



SIC-IT-006 Manual uso VPN-SSL para personal Unileon



	REDACTADO	REVISADO	APROBADO
NOMBRE	Jaime Álvarez Fernández	Víctor Coca Riega	Víctor Coca Riega
CARGO	Técnico informático - Redes		Responsable Área Comunicaciones SIC

Fecha de Revisión:	29 de enero de 2026	Revisión:	2.0
--------------------	---------------------	-----------	-----

Tabla de contenido

1.	Objeto	4
2.	Alcance	4
3.	Responsabilidades	4
4.	Instrucciones de uso de la VPN-SSL	4
4.1	Primera conexión al servicio VPN-SSL de la Universidad de León desde PC	4
4.1.1	<i>Acceso a url</i>	4
4.1.2	<i>Asistente de actualizaciones</i>	5
4.1.3	<i>Login</i>	6
4.1.4	<i>Sincronización con dispositivo generador de tokens</i>	6
4.1.5	<i>Instalación de aplicaciones específicas</i>	7
4.2	Segunda conexión y siguientes desde PC	8
5.	Referencias	9
6.	Glosario.....	9

Tabla de figuras

Ilustración 1. Aviso de responsabilidad	5
Ilustración 2. Asistente de actualizaciones.....	5
Ilustración 3. Instrucciones Asistente de actualizaciones.....	5
Ilustración 4. Login.....	6
Ilustración 5. Sincronización OTP	6
Ilustración 6. Iniciador de aplicaciones.....	7
Ilustración 7. Instrucciones de instalación.....	8
Ilustración 8. Advertencia	8
Ilustración 9. Autenticación de dos factores	9

Manual del Sistema Integrado de Gestión del SIC de la ULE		
Hoja de control de revisiones. Hoja 1 de 1		
Nº Revisión	Fecha	Naturaleza de la revisión
0.1	26.10.2021	Primer ejemplar
1.0	26.10.2021	Revisado y aprobado
1.1	20.10.2022	Eliminadas referencias al proceso de solicitud
2.0	29.01.2026	Versión actualizada Ivanti

1. Objeto

Facilitar la conexión de usuarios Unileon a equipos o redes concretas dentro de la Universidad de León, realizando un cifrado de las comunicaciones.

2. Alcance

Personal de la Universidad de León que necesiten por diversos motivos conectarse a servicios, equipos o redes de la Universidad desde instalaciones externas a la Universidad.

3. Responsabilidades

El usuario de la Universidad de León será el responsable de poner a buen recaudo sus credenciales, así como el uso que se dé a la conexión VPN-SSL.

El responsable último interno a la Universidad será la persona u órgano interno que autorizó dicha conexión.

4. Instrucciones de uso de la VPN-SSL

Los pasos generales para realizar una conexión VPN-SSL son:

1. Acceso a la URL <https://extranet.unileon.es/personal> (ver apartado 4.1.1) y mediante certificado digital identificarse.
2. Sincronización con el dispositivo generador de *tokens*, mediante *Google Authenticator* u otra autenticación de doble factor (2FA), solo en la primera conexión. En sucesivas conexiones será necesario disponer de la aplicación generadora de *tokens* (ver apartado 4.1.4).
3. Instalación de software específico a través del portal de conexión en los casos que sea necesario (ver apartado 4.1.5).

4.1 Primera conexión al servicio VPN-SSL de la Universidad de León desde PC

La primera conexión al servicio VPN-SSL se diferencia en varios pasos de las siguientes. Los pasos para seguir serán:

4.1.1 Acceso a url

Accederemos a la URL <https://extranet.unileon.es/personal>. Se nos mostrará un aviso de responsabilidad que debemos “Aceptar”, ya que si marcamos “Rechazar” no permitirá iniciar sesión en el sistema. (Ilustración 1. Aviso de responsabilidad).

