todos los escenarios VUELA, debe establecerse un túnel entre el AP y el CORE WIFI correspondiente, donde se conmuta el tráfico del usuario a la VRF VPNIP_VRF_VPNVUELA_238, donde el usuario tendrá exclusivamente acceso a Internet. De esta forma se garantizará que para todos los usuarios VUELA se puedan aplicar las mismas políticas de navegación, lo que supone un requisito del proyecto por parte de ADA.

* En los casos de conmutación local hay que distinguir dos escenarios técnicos:

- Si se trata de un escenario monosede, la interfaz LAN a la que se conecta la red WIFI, se mapea directamente en la VRF WAN del Organismo.
- Si se trata de un escenario multisede (compartido o multiVRF), la interfaz LAN a la que se conecta la red WIFI, se configura en modo TRUNK, y cada VLAN se hace corresponder con la VRF WAN del Organismo correspondiente.



Por ejemplo, si en el escenario multisede la VRF Organismo B se correspondiese con la VPN Internet, los usuarios VUELA se conmutarían localmente en la VLAN naranja que se mapearía con la VRF de VPN Internet.

Es requisito en todos los escenarios con conectividad a Internet, con independencia del SSID, que se garantice la conectividad entre el Cliente VPN y el terminador de túneles del servicio en los NIXA o en los NIAE, según corresponda.

Cada sede contará con un direccionamiento para WiFi asignado de su VPN que podrá consultarse en la herramienta de Gestión de Direccionamiento IP de RCJA (GDIP).

3.2 Protocolos de autenticación

Se han analizado los distintos protocolos de autenticación se han realizado pruebas y pilotos tanto con EAP-PEAP-GTC como EAP-TTLS-PAP, los cuales pueden convivir sin mayor problema en el servidor de autenticación.

Por tanto, se validan ambos métodos de autenticación para conectar en SSID RCJA puesto que la red actualmente dispone de ambos.

1. **EAP/PEAP/GTC** aporta un plus de seguridad interesante con el único inconveniente de requerir la instalación de un cliente en los equipos Windows.
2. **EAP-TTLS-PAP** es un paso inferior en seguridad el usar PAP dentro del túnel TTLS pero aporta la facilidad de uso en la configuración al no requerir del cliente para equipos Windows.

4 Configuración de dispositivos

A continuación, se indica cómo proceder para la configuración de los distintos dispositivos atendiendo al SSID.

4.1 SSID RCJA

Como se ha indicado anteriormente, la red permite dos protocolos de autenticación, GTC y PAP TTLS, en función del tipo de dispositivo que se conecte se propone uno u otro.

Para clientes móviles se recomienda configurar GTC mientras que para clientes Windows ambos son posibles, aunque se recomienda usar PAP TTLS. Para usar GTC como protocolo de autenticación en Windows se requiere instalar un plugin.

4.1.1 Dispositivos Android

Los siguientes pasos describen cómo configurar un dispositivo móvil con SO Android para autenticarse en una red móvil inalámbrica configurada para utilizar la Red Corporativa. El protocolo de autenticación recomendado es GTC.

El acceso dependerá de la ubicación del usuario y del atributo JAPERFILACCESO del LDAP como ya se ha indicado anteriormente.

1. En el apartado Wifi de su dispositivo seleccione la red RCJA. (Ajustes → WiFi).
2. Al seleccionar la red marque la casilla **“Opciones Avanzadas”**.
3. Método EAP: PEAP.
4. Autenticación de fase 2: GTC.

5. Certificado AC: Usar certificados del sistema.
6. Estado del certificado online: Solicitar estado del certificado.

The image displays two screenshots of the RCJA (Red de Conexión de la Junta de Andalucía) configuration interface. The left screenshot shows the 'Método EAP' screen with a 'Selección de certificado' dialog box open, highlighting 'Usar certificados de usuario'. The right screenshot shows the 'Certificado CA' section with 'Estado de certificado en línea' set to 'No validar' and 'Dominio' set to 'wifi.juntadeandalucia.es'.

7. Dominio: **wifi.juntadeandalucia.es**
8. Privacidad: Usar dispositivo MAC.
9. Identidad: Introducir nombre de usuario.
10. Contraseña: Introducir contraseña de usuario.
11. Seleccionar Conectar.
12. Comprobar que el dispositivo se ha conectado a la red correctamente.

4.1.2 Dispositivos IOS

Los siguientes pasos describen como configurar un dispositivo iOS para utilizar la Red Corporativa en función de sus permisos. El protocolo de autenticación recomendado es GTC.

1. Vaya al apartado Wi-Fi de su dispositivo (Ajustes → WiFi).
2. En el apartado redes, busque y seleccione la red "RCJA".
3. Introduzca los campos Nombre de Usuario y Contraseña de su identificador personal para el acceso a la Red Corporativa. Una vez introducidos, marque la opción "Acceder".
4. En el primer acceso a la red, el dispositivo móvil se descarga un certificado para su autenticación en la red. Seleccione la opción "**Confiar**" para permitir que su dispositivo haga uso de este certificado.

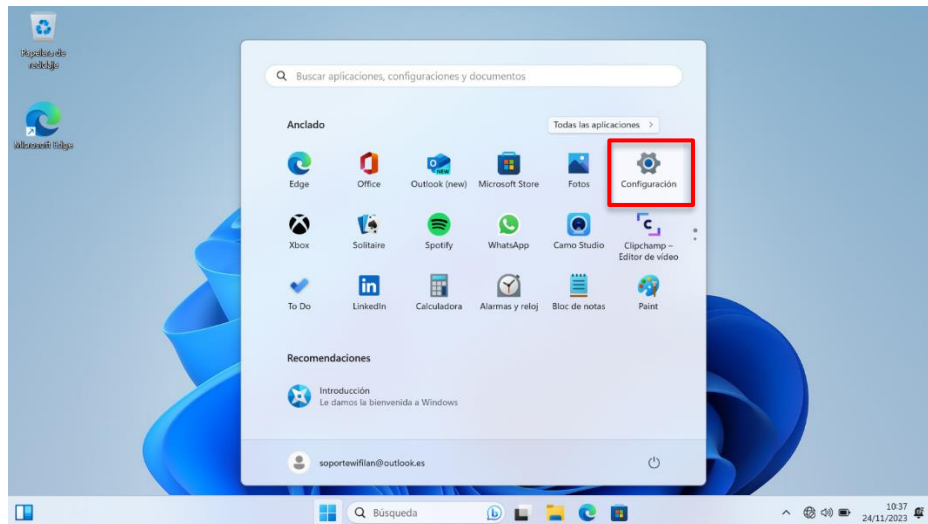


5. Hecho esto, el dispositivo se debe conectar a la red correctamente.

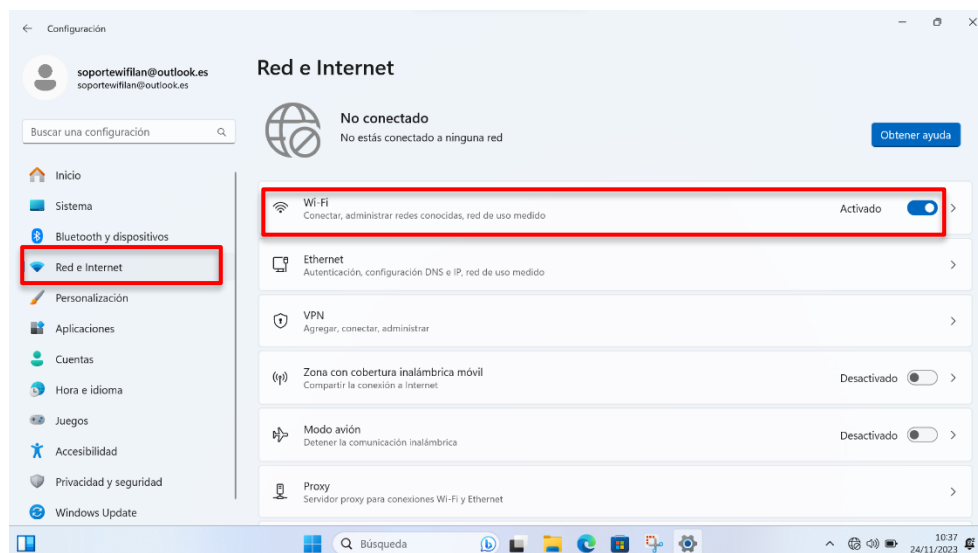
4.1.3 Dispositivos Windows 11

Los siguientes pasos describen cómo configurar un dispositivo Windows 11 para autenticarse en una red inalámbrica configurada para utilizar la Red Corporativa. El protocolo de autenticación recomendado es PAP TTLS.

