GUÍA PARA EL TRABAJO A DISTANCIA, OCTUBRE 2025

ANTES DE COMENZAR EL TRABAJO A DISTANCIA

¿UN EQUIPO DEL COLEGIO O TU PROPIO EQUIPO?

Antes de nada, recuerda que si tienes que llevarte un portátil del Colegio debes asegurarte de solicitarlo con tiempo suficiente para que desde el departamento de Tecnologías podamos gestionar tu petición según la demanda de equipos, y bajo tu responsabilidad debes antes de irte, asegurar de que tienes lo necesario para teletrabajar siguiendo estos pasos:

1. Antes de abandonar tu puesto de trabajo (en el caso de que tengas que conectarte en remoto)*:

A. Asegúrate que el equipo se queda encendido y que **no va entrar en modo suspensión o hibernación** (puedes saber más sobre este tema en este **enlace**).

B. **Anota la IP de tu equipo**, a veces puede cambiar, en el manual de conexión VPN puedes ver cómo hacerlo.

2. En el equipo portátil donde vas a teletrabajar:

⟶ Prueba la conexión a VPN: ten en cuenta que debes hacerlo fuera de la red local del Colegio. Puedes hacerlo conectándote a la wifi. Contáctanos para poder ayudarte a realizar esta prueba si lo haces desde el propio Colegio

Adjunto puedes encontrar un manual que indica muy requetebién cómo configurar y utilizar el acceso por VPN.

⟶ Se recomienda usar cable de red en lugar de WIFI. La VPN es muy estricta cuando detecta pérdidas de paquetes de datos y esto puede ocurrir con frecuencia a través de la WIFI.

3. Conéctate al escritorio remoto*

4. Comprueba que el sistema antivirus instalado en el equipo está operativo y actualizado.

* En el caso de que tu equipo en el lugar de trabajo sea un portátil y ese portátil lo uses para teletrabajar, no tienes que realizar este paso.

Si alguno de estos pasos te da algún problema que no puedes resolver, nos lo cuentas y vemos cómo resolverlo. Recuerda que **ya no deberás utilizar bajo ningún concepto cualquier otra forma de acceso remoto** como puede ser TeamViewer.

DURANTE EL TRABAJO A DISTANCIA

¿NECESITAS CONFIGURAR EL CORREO EN EL MÓVIL?

1. En este **enlace** puedes ver cómo hacerlo. Recuerda que tanto el correo electrónico en el móvil, como el acceso remoto conlleva riesgos a la seguridad de la información, en cuanto al móvil lo ideal sería tener un móvil profesional y otro privado, en todo caso para evitar posibles quiebras de seguridad en necesario tener en cuenta algunas medidas de seguridad que puedes consultar en estos enlaces, cualquier duda no dudes en comentarlo.
2. Puesta a punto de tu móvil
3. Quiero proteger mi correo electrónico
4. ¿Cómo actuar si me han robado o he perdido el teléfono móvil?

¿CUALQUIER WIFI VALE PARA EL TRABAJO A DISTANCIA?

En cuanto al trabajo de forma remota, es muy importante que no te conectes desde redes wifi públicas (aeropuertos, cafeterías, bibliotecas, etc.) más aun en estos momentos que no deberías salir de casa si no es imprescindible, porque puede que no sean seguras ya que, o no cifran la información que se transmite a través de ellas, por lo que cualquier usuario conectado con ciertos conocimientos podría hacerse con ella, o porque desconocemos quién está conectado a esa misma red y con qué fines, además, en casa deberás establecer un lugar de trabajo al que solo puedas acceder tú si dejas algún material profesional (un cajón cerrado bastaría, del que tengas tú solo la llave), y en cuanto al ordenador no debe poder acceder más personas al ordenador que utilices o hacerlo mediante usuario y contraseña y no almacenar ninguna información de carácter profesional en el disco duro de tu ordenador, debes almacenar la información en la unidad de red del Colegio.

¿MIS CLAVES DE ACCESO SON CONFIDENCIALES?

Por supuesto que sí: no le reveles a nadie las claves que usas para acceder a tu puesto de trabajo ni dejes sin la debida custodia las claves que se te han facilitado para acceder a los recursos del Colegio. En esta guía de privacidad y seguridad en internet puedes encontrar más información sobre cómo utilizar internet como herramienta de forma segura.

Además, ten en cuenta que:

1. Debes utilizar contraseñas de acceso robustas y diferentes a las utilizadas para acceder a cuentas de correo personales, redes sociales y otro tipo de aplicaciones utilizadas en el ámbito de tu vida personal.
2. No debes descargar ni instalar aplicaciones o software que no hayan sido previamente autorizados por el Colegio.
3. Si dispones de un equipo corporativo, no lo debes utilizar con fines particulares evitando el acceso a redes sociales, correo electrónico personal, páginas web con reclamos y publicidad impactante, así como otros sitios susceptibles de contener virus o favorecer la ejecución de código dañino.

4. Si el equipo utilizado para establecer la conexión remota es personal, debes evitar simultanear la actividad personal con la profesional y definir perfiles independientes para desarrollar cada tipo de tarea.
5. El sistema antivirus instalado en el equipo debe estar operativo y actualizado.
6. Desactiva las conexiones WIFI, bluetooth y similares que no estén siendo utilizadas.
7. Una vez concluida la jornada de trabajo en situación de movilidad debes desconectarte la sesión de acceso remoto y apagar o bloquear el acceso al dispositivo, **pero asegúrate de no apagar el equipo del Colegio de forma remota**, porque al hacerlo ya no podrás seguir teletrabajando y tendrás que desplazarte hasta el Colegio para encenderlo de nuevo.
8. En la medida de lo posible, debes prevenir que se puedan escuchar conversaciones por parte de terceros ajenos utilizando, por ejemplo, auriculares o retirándose a un espacio donde no haya nadie.
9. No utilices bajo ningún concepto aplicaciones no autorizadas por el colegio como servicios en nube de alojamiento de archivos, como puede ser Dropbox, WeTransfer, correos personales, mensajería rápida, etc.
10. Revisa y elimina periódicamente la información residual que pueda quedar almacenadas en el dispositivo, como archivos temporales del navegador o descargas de documentos.

Por último, **recuerda que cuando trabajas desde casa debes cumplir con todas las obligaciones de protección de datos con las que cumples en el Colegio:** no dejes sin supervisión materiales con datos personales y si utilizas impresoras o fax no dejes ningún material olvidado, si necesitas destruir algún papel con información hazlo de forma segura. En la documentación adjunta puedes consultar la política de protección de datos del Colegio.

Si tuvieras algún problema fuera del Colegio con el móvil o con tu acceso VPN en el que vieras comprometida información con datos de carácter personal del Colegio ponte en contacto con Lola Manzano en cuanto puedas para gestionar la quiebra de seguridad.

¡¡¡Mil gracias por tu colaboración!!!