sedian

Seguridad Digital
de Andalucía

Presentación

Teletrabajo seguro desde la perspectiva del responsable del sistema

25 de Junio de 2021

Junta de Andalucía

Unidad 1
Teletrabajo Inseguro y Vulnerable

sedian Seguridad Digital de Andalucía

Unidad 1. Teletrabajo Inseguro y Vulnerable

Antes de 2020, el tejido empresarial, administrativo y financiero de nuestro país no quería oír hablar de Teletrabajo:

- ✓ Sólo en contadas ocasiones.
- ✓ Se desconocía cómo hacerlo.

Unidad 1. Teletrabajo Inseguro y Vulnerable

El 14 de marzo de 2020, se declara el Estado de Alarma (BOE num 57)

Artículo 7. Limitación de la libertad de circulación de las personas.

1. Durante la vigencia del estado de alarma las personas únicamente podrán circular por las vías de uso público para la realización de las siguientes actividades:

a) Adquisición de alimentos, productos farmacéuticos y de primera necesidad.

b) Asistencia a centros, servicios y establecimientos sanitarios.

c) Desplazamiento al lugar de trabajo para efectuar su prestación laboral, profesional o empresarial.

d) Retorno al lugar de residencia habitual.

e) Asistencia y cuidado a mayores, menores, dependientes, personas con discapacidad o personas especialmente vulnerables.

f) Desplazamiento a entidades financieras y de seguros.

g) Por causa de fuerza mayor o situación de necesidad.

h) Cualquier otra actividad de análoga naturaleza que habrá de hacerse individualmente, salvo que se acompañe a personas con discapacidad o por otra causa justificada.

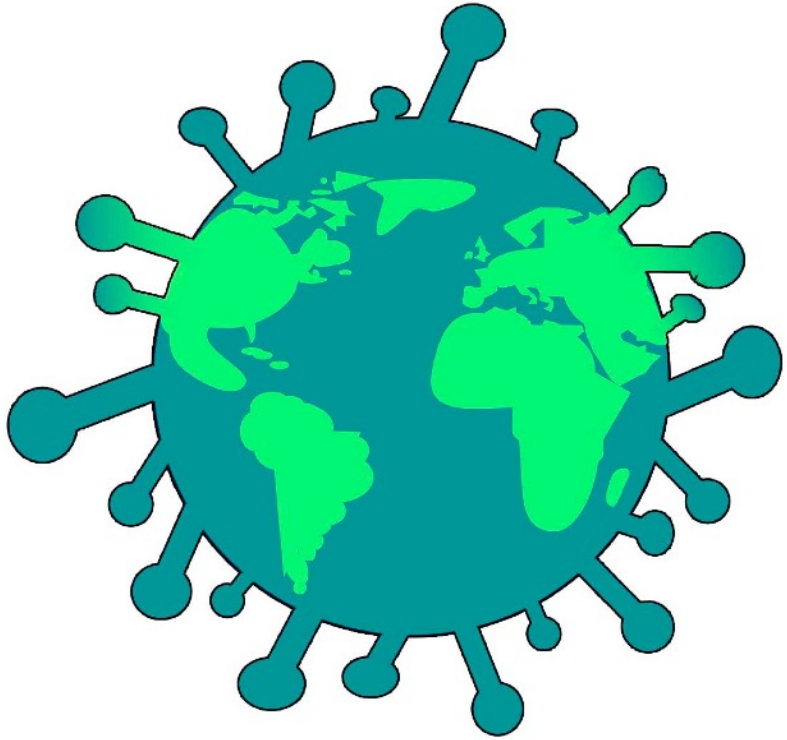
2. Igualmente, se permitirá la circulación de vehículos particulares por las vías de uso público para la realización de las actividades referidas en el apartado anterior o para el repostaje en gasolineras o estaciones de servicio.

3. En todo caso, en cualquier desplazamiento deberán respetarse las recomendaciones y obligaciones dictadas por las autoridades sanitarias.

4. El Ministro del Interior podrá acordar el cierre a la circulación de carreteras o tramos de ellas por razones de salud pública, seguridad o fluidez del tráfico o la restricción en ellas del acceso de determinados vehículos por los mismos motivos.

Cuando las medidas a las que se refieren los párrafos anteriores se adopten de oficio se informará previamente a las administraciones autonómicas que ejercen competencias de ejecución de la legislación del Estado en materia de tráfico, circulación de vehículos y seguridad vial.

Las autoridades estatales, autonómicas y locales competentes en materia de tráfico, circulación de vehículos y seguridad vial garantizarán la divulgación entre la población de las medidas que puedan afectar al tráfico rodado.



Unidad 1. Teletrabajo Inseguro y Vulnerable

El 17 de marzo de 2020, RD 8/2020, de medidas urgentes extraordinarias, en su Título II:

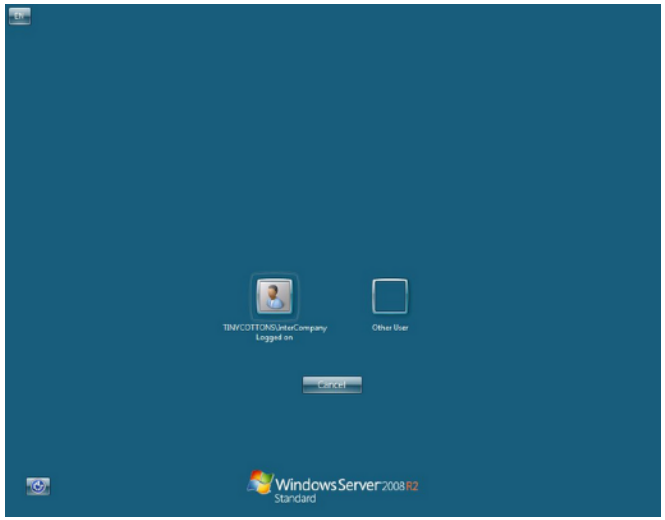
> Gracias a las herramientas informáticas y digitales, pueden realizarse las tareas laborales diarias desde dispositivos conectados a Internet, incluyendo reuniones online, llamadas «virtuales» vía voz, videoconferencias o envío de documentos internos.

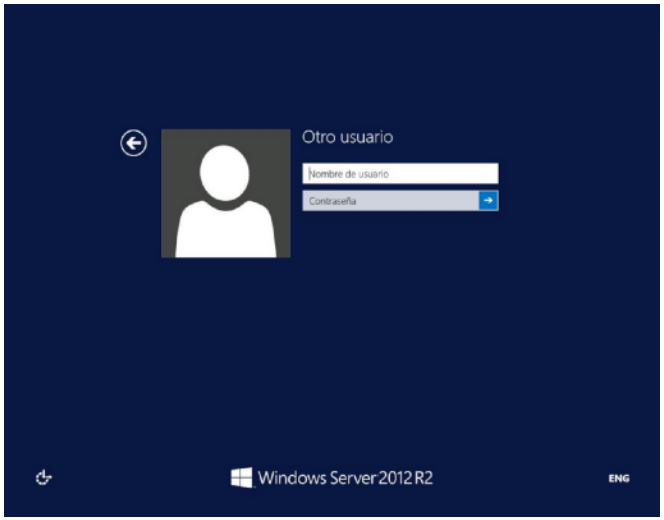
> Para las empresas y puestos en los que la modalidad del trabajo no presencial no estaba implementada con anterioridad, la urgencia de la actual situación de excepcionalidad exige una relajación de estas obligaciones, con carácter temporal y exclusivamente a los efectos de responder a las necesidades sanitarias de contención actualmente vigentes.

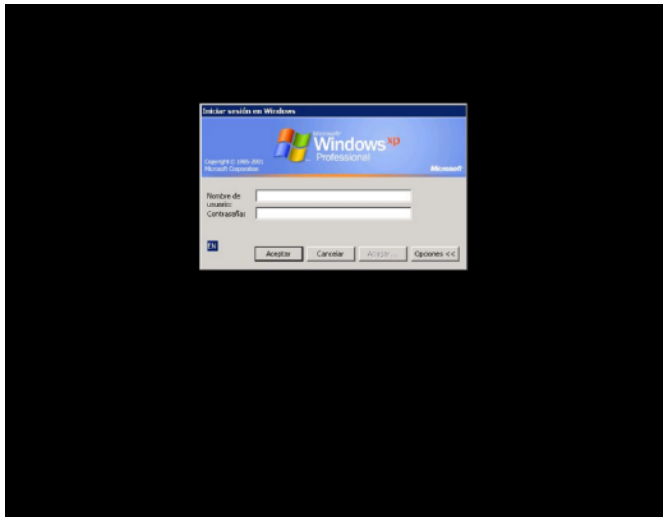
Unidad 1. Teletrabajo Inseguro y Vulnerable

El 18 de marzo de 2020, se detectan en el territorio español más de 37.000 routers con el puerto 3389 abierto.

