Indicaciones para la utilización de un equipo de teletrabajo

Objetivo: facilitar a los trabajadores de la Universidad el desarrollo de sus funciones a través de un sistema de acceso remoto seguro.

Los equipos que se usen para acceso desde fuera de la universidad deberían estar preparados con un mínimo de elementos de seguridad. A modo de recomendación, serían los siguientes:

- Tener instalado y actualizado un AntiVirus.
- Sistema operativo con soporte y parches de seguridad actualizados.
- Únicamente se podrá administrar el sistema desde un usuario administrador.

Los únicos equipos que garantizan estos requerimientos mínimos son los equipos entregados por el Área TIC y por lo tanto son los únicos que deben utilizarse para acceder a las **aplicaciones corporativas de la UNIA** (UXXI-AC, UXXI-EC, Savia, etc.). **Queda prohibido el acceso a dichas aplicaciones desde un equipo distinto a los equipos proporcionados para el teletrabajo**.

Para distribuir la carga en la conexiones que se realicen a nuestra red corporativa, se han creado conexiones diferenciadas por sede. Por ejemplo un usuario de la Sede de Sevilla se conectara a la VPN de Sevilla, un usuario de Baeza se conectará a la VPN de Baeza, … Esto es trasparente para el usuario, sólo afecta a la aplicación que deberá ejecutar para conectarse a la VPN que le corresponde.

Por lo tanto, los equipos se entregarán configurados según la ubicación física del puesto de trabajo del solicitante de teletrabajo.

Índice del documento:

Perfiles de Trabajo 2

Pasos a seguir para la Conexión y el Teletrabajo 3

Asistencia al Usuario 6

URLs que puedes necesitar para tu trabajo (y que quizás no recuerdes) 7

Existen dos Perfiles de Trabajo

Perfil 1: Usuario que **no hace uso de aplicaciones corporativas**

- Este perfil corresponde a aquel usuario que sólo utiliza las **google app** (gestión del correo, calendario y herramientas de ofimática).
- Las funciones de este usuario se basan en gestionar su correo y acceder a su documentación de trabajo a través de google File Stream o Google drive.
- En este caso, el usuario puede acceder desde **cualquier equipo,** ya sea un equipo personal, un dispositivo móvil, etc., a su cuenta de correo, utilizar google drive para el trabajo en equipo, … y sólo requiere de disponer del **terminal telefónico corporativo** para que pueda recibir llamadas entrantes desde la centralita.

> **IMPORTANTE**: Si el usuario no tiene sus documentos de trabajo sincronizados en google drive, no dispondrán de la información en la nube y no podrá acceder a esos documentos (documentos odt, hojas de cálculo, pdf, etc…)

Perfil 2: Usuario que requiere **acceder a aplicaciones corporativas (UXXI-AC, UXXI-EC, Savia**, …).

- Este usuario tiene las mismas funciones que el usuario Perfil 1 pero además necesita acceder a aplicaciones que sólo son accesibles desde la red de la UNIA (ejemplo UXXI-AC, UXXI-EC, Savia, …).
- Requiere de un equipo securizado y configurado correctamente para que se **conecte a la VPN indicada para el personal de su sede**.
- Este usuario, al necesitar que su **equipo esté securizado,** es el candidato principal a la solicitud y asignación de un portátil para el teletrabajo, configurado correctamente para que le permita acceder a la VPN de su sede. También requiere de su **terminal telefónico corporativo** para poder recibir las llamadas entrantes desde centralita.

> **IMPORTANTE:** Es necesario que el equipo de trabajo de la oficina esté encendido para que puedas conectarte a tu escritorio remoto.

Pasos a seguir para la Conexión y el Teletrabajo

PASO 1: Establecimiento de la conexión con VPN para usuarios de Perfil 2

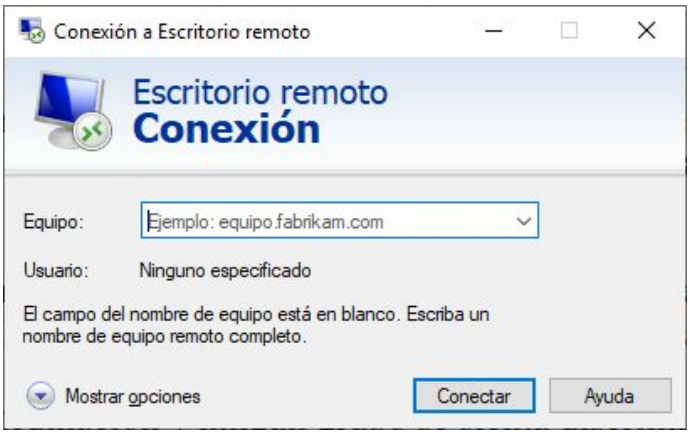
- ¿Qué hago para conectar la VPN?
  - **Si tu sede de trabajo es Sevilla o La Rábida** utilizarás la aplicación **FortiClient** que tu portátil debe tener instalada.
  - **Si tu sede de trabajo es Baeza o Málaga** utilizarás la aplicación **OpenVPN** que tu portátil debe tener instalada y configurada.
- La aplicación de conexión a la VPN te solicitará unas credenciales para establecer la conexión:
  - **Si tu sede de trabajo es Sevilla o La Rábida,** y por lo tanto estas utilizando **FortiClient,** debes utilizar tu **usuario y contraseña del correo electrónico** para establecer la conexión segura (VPN).
  - **Si tu sede de trabajo es Baeza o Málaga,** y por tanto utilizas la aplicación **OpenVPN,** debes utilizar las **credenciales que te entregarán** junto con el portátil para establecer la conexión con la VPN.

