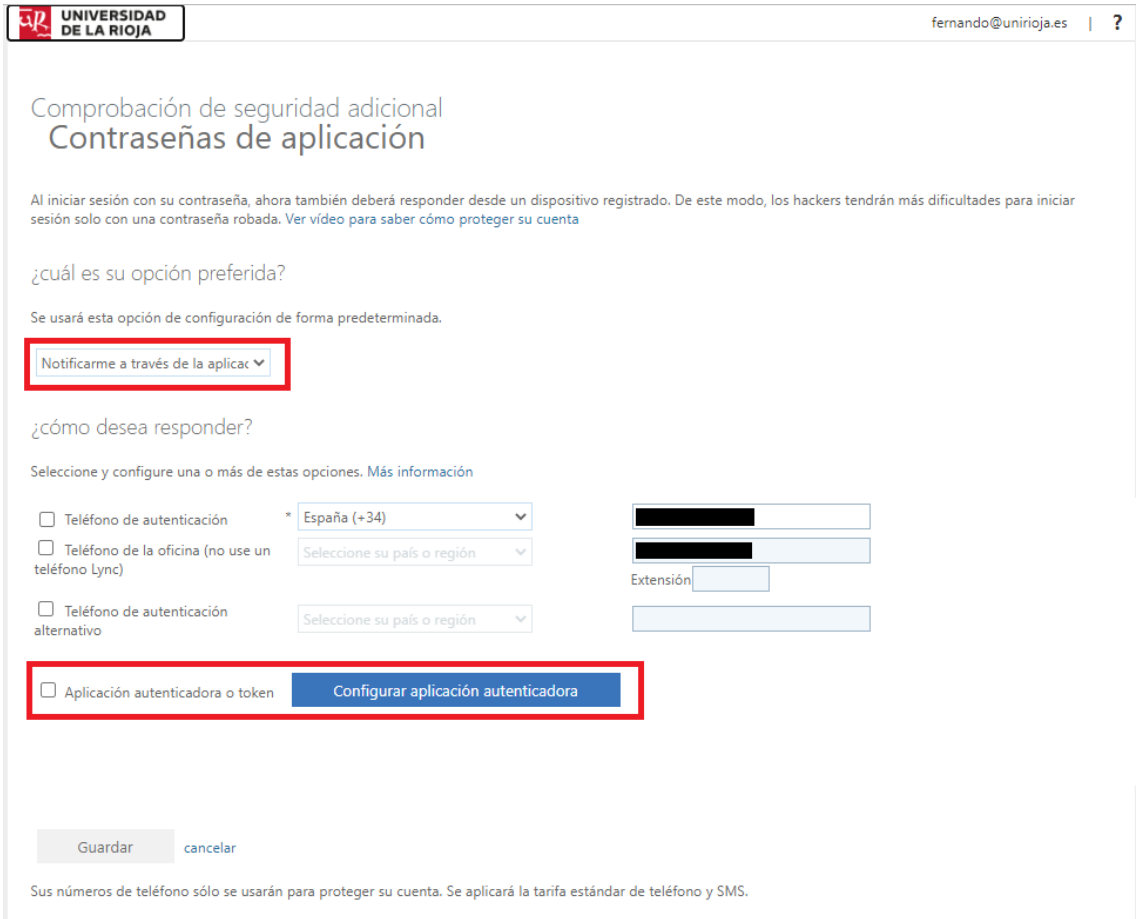
# ***CONFIGURAR OPCIONES DE MFA EN LA CUENTA DE USUARIO***

Antes de empezar con la configuración del cliente de VPN para MFA es recomendable que el usuario tenga configuradas las opciones para recibir el segundo factor de autenticación.

Si es la primera vez que va a usar este sistema de MFA, siga estos pasos, que figuran a continuación. Si ya está usando el MFA para otros servicios de M365, puede obviar este paso previo y puede pasar directamente al apartado 2 para la configuración del MFA para el cliente de VPN (forticlient) de este documento.

