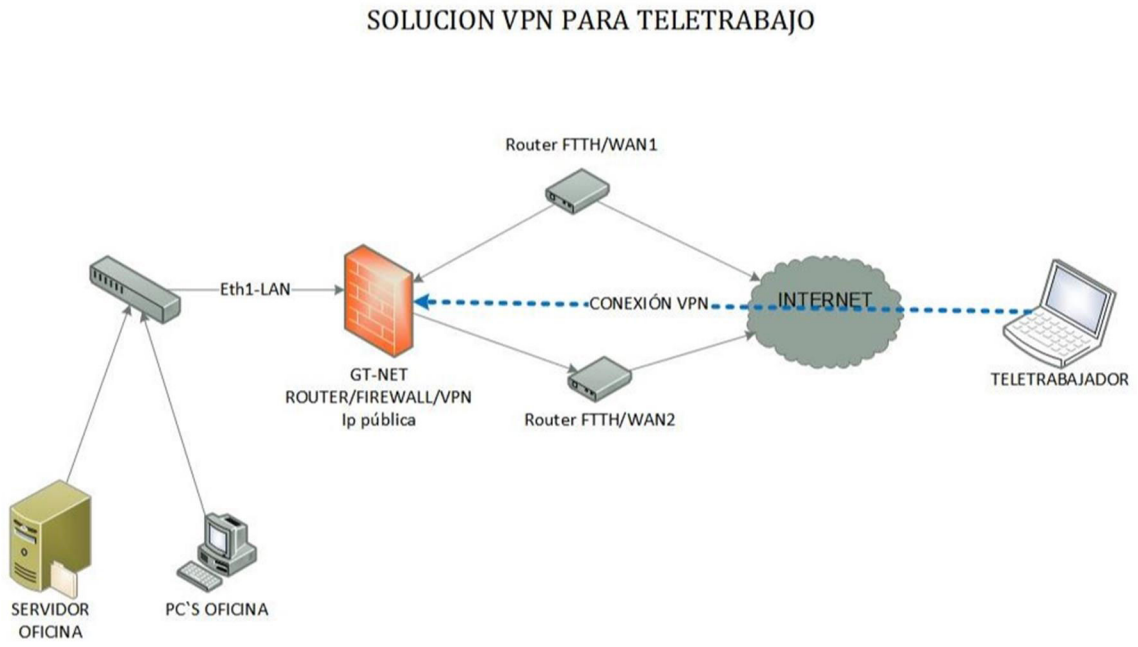
Recomendaciones para el Trabajo Remoto

SINTECROM

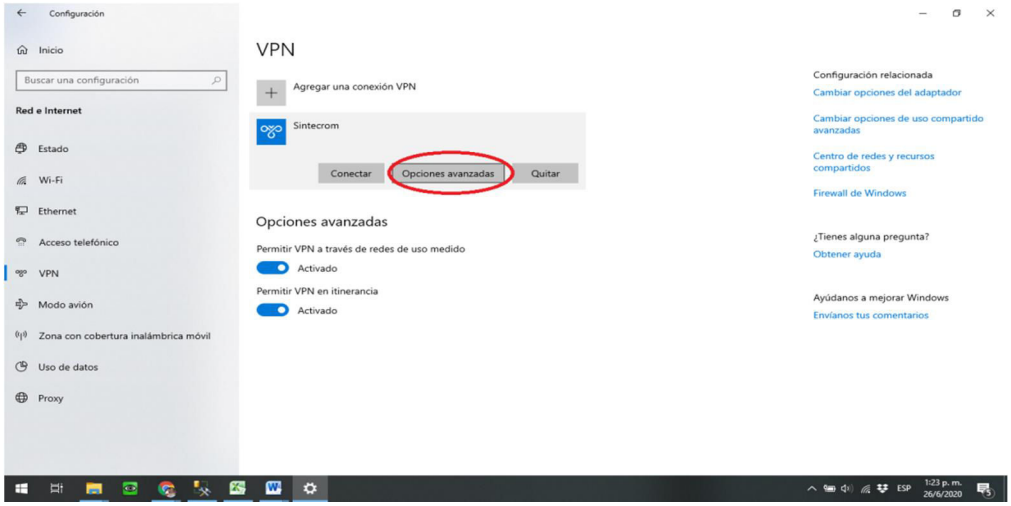
Trabajo Remoto

El esquema que estamos usando para que podamos desempeñar nuestras tareas remotamente en Sintecrom es la utilización de una VPN para conectarse a la Red Privada y, una vez establecida la conexión, acceder mediante "Escritorio Remoto" a los equipos que utilizan los usuarios habitualmente en las oficinas de la empresa, como indica la imagen que nos precede.