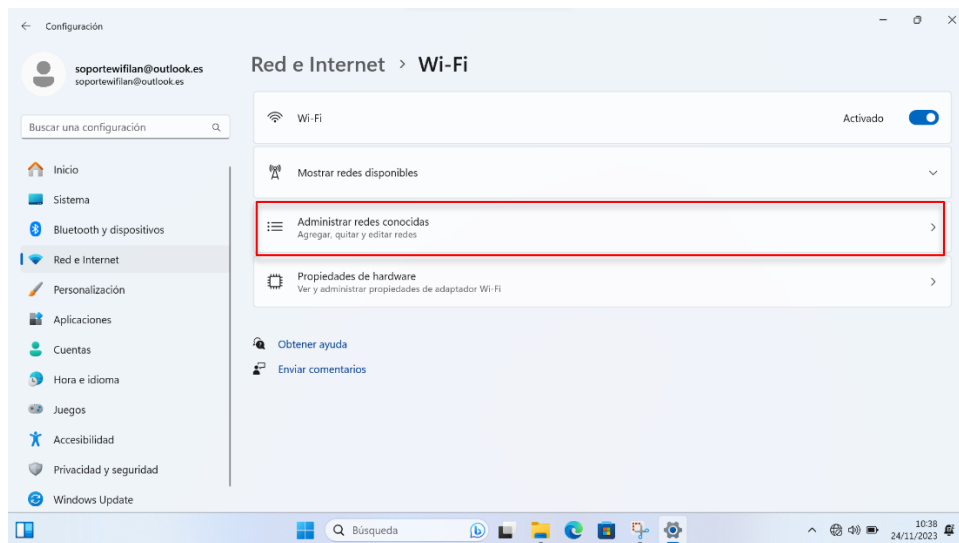
1. Seleccionar el botón Windows y **Configuración**.



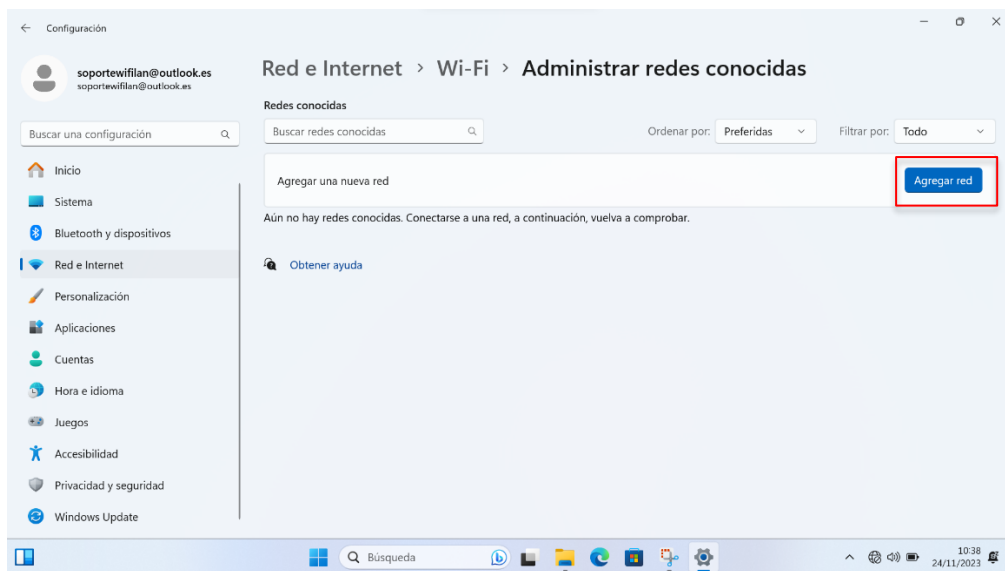
2. Se abrirá la siguiente ventana y se pulsa en Red e Internet – Wi-Fi:



3. A continuación, seleccionar **Administrar Redes Conocidas**

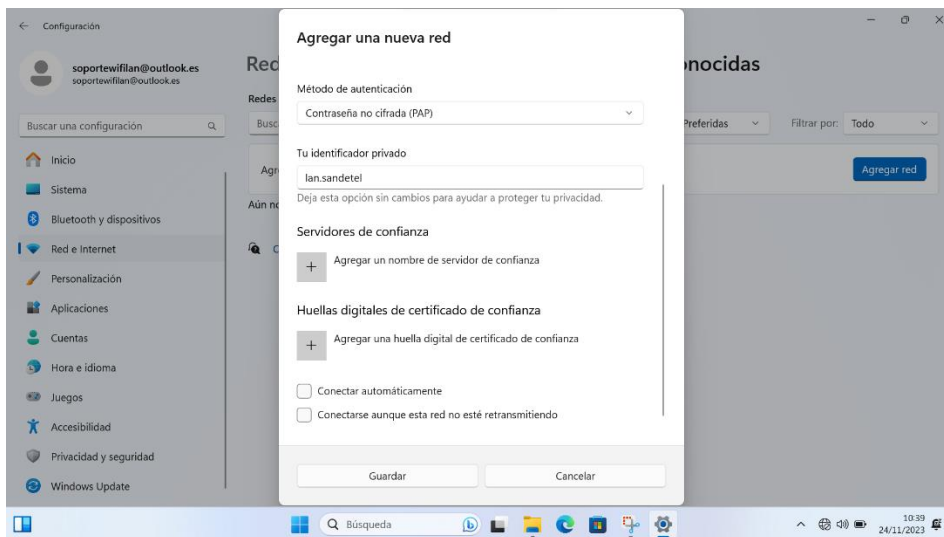
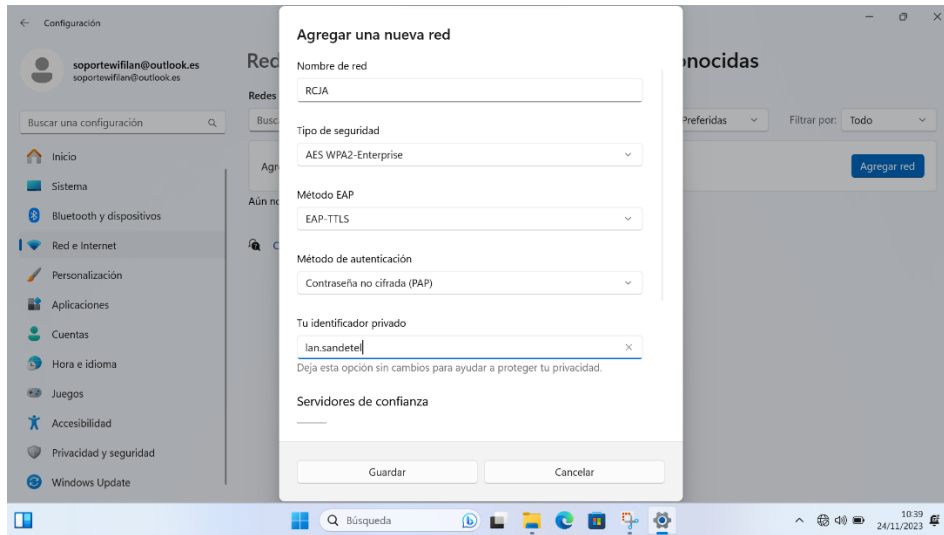