NOTA IMPORTANTE:

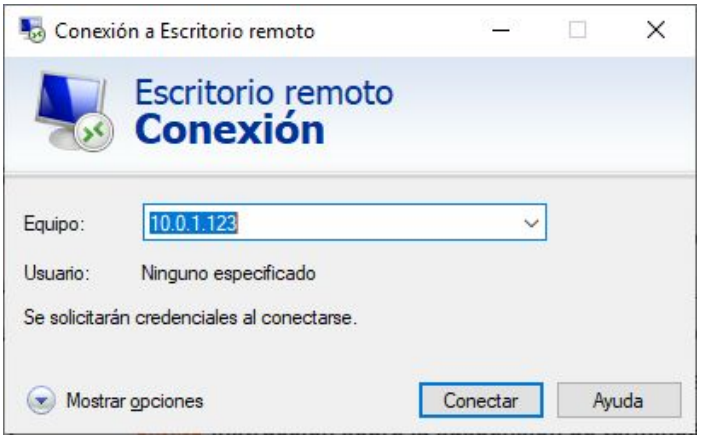
Si no vas a hacer uso de las aplicaciones corporativas y sólo quieres gestionar tus correos o acceder a tu google drive (**usuario Perfil 1**), no necesitas establecer la conexión VPN. **Cierra la conexión VPN en cuanto deje de ser necesaria**. Mientras tienes establecida la conexión todo el tráfico pasa por la UNIA y queda registrado (LIMITA EL USO DE LA CONEXIÓN VPN PARA ACCEDER A LAS HERRAMIENTAS DE TRABAJO)

PASO 2: Conexión a tu PC de trabajo mediante el escritorio remoto de Windows (requiere haber establecido la conexión VPN, "PASO 1")

El siguiente paso es conectarte a tu equipo de trabajo (PC de tu oficina) mediante la aplicación de Windows "Conexión a escritorio remoto".

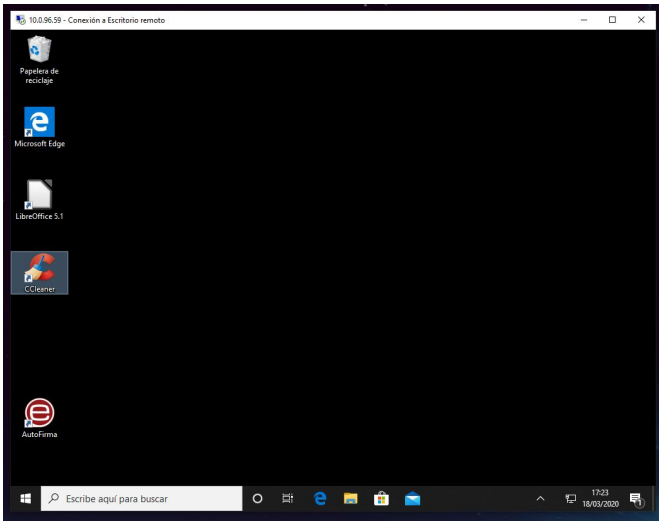


En **Equipo** debes poner la **dirección IP** de tu equipo de trabajo de la oficina. Algo similar a 10.0.1.34 que te **habrán indicado cuando te entregaron el portátil.**

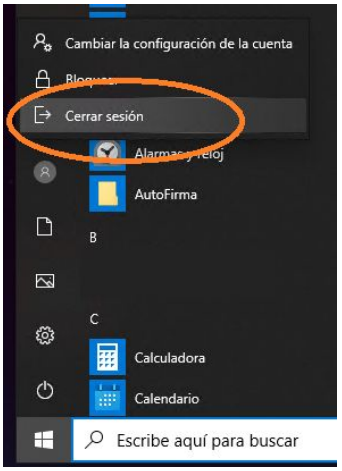


Cuando pulses **Conectar** te solicitará el **usuario y password de tu equipo de trabajo de la oficina**. Debes conocerla para poder acceder.