## 1.- CONFIGURAR LAS OPCIONES Y EL MODO DE AUTENTICACIÓN MFA QUE SE PEDIRÁ EN LAS APLICACIONES.

1. Acceder a https://aka.ms/mfasetup
   Se presentará una pantalla similar a la siguiente.
   De entre las opciones que se presenta, os recomendamos activar al menos 2 (Teléfono de autenticación y Aplicación de autenticación o token).



2. Para el uso de la Aplicación de Autenticación, se necesitará instalar en el dispositivo móvil una APP (Microsoft Authenticator, Google Authenticator, otras).
   **Recomendamos instalar "Microsoft Authenticator"** que está disponible para Android e iOS.


3. Para integrar la autenticación MFA de la VPN, escanear el código QR que se proporcionará por Microsfoft que se genera en el apartado 1 de este documento en "***Configurar aplicación autenticadora***".

## 2.- CONFIGURACIÓN DE DOBLE FACTOR DE AUTENTICACIÓN EN CLIENTE VPN (FORTICLIENT)

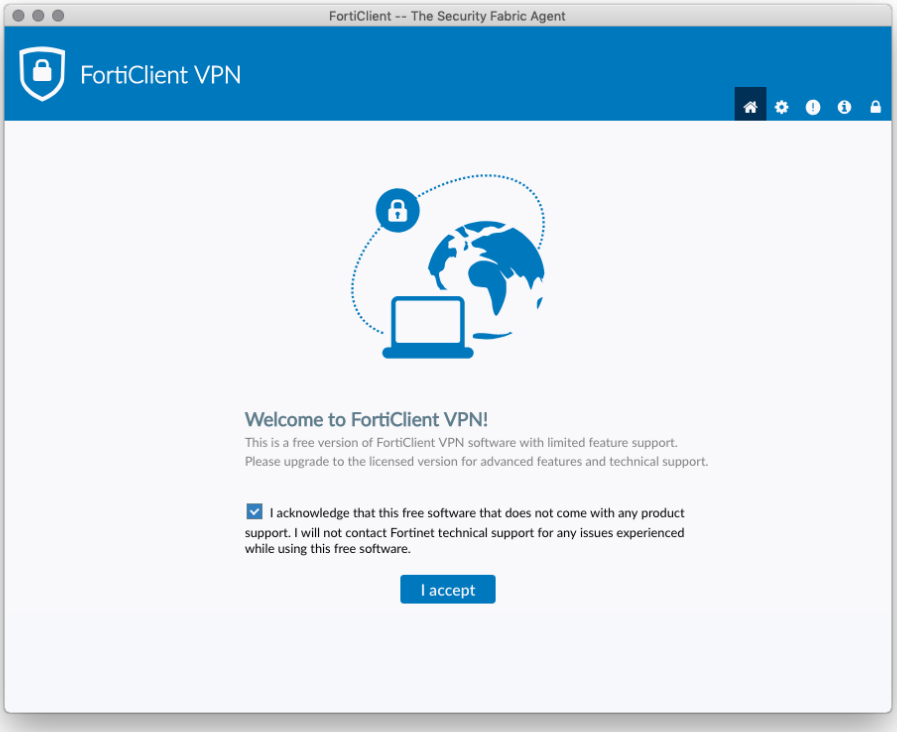
Para la configuración del 2FA en el acceso al servicio de VPN de la UR con el SW forticlient, seguir los siguientes pasos:

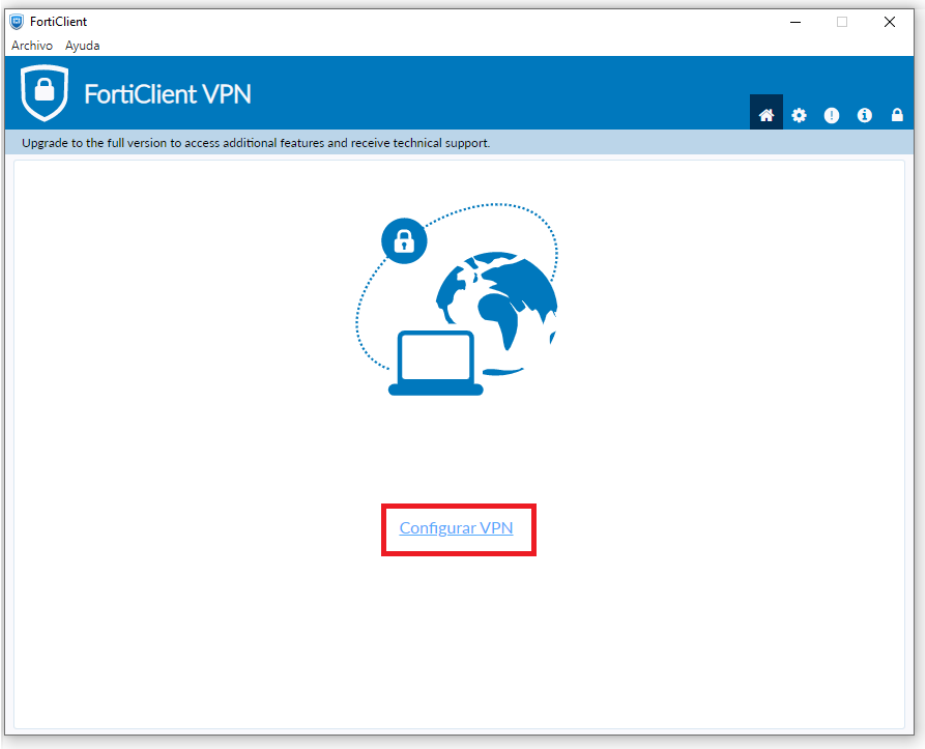
1. El PAS y PDI no necesita hacer este paso. Los alumnos tienen que autosuscribirse al grupo que permite el acceso por vpn: fwgs_vpn_alum_ok.
   En este enlace puedes ver un video de cómo hacerlo.
   Una vez hecho tendrás que esperar a que se sincronicen los sistemas de gestión de identidad. Como se realiza cada hora tendrás que esperar eso como máximo para acceder.

2. Instalar el software
   En función del dispositivo y/o sistema operativo desde el que va a acceder, descargue e instale en el equipo **la última versión** del cliente de VPN que le corresponda
   para Windows 10 o superior
   Mac OS 11 Big Sur o superior
   Linux tipo Debian
   Linux tipo Redhat

3. Una vez instalado, inicie FortiClient, marque la casilla de verificación y haga clic en el botón "*Aceptar*".

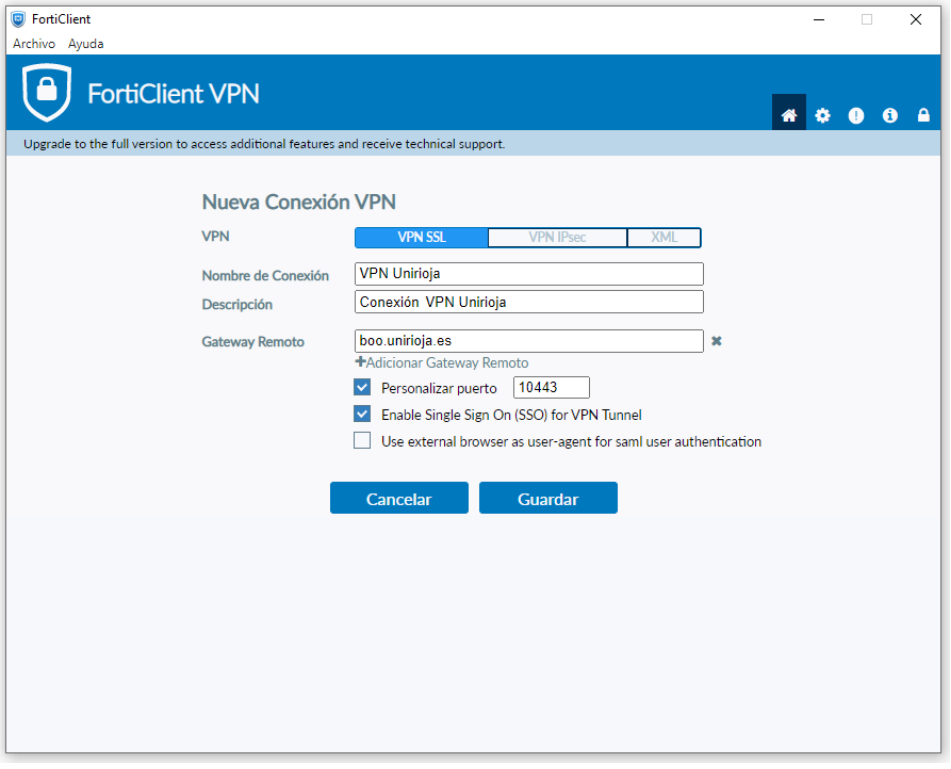
4. En la siguiente pantalla, deberá hacer clic en "*Configurar VPN*".