4. Se abrirá la siguiente ventana y se pulsa en el botón **Agregar red**:

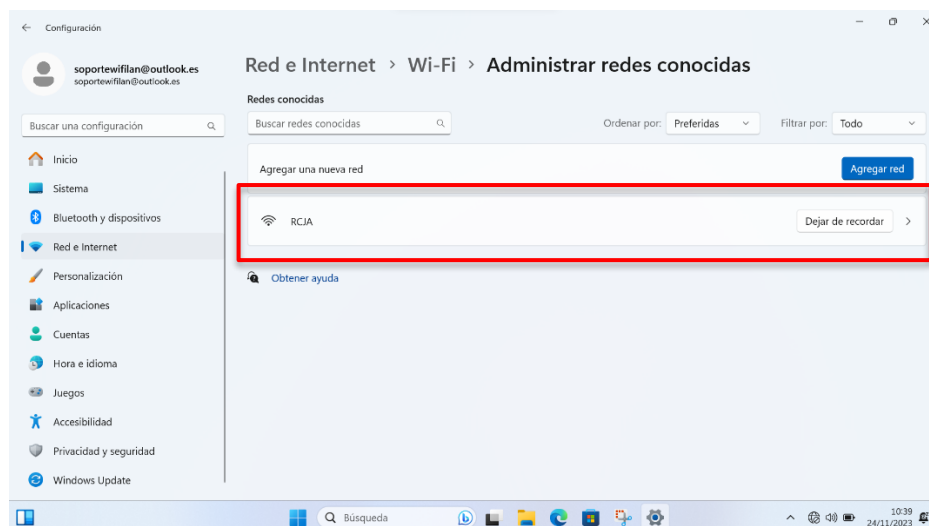


5. Se abre una nueva siguiente ventana en la que hay que rellenar los siguientes datos:

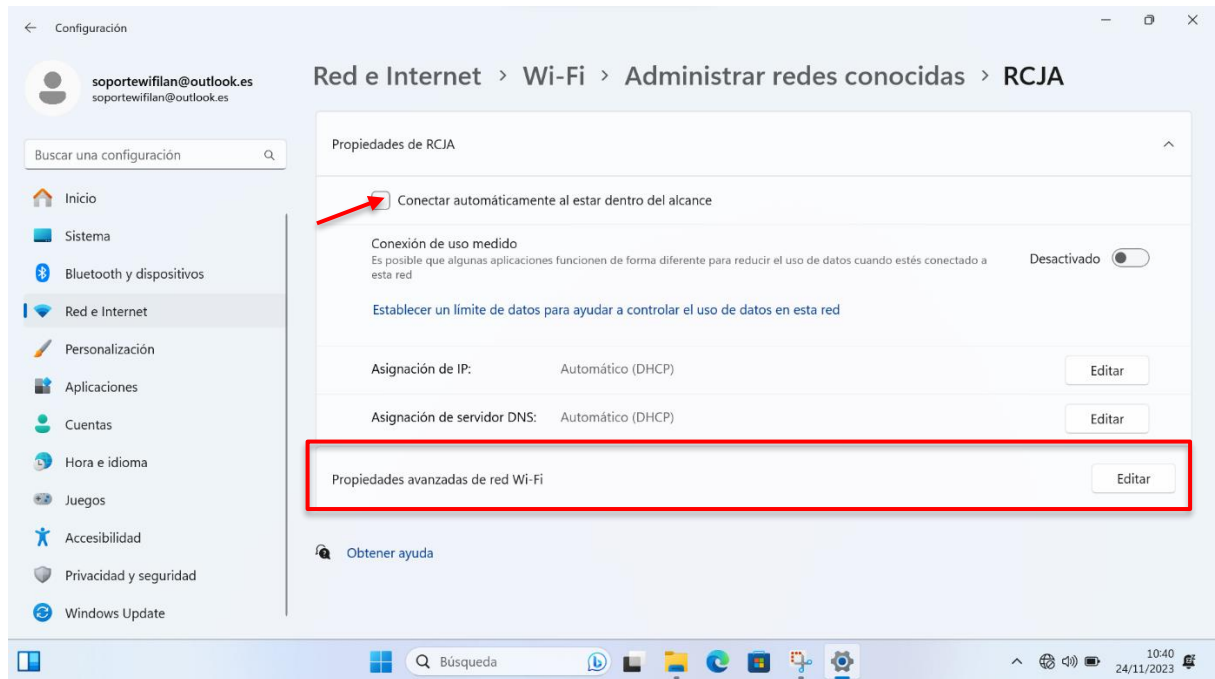
- Nombre de red: **RCJA**
- Tipo de seguridad: **AES WPA2-Enterprise**
- Método EAP: **EAP-TTLS**
- Método de autenticación: **Contraseña no cifrada (PAP)**
- Tu identificador privado: **[Tu usuario ldap – cuenta de correo corporativo]**
- Guardar



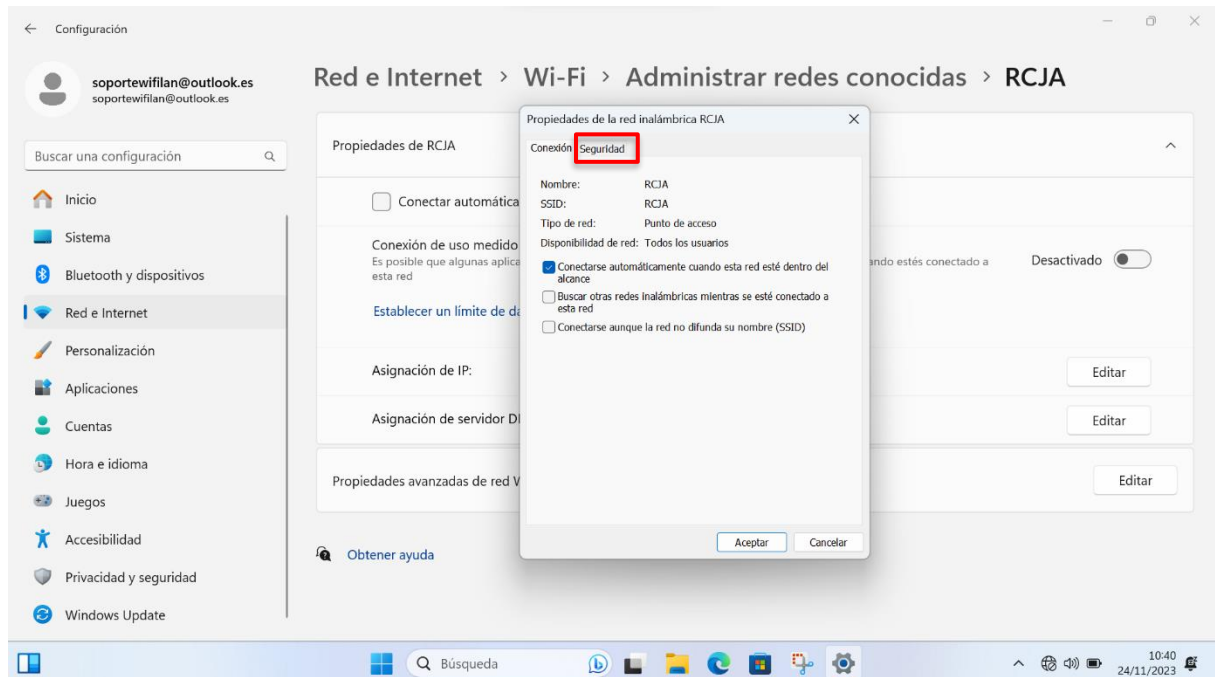
6. Verificamos la configuración pulsando en RCJA:



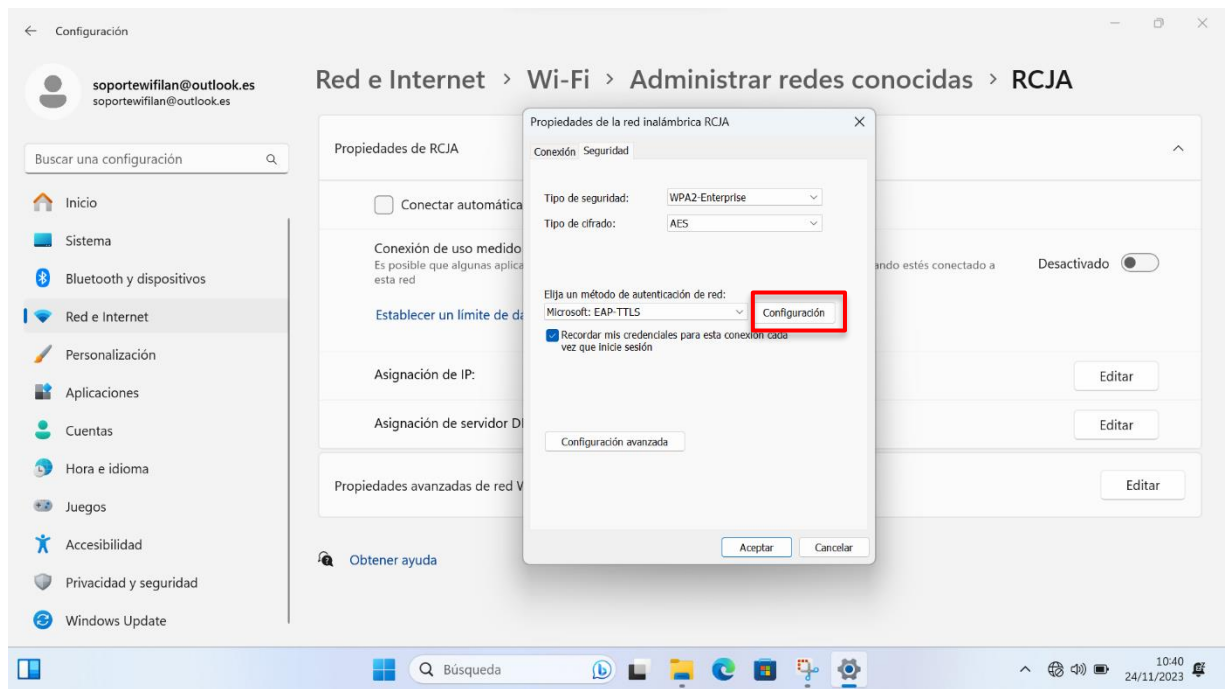
7. Se abrirá la siguiente ventana, se selecciona la casilla de **“Conectar automáticamente al estar dentro del alcance”** y Verificamos las propiedades pulsando en Propiedades avanzadas de red Wi-Fi:



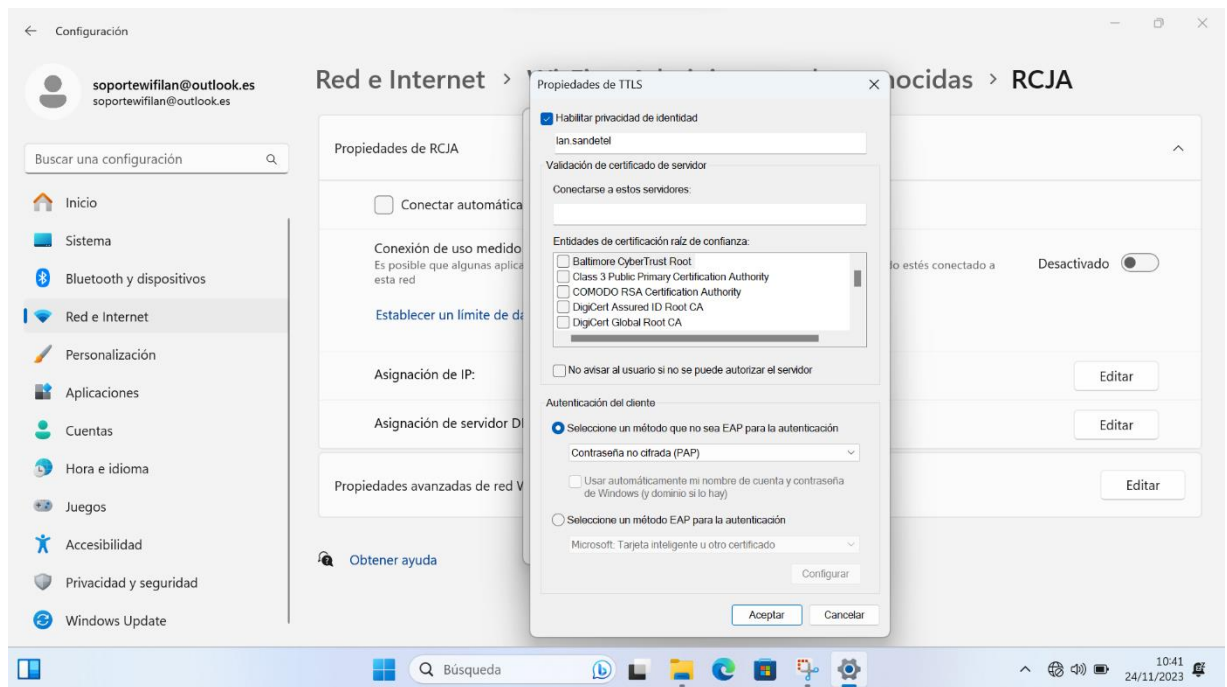
8. Se abre la siguiente ventana y se selecciona pestaña Seguridad:



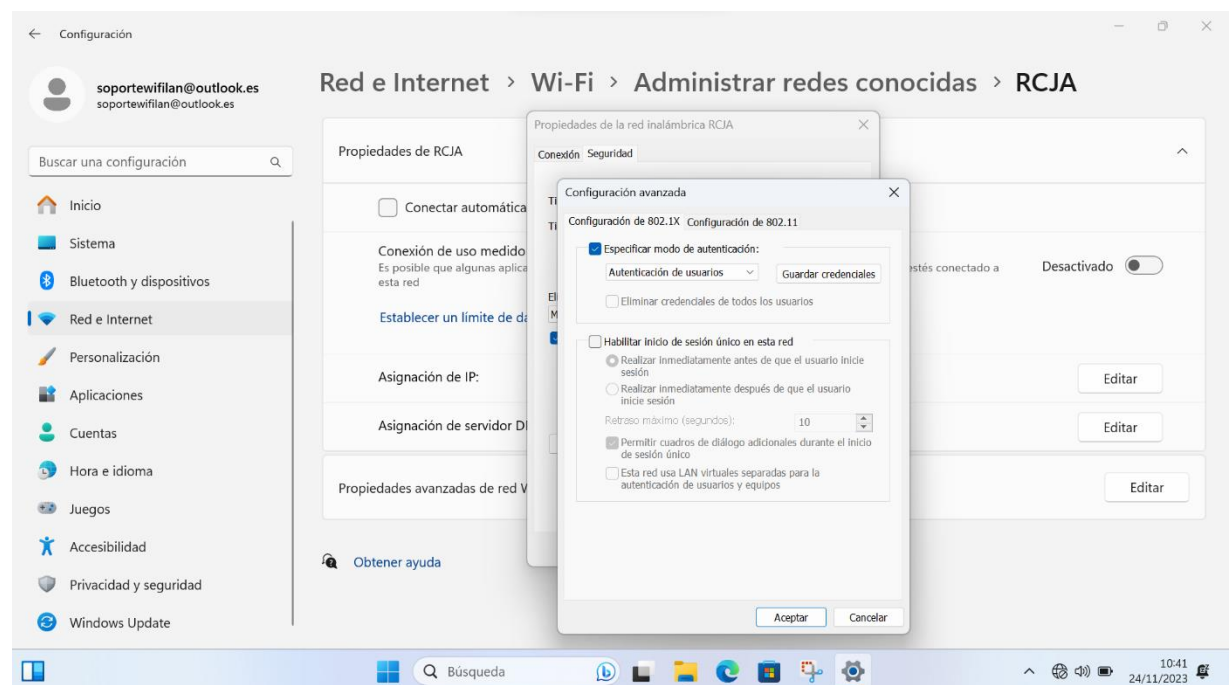
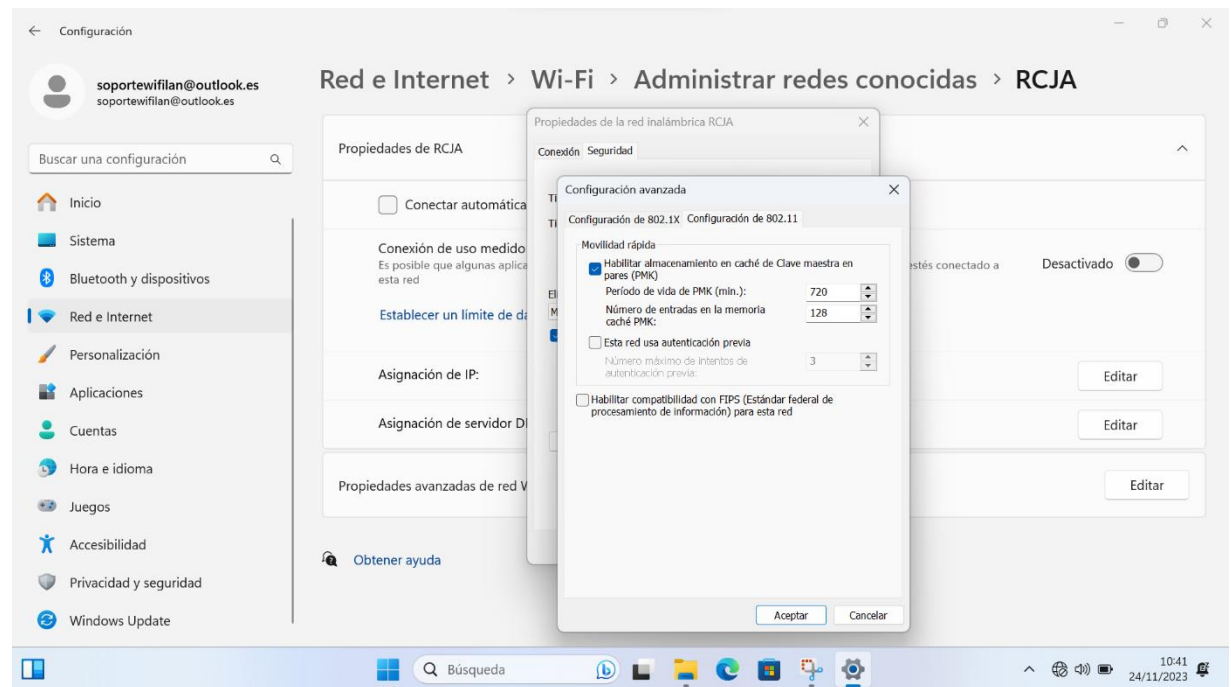
9. Se abre una nueva y se pulsa en **Configuración**:



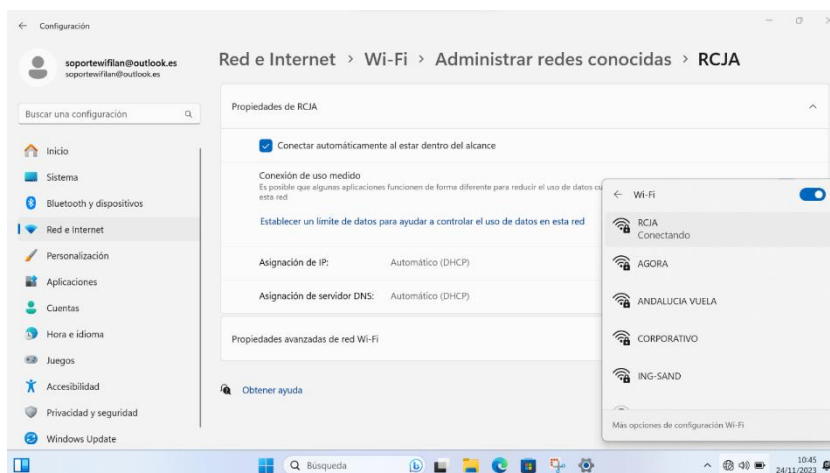
10. Se abrirá la siguiente ventana, aceptamos si los datos son correctos:



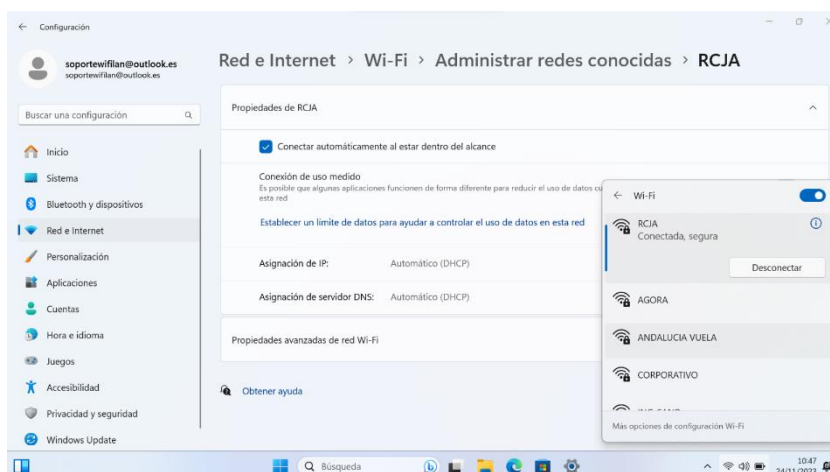
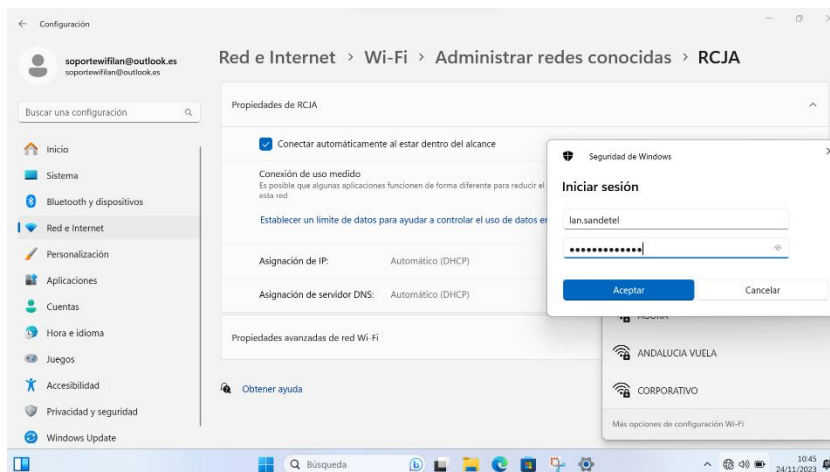
11. Se abrirá la siguiente ventana y se selecciona en **Configuración Avanzada**:



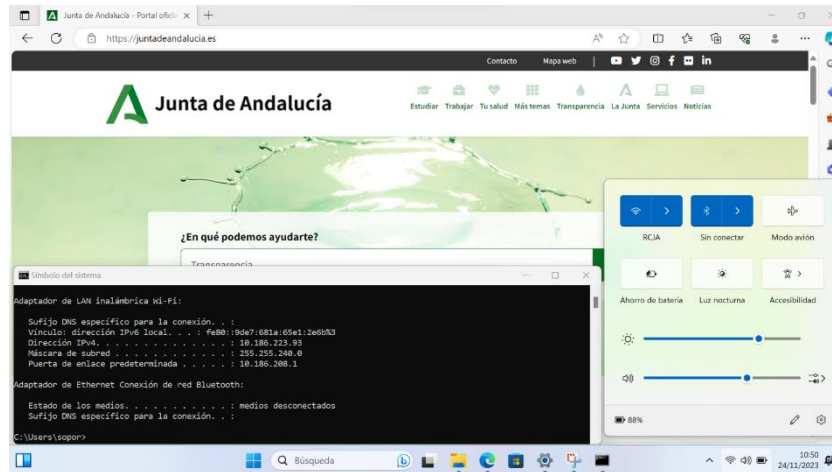
12. Seguidamente nos conectamos a la red RCJA:



13. Requerirá las credenciales de autenticación LDAP del usuario:



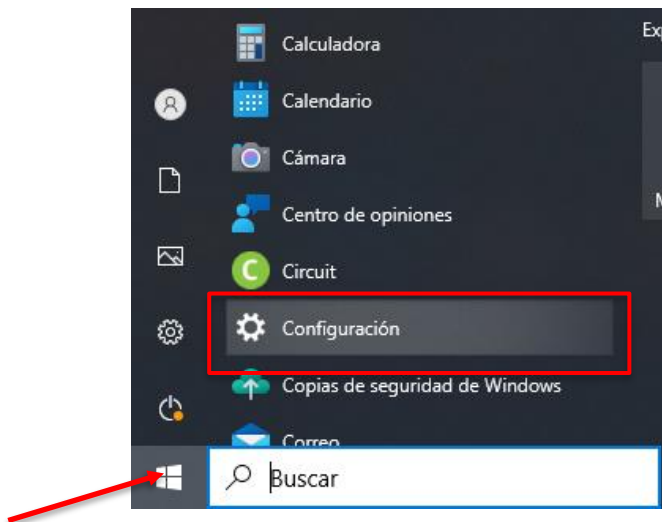
14. Se verifica el correcto funcionamiento:



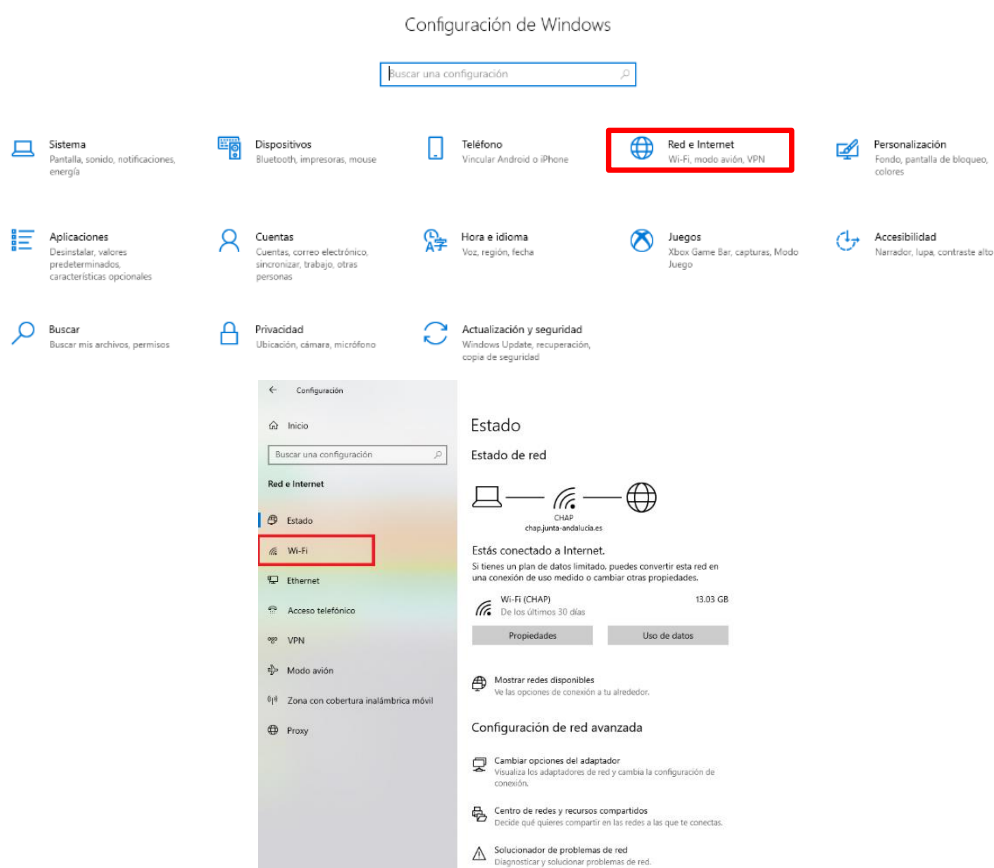
4.1.4 Dispositivos Windows 10

Los siguientes pasos describen cómo configurar un dispositivo Windows 10 o superior para autenticarse en una red inalámbrica configurada para utilizar la Red Corporativa. El protocolo de autenticación recomendado es PAP TTLS.