SHODAN
Computer Search Engine





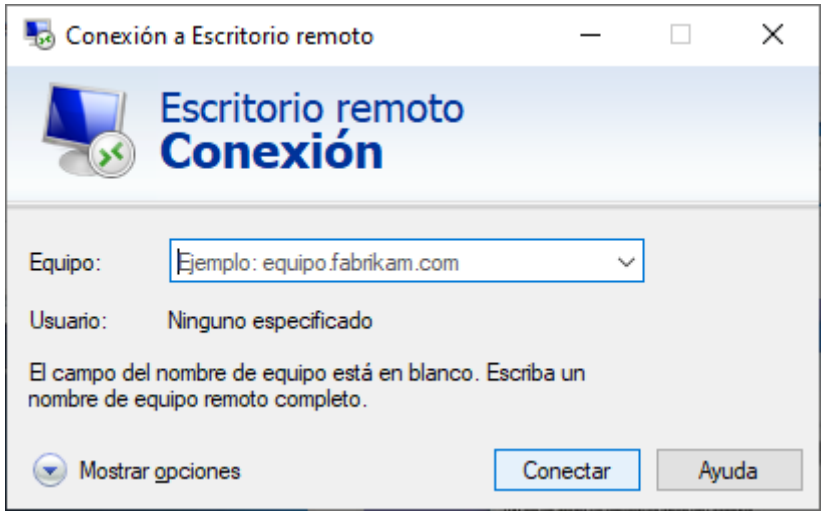


Unidad 1. Teletrabajo Inseguro y Vulnerable

SHODAN
Computer Search Engine

A junio de 2021, la misma plataforma de búsqueda arroja un resultado de 21.562 dispositivos de acceso a Internet con el puerto 3389.

RDP: Remote Desktop Protocol, es un protocolo de comunicaciones que permite conectar directamente al servicio de escritorio remoto del equipo.

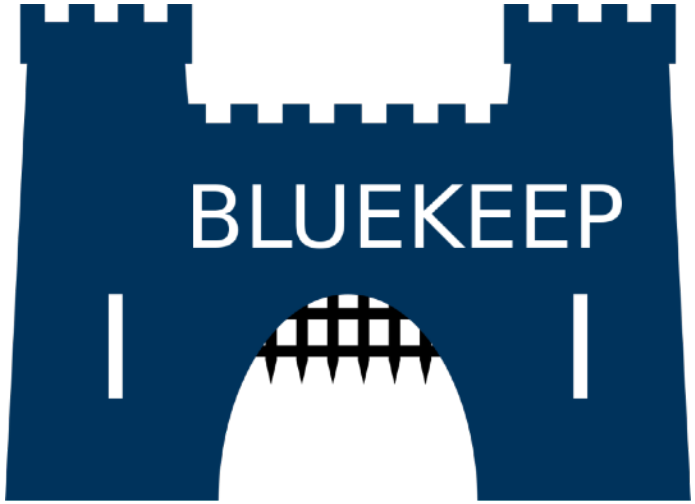


Unidad 1. Teletrabajo Inseguro y Vulnerable

Se desconoce el número de equipos con el servicio RDP abierto y conectados a Internet.

Pero se sabe que, en un escaneo de puertos de cualquier dirección IP, es uno de los puertos más comunes a comprobar.

Porque existe una vulnerabilidad específica de dicho puerto.



CVE-2019-0708

CVE-2019-0708

accenture

CADENA SER

everis
attitude makes the difference

http://trends.inycom.es/bluekeep-nuevo-ataque-masivo/

Unidad 1. Teletrabajo Inseguro y Vulnerable

Otro gran problema:

Los trabajadores emplean sus equipos domésticos, sin protección, sin antivirus, sin cortafuegos de software...

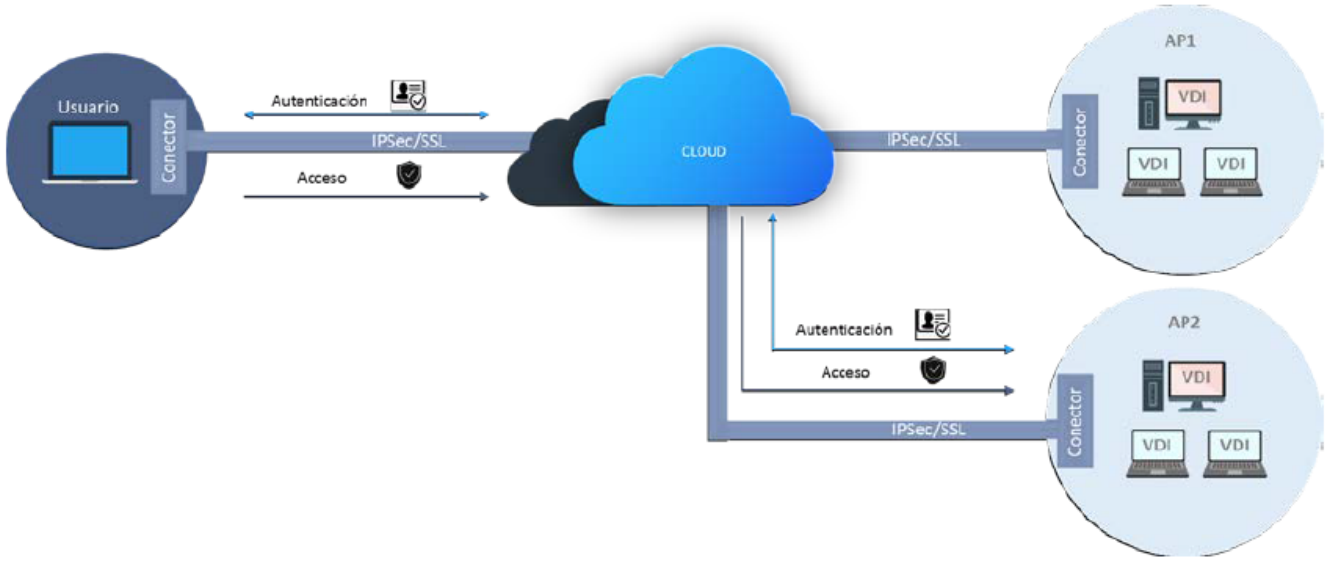
Literalmente, son pasto del malware.

Lo propagan al interior de las propias empresas

Unidad 2
Recomendaciones CCN-CERT

Desde el Centro Criptológico Nacional se proponen unas soluciones técnicas de Acceso Remoto Seguro.

1- Solución basada en la nube



Consiste en que cada usuario puede acceder remotamente a su equipo a través de una página web, una autenticación fuerte o un 2FA, empleando protocolo https y una trazabilidad total de las conexiones realizadas por los usuarios remotos.

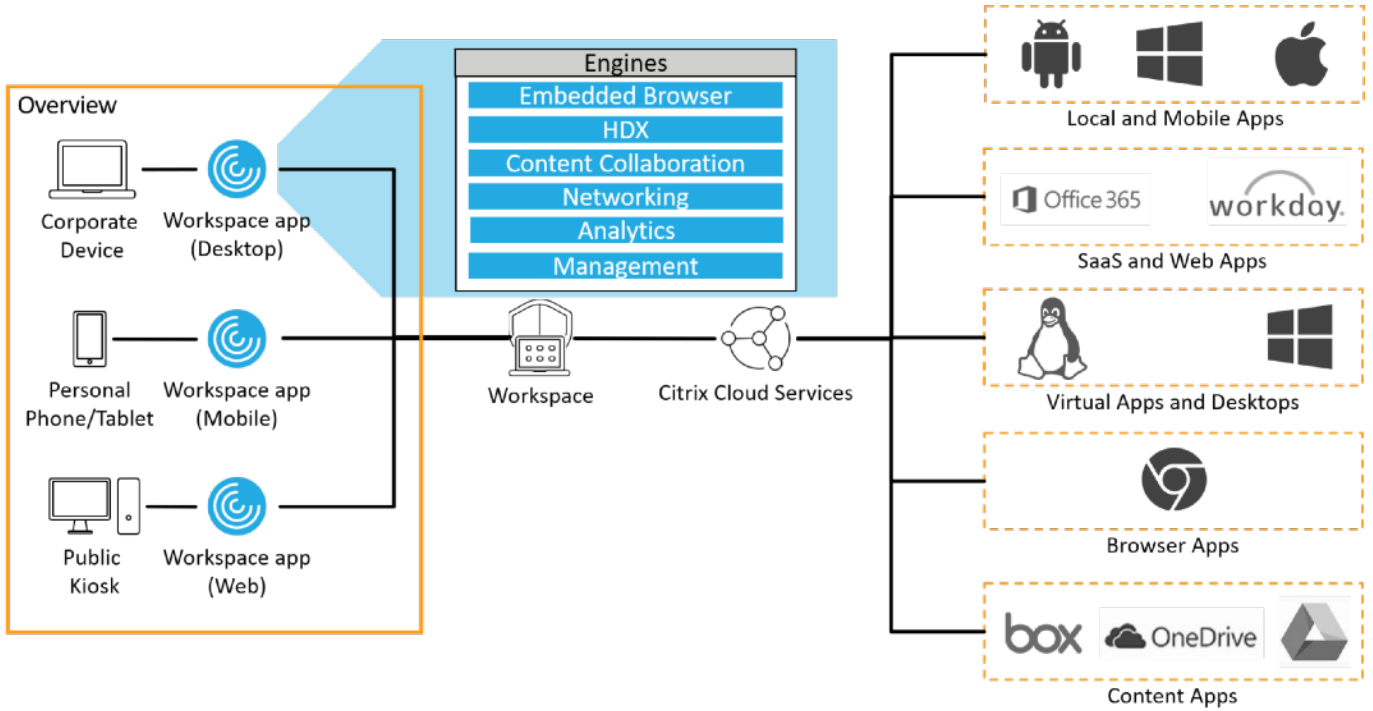
La responsabilidad recae sobre una máquina virtual, llamada “Conector”:

Establece una comunicación segura entre la nube y los servicios corporativos.

Unidad 2. Recomendaciones CCN-CERT

vmware

Workspace ONE



2- Solución basada en sistemas locales

Se caracteriza por emplear un canal seguro de la organización más allá de sus instalaciones, con equipamiento de hardware configurados por la organización, con medidas de seguridad estándar establecidas por ella y con medidas adicionales que permitan la comunicación por los servicios corporativos a través de Internet.

