LEGISLACIÓ DE SEGURETAT I PROTECCIÓ DE DADES.

TEMA 5 :: UF3

Iker Testa, Adrián Torres, Xavi Murcia

Índice

Eliminación segura de ficheros

Sistema de alimentación ininterrumpida:

Información del SAI:

Para prevenirnos de posibles cortes repentinos de energía, tenemos instalados dentro de nuestro CPD potentes SAI's. Concretamente tenemos un Salicru SLC-2000-TWIN RT3 SAI IoT On-Line Doble Conversión Torre/Rack 3000VA 2000W. En Xhosting, contamos con 2 unidades de este SAI, para poder estar prevenidos ante averias ajenas a nuestro trabajo.

Este SAI cuenta con una pequeña pantalla integrada en la parte superior del SAI que nos puede dar información sobre el nivel de carga y de batería del SAI, la tensión de entrada y de salida, nos permite navegar por la configuración básica del SAI…

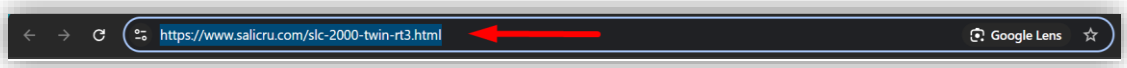
Este SAI es enracable, por lo tanto los tendremos integrados en nuestros racks del CPD. Tiene una altura de 2U, profundidad de 600mm y al comprarlo viene con las orejas y petinas de anclaje al rack.

Podremos conectar nuestro servidor al SAI a traves de un puerto RS-232 o un cable Ethernet (es preferible usar un puerto RS-232, según el fabricante) para configurar el SAI desde el software del mismo.

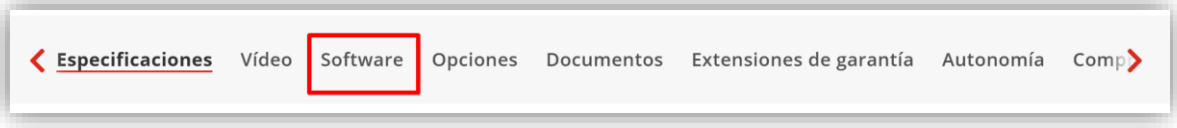
Descarga de software:

Para descargar en nuestro servidor el software del SAI, tendremos que seguir los siguientes pasos:

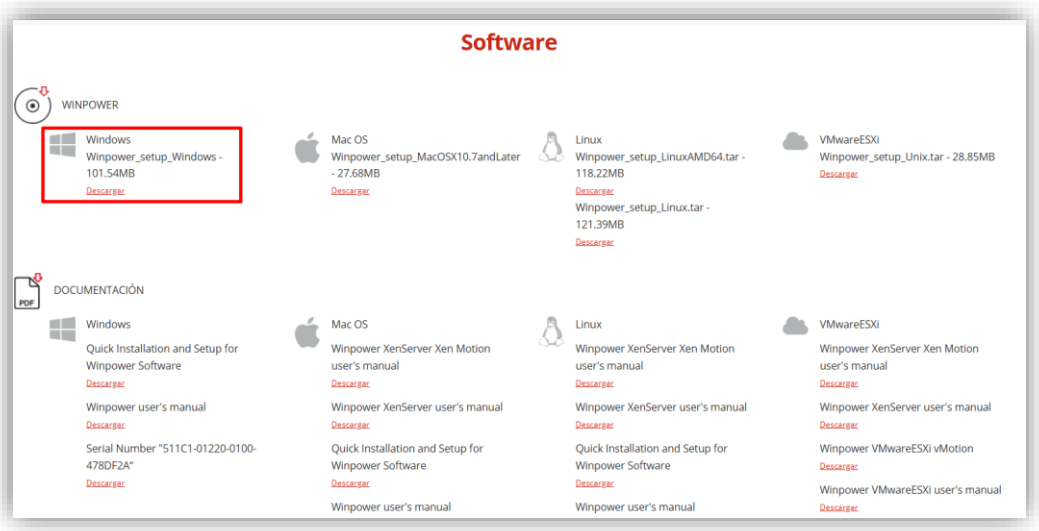
Iremos al sitio oficial del fabricante.