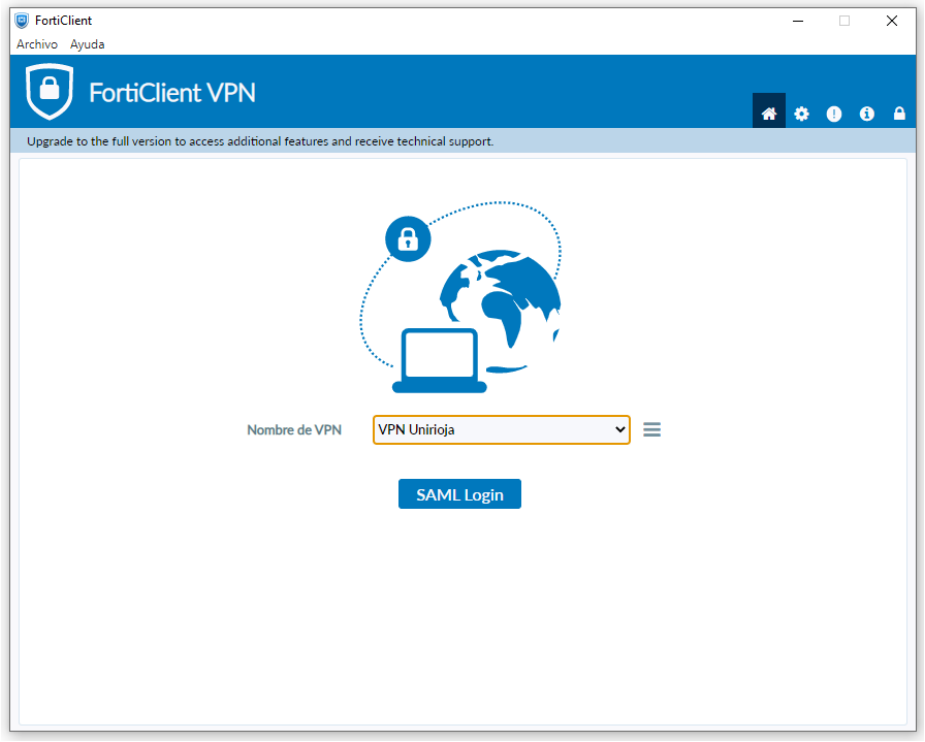



5. En la nueva pantalla, deberá completar la información como se especifica a continuación y se ve en la siguiente captura. Después hacer clic en "*Guardar*".