El canal seguro se presenta como una VPN.

Se plantean 3 escenarios:

1) Acceso a los servicios a través del Sistema VDI.

Consiste en que cada usuario tiene una máquina virtual que, a todos los efectos, será un equipo de la propia organización.

2) Acceso a los servicios a través de un Servidor de Escritorios Remoto (MTSC)

Los usuarios accedería a una especie de máquina virtual con acceso a todos los servicios de la oficina. Necesita un servidor con la capacidad necesaria para dar servicio a todos los usuarios.

Se plantean 3 escenarios:

3) Acceso directo a la Red Corporativa.

Se permite acceder a la red corporativa de forma contrlada, cumpliendo las siguientes medidas de seguridad:

- Restricción de direcciones IP desde las que conectar.
- 2FA.
- Antivirus y Cortafuegos en equipo remoto.
- Lista de acceso del túnel para entrar en servicios y app específicas.
- Registro de autoría de conexiones, e inspección del tráfico.

Unidad 3
VPN PRIVADAS

sedian Seguridad Digital de Andalucía

Unidad 3. VPN Privadas

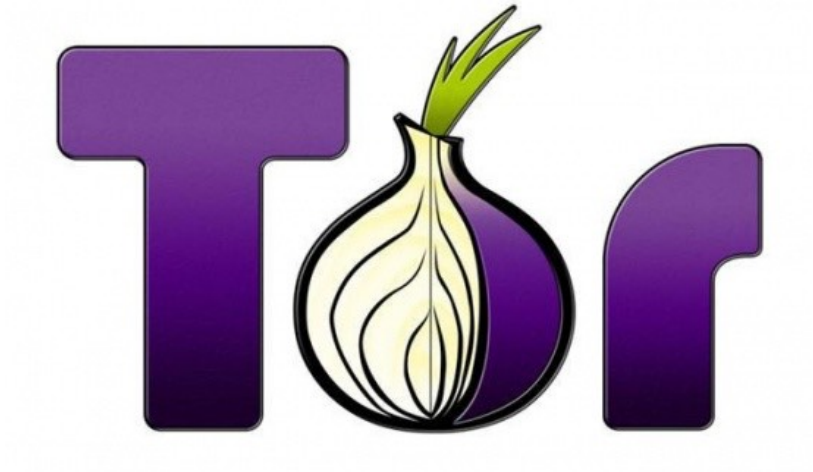
Virtual Private Networks.

Permiten conectar equipos en una red “local” sin que los integrantes de la red estén físicamente conectados entre sí.

Unidad 3. VPN Privadas

Virtual Private Networks.

También se pueden utilizar para ocultar tu ubicación real, incluso para acceder a servidores de contenidos censurados o bloqueados. El caso más conocido es The Onion Router, conocido como TOR.



Hamachi by LogMeIn

Windows

Crea redes virtuales a demanda.

Comunicaciones cifradas, empleando AES-256 bits, consiguiéndolo sobre redes públicas y privadas.

Control centralizado de acceso, con autenticación y bloqueo de redes, y adición de nuevos miembros con facilidad.

Configuración de cliente y red muy sencillo.

Cuenta gratuita limitada pero muy polivalente.

