Servicio de Informática y Comunicaciones

SIC-IT-003 Manual uso VPN-SSL para usuarios externos

universidad de león

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

Fecha de Revisión: 02 de febrero de 2026	**Revisión:** 2.0

Tabla de contenido

Tabla de figuras

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	24.04.2017	Primer ejemplar
0.2	27.04.2018	Primera revisión
0.3	03.05.2018	Segunda revisión
1.0	30.05.2018	Revisión y aprobación del documento
2.0	02.02.2026	Versión actualizada Ivanti

1. Objeto

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

2. Alcance

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

3. Responsabilidades

Una vez creadas las credenciales y entregadas al usuario final (personal externo a la Universidad de León), la responsabilidad de poner a buen recaudo estas credenciales, así como el uso que se dé a la conexión VPN-SSL, queda en manos del usuario.

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

4. Instrucciones de uso de la VPN-SSL

Los pasos generales para realizar una solicitud y uso de conexión VPN-SSL:

1. Solicitud al Servicio de Informática y Comunicaciones (en adelante SIC) de conexión VPN-SSL por escrito mediante la herramienta telemática proporcionada (CAU).
2. Entrega al usuario final de credenciales para realizar la conexión mediante un medio acordado (email, teléfono, etc). La contraseña entregada será de un solo uso y se solicitará su cambio en la primera conexión.
3. Acceso a la URL https://extranet.unileon.es/tecnicos (ver apartado 4.1.1) y mediante el usuario y contraseña proporcionados identificarse.
4. 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 4.1.6).
5. Instalación de software específico a través del portal de conexión en los casos que sea necesario (ver apartado 4.1.7).

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 a 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).

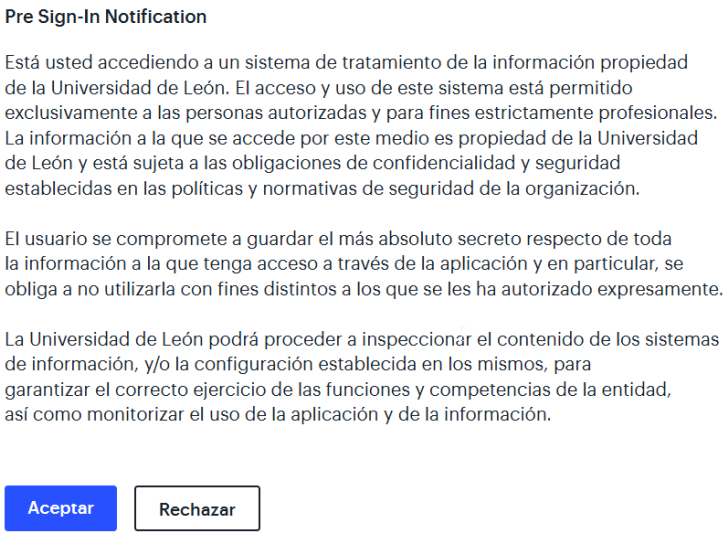

Ilustración 1. Aviso de responsabilidad

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.

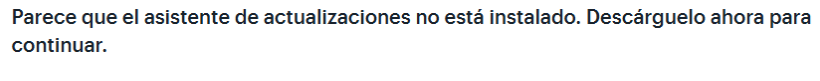

Ilustración 2. Asistente de actualizaciones

Ilustración 3. Instrucciones Asistente de actualizaciones

4.1.3 Login

Introducimos el usuario (sin @unileon.es) y contraseña proporcionada por el SIC. Esta contraseña será de un solo uso y será necesario cambiarla en la primera conexión. (Ilustración 4. Login)