Posteriormente bajaremos hasta encontrar este encabezado de menús:



Aquí ahora lo que nos quedará es seleccionar el sistema operativo para el que queremos descargar el software del SAI:



Al hacer click en descargar se descargará un .exe, es decir el instalador.

Para más información de cómo hacer funcionar el SAI, tenemos la guía de uso dos del fabricante, son 2 archivos PDF. Al hacer click en las siguientes imágenes podeis ir a los manuales.

Guía de Usuario

Guía de Software

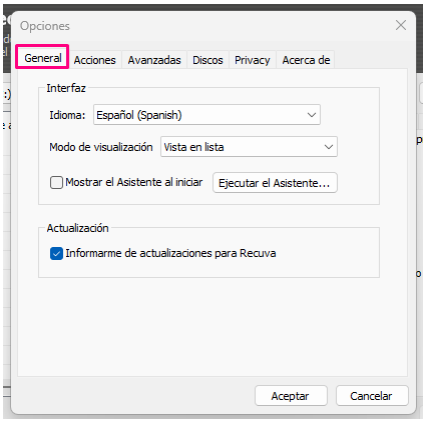
Recuperación de ficheros:

En Xhosting, necesitaremos una herramienta de recuperación de archivos. Para ello utilizamos la herramienta Recuva (click en la imagen para ir al sitio oficial).

Hemos seleccionado Recuva, ya que es un programa de recuperación de archivos eliminados. Esto nos será muy útil en caso de que hayamos eliminado sin querer algún archivo. Una de las ventajas de usar Recuva a la hora de recuperar archivos, es que realiza un escaneo profundo para recuperar los archivos, así consigue detectar archivos, que otros programas no pueden.

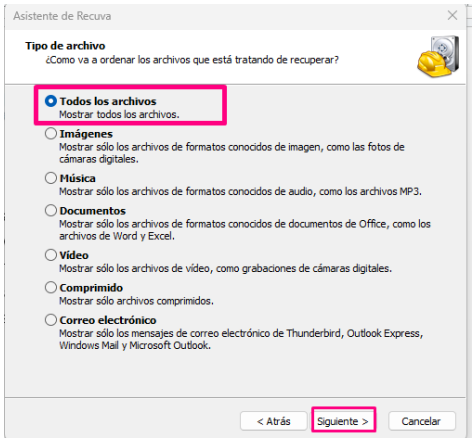
Configuraciones importantes

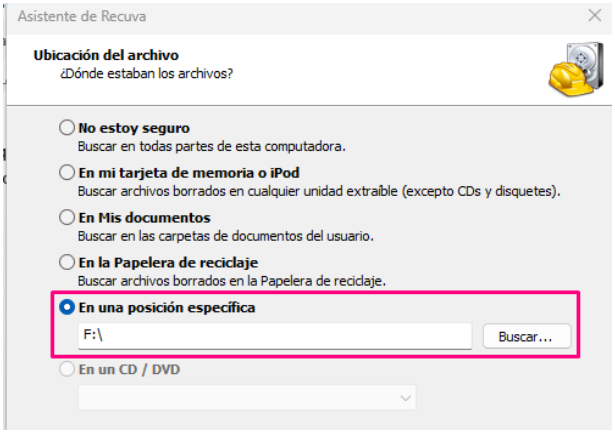
- **Idioma:** Español (el trabajador que lo use, puede cambiarlo si domina mejor otro idioma como el inglés o el catalán; por ejemplo).
- **Modo de visualización:** En lista, que nos permite visualizar mejor los archivos
- **Asistente:** NO, ya que no queremos que el software se inicie nada más arranquemos el PC, se usará solo cuando sea necesario.