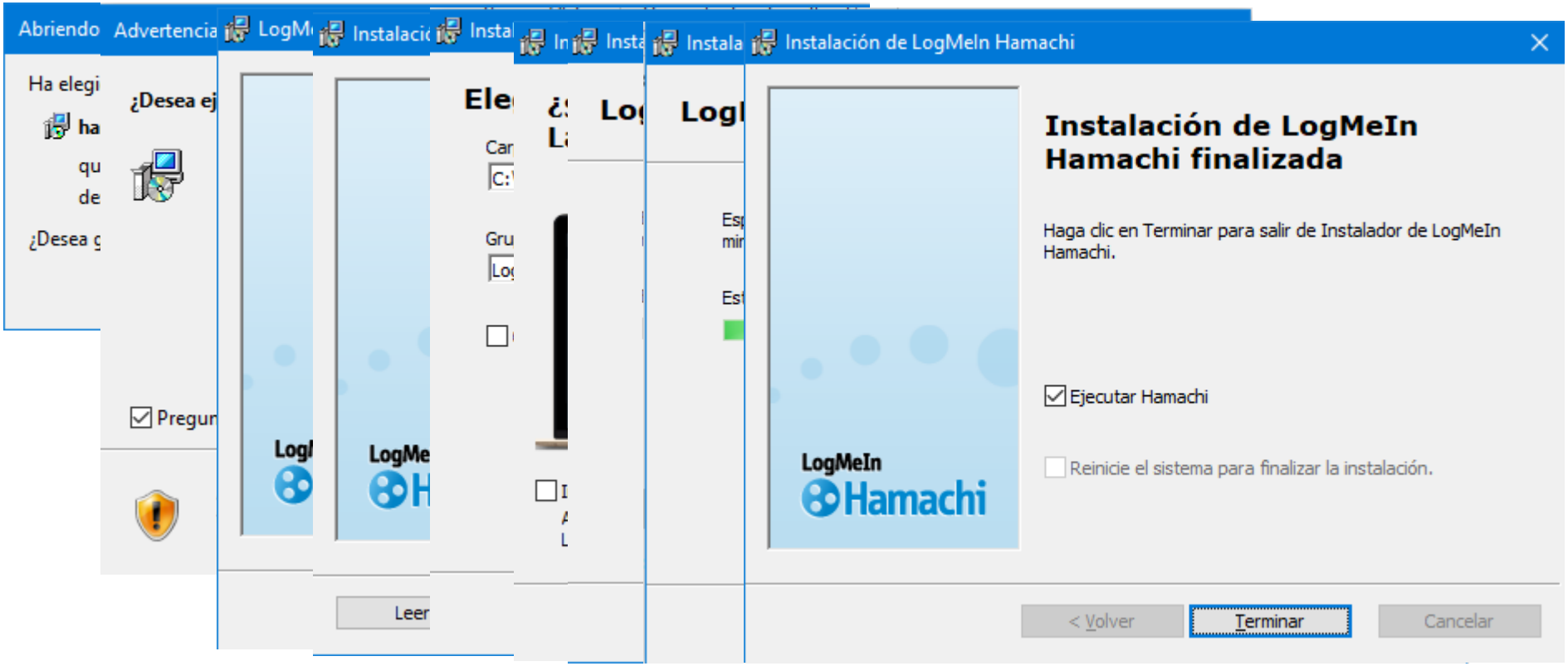
https://www.vpn.net/

Unidad 3. VPN Privadas

Hamachi by LogMeIn

Windows

https://www.vpn.net/

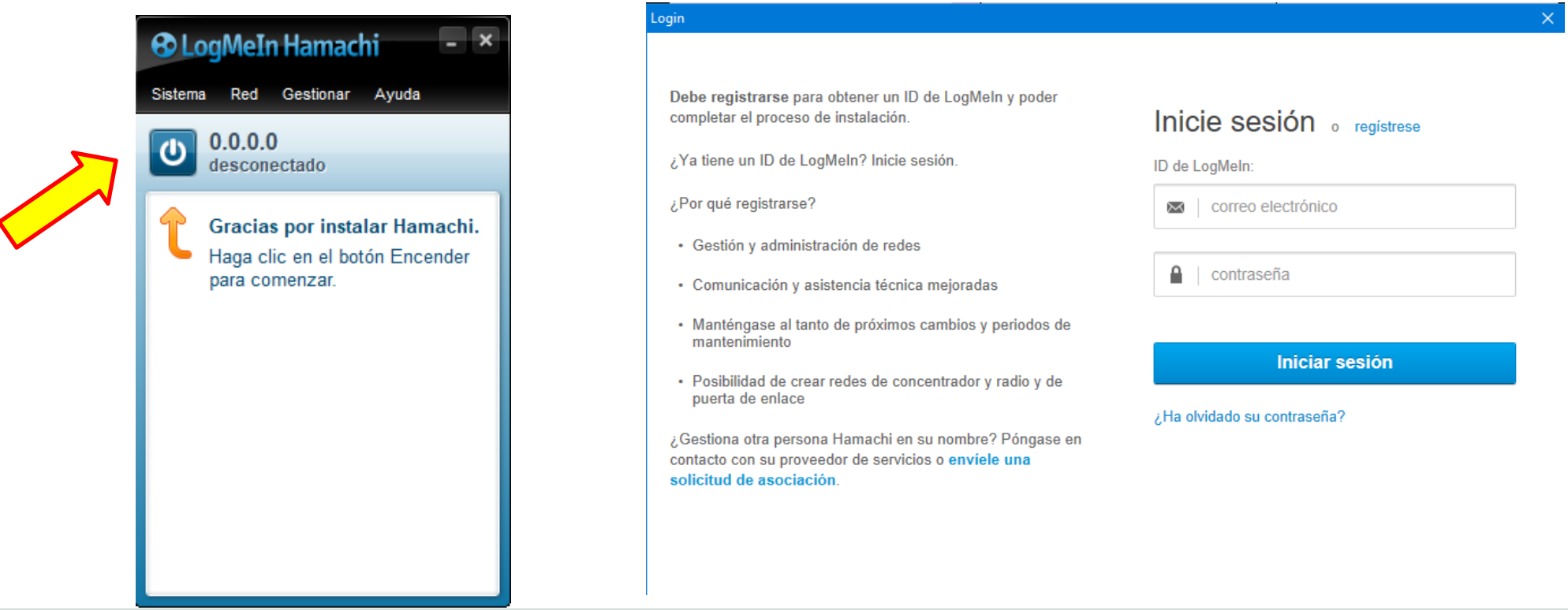


Unidad 3. VPN Privadas

Hamachi by LogMeIn

Windows

https://www.vpn.net/

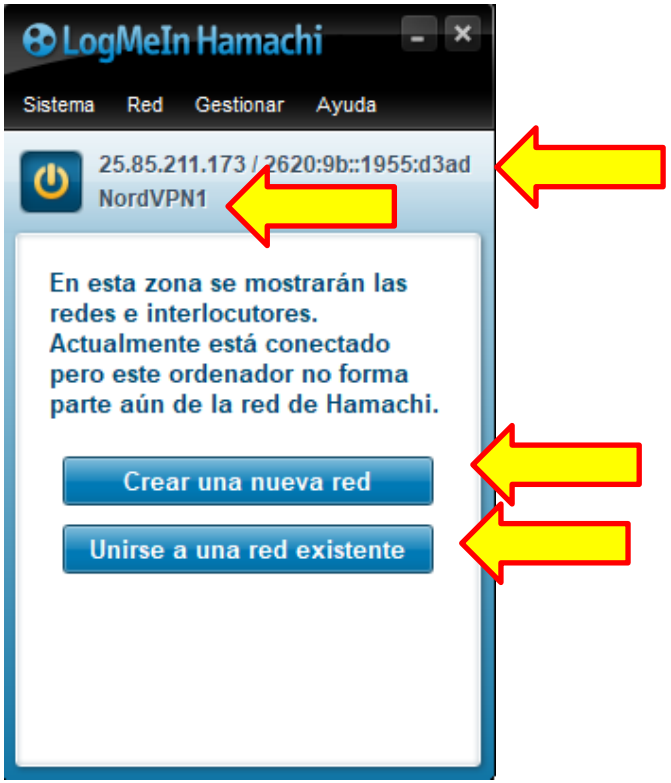


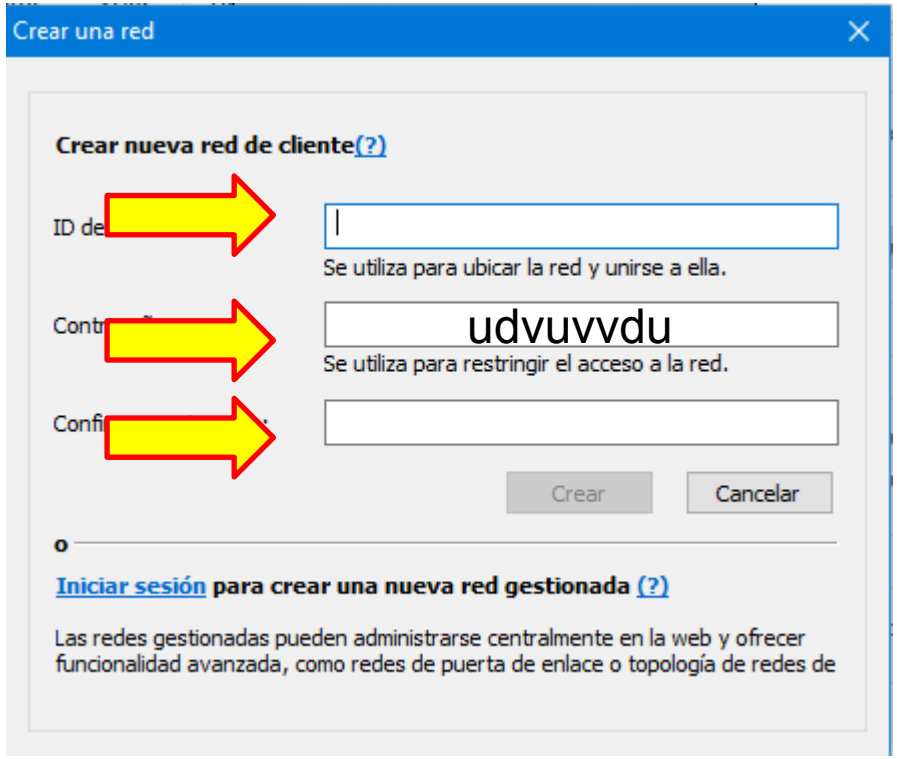
Unidad 3. VPN Privadas

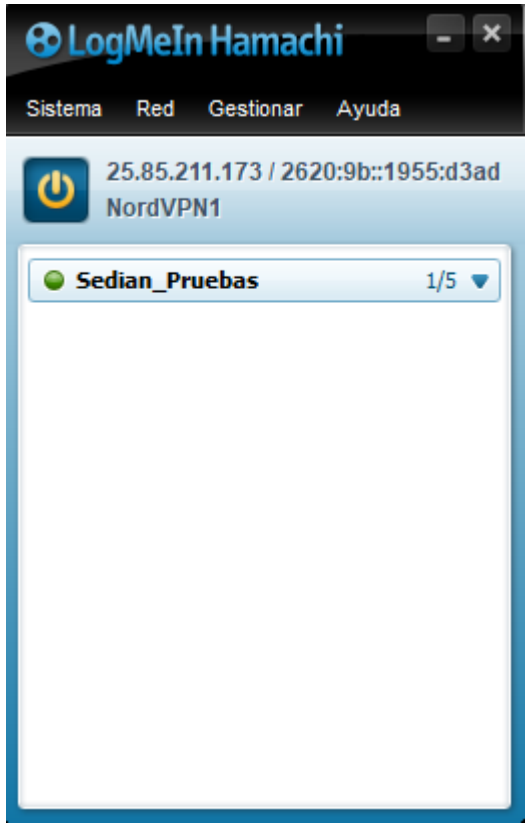
Hamachi by LogMeIn

Windows

https://www.vpn.net/







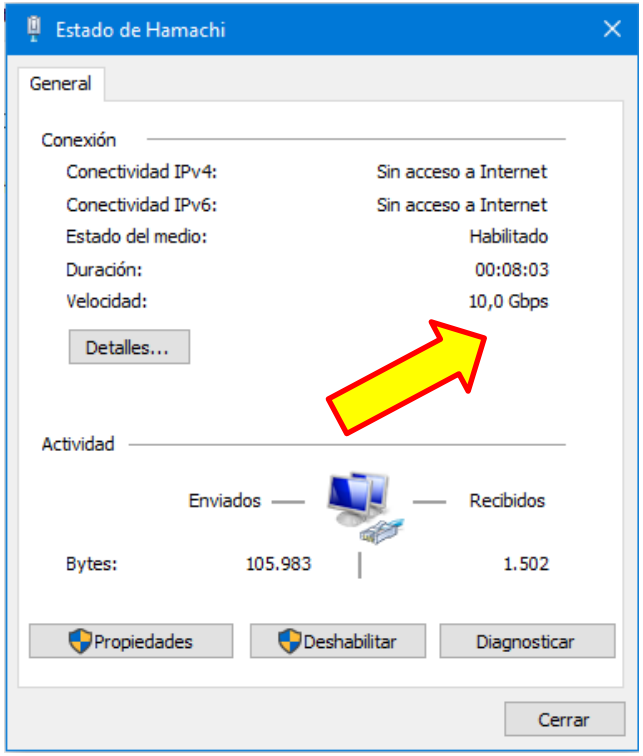
Hamachi by LogMeIn

Windows https://www.vpn.net/

Limitaciones:

5 equipos por red.

No hay límite de redes.



Hamachi by LogMeIn

https://www.vpn.net/linux

Lo bueno de esta VPN es que su versión gratuita es compatible para equipos Windows, Mac y Linux, e incluso tienen una versión para Raspberry Pi:

Hamachi for Linux (x86/x64)

Download the installer from here:

32 bit version:
logmein-hamachi-2.1.0.203-1.i486.rpm
logmein-hamachi_2.1.0.203-1_i386.deb
logmein-hamachi-2.1.0.203-x86.tgz
64 bit version:
logmein-hamachi-2.1.0.203-1.x86_64.rpm
logmein-hamachi_2.1.0.203-1_amd64.deb
logmein-hamachi-2.1.0.203-x64.tgz

Hamachi for Linux on ARM (BETA)

ARM version (BETA):
logmein-hamachi-2.1.0.203-1.armel.rpm
logmein-hamachi_2.1.0.203-1_armel.deb
logmein-hamachi-2.1.0.203-armel.tgz
ARM HF version (BETA):
logmein-hamachi-2.1.0.203-1.armhf.rpm
logmein-hamachi_2.1.0.203-1_armhf.deb
logmein-hamachi-2.1.0.203-armhf.tgz

https://www.vpn.net/linux

Unidad 3. VPN Privadas

RADMIN VPN

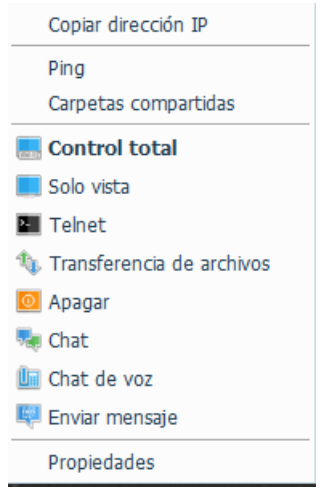
Windows

https://www.radmin-vpn.com

Solo para Windows.

Permite infinitos equipos en la misma red.

Si se adquiere la licencia de control remoto, es el mejor.