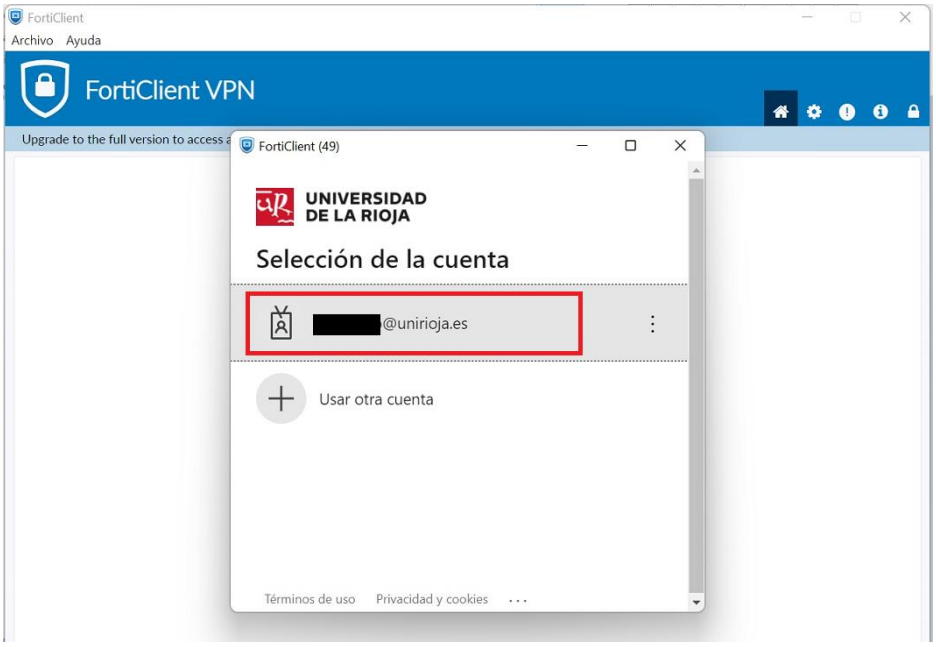
    a. Seleccione la pestaña “VPN SSL”
    b. Nombre de conexión “VPN Unirioja”
    c. Descripción “Conexión VPN Unirioja”
    d. Gateway Remoto: “boo.unirioja.es”
    e. Personalizar puerto: 10443
    f. Enable SSO for VPN Tunel



