

ANEXO I “Requisitos tecnológicos para el teletrabajo.”

1. Conexión a internet.

La oficina a distancia debe disponer de una conectividad a internet suficiente, estable y segura.

Para evaluar la calidad de la conectividad puedes utilizar el test de velocidad disponible en el siguiente enlace: <https://www.testdevelocidad.es/>.

Se debe evitar la conexión de los dispositivos a la red corporativa desde lugares públicos, así como la conexión a redes WIFI abiertas no seguras.

2. Equipo informático.

El equipo informático debe ser adecuado para el desempeño del trabajo a distancia.

Requisitos mínimos hardware y software.

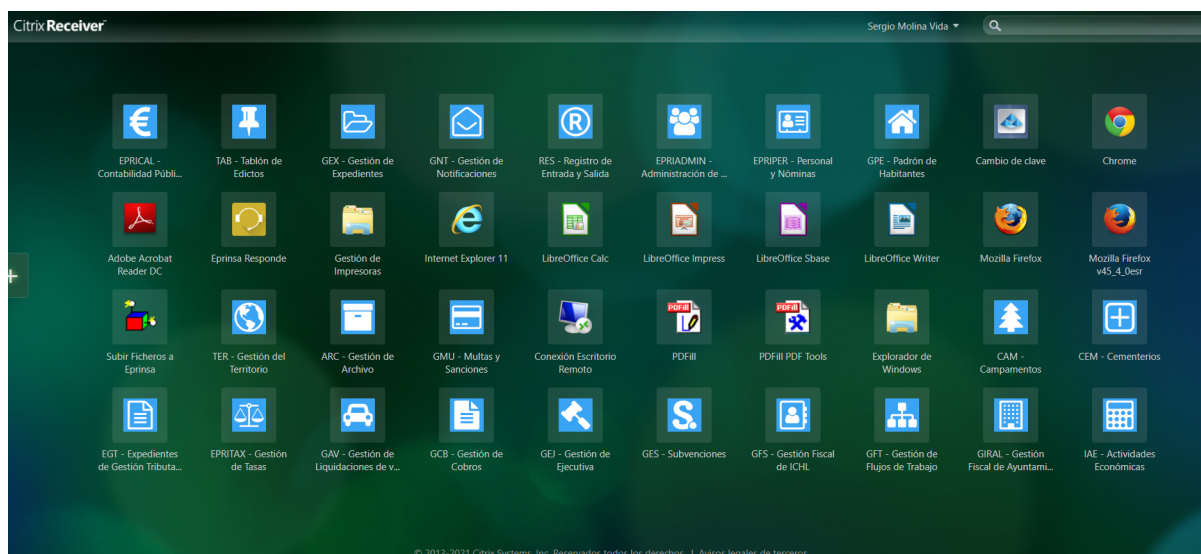
- Procesador Intel® Core™ i3 o Ryzen 3
- Memoria RAM 4GB
- Disco duro 256GB () SSD
- Pantalla 14" HD (1366 x 768)
- Conectividad WiFi 5 (802.11ac, 1x1) o RJ45 (cable de red)
- Conexión de auriculares/micrófono jack 3.5 mm
- Webcam con micrófono
- Auriculares.
- **Sistema operativo:** Windows 10 o Windows 11.
- Software antivirus.

Muy importante: Tanto el sistema operativo, el software antivirus y los navegadores utilizados deben estar actualizados a la última versión disponible, incluidos todos los parches de seguridad.

3. Conexión a los sistemas corporativos.

La conexión a la red corporativa o a los equipos del ayuntamiento se realizará por los medios que se habiliten desde el departamento de informática.

La forma habitual de conexión será mediante la dirección de acceso externa de eprinsa: <https://apl.eprinsa.es/Citrix/AzaharaWeb/>



No se podrá utilizar ningún software no autorizado de conexión remota. (TeamViewer, Anydesk, etc.).

Para acceder a otros portales de internet se debe tener en cuenta que utilicen el protocolo https. Para verificar que la página cumple con este protocolo debemos comprobar la dirección URL empiece por **https://** seguido del nombre de dominio de la web.

El Protocolo Seguro de Transferencia de Hipertexto (HTTPS por sus siglas en inglés) garantiza que los visitantes tengan una conexión segura con tu sitio. El tener un sitio seguro con HTTPS significa que la información sensible, como las contraseñas o los datos bancarios está protegida, y tus visitas pueden navegar por tu sitio de forma segura.

4. Ciberseguridad.

La seguridad es un elemento vital, por ello debemos seguir las recomendaciones de navegación segura, protección de datos, uso adecuado de contraseñas.

Puedes consultar más información y guías de ciberseguridad en el portal del Instituto Nacional de Ciberseguridad. <https://www.incibe.es/ciudadania/>