# Antecedentes: Teletrabajo durante el confinamiento

La crisis sanitaria provocada por la COVID-19 ha obligado a gran parte de la sociedad a adaptarse de manera veloz e inesperada al trabajo en remoto, una práctica relativamente minoritaria antes de la eclosión de la pandemia.

# Cambios realizados en Metropolis

## Inicio de las restricciones de movilidad

Metropolis empezó las restricciones de movilidad accediendo de forma remota a los equipos de las oficinas. Se realizó un rápido despliegue del software en todos los equipos de la oficina y se preparó un manual para que los usuarios pudieran conectar desde sus casas. Se compraron algunos equipos portátiles y monitores para aquellos usuarios que no disponían de recursos propios para trabajar desde sus respectivos hogares.

La puesta en marcha de solución fue todo un éxito y los usuarios se adaptaron rápidamente. Algunos de ellos trabajaban completamente con el equipo remoto y otros usaban la conexión remota únicamente para acceder a los archivos del servidor aprovechando que el correo electrónico, el CRM y algunas de las herramientas que utilizan están disponibles a través de Internet.

Durante los meses de junio y julio Metropolis decidió mejorar la situación de teletrabajo y se plantearon los siguientes objetivos a aplicar durante el mes de setiembre:

* Proporcionar a los usuarios todo el material necesario para teletrabajar usando recursos de la empresa, no equipos particulares
* Aplicar medidas que mejoren la seguridad de los usuarios y equipos informáticos.
* Proporcionar a los usuarios una solución que no dependa de las estaciones de trabajo para acceder a los archivos del servidor.

## Segunda ampliación de las restricciones de movilidad

Durante el mes de Setiembre se realizaron una serie de medidas correctivas que solucionaran los problemas detectados durante el inicio de las restricciones de movilidad y que permitieran cumplir con los objetivos planteados.

El primer paso fue instalar un **Firewall** en la red que permitiera una conexión segura entre los equipos remotos y los recursos de la red interna a la vez que mejoraba la seguridad de la red interna. El proceso de conexión VPN se integró con un sistema de verificación en 2 pasos que, además el nombre de usuario y contraseña, requiere un código de 6 dígitos generado a través de una aplicación instalada en el móvil. Dicho código se regenera cada 30 segundos, lo que dificulta muchísimo el acceso a la red interna para cualquier posible atacante.

Se realizó una sesión de formación a los usuarios para explicarles el funcionamiento de la conexión VPN y el acceso a los recursos de la red interna. Se solventaron las dudas y se resolvieron algunos problemas surgidos durante los primeros días de trabajo.

## Tercera ampliación de las restricciones de movilidad

En esta tercera fase nos estamos centrando en apagar definitivamente los equipos de la oficina de los usuarios que no los están utilizando a la vez que animamos a los usuarios de los grupos 2 y 3 a que dejen de usarlo. De ese modo evitaremos el consumo innecesario de energía y el rápido desgaste de los equipos.

Estamos realizando pruebas de trabajo con el ERP instalado en su equipo remoto y accediendo a la Base de Datos a través de la VPN. Si los resultados no son satisfactorios, seguiremos con la solución actual hasta encontrar alguna solución más adecuada a las necesidades de este grupo de usuarios.

Estamos también migrando la solución de antivirus a la nube para permitir tener visibilidad de los equipos portátiles ubicados fuera de la oficina estén o no conectados a la red VPN.