6. Una vez creada la conexión VPN, haga clic en "SAML Login".

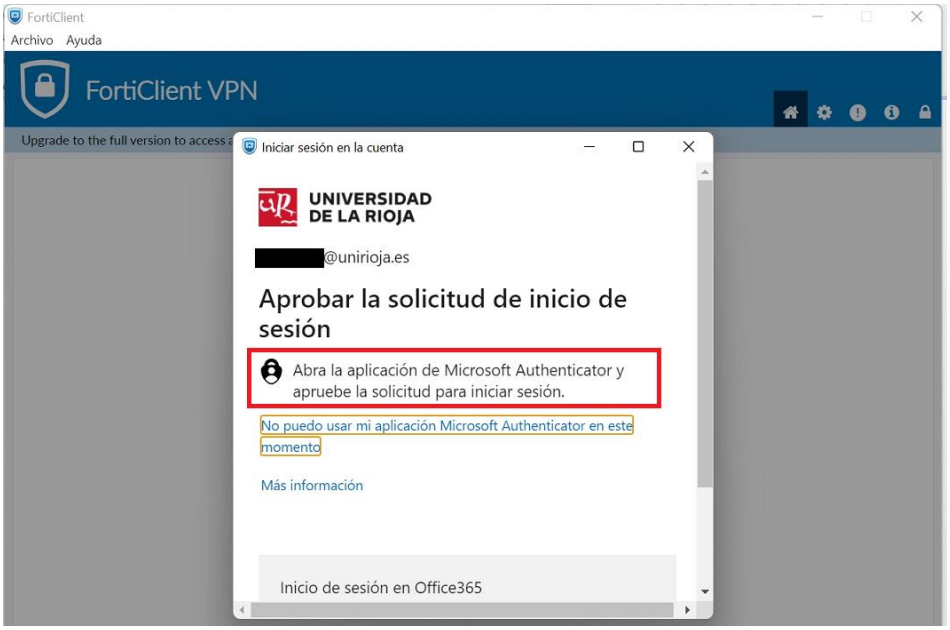



7. Luego ingrese los datos de su CUASI: *"Nombre_Usuario y contraseña"*.

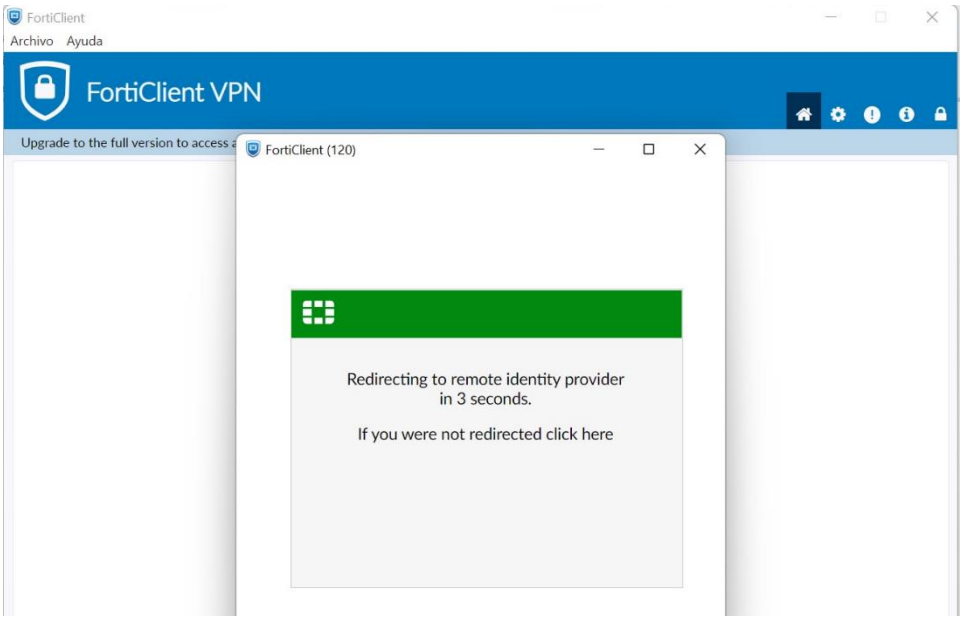


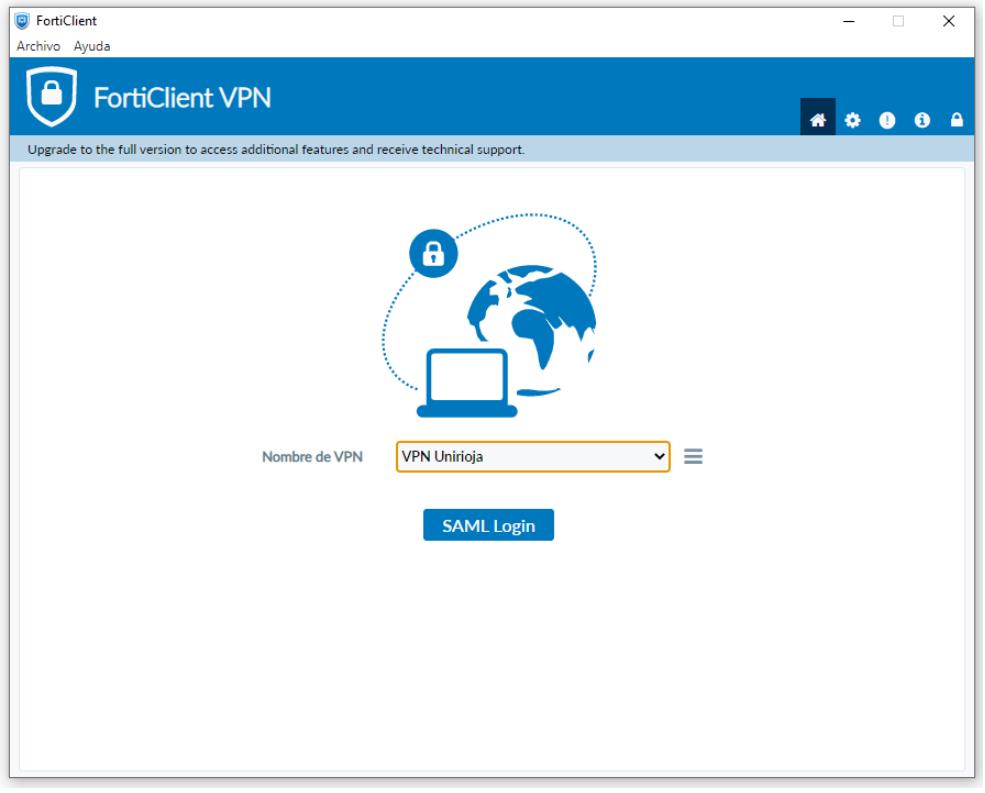

8. Se le pedirá que autorice el inicio de sesión con Multi-Factor Authentication (MFA) utilizando el método de su elección: Token, llamada telefónica, SMS, aprobación. Estos son las posibles opciones:


9. En la siguiente imagen aparece la opción de “aprobación”, por lo que según el método elegido, pueden aparecer otro tipo de pantallas diferentes.

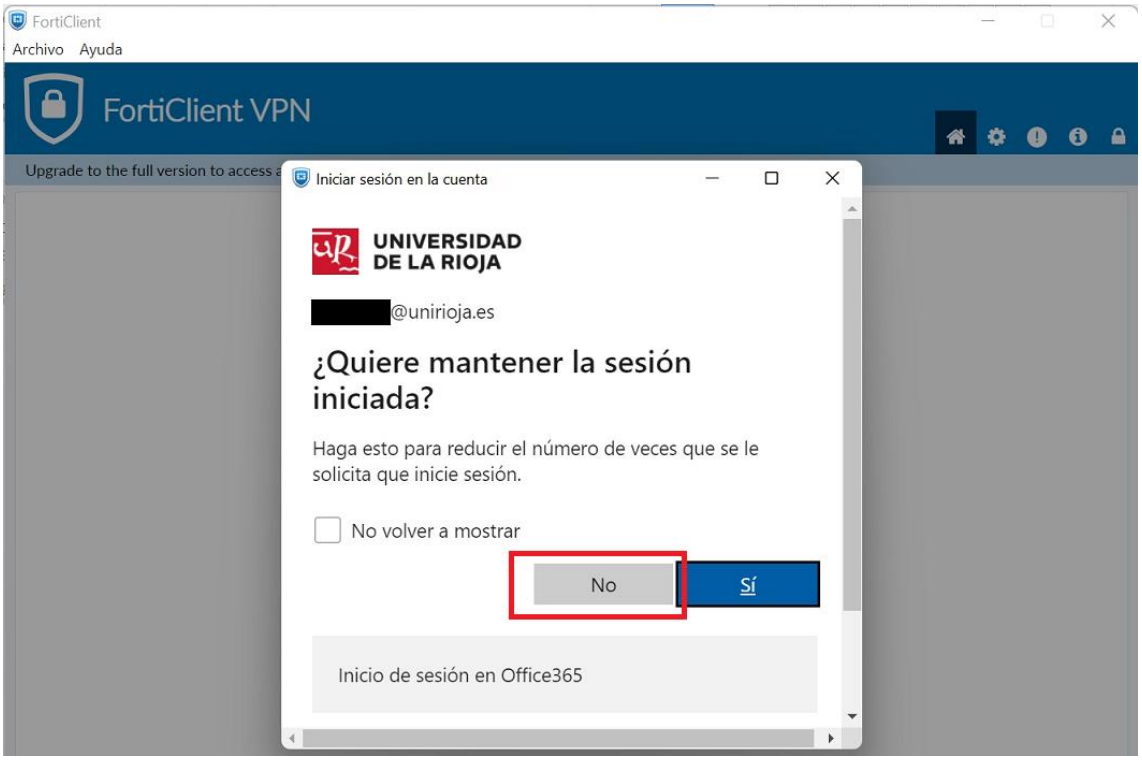


10. Si se encuentra bloqueado en una pantalla con una cuenta atrás, o no le conecta al servicio de VPN, cierre la ventana "Inicio sesión en la cuenta" y haga clic de nuevo en "Inicio de sesión SAML".