Pre Sign-In Notification

Está usted accediendo a un sistema de tratamiento de la información propiedad de la Universidad de León. El acceso y uso de este sistema está permitido exclusivamente a las personas autorizadas y para fines estrictamente profesionales. La información a la que se accede por este medio es propiedad de la Universidad de León y está sujeta a las obligaciones de confidencialidad y seguridad establecidas en las políticas y normativas de seguridad de la organización.

El usuario se compromete a guardar el más absoluto secreto respecto de toda la información a la que tenga acceso a través de la aplicación y en particular, se obliga a no utilizarla con fines distintos a los que se les ha autorizado expresamente.

La Universidad de León podrá proceder a inspeccionar el contenido de los sistemas de información, y/o la configuración establecida en los mismos, para garantizar el correcto ejercicio de las funciones y competencias de la entidad, así como monitorizar el uso de la aplicación y de la información.



Ilustración 1. Aviso de responsabilidad

4.1.2 Asistente de actualizaciones

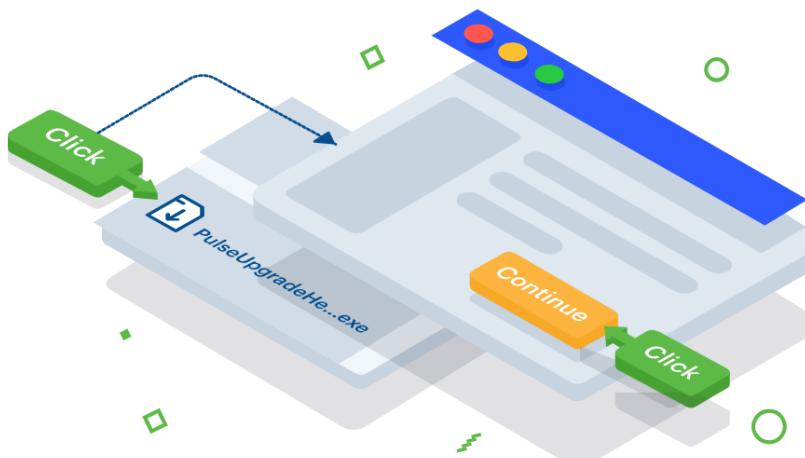
En el caso de que la plataforma VPN-SSL detecte que está instalada una versión antigua del cliente de Ivanti, aparecerá una ventana pidiendo la instalación del Asistente de actualizaciones (Ilustración 2. Asistente de actualizaciones). Una vez hecho clic en “Descargar” se nos darán unas instrucciones para instalar la utilidad (Ilustración 3. Instrucciones Asistente de actualizaciones) y se nos permitirá hacer login en la plataforma.

Parece que el asistente de actualizaciones no está instalado. Descárguelo ahora para continuar.



Ilustración 2. Asistente de actualizaciones

Cuando se haya completado la descarga del asistente de actualizaciones, siga estos pasos para la instalación.



Cuando haya completado los pasos anteriores, haga clic [AQUÍ](#) para continuar con las actividades.

Ilustración 3. Instrucciones Asistente de actualizaciones

4.1.3 Login

Introducimos el usuario (sin @unileon.es) y contraseña de Unileon. (Ilustración 4. Login)

The image shows the login page for the University of León's Personal SSL-VPN portal. On the left, there is a logo of the University of León and the text "Universidad de León" and "Portal SSL-VPN: PERSONAL". On the right, there is a "Bienvenido" section with the sub-instruction "Introduzca los datos para acceder a su portal". It features two input fields: "Usuario" and "Contraseña", both with placeholder text. Below the fields is a "Acceder" button. At the bottom left is a "Ayuda" link.

Ilustración 4. Login

4.1.4 Sincronización con dispositivo generador de tokens

En este paso convertiremos un dispositivo en un generador de *tokens* para acceder a la conexión. Para ello usaremos de ejemplo un smartphone y usaremos como generador de tokens la aplicación *Google Authenticator*, disponible tanto para Android como para IOS.