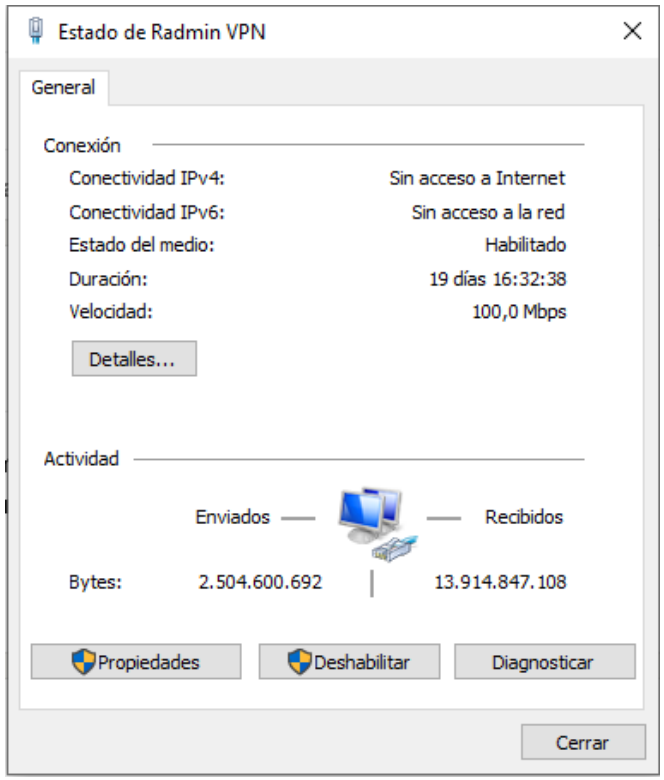


Unidad 3. VPN Privadas

RADMIN VPN

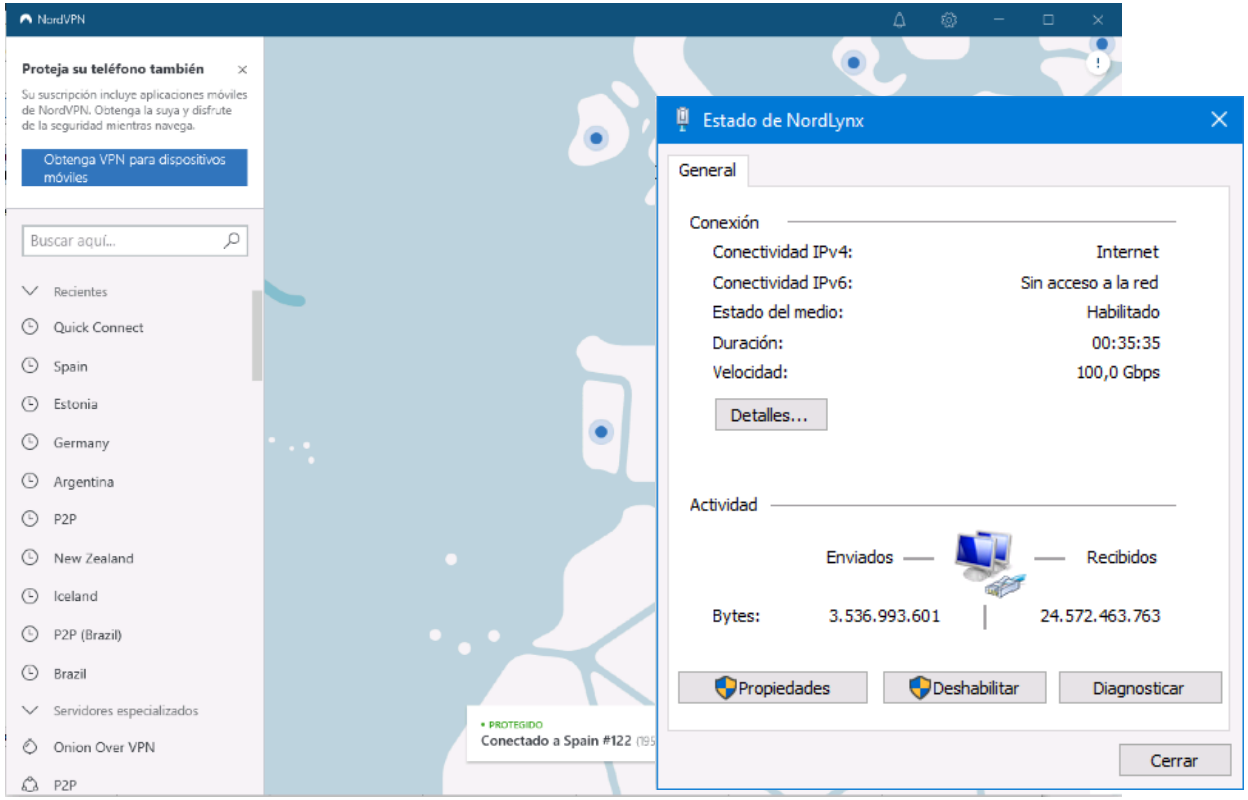
Windows

https://www.radmin-vpn.com



Unidad 3. VPN Privadas

Unidad 3. VPN Privadas



Unidad 3. VPN Privadas

Características principales:

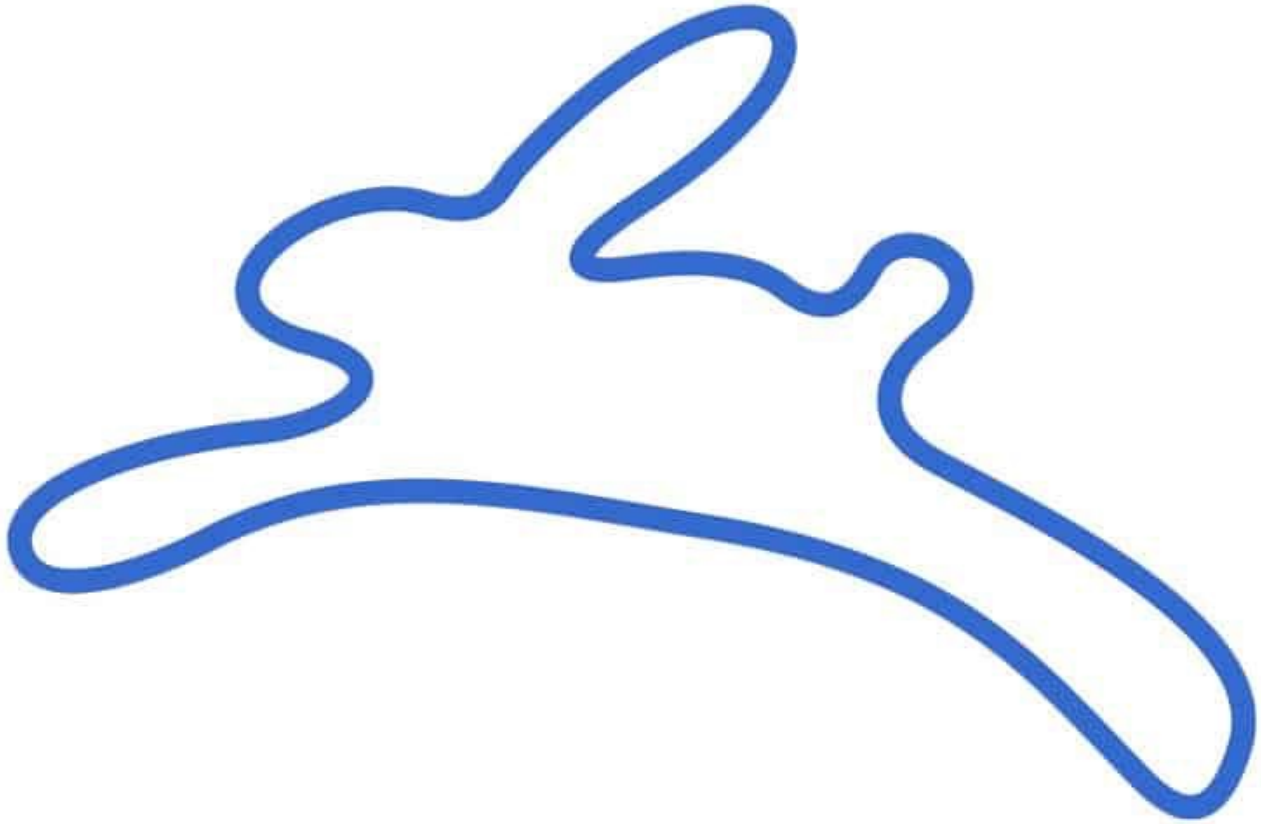
- Todas tienen una pérdida de velocidad, aunque te muestren que tu conexión es más rápida que tu línea.
- Se pueden banear las direcciones de salida, pues son fijas y conocidas en el tiempo por el resto de proveedores de servicios.
- Pueden combinarse con otras, a costa de una mayor pérdida de velocidad.

Unidad 4
VPN OCULTAS

sedian Seguridad Digital de Andalucía

Unidad 4. VPN Ocultas

Freenet



Freenet

Su principal publicidad no es como VPN, sino como red de distribución de información descentralizada y resistente a la censura.