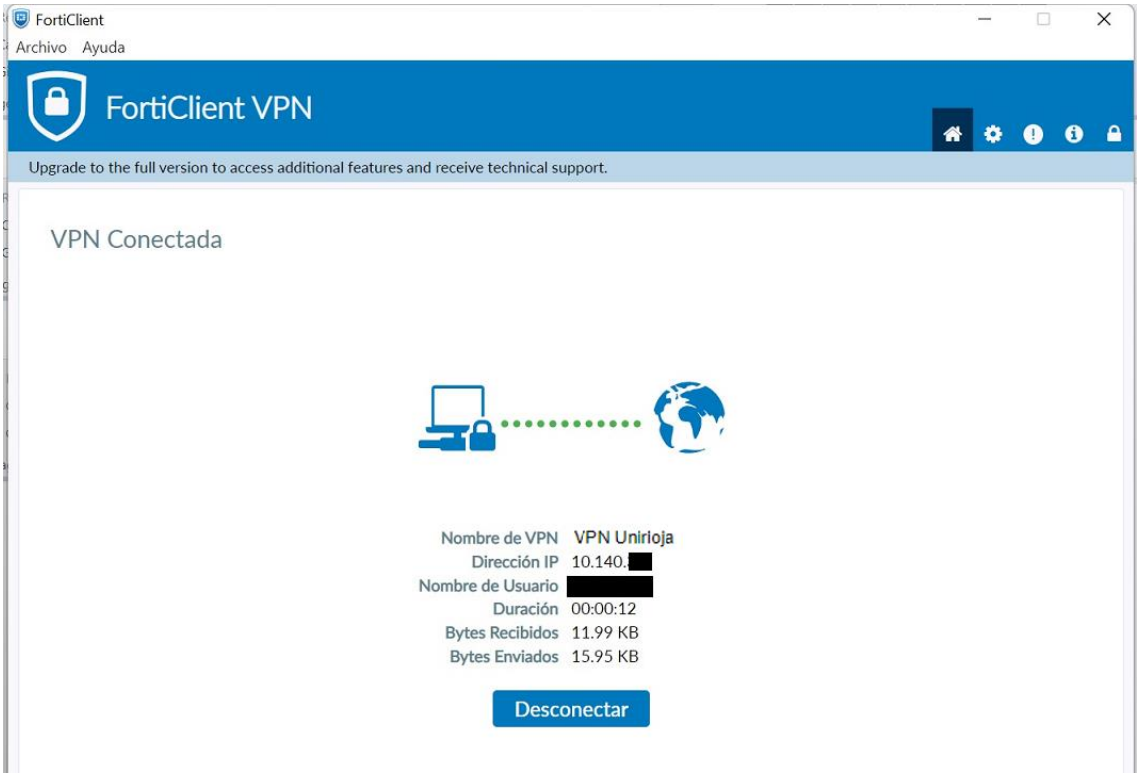



11. Ante la aparición de pregunta de “¿Quiere mantener la sesión iniciada?” que aparece en la siguiente ventana, pulse “NO”, ya que en caso contrario no se le volverá a pedir la autenticación, y cualquier otra persona que use ese equipo podrá establecer la VPN con sus credenciales.




12. Si ha configurado bien el perfil y ha introducido correctamente los datos de autenticación, debería estar conectado.




13. Cuando haya finalizado la sesión de VPN, **recuerde desconectar el cliente**.