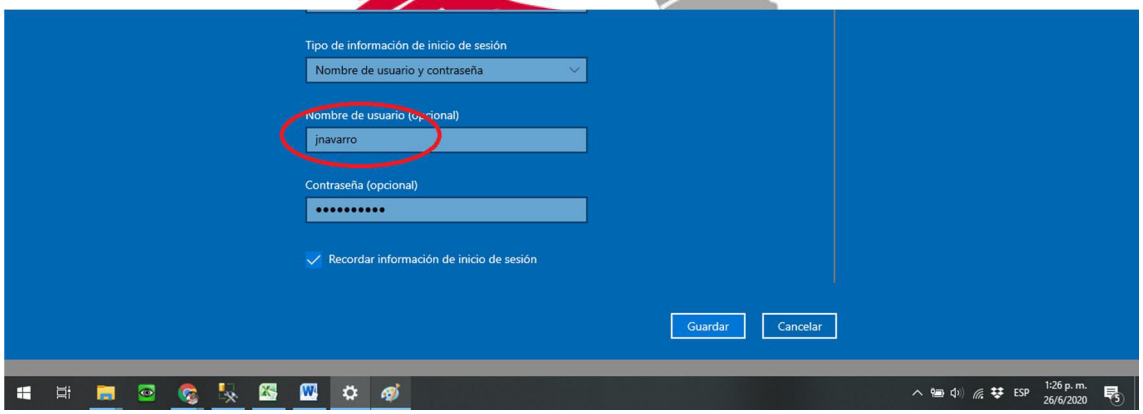


Desde el comienzo del aislamiento obligatorio, configuramos una VPN única, oportunamente se envió un instructivo para poder establecer el vínculo con la red de Sintecrom, el usuario que utilizamos fue "Sintehome", a partir de ahora cada conexión será personalizada, con la finalidad de, por un lado poder tener una trazabilidad de los picos de tráfico y por el otro incrementar la seguridad de cada VPN.

Entonces lo único que tendrán que hacer es editar la conexión a la VPN como indica la siguiente imagen



Y una vez ingresado tendrán que poner su usuario (el mismo que utilizan en la red cuando se conectan al Escritorio remoto) y la contraseña que les enviaremos por celular



En lo referido al segundo paso (la conexión específica a sus equipos mediante escritorio remoto) todo continúa de la misma manera.

Aspectos para tener en Cuenta

En los últimos meses como consecuencia de la Pandemia que nos aqueja, el teletrabajo ha crecido de manera exponencial. Lamentablemente esta situación trajo aparejados efectos no deseados como los problemas de ciberseguridad que, si bien existían con anterioridad, recrudecieron en los últimos días.

La red de Sintecrom se encuentra protegida por Firewalls, Antivirus actualizado y configuración de Proxy para que la navegación en internet sea lo más segura posible, pero en el contexto actual, las computadoras hogareñas con sus vulnerabilidades están siendo utilizadas para conectarse a la red de la compañía y, si bien el túnel de datos y la encriptación de la conexión mediante VPN a los servidores nos otorga un alto grado de seguridad a veces esto no llega a ser suficiente.

Vamos a enunciar algunos de las principales causas que vulneran la seguridad informática

- ***Ransomware***: *Ransom* quiere decir rescate en inglés, y de hecho lo que hace este tipo de software malicioso (malware) es **secuestrar los datos de un computadora y pedir un rescate** económico a cambio de liberarlo. Normalmente lo que hace es cifrar tus datos, y lo que te ofrecen a cambio del rescate económico es la clave para poder descifrarlos. En un principio este tipo de "virus" se utilizaba para extorsionar a grandes empresas, pero últimamente hemos tenido conocimiento que varias Pymes han caído en este problema, días atrás tuvimos una conferencia con el CEO de Cortestan que es una

metalúrgica de alrededor de 100 empleados que fue víctima de esta modalidad de delito.

- ***Pishing***: El phishing es el acto de intentar engañar al destinatario de un correo electrónico malicioso para que lo abra y siga sus instrucciones. El "remitente" del correo electrónico engaña a la víctima haciendo que el mensaje parezca provenir de una fuente fiable, como un organismo estatal, un proveedor o un cliente de la empresa. El correo electrónico de phishing puede tener adjunto un archivo malicioso, como un documento de Word o PDF, que, una vez abierto, daña el equipo del usuario instalando malware. El ataque también puede esconderse en un enlace URL malicioso en el cuerpo del mensaje del correo. Cuando el usuario hace clic en ese enlace, accede a un sitio que parece legítimo, pero que en realidad se utiliza para recopilar información confidencial, como nombres de usuario y contraseñas, o instalar malware en el dispositivo.

- ***Malware de Dispositivo***: En los últimos días hemos visto que varias empresas han sido atacadas por un malware conocido como “Manuel”, es un archivo que se incorpora a dispositivos como discos externos o Pen Drive’s bajo el nombre “Manuel.doc” que es un archivo malicioso que se encarga de secuestrar todos sus documentos en tus memorias USB y **llenar tus carpetas de un montón de accesos directos.** Lo peor de todo es que al mismo tiempo contagia el ordenador para que las próximas memorias USB también adquieran el virus.

Como señalábamos en párrafos anteriores, nuestras computadoras personales no tienen la misma seguridad que las que utilizamos en Sintecrom y las redes WIFI son abiertas y no están cifradas, por lo expresado les solicitamos que tengan especial precaución a la hora de abrir correos

que resultan sospechosos y, en el caso ver en sus dispositivos de almacenamiento portables archivos que desconocen por favor tomar la precaución de no abrirlos.

Por último recomendamos modificar sus contraseñas, tanto de correo como las de sesión, evitando mantener las que les enviamos desde Sistemas cuando nos solicitan el reseteo de la misma.

SINTECROM