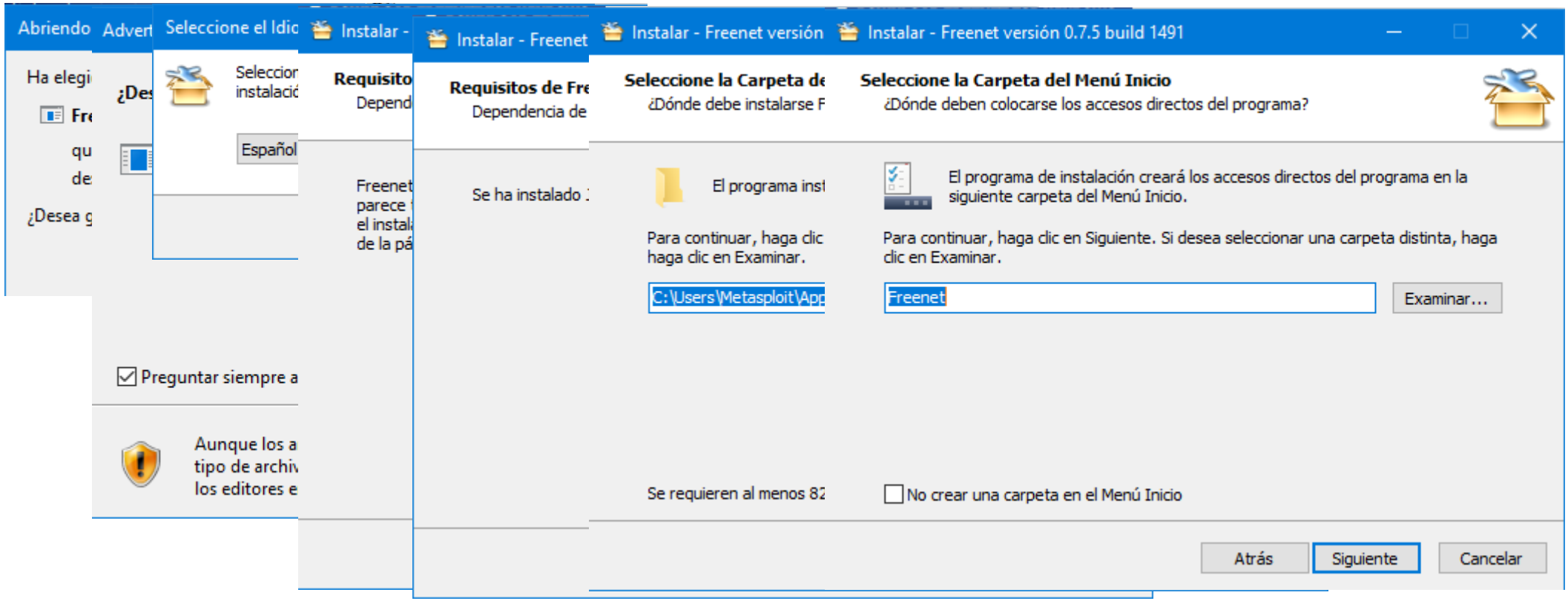
Freenet distingue 2 tipos de redes:

- **Opennet**, que se conecta a nodos desconocidos.
- **Darknet**, que se conecta solo a amigos.

Se trata de una aplicación realizada en java, que funciona como un contenedor dentro de Google Chrome, creando un proxy hacia el puerto 8888, y conectándose bajo la url: http://localhost:8888

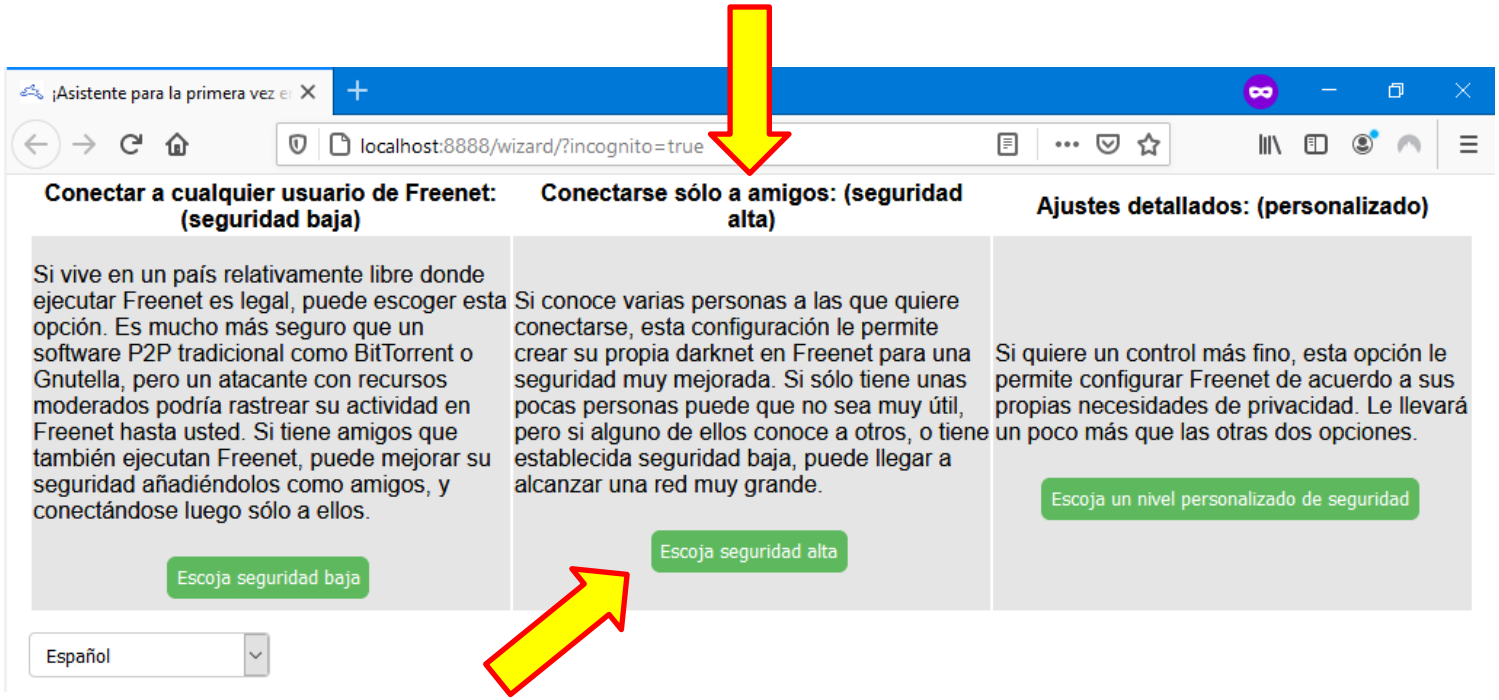
Unidad 4. VPN Ocultas

https://freenetproject.org/pages/download.html#windows



Freenet

Es una aplicación que se queda residente en la bandeja del sistema, y que si hacemos doble clic en ella, nos abre directamente el navegador.



Unidad 4. VPN Ocultas

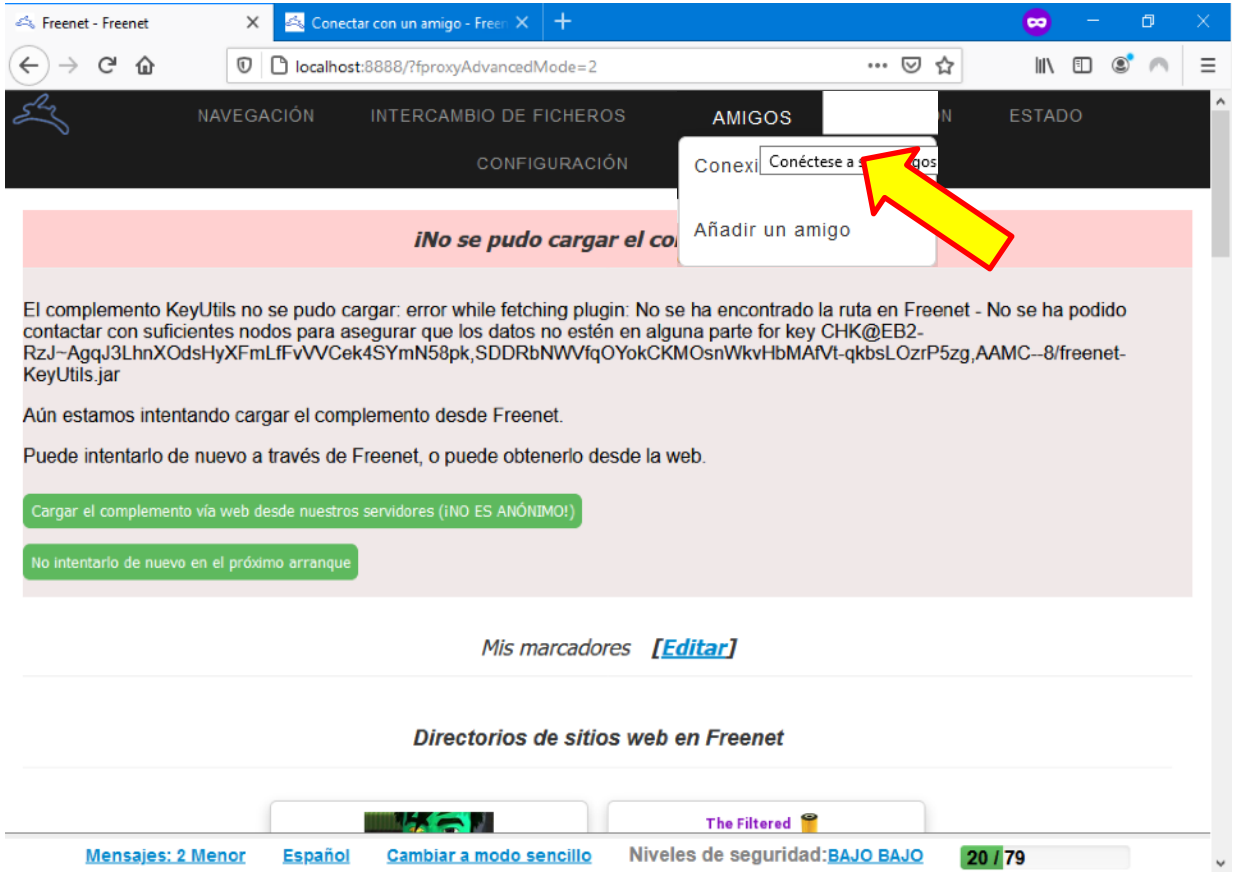
Freenet

Freenet


Seguridad de la red - Freenet
localhost:8888/wizard/?step=SECURITY_NETWORK&preset=HIGH&co
¡Añada amigos o Freenet no podrá conectar!
POR FAVOR, OBSERVE: Que en el modo de alta seguridad, Freenet sólo conecta con sus amigos (estilo darknet). Sus amigos son personas en las que confía, a quienes ha añadido a través de la página Añadir un amigo en el menú Amigos. En el modo de alta seguridad Freenet no operará hasta que haya añadido al menos un amigo, y debe añadir al menos 3 - preferiblemente de 5 a 10 - para un mejor rendimiento. Freenet no puede ocultar las conexiones que realice hacia otros, sólo lo que se transfiere a través de ellas. No conecte con cualquiera en quien no confíe o con quien no querría que se le vinculara en su vida normal.
Confío al menos en una persona que ya usa Freenet, y la añadiré a través de la página de amigos Añadir un amigo
Atrás
Siguiente