En pantalla (Ilustración 5. Sincronización OTP) se nos pide que configuremos la aplicación de nuestro Smartphone para generar el *token* de acceso que se pide en el punto “2. Introducir el código token que genera la aplicación”.

The image shows the synchronization screen for a two-factor authentication application. It has the header "UNIVERSIDAD DE LEÓN" and "PORTAL SSL-VPN: PERSONAL". A red box highlights the text "Agregar [redacted] cuenta de usuario para la aplicación de autenticación de dos factores". Below it, a blue box contains the instruction "Para obtener el código de acceso debe instalar una app de doble factor(Google Authenticator) en su smartphone o tablet.". The first step, "1. Configure la aplicación:", shows a QR code with a red cross over it and the text "Abra la aplicación de autenticación de dos factores y añada la cuenta de usuario [redacted] escaneando el código QR siguiente. Si no puede utilizar un código QR, introduzca este texto". The second step, "2. Introducir el código token que genera la aplicación:", has a text input field labeled "Enter Token Code" and a "Iniciar sesión" button at the bottom.

Ilustración 5. Sincronización OTP

Debemos buscar e instalar en la tienda de aplicaciones de nuestro Smartphone la aplicación *Google Authenticator*.

Una vez instalada, al abrir la aplicación por primera vez nos pedirá añadir una cuenta. Podemos usar el método “Escanear código de barras” o “Introducir una clave proporcionada”. Para “Escanear código de barras” simplemente pulsaremos y nos aparecerá en la pantalla del Smartphone la cámara de este. Con apuntar al cuadro del BIDI que nos ha salido en la pantalla de la “Ilustración 5. Sincronización OTP” nos aparecerán en pantalla los datos de nuestra cuenta.

Se nos pedirá confirmación de la cuenta que vamos a añadir. Pulsaremos en “Añadir cuenta”.

Con estos pasos ya se estarán generando *tokens* en nuestra aplicación *Google authenticator* para poder acceder al servicio VPN-SSL. Estos *tokens* se componen de 6 dígitos numéricos que van cambiando cada 30 segundos y se muestran en pantalla.

Podremos añadir más cuentas si fuese necesario en el botón “+” que nos aparece en la parte inferior de la pantalla.

Este *token* de 6 dígitos se debe introducir en el punto “2. Introducir el código token que genera la aplicación” mostrado en la “Ilustración 5. Sincronización OTP”, y pulsar “Iniciar sesión”.

4.1.5 Instalación de aplicaciones específicas

Se nos mostrará una pantalla (Ilustración 6. Iniciador de aplicaciones), donde se nos pide que descarguemos el software “Iniciador de aplicaciones” si es la primera vez que accedemos. Una vez hagamos clic en “Descargar”, nos aparecerán unas breves instrucciones para la correcta instalación (Ilustración 7. Instrucciones de instalación).