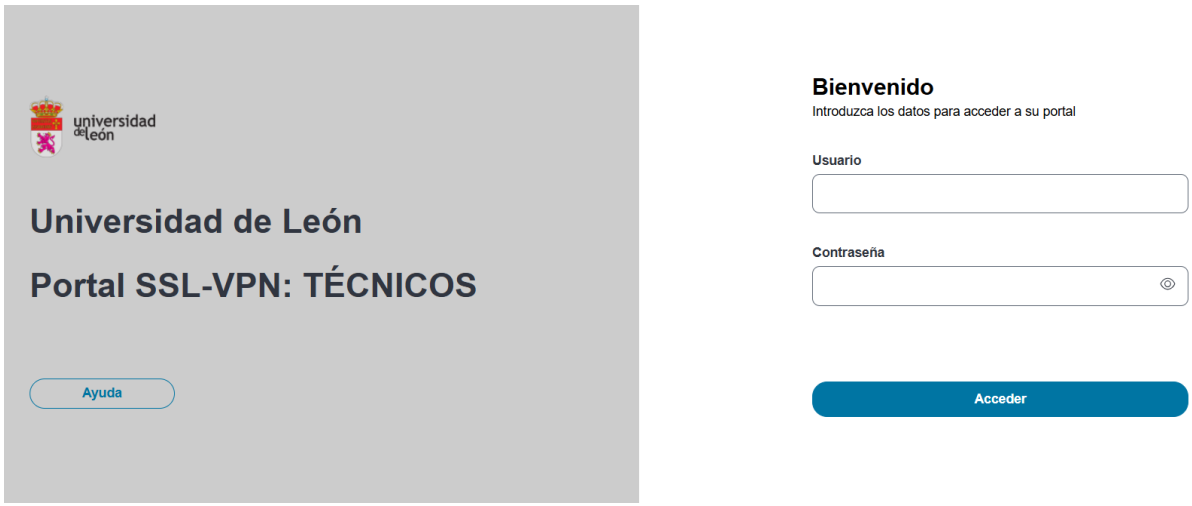

Ilustración 4. Login

4.1.4 Cambio de contraseña

Se nos pedirá el cambio de contraseña por ser la primera conexión realizada con este usuario. Introduciremos la contraseña antigua (proporcionada por el SIC) y dos veces la nueva contraseña que elijamos. Esta contraseña debe tener al menos un número, una letra y como mínimo 8 caracteres. Después pulsaremos "Cambiar contraseña" (Ilustración 5. Cambio contraseña).

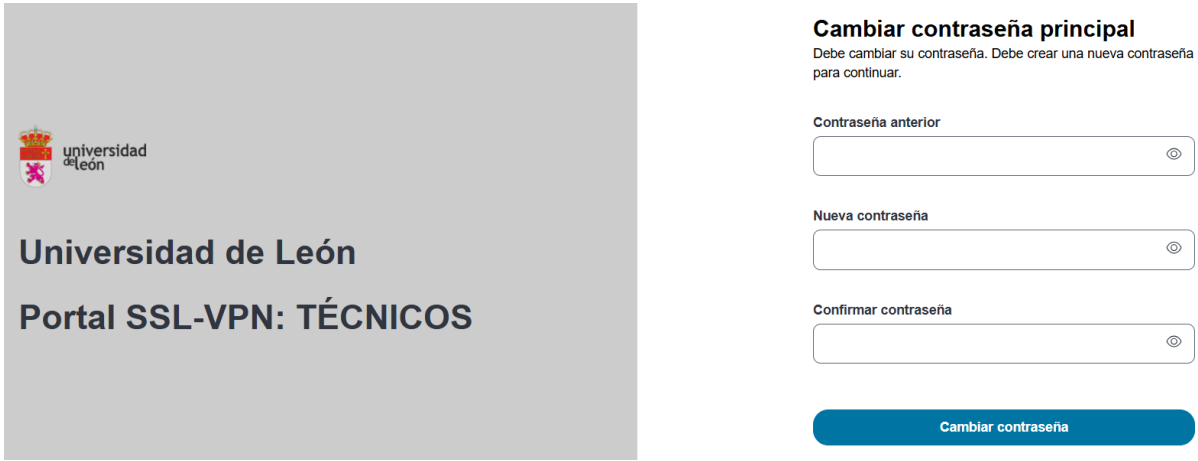

Ilustración 5. Cambio contraseña

4.1.5 Confirmación de cambio de contraseña y login

Se nos confirmará que el cambio se ha realizado y podremos insertar usuario y contraseña nueva. Pulsamos "Acceder" (Ilustración 6. Confirmación cambio contraseña)