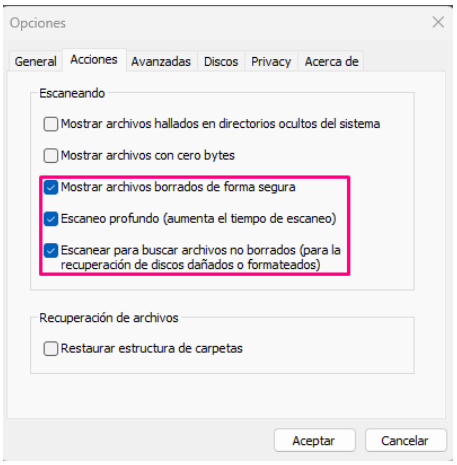


Opciones clave activadas

- Buscar todos los archivos.
- Indicar la ruta específica del dispositivo (pendrive).
- En la pestaña Acciones:
    - Escaneo profundo.
    - Mostrar archivos borrados de forma segura.
    - Escanear archivos no borrados.


Asistente de Recuva
Tipo de archivo
¿Como va a ordenar los archivos que está tratando de recuperar?
Todos los archivos
Mostrar todos los archivos.
Imágenes
Mostrar sólo los archivos de formatos conocidos de imagen, como las fotos de cámaras digitales.
Música
Mostrar sólo los archivos de formatos conocidos de audio, como los archivos MP3.
Documentos
Mostrar sólo los archivos de formatos conocidos de documentos de Office, como los archivos de Word y Excel.
Vídeo
Mostrar sólo los archivos de vídeo, como grabaciones de cámaras digitales.
Comprimido
Mostrar sólo archivos comprimidos.
Correo electrónico
Mostrar sólo los mensajes de correo electrónico de Thunderbird, Outlook Express, Windows Mail y Microsoft Outlook.
< Atrás
Siguiente >
Cancelar


Asistente de Recuva
Ubicación del archivo
¿Dónde estaban los archivos?
No estoy seguro
Buscar en todas partes de esta computadora.
En mi tarjeta de memoria o iPod
Buscar archivos borrados en cualquier unidad extraíble (excepto CDs y disquetes).
En Mis documentos
Buscar en las carpetas de documentos del usuario.
En la Papelera de reciclaje
Buscar archivos borrados en la Papelera de reciclaje.
En una posición específica
F:\
Buscar...
En un CD / DVD


Opciones
General
Acciones
Avanzadas
Discos
Privacy
Acerca de
Escaneando
Mostrar archivos hallados en directorios ocultos del sistema
Mostrar archivos con cero bytes
Mostrar archivos borrados de forma segura
Escaneo profundo (aumenta el tiempo de escaneo)
Escanear para buscar archivos no borrados (para la recuperación de discos dañados o formateados)
Recuperación de archivos
Restaurar estructura de carpetas
Aceptar
Cancelar

Antivirus y Antiespia:

En la compañía, es muy importante proteger la información y los sistemas. Por ello, integraremos un Antivirus y un Antiespia.

¿Para qué los necesitamos?

1. **Protección contra Virus y Malware**: Los antivirus y antiespías nos ayudan a detectar y eliminar programas dañinos que pueden infectar nuestros equipos y robar información.
2. **Evitar Pérdida de Datos**: Los ataques de malware pueden borrar o dañar datos importantes. Con un buen antivirus, podemos prevenir estos problemas y mantener nuestros datos seguros.
3. **Seguridad de Información Confidencial**: Tenemos datos sensibles como información financiera y de clientes. Los antiespías nos protegen contra programas que intentan robar esta información.
4. **Reducción de Riesgos de Ciberataques**: Las amenazas cibernéticas cambian constantemente. Un antivirus actualizado nos protege contra nuevas amenazas y reduce el riesgo de ataques que pueden afectar nuestras operaciones.
5. **Cumplimiento de Normativas**: Muchas leyes y regulaciones requieren que tengamos medidas de seguridad. Usar antivirus y antiespías nos ayuda a cumplir con estos requisitos y evitar sanciones.
6. **Mejora de la Productividad**: El malware puede hacer que nuestros sistemas funcionen más lentos. Un buen antivirus asegura que los equipos funcionen bien, permitiendo a los empleados trabajar sin interrupciones.