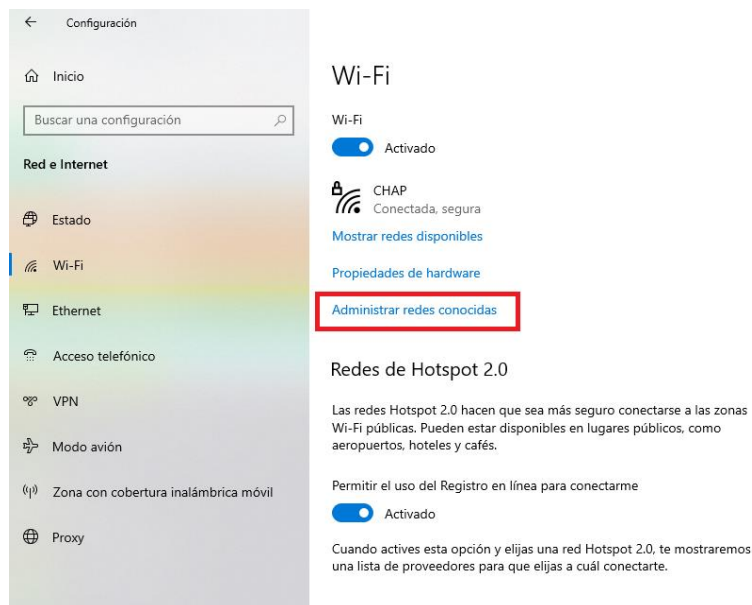
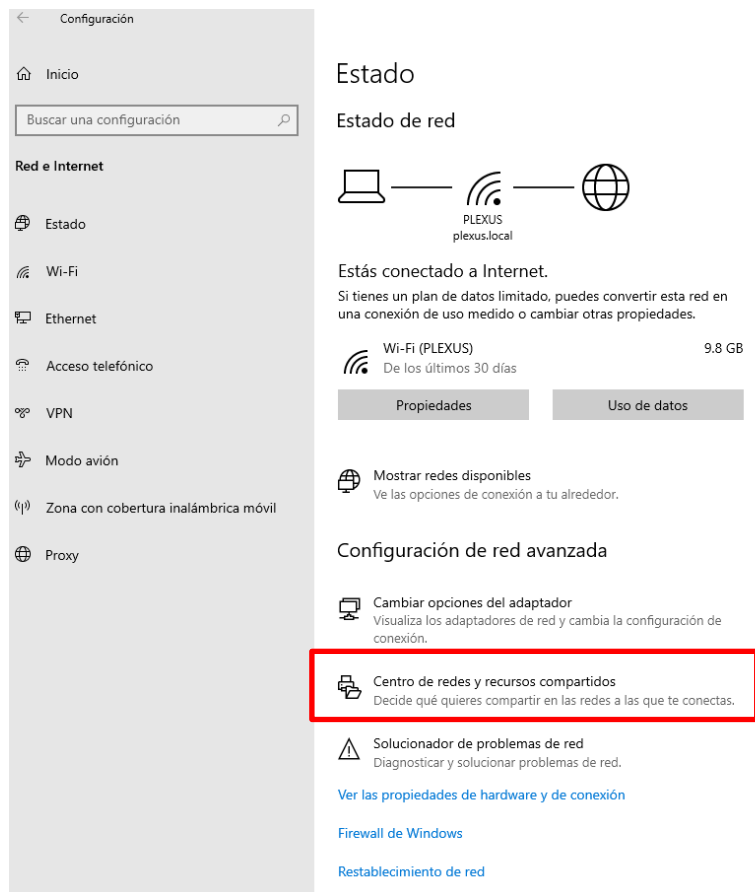
1. En Windows vaya a Inicio → **Configuración**.



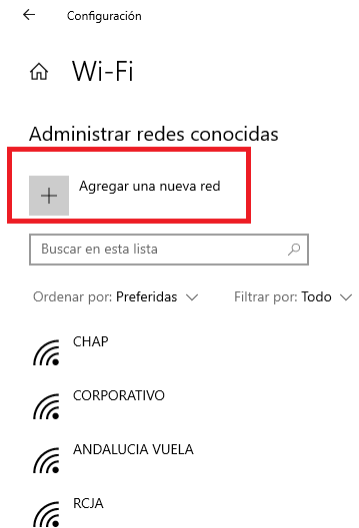
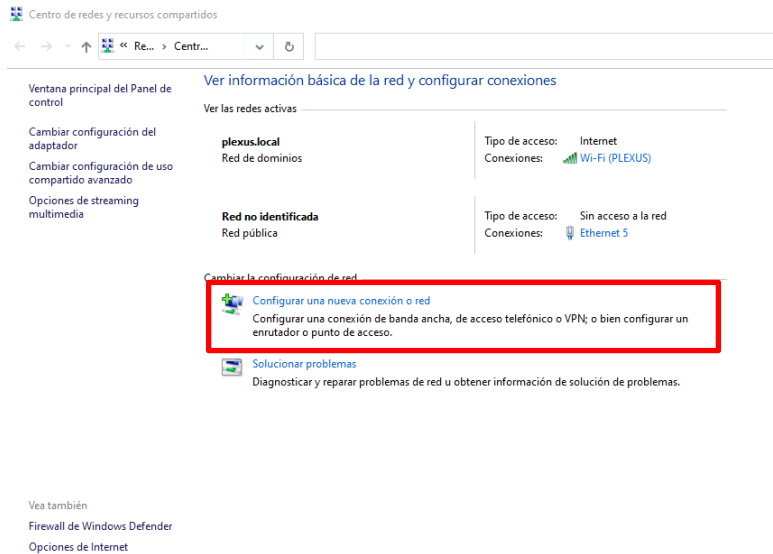
2. Se abrirá la siguiente ventana, seleccionar **Red e Internet** (se adjuntan diversas capturas en función del plataforma del equipo)



3. A continuación, seleccionar **Centro de redes y recursos compartidos** (se adjuntan diversas capturas en función del plataformado del equipo)



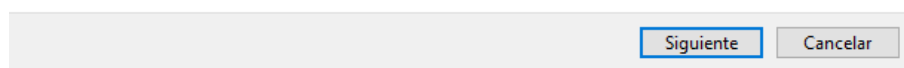
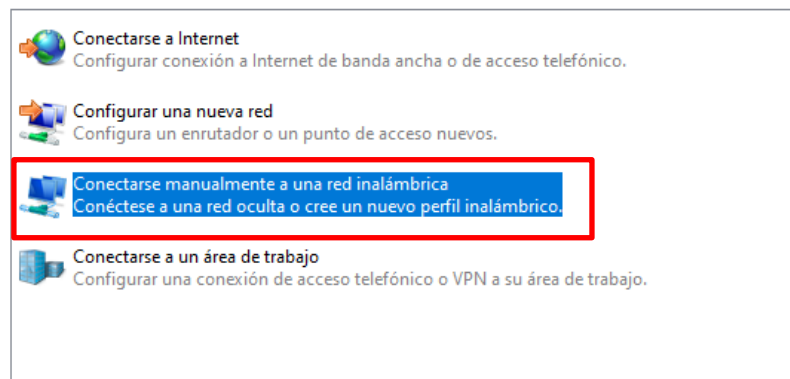
4. Elegir **Configurar una nueva conexión o red** (se adjuntan diversas capturas en función del plataformado del equipo)



5. Seleccionar **Conectarse manualmente a una red inalámbrica**.

← Configurar una conexión o red

Elegir una opción de conexión



6. Se abrirá la siguiente ventana (según equipo), rellenar:

- Nombre de la red: RCJA
- Tipo de Seguridad: WPA2-Enterprise
- Seleccionar Siguiente

← Conectarse manualmente a una red inalámbrica

Escriba la información de la red inalámbrica que desea agregar.

Nombre de la red:

Tipo de seguridad:

Tipo de cifrado:

Clave de seguridad: ☐ Ocultar caracteres

☒ Iniciar esta conexión automáticamente

☐ Conectarse aunque la red no difunda su nombre

Advertencia: esta opción podría poner en riesgo la privacidad del equipo.

Agregar una nueva red

Nombre de red

Tipo de seguridad

Método EAP

Método de autenticación

☐ Conectar automáticamente

☐ Conectarse aunque esta red no esté retransmitiendo

7. Seleccionar **Cambiar la configuración de la conexión**:

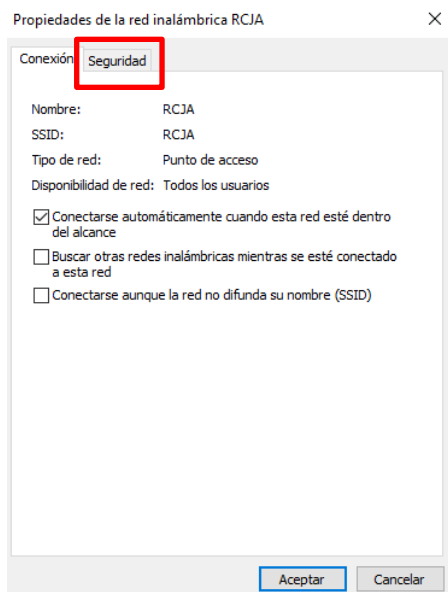
← Conectarse manualmente a una red inalámbrica

RCJA se agregó correctamente.

→ [Cambiar la configuración de conexión](#)

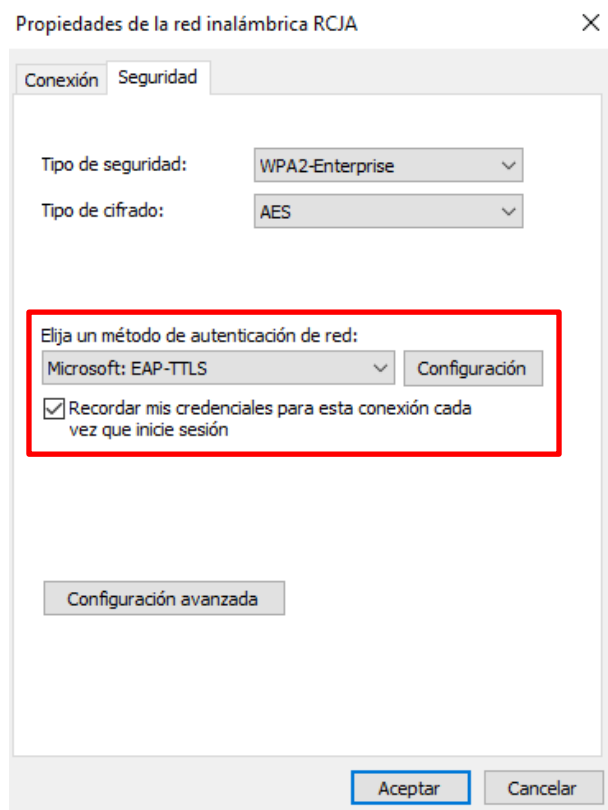
Abra las propiedades de la conexión para cambiar la configuración.