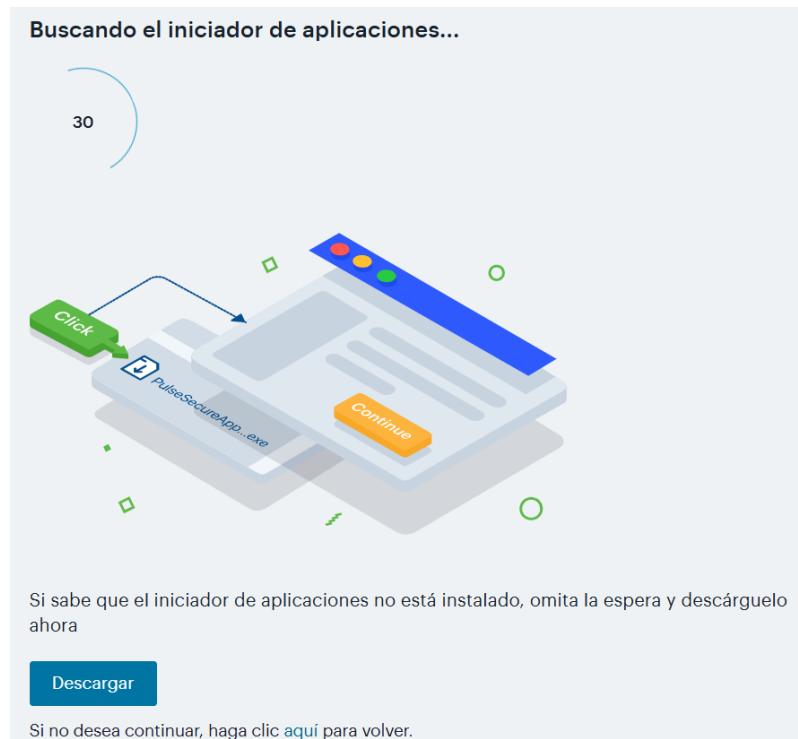


Ilustración 6. Iniciador de aplicaciones



Ilustración 7. Instrucciones de instalación

A continuación, se instalará el cliente de Ivanti automáticamente y nos aparecerá un icono que cuando se realice la conexión correctamente pasará a ser , con la esquina superior derecha verde, lo que indica que la conexión se ha establecido con éxito. Este icono estará en barra de tareas de Windows a la izquierda del reloj (puede que esté oculto y haya que desplegar (^)).

Es posible que, en algún momento de la instalación, a parte de los permisos pertinentes que pide Windows para instalar aplicaciones, aparezca una ventana de advertencia (Ilustración 8. Advertencia) en donde debemos dar permiso a la aplicación pulsando en "Siempre" para que se conecte al servidor.



Ilustración 8. Advertencia

4.2 Segunda conexión y siguientes desde PC

Una vez realizada la primera conexión, para realizar las siguientes conexiones, solo se nos pedirá:

- Acceso a url [https://extranet.unileon.es/personal\(apartado](https://extranet.unileon.es/personal(apartado) 4.1.1)
- Login (apartado 4.1.3)

-Autenticación de dos factores, que será un código de 6 dígitos generado en nuestro generador de tokens
(Ilustración 9. Autenticación de dos factores)

UNIVERSIDAD DE LEÓN
PORTAL SSL-VPN: PERSONAL

Página de credenciales adicionales de Ivanti Secure Access for [REDACTED]

Abra la aplicación de autenticación de dos factores en el dispositivo para ver su código de autenticación y verificar su identidad.

Si actualmente no tiene acceso al dispositivo, utilice uno de los códigos de copia de seguridad que ha guardado anteriormente.

CÓDIGO DE AUTENTICACIÓN:
[REDACTED]

Iniciar sesión

Ilustración 9. Autenticación de dos factores

Con esto ya habremos realizado la conexión satisfactoriamente y aparecerá el icono , con la esquina superior derecha verde, lo que indica que la conexión se ha establecido con éxito. Este icono estará en barra de tareas de Windows a la izquierda del reloj (puede que esté oculto y haya que desplegar (^)).

5. Referencias

Se ha utilizado manuales e información técnica del fabricante Pulse Secure, en concreto:

<https://www.pulsesecure.net/download/techpubs/current/567/pulse-client/pulse-secure-client-mobile/5.2rx/ps-pulse-android-for-work-guide.pdf>

https://www.pulsesecure.net/download/techpubs/current/1181/pulse-workspace/2.0.x/ps_pws_appliance_admin-guide-1743.1.pdf

6. Glosario

VPN-SSL: Una red VPN SSL (Virtual Private Network – Secure Sockets Layer) es una forma de red privada virtual (VPN) que se puede usar con un navegador web estándar. En contraste con la VPN IPsec (Internet Protocol Security) tradicional, una VPN SSL no requiere la instalación de software cliente especializado en la computadora del usuario final. Se utiliza para proporcionar a usuarios remotos con acceso a aplicaciones Web, aplicaciones cliente/servidor y conexiones de red internas.

TOKENS: Conjunto de números generado aleatoriamente y con caducidad limitada, para facilitar la doble autenticación de un servicio.