Una vez autenticado se mostrará el **escritorio de tu equipo de trabajo de tu oficina** (ver siguiente figura). Ahora ya puedes hacer uso de todas aplicaciones y acceder a toda la información como si estuvieras sentado delante de tu ordenador de oficina.



Es importante que si trabajas con una **conexión de escritorio remoto al finalizar NO APAGUES el ordenador remoto** (equipo de trabajo de la sede); **en su lugar CERRAR SESIÓN.**



OBSERVACIONES:

Es necesario que **el equipo de trabajo de la oficina esté encendido** para que te puedas conectar a tu escritorio remoto. Si el equipo, por cualquier razón, se apagase, alguien tendría que acceder físicamente al puesto de trabajo para volver a encenderlo.

Asistencia al Usuario

La asistencia al usuario siempre pasa por la creación de una incidencia en CAU https://cau.unia.es
No se atenderán llamadas telefónicas directas al Técnico.

El Técnico prioriza y organiza su trabajo según las incidencias reportadas al CAU:

- Sin Ticket, no hay incidencia.
- Si no puedes poner un ticket, solicita a algún compañero de trabajo que lo haga por ti mediante una llamada telefónica.
- La incidencia debe describir, lo más detallada y explícitamente que puedas, cuál es el problema. Hazte a la idea de que el técnico debe tener toda la información para poder clasificar la incidencia y, por lo tanto, poder atenderla. Si no describes correctamente cuál es tu problema, la resolución de tu incidencia se verá retrasada.
- Las notificaciones de la evolución de la incidencia se notifican por el mismo sistema de tickets, mediante las "notas" que irá añadiendo el técnico que esté gestionado tu incidencia. **DEBES** estar pendiente de esas notas, ya que te pueden estar solicitando información adicional o informando de que ya ha sido resuelta tu incidencia.
- Si fuera necesario, el técnico podrá ponerse en contacto contigo mediante el teléfono institucional o, incluso, ofrecer soporte mediante asistencia remota.
- La asistencia remota se realizará utilizando la herramienta Chrome Remote Desktop o Google Meet, que permiten que el técnico vea tu equipo y qué es lo que te está ocurriendo.

URLs que puedes necesitar para tu trabajo (y que quizás no recuerdes)

Herramientas Colaborativas:

- Gmail: **correo** electrónico corporativo
  - https://webmail.unia.es
- CAU UNIA – **OTRS** Sistema de Gestión de incidencias
  - https://cau.unia.es
- Google Hangouts: Mantener conversaciones/**chats:** disponible una vez iniciada sesión con tu cuenta de correo corporativo.
  - https://hangouts.google.com
  - Acceso directo con tus Credenciales
- Google **Calendar:** disponible una vez iniciada sesión con tu cuenta de correo corporativo.
  - https://calendar.google.com
  - Acceso directo con tus Credenciales
- Google **Drive:** disponible una vez iniciada sesión con tu cuenta de correo corporativo o utilizando Google File Stream.
  - https://drive.google.com
  - Acceso directo con tus Credenciales
- Hangouts **Meet:** disponible una vez iniciada sesión con tu cuenta de correo corporativo o a través del calendar si te han convocado a una reunión virtual.
  - https://meet.google.com
  - Acceso directo con tus Credenciales
- **Viafirma** - Portafirmas de la UNIA. Para firmar necesitas un certificado digital instalado en el equipo de trabajo. Si sólo quieres enviar documentos para la firma de otros, sólo necesitas autenticarte con el usuario de tu cuenta de correo.
  - https://services.viafirma.com/inbox/app/unia/
- Plataforma de **Comunicación Interna de la UNIA** - A través de la cual puedes publicar y conocer las últimas noticias y novedades de la UNIA (a nivel interno).
  - https://ci.unia.es
  - Acceso directo con tus Credenciales

Otras Herramientas:

- **Escritorio Remoto de Chrome:** hay que emplear la última versión del navegador Google Chrome.
    - **Asistencia Remota.** Esta herramienta permite que, previa autorización, otra persona se pueda conectar en remoto a tu PC para ayudarte a resolver un determinado problema. (Sólo utilizado si fuera necesaria la asistencia paso a paso guiada por un técnico)
        - https://remotedesktop.google.com/access
        - Acceso directo con tus Credenciales
    - **Acceso Remoto**.
        - https://remotedesktop.google.com/support
        - Acceso directo con tus Credenciales
    - Manual de ayuda sobre el uso de Chrome Remote Desktop https://support.google.com/chrome/answer/1649523?co=GENIE.Platform%3DDesktop&hl=es