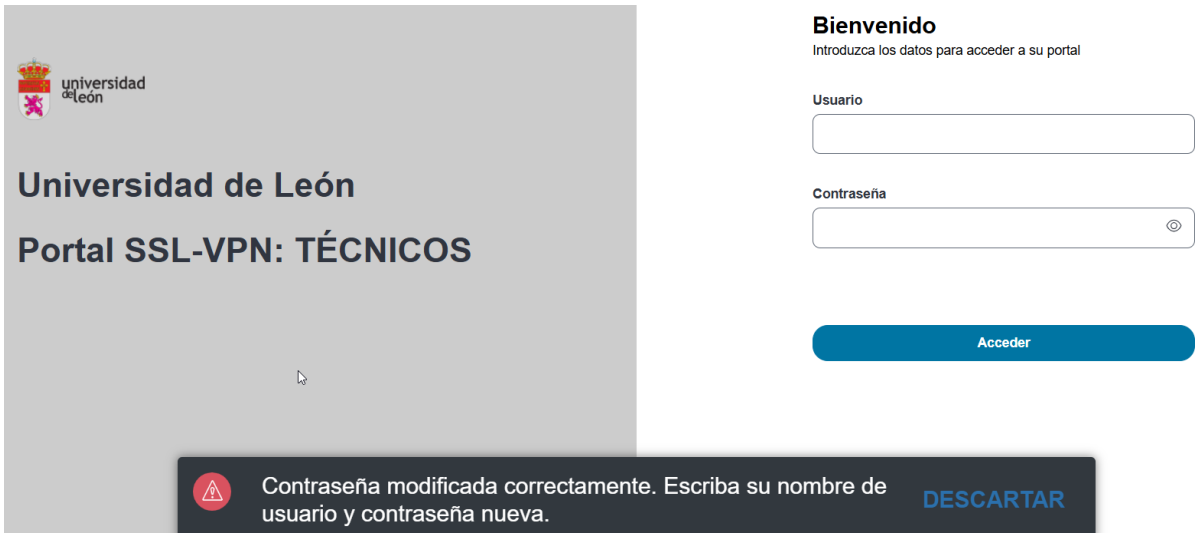

Ilustración 6. Confirmación cambio contraseña

4.1.6 Sincronización Smartphone para generar 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 7. 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*".

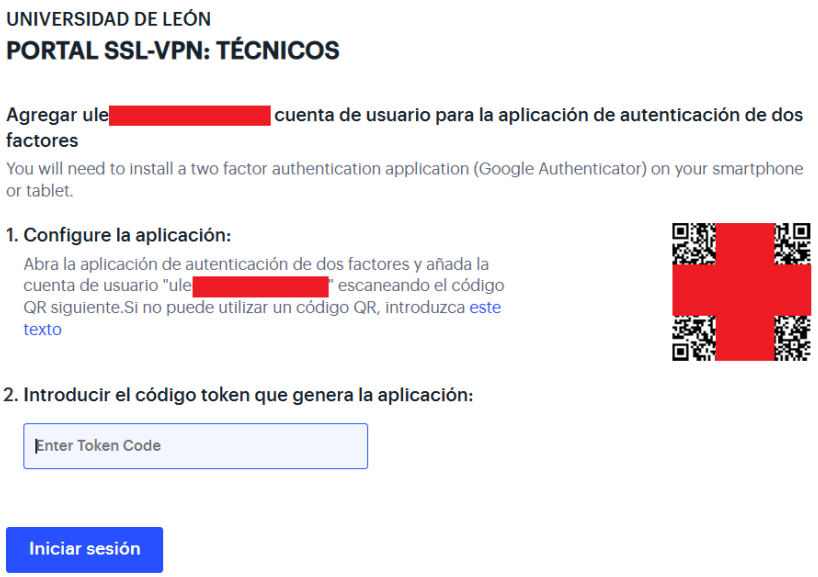

Ilustración 7. Sincronización OTP

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 7. 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 7. Sincronización OTP", y pulsar "Iniciar sesión".

4.1.7 Instalación de aplicaciones específicas

Se nos mostrará una pantalla (Ilustración 8. 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 9. Instrucciones de instalación).

Ilustración 8. Iniciador de aplicaciones

Ilustración 9. 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 10. Advertencia) en donde debemos dar permiso a la aplicación pulsando en “Siempre” para que se conecte al servidor.

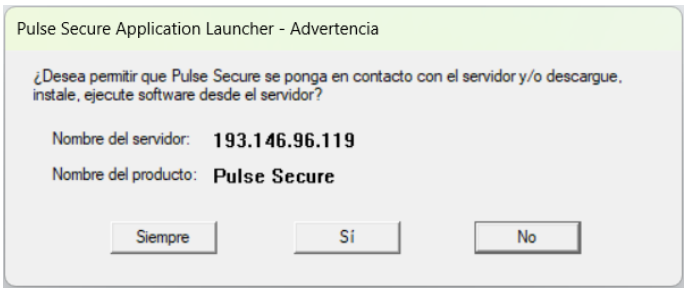

Ilustración 10. Advertencia

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 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 11. Autenticación de dos factores)

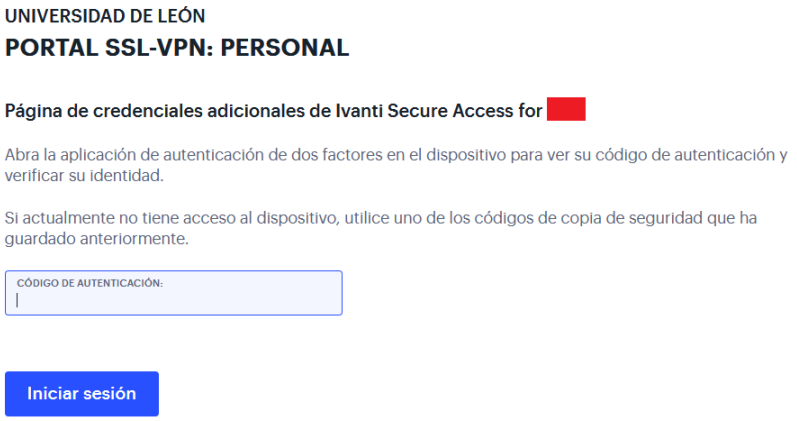

Ilustración 11. Autenticación de dos factores

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.