INSTALACIÓN, CONFIGURACIÓN Y ADMINISTRACIÓN

USERS

Argentina $ 22.- // México $ 49.-

Técnico en REDES & SEGURIDAD

17

ADMINISTRACIÓN Y ASISTENCIA REMOTA

En esta clase conoceremos los protocolos necesarios para administrar y ofrecer asistencia a la distancia. También veremos los servicios DDNS y de qué forma podemos hacer uso de las plataformas VNC.

- ADMINISTRACIÓN REMOTA
- TEAMVIEWER
- TERMINAL SERVER
- PLATAFORMA CITRIX
- TECNOLOGÍA INTEL VPRO

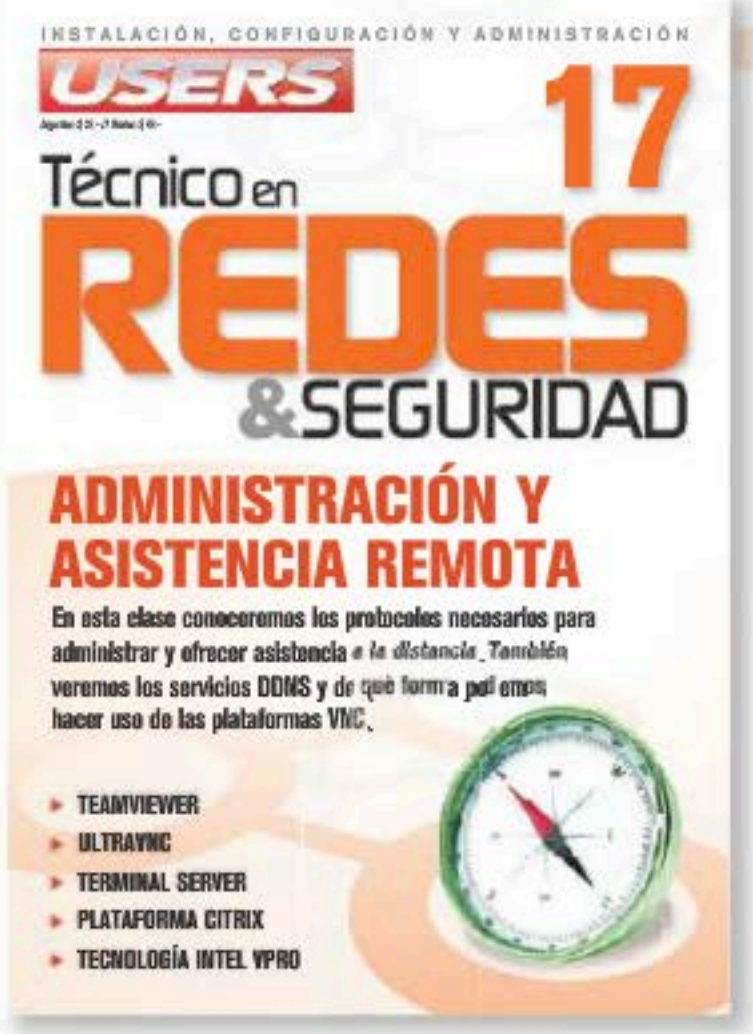
USERS

Técnico en REDES &SEGURIDAD

Coordinador editorial
Paula Budris

Asesores técnicos
Federico Pacheco
Javier Richarte

Nuestros expertos
Valentín Almirón
José Bustos
Gustavo Cardelle
Rodrigo Chávez
Alejandro Gómez
Javier Medina
Gustavo Martín Moglie
Pablo Pagani
Gerardo Pedraza
Ezequiel Sánchez



Impreso en Sevagraf S.A. Impreso en Argentina.

Técnico en redes y seguridad / coordinado por Paula Budris. - 1a ed. - Buenos Aires: Fox Andina, 2013
576 p. ; 28 x 20 cm. (Users; 22)

ISBN 978-987-1857-78-4

1. Informática. 2. Redes. I. Budris, Paula, coord.
CDD 004.68

En esta clase veremos...

Características y ventajas de la administración remota. Analizaremos qué aplicaciones utilizar, la forma de realizar su instalación y los primeros pasos en su uso.

En la clase anterior vimos en detalle la manera en que se administra un sistema Linux. Conocimos los comandos de consola básicos y las tareas de Linux Hardening. También realizamos diagnósticos de red y procesos a través de una consola de comandos, y detallamos la seguridad a nivel de kernel. Luego conocimos los sistemas de verificación de integridad y nos protegimos contra rootkits, estudiamos el malware en Linux y dimos consejos sobre la seguridad. En esta entrega nos dedicaremos a las tareas de administración remota. Revisaremos las opciones de software que pueden ayudarnos, detallaremos los usos de la administración remota, y aprenderemos a instalar un cliente y servidor UltraVNC. Veremos las ventajas de TeamViewer y lo pondremos en marcha, conoceremos algunas aplicaciones similares y nos adentraremos en la tecnología SSH, plataforma Citrix e Intel vPro.