8. Se abrirá la siguiente ventana y hay que seleccionar en la pestaña **Seguridad**:



9. Se abrirá la siguiente ventana. Seleccionar:

- Elija un método de autenticación de red: Microsoft: EAP-TTLS
- Pulsar en Configuración



10. Seleccionar lo siguiente:

- Especificar modo de autenticación: Autenticación de usuarios
- Pulsar en Guardar credenciales

Configuración avanzada

Configuración de 802.1X Configuración de 802.11

☒ Especificar modo de autenticación:

Autenticación de usuarios Guardar credenciales

☐ Eliminar credenciales de todos los usuarios

☐ Habilitar inicio de sesión único en esta red

☒ Realizar inmediatamente antes de que el usuario inicie sesión

☐ Realizar inmediatamente después de que el usuario inicie sesión

Retraso máximo (segundos): 10

☒ Permitir cuadros de diálogo adicionales durante el inicio de sesión único

☐ Esta red usa LAN virtuales separadas para la autenticación de usuarios y equipos

Aceptar Cancelar

11. Insertar las credenciales del usuario LDAP:

Seguridad de Windows

Guardar credenciales

Al guardar las credenciales, permites que el equipo se conecte a la red cuando no tienes la sesión iniciada (por ejemplo, para descargar actualizaciones).

lan.sandetel

••••••••••

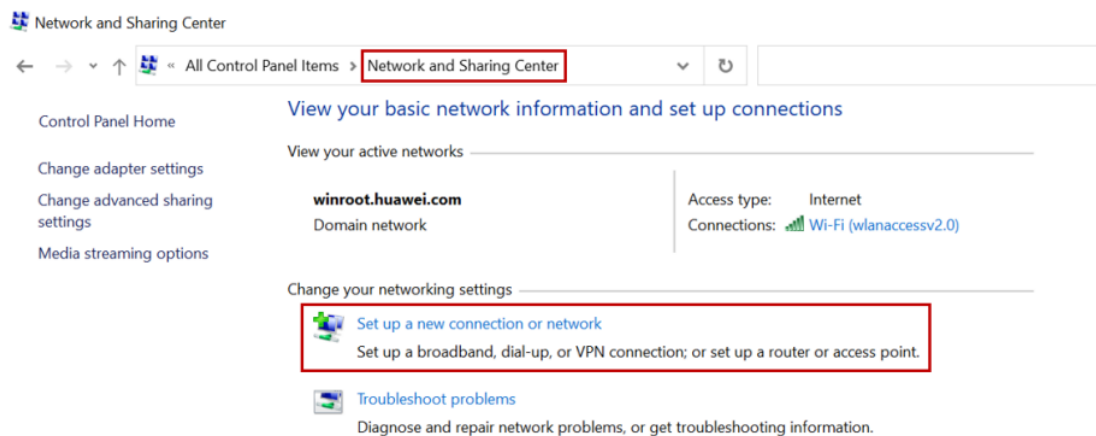
Aceptar Cancelar

12. Aceptar y guardar todos los cambios anteriores.

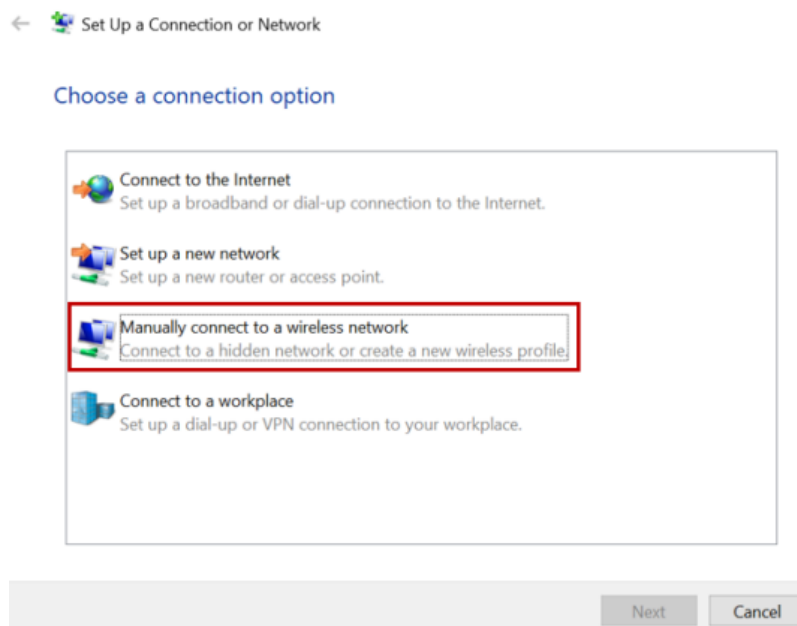
4.1.5 Dispositivos Windows 8

Los siguientes pasos describen cómo configurar un dispositivo Windows 8 para autenticarse en una red inalámbrica configurada para utilizar la Red Corporativa. El protocolo de autenticación recomendado es PAP TTLS.

1. En Windows, vaya al Centro de redes y recursos compartidos.
2. Haga clic en Configurar una nueva conexión o red.



3. Seleccione Conectarse manualmente a una red inalámbrica.



4. Introduzca la información de la red inalámbrica:
 - Especifique el nombre del SSID: **RCJA**
 - Seleccione WPA2-Enterprise como tipo de seguridad.

← Conectarse manualmente a una red inalámbrica

Escriba la información de la red inalámbrica que desea agregar.

Nombre de la red:

Tipo de seguridad:

Tipo de cifrado:

Clave de seguridad: ☐ Ocultar caracteres

☒ Iniciar esta conexión automáticamente

☐ Conectarse aunque la red no difunda su nombre

Advertencia: esta opción podría poner en riesgo la privacidad del equipo.

- Una vez añadida correctamente la nueva configuración WiFi, haga clic en Cambiar configuración de conexión para abrir las propiedades de la conexión.

← Conectarse manualmente a una red inalámbrica

RCJA se agregó correctamente.

[→ Cambiar la configuración de conexión](#)
Abra las propiedades de la conexión para cambiar la configuración.

- Vaya a la pestaña Seguridad de la página de propiedades de la conexión:
 - Elija Microsoft: EAP-TTLS como método de autenticación.

a. Haga clic en Configuración.

Propiedades de la red inalámbrica RCJA

Conexión Seguridad

Nombre: RCJA
SSID: RCJA
Tipo de red: Punto de acceso
Disponibilidad de red: Todos los usuarios

☒ Conectarse automáticamente cuando esta red esté dentro del alcance
☐ Buscar otras redes inalámbricas mientras se esté conectado a esta red
☐ Conectarse aunque la red no difunda su nombre (SSID)

Aceptar Cancelar

- Seleccione PAP como método de autenticación no EAP

TLS Properties

☐ Enable identity privacy
anonymous

Server certificate validation

Connect to these servers:

Trusted Root Certification Authorities:

- ☐ AAA Certificate Services
- ☐ AC RAIZ DNIE
- ☐ AC RAIZ DNIE
- ☐ AC RAIZ DNIE 2
- ☐ AC RAIZ FNMT-RCM

☐ Don't prompt user if unable to authorize server

Client authentication

☒ Select a non-EAP method for authentication
Unencrypted password (PAP)

☐ Automatically use my Windows account name and password (and domain, if any)

☐ Select an EAP method for authentication
Huawei EAP-GTC

Configure

OK Cancel

7. Cierre la ventana Configuración de TTLS y seleccione Configuración avanzada.

Propiedades de la red inalámbrica RCJA

Conexión Seguridad

Tipo de seguridad: WPA2-Enterprise

Tipo de cifrado: AES

Elija un método de autenticación de red:
Microsoft: EAP-TTLS Configuración

☒ Recordar mis credenciales para esta conexión cada vez que inicie sesión

Configuración avanzada

Aceptar Cancelar

8. Marque Especificar modo de autenticación.
9. Seleccione Autenticación de usuario.

Configuración avanzada

Configuración de 802.1X Configuración de 802.11

☒ Especificar modo de autenticación:
Autenticación de usuarios Guardar credenciales
☐ Eliminar credenciales de todos los usuarios

☐ Habilitar inicio de sesión único en esta red
☒ Realizar inmediatamente antes de que el usuario inicie sesión
☐ Realizar inmediatamente después de que el usuario inicie sesión
Retraso máximo (segundos): 10

☒ Permitir cuadros de diálogo adicionales durante el inicio de sesión único
☐ Esta red usa LAN virtuales separadas para la autenticación de usuarios y equipos

Aceptar Cancelar

10. Haga clic en Guardar credenciales.

11. Introduzca las credenciales del usuario.

Seguridad de Windows

Guardar credenciales

Al guardar las credenciales, permites que el equipo se conecte a la red cuando no tienes la sesión iniciada (por ejemplo, para descargar actualizaciones).