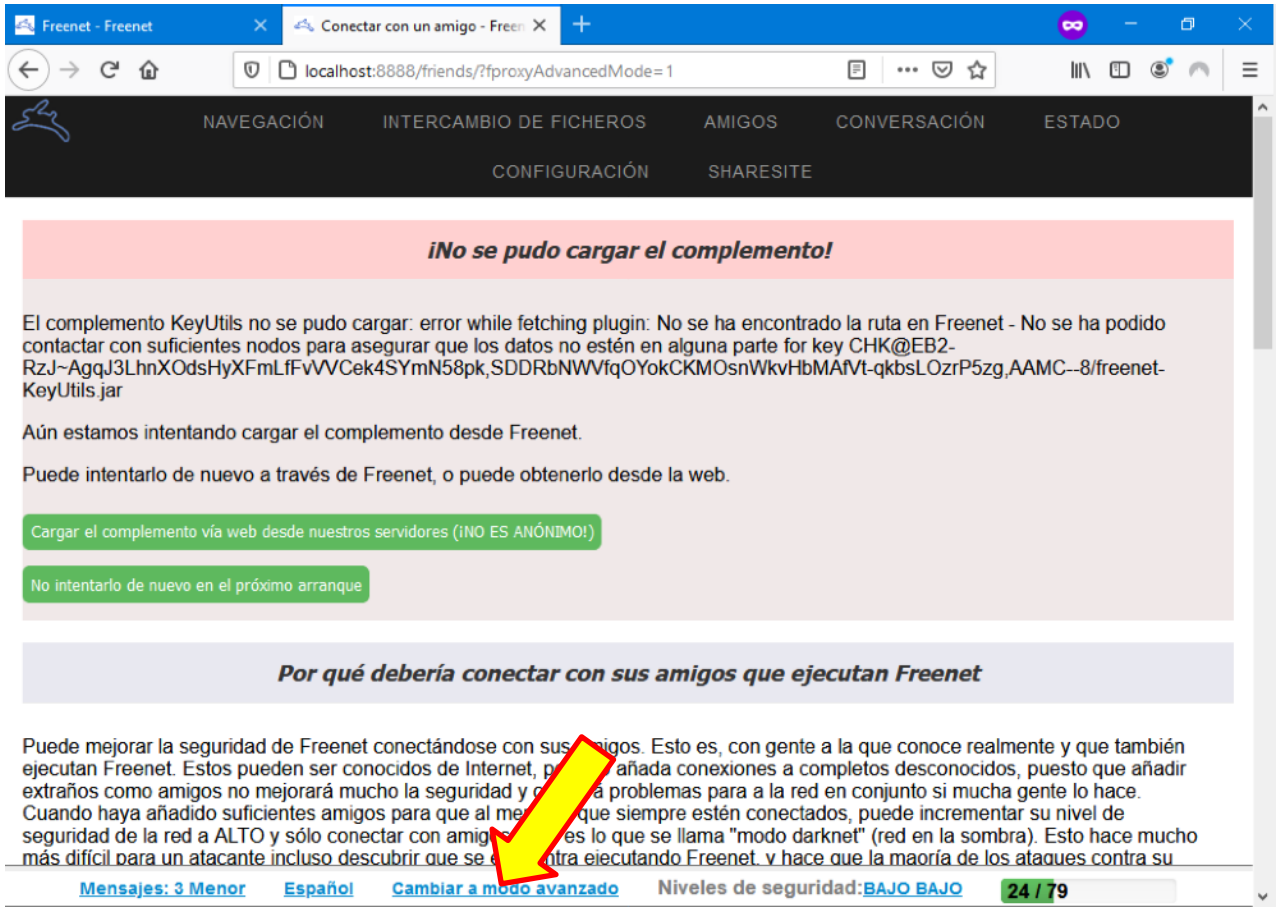
Unidad 4. VPN Ocultas

Freenet



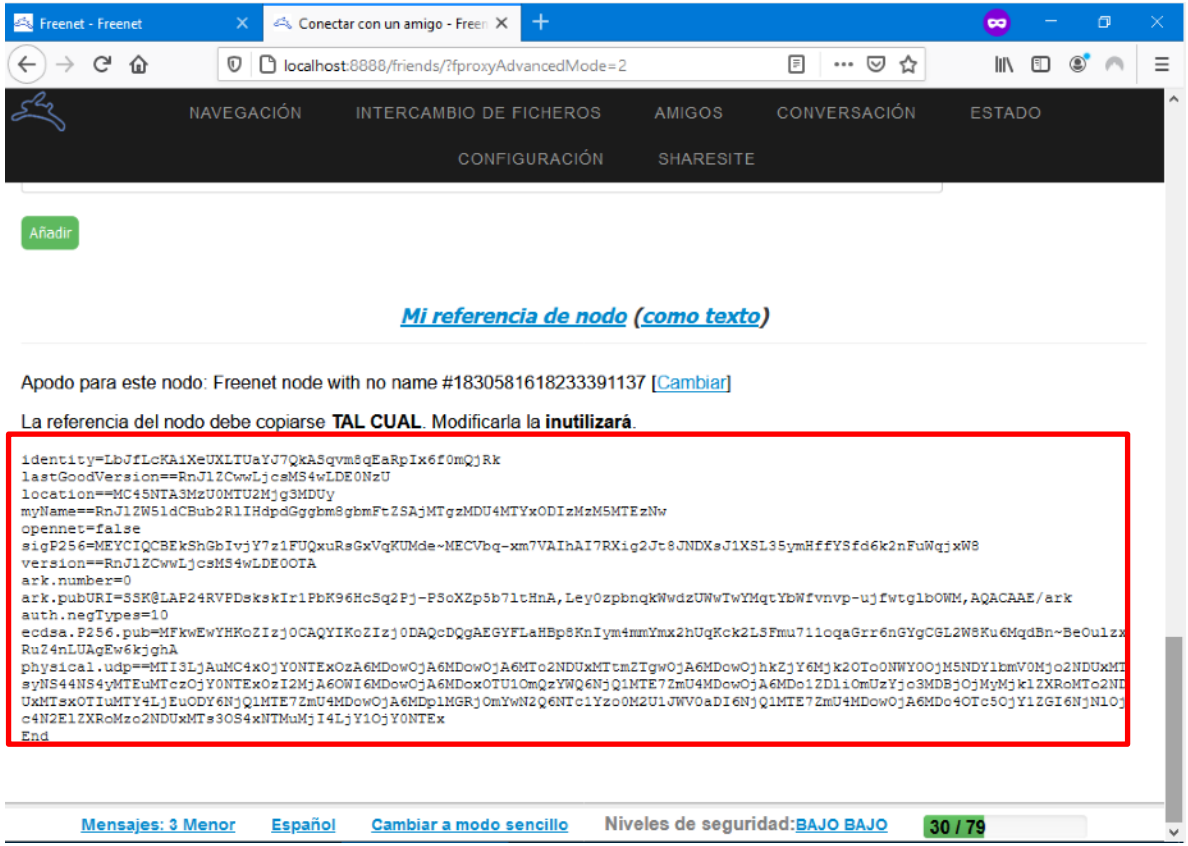
Unidad 4. VPN Ocultas

Freenet



Unidad 4. VPN Ocultas

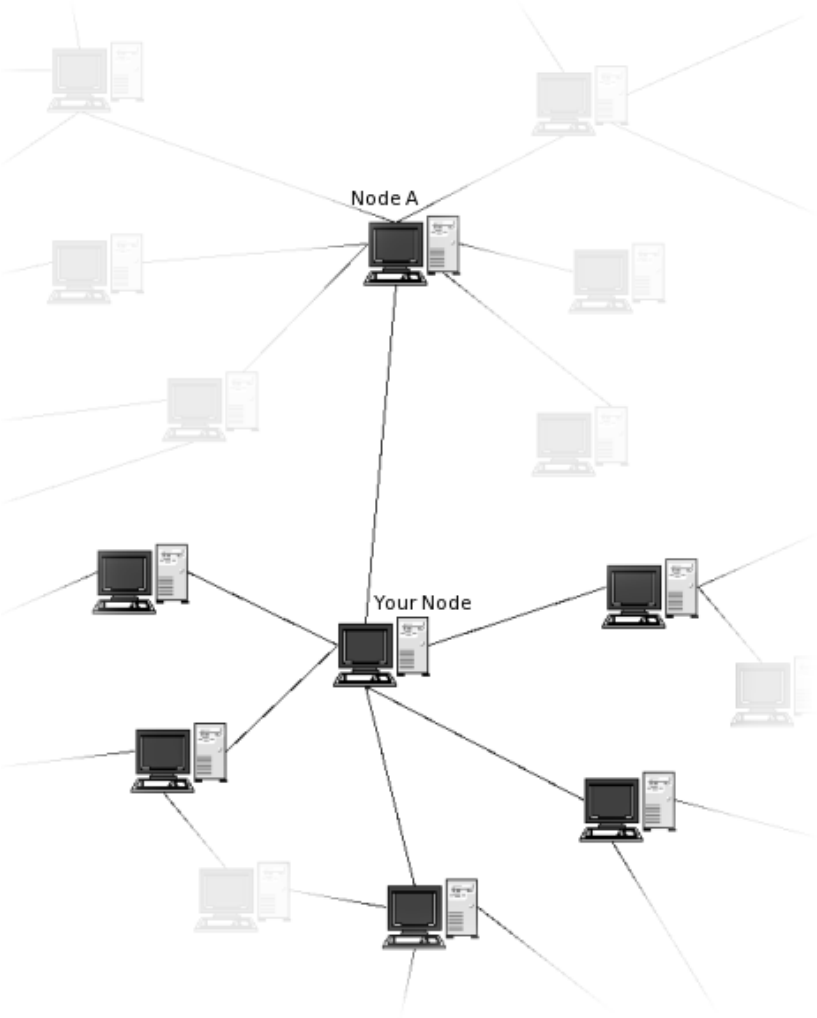
Freenet



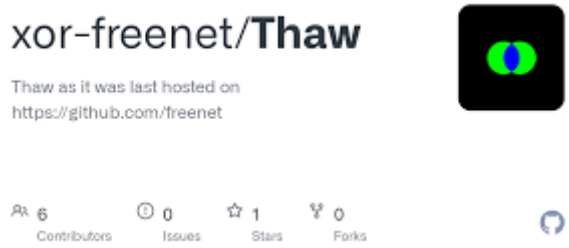
Freenet

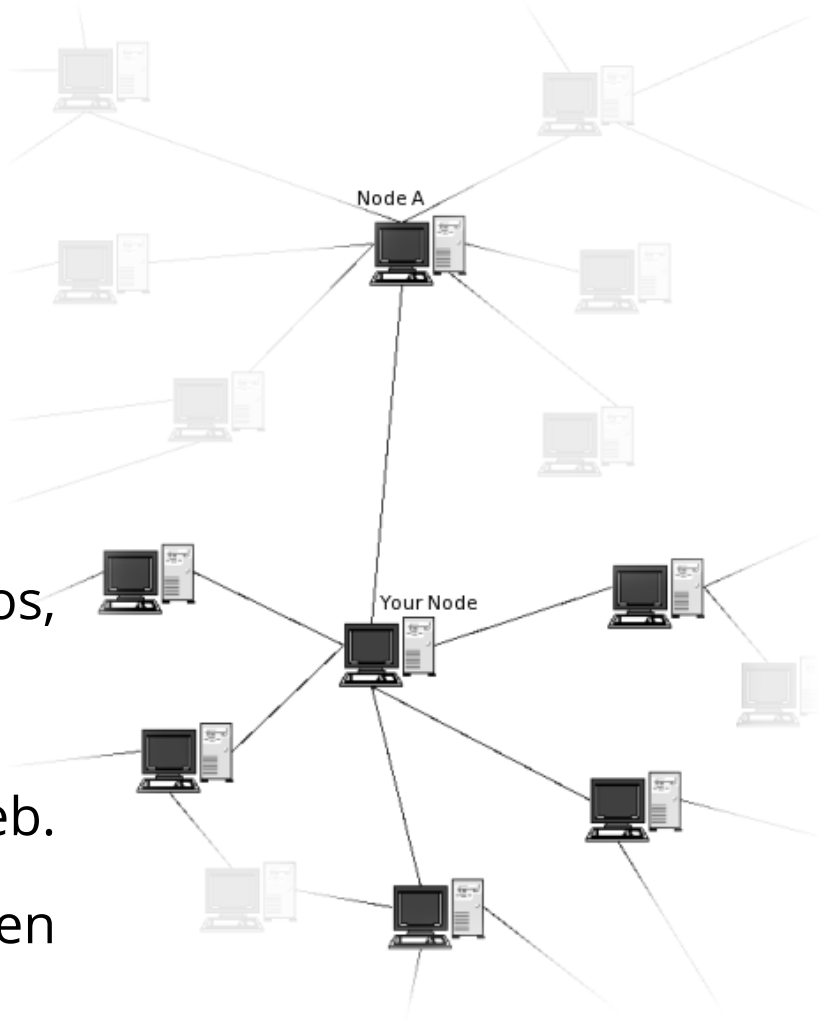
En modo **Darknet**, sólo te ven tus «amigos» y, como tal, todos los documentos que tengas almacenados los puedes compartir con ellos.

La información se enlaza mediante una clave, a modo de índice, de forma que es a través de éste como se localiza la información.



Freenet





Gestor de descargas e intercambio de archivos, compartidos mediante índices, para Freenet.

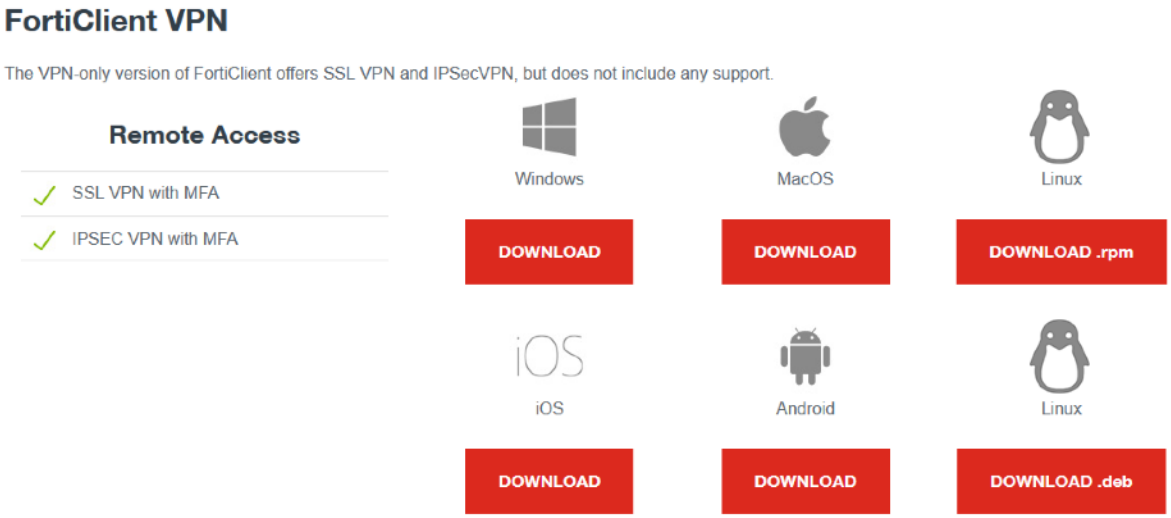
Freesites es la denominación a los sitios web. Desde la misma app Jsite de instalación se pueden crear.

Unidad 5
VPN + Firewall

sedian Seguridad Digital de Andalucía

Unidad 5. VPN + Firewall físico

Una de las soluciones más adecuada es la de utilizar un firewall físico, el cual tiene un puerto abierto bajo protocolo SSL a Internet, y por medio del software adecuado, realiza la tunelización del acceso.



Unidad 5. VPN + Firewall físico

Cisco AnyConnect Secure Mobility Client

Ubiquiti Secure Gateway USG Router

Unidad 6
Comparativa de soluciones

sedian Seguridad Digital de Andalucía

Unidad 6. Comparativa de soluciones

Por precio:

- Hamachi y RadminVPN son líderes indiscutibles.
- Hamachi se puede adquirir como versión pro (44 €/año x 32 eq).