17

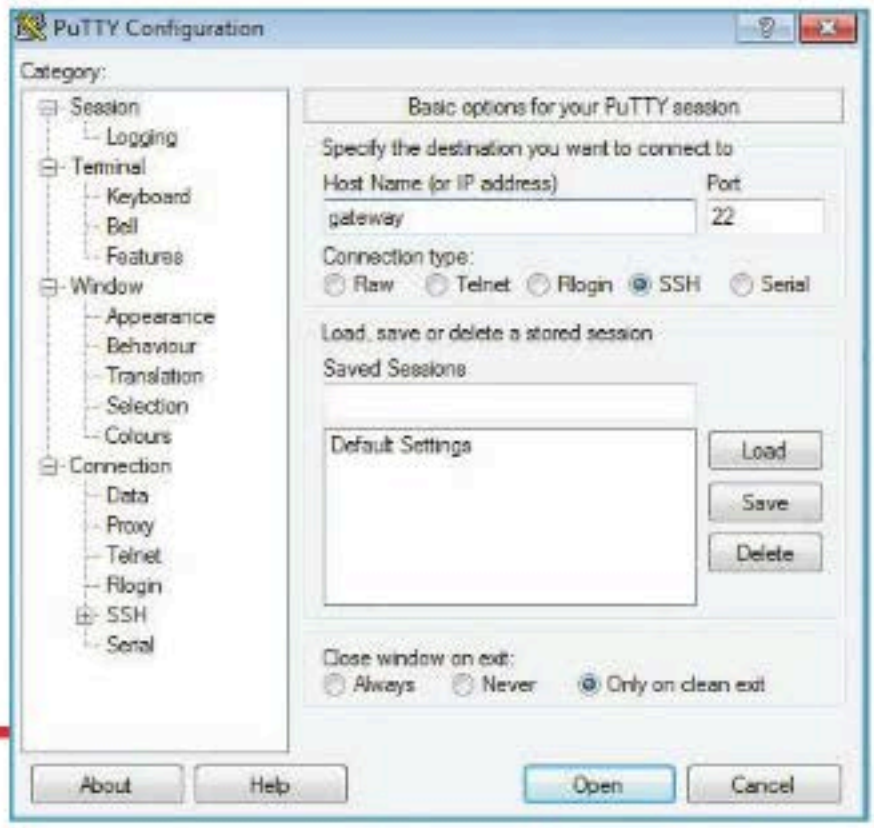
Introducción a la administración remota

La administración remota ha mejorado la forma de gestionar los sistemas y tuvo una gran evolución desde sus comienzos hasta la actualidad.

Cuando hablamos de administración remota, normalmente nos referimos a cualquier método que permita controlar una computadora o sistema desde una ubicación distinta de aquella donde esta se encuentra. Para realizar esta acción, se necesita un software que realice las tareas a nivel tanto del sistema operativo como de la comunicación. Como podemos ver en casi cualquier entorno informático, oficina y red existente, hoy en día, la administración remota se está volviendo cada vez más habitual, dado que las velocidades de las redes, tanto de las locales como de las conexiones a Internet, son cada vez mayores y más confiables. Esto permite transferir más y más datos conforme avanzan las tecnologías de conexión de los proveedores de servicios de Internet (**ISP**), los **carriers** (grandes conexiones de datos, normalmente, internacionales) y, en el caso de las redes locales, la calidad del cableado y las tecnologías inalámbricas (**Wi-Fi**, **3G**, **EDGE**, **WiMax**, etc.). De esta manera, se llega al uso remoto de un sistema por cuestiones ya sea de dificultad de acceso físico, comodidad o emergencias.