Software seleccionado:

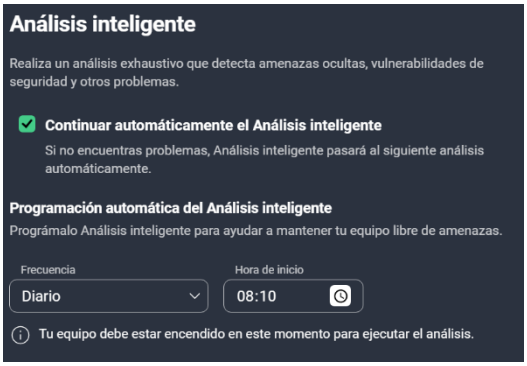
En Xhosting, hemos decidido implementar Kaspersky como antivirus, y Spybot como antiespía. Han sido seleccionados porque, tras haber trabajado cada uno de nosotros con diferentes softwares de ciberseguridad, hemos llegado a la conclusión que son los dos sistemas que mejor se adaptan a nuestras necesidades.

Análisis pequeño (diario):

En la empresa, se empieza a trabajar alas 8, por ello el primer análisis se realizará a las 8:10, se demorará entre 3 y 5 minutos como mucho. Damos 10 minutos de margen porque entendemos que algún trabajador se puede retrasar un poco en su hora de llegada de manera esporádica. Si lo hacemos a primera hora, dejamos que el trabajador se tome el café, programe su trabajo...

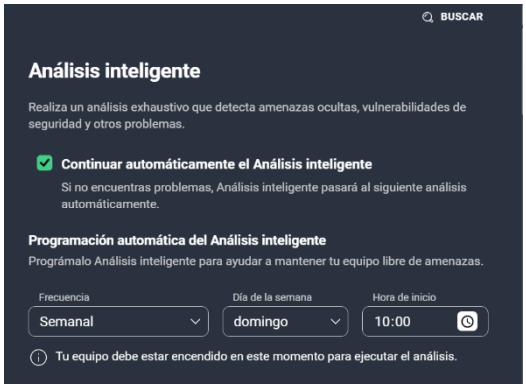
¿Que se analiza?

- Archivos de Inicio
- Claves del Registro
- Archivos en Ejecución
- Carpetas Comunes
- Dispositivos Extraíbles
- Navegación Web



Análisis completo de antivirus (semanal):

En este Análisis, se analiza el Sistema Completo, de arriba abajo. Puesto que se realiza en domingo, día que la empresa cierra, da igual el tiempo que se demoré cada análisis.



Antiespía:

Necesitamos el antiespía para proteger nuestra red y sistemas contra programas espías que roban información confidencial, asegurando la privacidad y seguridad de nuestros datos.

Análisis pequeño (6 horas):

- **Detección de Spyware:** El antiespía busca programas espías que recopilan información sin tu consentimiento, como keyloggers y adware.
- **Análisis de Comportamiento:** Monitorea el comportamiento de los programas y archivos para identificar actividades sospechosas que podrían indicar la presencia de spyware.
- **Protección de Navegación Web:** El antiespía revisa el historial y los archivos temporales del navegador para detectar y bloquear contenido malicioso que pueda haber sido descargado.
- **Escaneo de Dispositivos Extraíbles:** Analiza unidades USB y discos externos conectados para detectar y eliminar spyware.

- **Revisión de Archivos Adjuntos de Correo Electrónico:** Revisa los archivos adjuntos y enlaces en los correos electrónicos para detectar spyware.