- RadminVPN demuestra una fiabilidad inquebrantable desde marzo de 2020, en varios casos muy señalados.

Unidad 6. Comparativa de soluciones

Por Seguridad:

- Las soluciones basadas en cortafuegos con clientes SSL para tunelizar, son escalarmente más caras pero más fiables en el tiempo.
- Suelen tener un Servicio Técnico de atención al cliente.
- En algunos casos, el propio cliente SSL dispone

de protección antivirus.

Unidad 6. Comparativa de soluciones

Por Anonimato:

- Las VPN de pago para anonimizar la conexión y tener IP de salida por otro país u otra dirección IP pueden ser baneadas por servidores ajenos.
- Con las VPN se pierde del orden de un 30%-50% de velocidad de conexión.

Unidad 6. Comparativa de soluciones

Por Ocultación:

- Las Darknets aseguran la completa ocultación a ojos ajenos, pero se ha de tener especialmente cuidado con los usuarios inexpertos.
- Los servicios que se pongan a disposición de los usuarios deberán tener una capa adicional de protección,
- Los equipos deben ser de uso exclusivamente empresarial.

Unidad 7

Conclusiones

Unidad 6. Comparativa de soluciones

El Teletrabajo es seguro siempre que:

- No se tengan puertos abiertos al exterior
- En función de la arquitectura de la empresa:
  - Si cada usuario tiene un equipo local y remoto
  - Si se tienen máquinas virtuales a las que se conecte en remoto
  - Si se dispone de un servidor centralizados y equipos remotos
- Siempre contar con sistemas de protección individual (mínimo, antivirus)

sedian Seguridad Digital de Andalucía