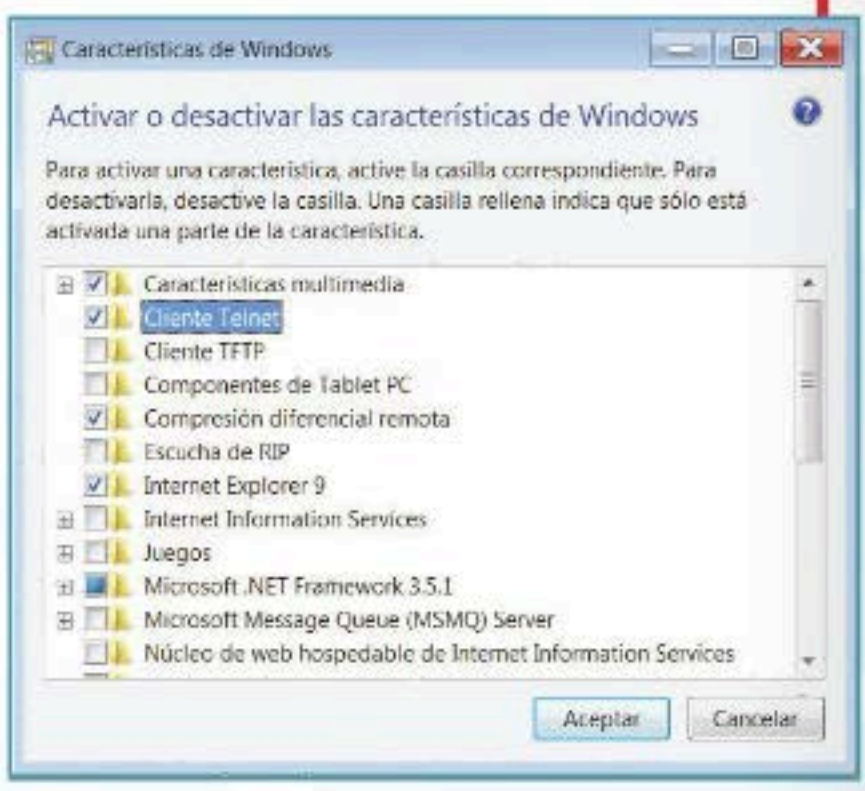
Cliente/servidor

La administración remota se basa en la existencia de un **modelo cliente/servidor**, donde una de las dos partes suele ser la que dirige las acciones, y la otra, la que las realiza a medida que se van solicitando. El equipo desde donde se establece la conexión contará con el software cliente, en tanto que el punto remoto por conectarse tendrá un software de servidor, que interpretará las órdenes del cliente y las ejecutará en el entorno local. A fin de poder conectarse de modo remoto a un equipo para administrarlo, es necesario, como mínimo, que ambos extremos tengan conectividad, es decir, que estén en redes que, aunque se encuentren distanciadas y separadas, puedan estar física



El software **Putty** ofrece la posibilidad de establecer conexiones remotas utilizando distintos protocolos.

Debido a sus limitaciones de seguridad, el cliente de **Telnet** de Windows 7 ha sido deshabilitado por defecto, y debe habilitarse explícitamente.



o virtualmente unidas por el camino de datos. Para esto se requiere, por supuesto, de un protocolo, que en general es **TCP/IP**, por lo que suele ser necesario conocer las direcciones **IP** de los extremos y realizar dicha conexión en el mismo puerto **TCP** o **UDP**. También se cuenta, en general, con un protocolo específico además del antes mencionado, de forma que el servidor y el cliente puedan hablarse en un lenguaje más determinado. En caso de que sea imposible conocer las direcciones de los extremos, pueden tomarse medidas alternativas, como el uso de un protocolo de resolución dinámica de nombres, como **DNS**, que permita saber en distintos momentos dónde se encuentra (qué dirección posee) el extremo en el que se desea realizar la conexión.

LA ADMINISTRACIÓN REMOTA ES MÁS COMÚN, DADA LA MAYOR VELOCIDAD DE LAS REDES.