Análisis completo (24 horas):

- **Detección de Spyware**: Buscará y eliminará programas espías que recopilan información sin consentimiento.
- **Análisis de Comportamiento**: Monitoreará el comportamiento de los programas y archivos para identificar actividades sospechosas.
- **Protección de Navegación Web**: Revisará el historial y los archivos temporales del navegador.
- **Escaneo de Dispositivos Extraíbles**: Analizará unidades USB y discos externos conectados.
- **Revisión de Archivos Adjuntos de Correo Electrónico**: Revisará los archivos adjuntos y enlaces en los correos electrónicos.
- **Eliminación de Cookies y Caché**: Borrará cookies y caché del navegador que puedan contener rastreadores o spyware.

Configuraciones de Firewall:

En nuestra compañía, dentro del CPD, tenemos colocado el ZyXEL USG Flex 200, un cortafuegos potente, diseñado para la ciberseguridad del mundo empresarial.

Características del Firewall:

Algunas de las características más destacables de este ZyXEL USG Flex 200 son:

- **Rendimiento del cortafuegos (SPI):** hasta 1.8 Gbps
- **Rendimiento VPN:** hasta 450 Mbps
- **Conexiones TCP simultáneas:** hasta 600,000
- **Conexiones VPN/SSL simultáneas:** hasta 200
- **Soporte VPN:** IKEv2, IPSec, SSL y L2TP/IPSec
- **Algoritmos de seguridad:** IPSec y SSL/TLS

Este firewall no cuenta con pantalla integrada para una configuración básica ni para una consulta rápida del estado (temperatura, rendimiento…). Lo que si tiene es un software descargable para configurar el firewall y poder consultar su estado en todo momento.

Guías de uso:

Para conseguir dominar el firewall y todas sus configuraciones, el fabricante tiene varias guías de usuario separadas por temas. También tiene una completa en la que aparece toda la información del producto, esta es a la que tenemos acceso haciendo click en la imagen del documento que tenemos a continuación:

Guía de usuario completa

Cifrado de dispositiovos:

Cifrar los dispositivos en Xhosting, es esencial para proteger datos sensibles contra accesos no autorizados, cumplir con normativas de protección de datos, reducir riesgos de ciberataques y garantizar la confidencialidad y privacidad de la información, incluso en caso de pérdida o robo de los dispositivos.

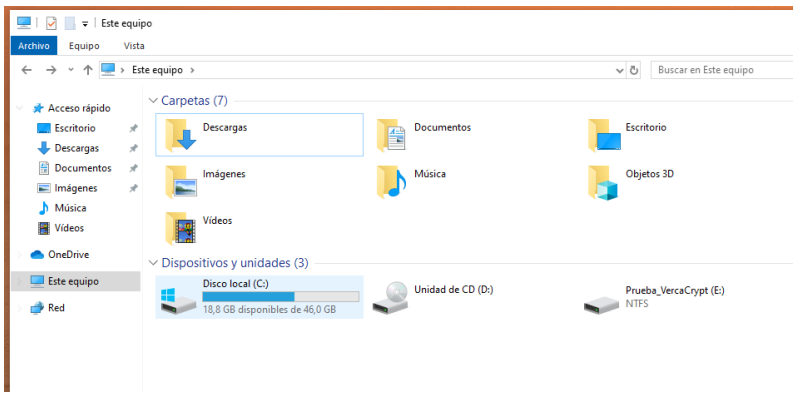
Software seleccionado:

El software con el que trabajamos en Xhosting, será el Veracrypt, cifraremos los dispositivos de las máquinas clientes de la empresa; es decir, con lo que trabajan los empleados

Configuraciones del Veracrypt:

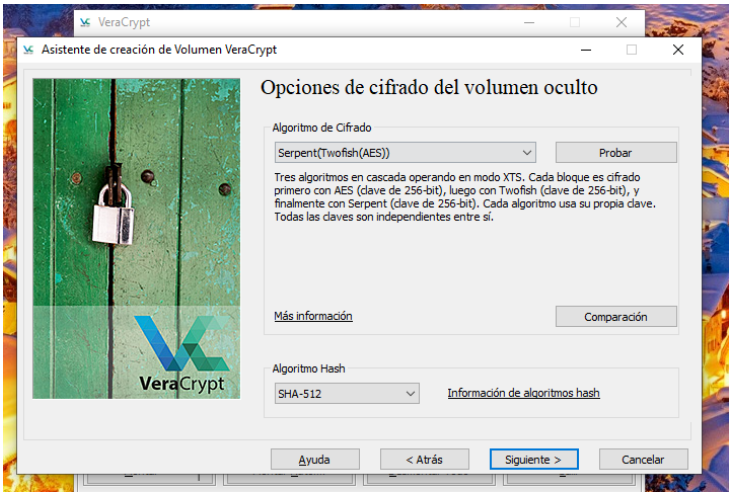
Uso de volúmenes ocultos

- Se crea un volumen cifrado visible y, dentro de él, un volumen oculto.
- Esta técnica permite proteger datos críticos incluso si se obliga a revelar la contraseña del volumen visible.



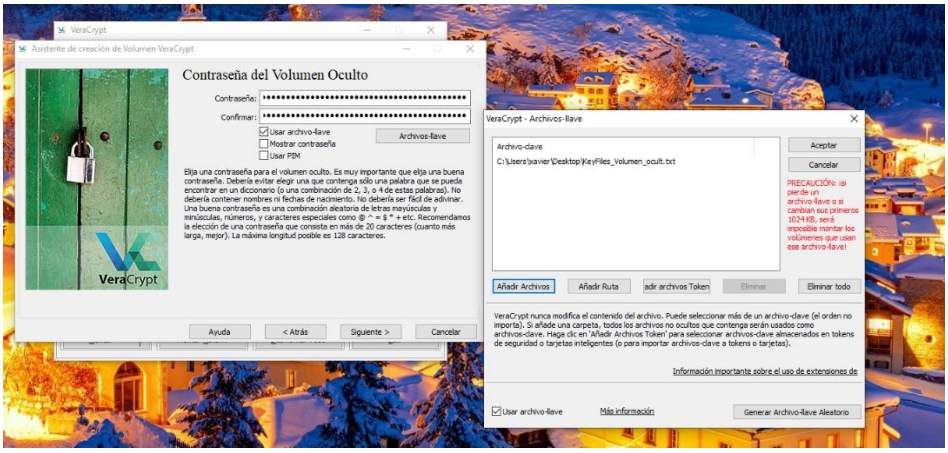
Triple cifrado en cascada

- Se utiliza un sistema de triple cifrado (AES-Twofish-Serpent) para aumentar la resistencia frente a ataques.