Aceptar Cancelar

4.1.6 Dispositivos MAC

Los siguientes pasos describen cómo configurar un dispositivo MacOS para autenticarse en una red inalámbrica configurada para utilizar la red Corporativa. El protocolo de autenticación recomendado es PAP TTLS.

4.1.6.1 Procedimiento en versiones más antiguas de MacOS

General
Mandatory

Passcode
Not configured

Restrictions
Not configured

Global HTTP Proxy
Not configured

Content Filter
Not configured

Domains
Not configured

Wi-Fi
1 Payload Configured

VPN
Not configured

AirPlay
Not configured

AirPrint
Not configured

Mail
Not configured

Exchange ActiveSync
Not configured

LDAP
Not configured

Calendar
Not configured

Contacts
Not configured

Subscribed Calendars
Not configured

Web Clips
Not configured

Fonts
Not configured

Certificates
Not configured

SCEP
Not configured

Wi-Fi

Service Set Identifier (SSID)
Identification of the wireless network to connect to
<YOUR SSID NAME>

☐ **Hidden Network**
Enable if target network is not open or broadcasting

☐ **Auto Join**
Automatically join this wireless network

Proxy Setup
Configures proxies to be used with this network
None

Security Type
Wireless network encryption to use when connecting
WPA / WPA2 Enterprise

Enterprise Settings
Configuration of protocols, authentication, and trust
Protocols Trust

Accepted EAP Types
Authentication protocols supported on target network
☐ TLS ☐ LEAP ☐ EAP-FAST ☐ EAP-AKA
☒ TTLS ☐ PEAP ☐ EAP-SIM

Username
Username for connection to wireless network
[set on device]

☒ **Use Per-Connection Password**
Request during connection and send with authentication

Password
Password for the provided username
[set on device]

Identity Certificate
Credentials for connection to wireless network
No applicable Certificate payload is configured

Inner Authentication
Authentication protocol (for use only with TTLS)
PAP

Outer Identity
Externally visible identification (for TTLS, PEAP, and EAP-FAST)

Network Type
Configures network to appear as legacy or Passpoint
Standard

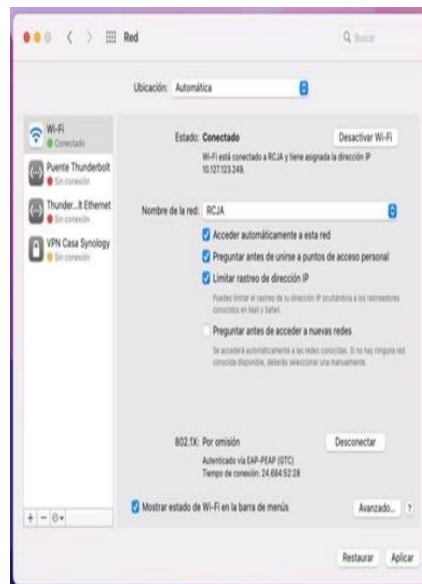
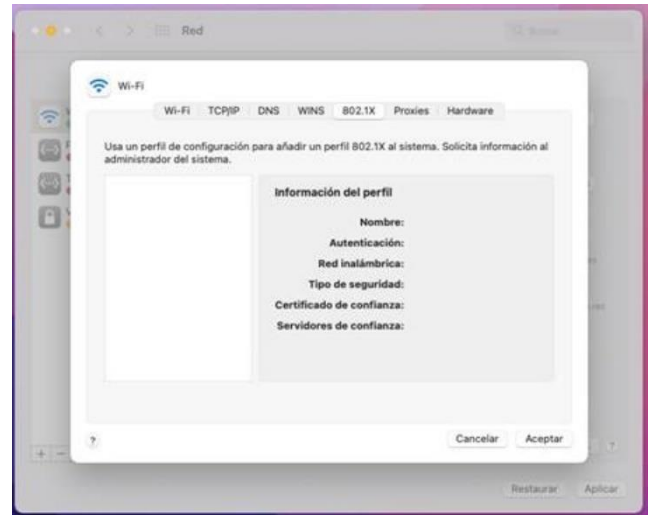
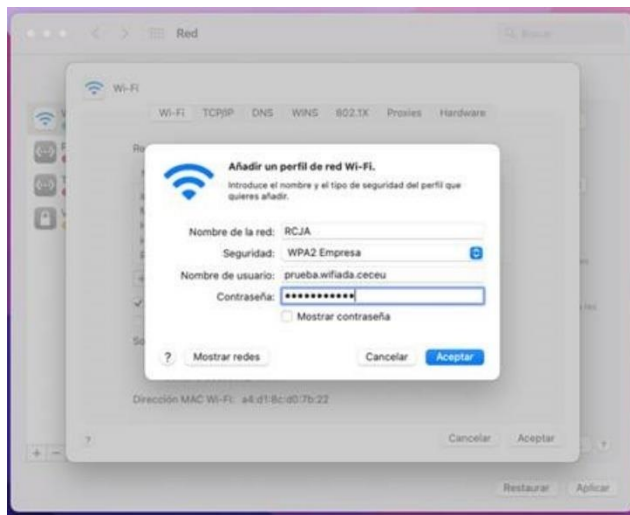
1 validation error

Cancel Save

4.1.6.2 Procedimiento con versiones actuales.

Los pasos a seguir son:

1. Añadir un nuevo perfil inalámbrico
2. Introducir los siguientes valores:
 - Nombre de la red: RCJA
 - Seguridad: WPA2 Empresa
 - Introducir LDAP como nombre de usuario y la contraseña



4.1.7 Dispositivos Linux

Los siguientes pasos describen cómo configurar un dispositivo Linux para autenticarse en una red inalámbrica configurada para utilizar la red Corporativa.

Servidor Debian

Descargar wpa_supplicant

```
sudo apt-get install wpa_supplicant
```

Editar /etc/wpa_supplicant.conf

```
ctrl_interface=DIR=/var/run/wpa_supplicant GROUP=wheel
network={
    ssid="CORPORATIVO"
    scan_ssid=1
    key_mgmt=WPA-EAP
    eap=PEAP
    identity="usuario"
    password="foobar"
    ca_cert="/etc/cert/ca.pem"
    phase1="peaplabel=0"
    phase2="auth=MSCHAPV2"
}
```

4.2 SSID IoT

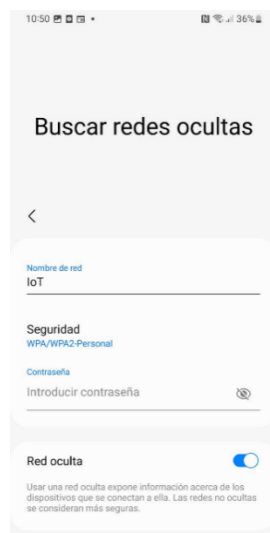
Para que un dispositivo se conecte a la red IoT previamente debe estar identificado y dado de alta en la plataforma ya que autenticación será por contraseña y MAC.

El primer paso será que el responsable del organismo remita al cau WIFI (cau.wifi.sandetelel@juntadeandalucia.es) el listado de dispositivos que podrán conectarse a la red, así como la MAC asociada a cada uno.

Los siguientes pasos describen cómo conectarse a la red IoT. Estos pasos son válidos tanto para ordenadores (Windows/MAC/Linux) como para dispositivos móviles (Android/IOS).

Diríjase a la sección WiFi de su dispositivo. (Ajustes → Redes e Internet → WiFi). La red IoT es una red oculta por lo que NO se mostrará en la lista de redes disponibles. Para conectarse, seleccione la opción "Añadir red".

1. En el apartado "SSID" o "Nombre de Red", escriba **"IoT"**.
2. Seguridad: WPA2/WPA3.
3. Privacidad: Filtrado MAC^{1 2}
4. Guardar.



¹ Para dispositivos con versión Android 13 o superior, al crear la red, en opciones avanzadas, se debe indicar que la red está oculta.

² Hay que tener especial cuidado de configurar el tipo de MAC del dispositivo y fijarlo en **"MAC del Dispositivo"**, ya que muchas versiones actuales permiten y utilizan por defecto **"MAC Aleatoria"**

5. Seleccione esta red. Deberá introducir la contraseña correspondiente, si no dispone de ella el administrador podrá solicitarla al CAU WIFI y, si el dispositivo está autorizado para conectarse a esta red, automáticamente se autentica y se muestra en la pantalla un mensaje de “Conectado”.



5 Gestión de Incidencias

La gestión de incidencias se realizará siguiendo los mismos procedimientos establecidos para los servicios de Red Corporativa.

Se habilitará un flujo específico dentro de la herramienta definida (<https://sio-rcja.juntadeandalucia.es/>). A su vez, y mientras que esté definido se podrán comunicar vía teléfono (300 004 / 955 061 031) y correo electrónico (cau.wifi.sandetel@juntadeandalucia.es).