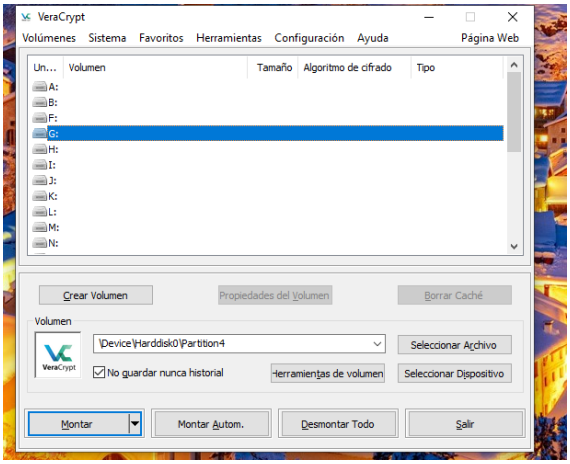
Contraseñas robustas y KeyFiles

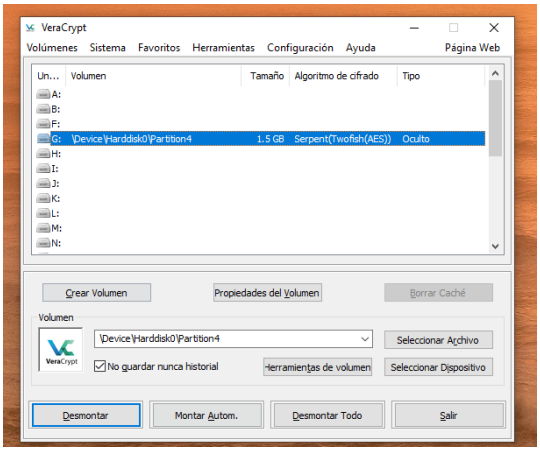
- Se definen contraseñas largas y complejas (ej. 43 caracteres con símbolos, mayúsculas y números).
- Se emplean KeyFiles (archivos necesarios para descifrar), que deben guardarse en ubicaciones seguras y no modificarse nunca.



Montaje y desmontaje seguro

- Los volúmenes se pueden montar y desmontar fácilmente con VeraCrypt, manteniendo los datos protegidos cuando no están en uso.





Túneles VPN:

En Xhosting, queremos implementar túneles VPN para trabajadores que puedan trabajar desde casa, p directivos que hayan hecho un viaje de parte de la empresa, para visitar clientes, conocer nuevos posibles clientes… Los trabajadores que podrán teletrabajar de manera habitual son los encargados de las áreas de Marketing, Administración y Finanzas, RRHH y los directivos; obviamente no teletrabajaran todos los días ni lo harán todos a la vez, pero es una opción que le ofrecemos a nuestros trabajadores para que estén más relajados y cumplan mejor con sus funciones.

Utilidad de la herramienta:

Un túnel VPN, permite a los empleados conectarse a la red de la empresa, sin la necesidad de estar en la oficina. Aparte de esto la conexión gracias a los túneles VPN, es cifrada y segura.

¿Cómo lo haremos?

Lo haremos mediante Windows 2019 Server, en el Server, deberemos de tener las características de DirectAccess y VPN (RAS) activadas para configurarlas posteriormente.

No solo necesitaremos hacer esto, también tendremos que ir a nuestro Firewall para configurarlo y dejar abiertos los siguientes puertos:

- **PPTP:** Puerto 1723 TCP y protocolo GRE (47).
- **SSTP:** Puerto 443 TCP (recomendado si tienes un certificado SSL).
- **L2TP/IPsec:** Puertos 1701, 500, 4500 UDP.

Entre otras configuraciones también tendremos que seleccionar desde el servidor que usuarios queremos que tengan acceso remoto a sus máquinas físicas de la empresa.

¿Qué debe hacer el trabajador?

El trabajador simplemente tendrá que acceder a la herramienta Escritorio Remoto de su portátil (proporcionado por Xhosting) e introducir la IP de la empresa, posteriormente tendrá que iniciar sesión con sus credenciales (nombre de usuario y contraseña).

Eliminación segura de ficheros:

En nuestra compañía, es fundamental que tengamos un sistema para deshacernos de manera segura y correcta de los ficheros. Tanto para proteger la información sensible de la empresa, además de que también debemos de cumplir con la normativa de privacidad, como el RGPD.

¿Como lo haremos?

Para hacerlo, usaremos herramientas que ya vienen incluidas en Windows Server, sin necesidad de instalar nada nuevo. El proceso consiste en dos pasos: primero se borra el archivo normalmente, y después se ejecuta una herramienta que limpia el espacio del disco donde estaba ese archivo, sobrescribiéndolo para que no quede rastro.

A esta acción de eliminar de manera segura los ficheros en entornos Windows, también se le conoce como chiper /w.

Proceso automatizado:

Además de eso, en nuestros servidores automatizaremos este procedimiento mediante scripts de PowerShell, lo que permitirá ejecutar la limpieza de forma periódica o al cierre de sesión, según las necesidades de cada servidor o entorno de trabajo.