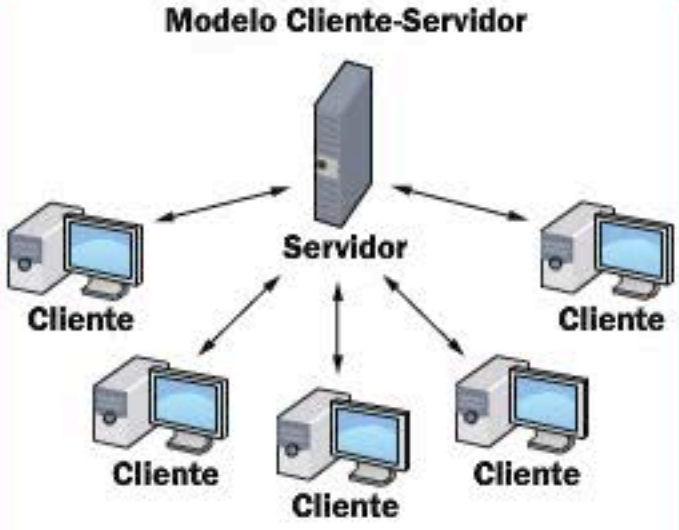
Conexiones remotas

Las conexiones a sistemas remotos suelen implementarse para cumplir con tareas de administración general o bien para tomar acciones puntuales sobre los sistemas, como reinicio o apagado, acceso a periféricos, instalación de programas, monitoreo, y otras. Más adelante ampliaremos los usos puntuales de la administración remota. En sistemas Windows, la conexión remota está provista naturalmente por los servicios llamados **Remote Desktop Services** (conocidos como **Terminal Services**) haciendo uso del protocolo **Remote Desktop Protocol** (**RDP**). También es común el uso del sistema VNC para la conexión remota, o bien de programas específicos que cuentan con funciones especialmente diseñadas para la gestión de sistemas. Algunos de los ejemplos que veremos más adelante son: **TeamViewer**, **RealVNC**, **TightVNC**, **Radmin** y **LogMeIn**. Por su parte, los sistemas tipo **UNIX**, **Linux** y **BSD** suelen administrarse remotamente utilizando alguna herramienta que funcione bajo el protocolo **SSH**, que brinda conexión segura y capacidades de acceso a la línea de comandos de manera directa, lo cual es más natural en los entornos mencionados. De todos modos, hoy en día es habitual utilizar también protocolos que provean directamente de una conexión gráfica a escritorios remotos de usuarios, que se encuentren con estos entornos.

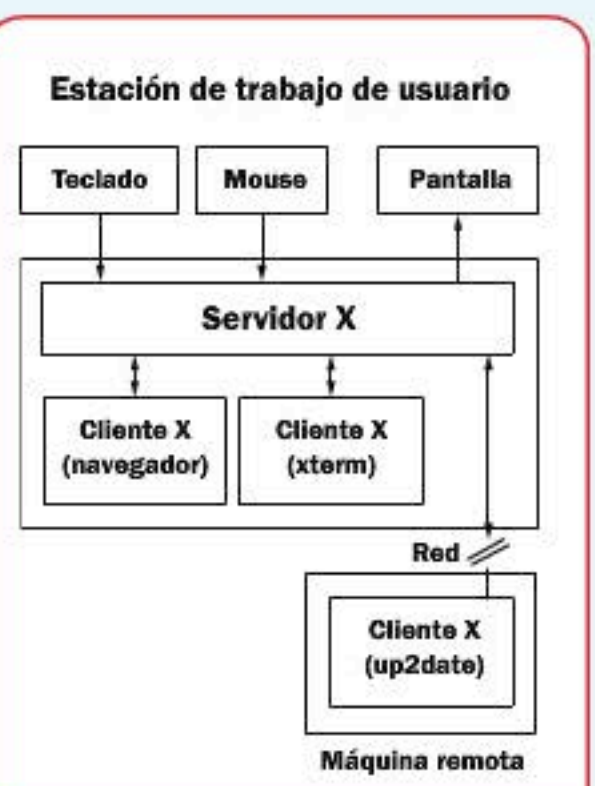
En sistemas tanto **UNIX** como **Windows**, quizá la primera forma de administración remota por línea de comandos fue el clásico protocolo **Telnet** (desarrollado en el año 1969), llamado así por ser el acrónimo de **TELecommunication NETwork**. En ese caso, mediante el puerto **23/TCP** y definido en el **RFC 854**, se permitía acceder a consolas de cualquier sistema que lo soportara, incluyendo dispositivos de red y otros equipos administrables. Si bien este protocolo ha caído completamente en desuso, todavía se lo usa para acceder a sistemas de **BBS**, a los que, en un principio, solo podía accederse a través de un módem con línea telefónica (se requiere un cliente que soporte gráficos **ANSI** y protocolos de transferencia de archivos). Entre los protocolos de transferencia, el que más se usa es **ZModem**. Telnet ha dejado de utilizarse, principalmente, debido a sus limitaciones de seguridad, como el hecho de que no cifra ninguno de los datos que envía (incluyendo contraseñas), con lo cual puede ser **sniffeado**; y que no cuenta con un esquema de autenticación para garantizar que ambas partes son quienes dicen ser. De hecho, los especialistas del **SANS Institute** recomiendan que deje de usarse por completo.

SSH y RFB

El desarrollo de SSH en 1995 reemplazó la funcionalidad de Telnet al agregar cifrado para evitar la intercepción de mensajes y proveer un esquema de autenticación adecuado. Por último, otro protocolo desarrollado principalmente para la administración remota es **RFB** (*Remote Frame Buffer*). Está orientado a interfaces gráficas, y puede utilizarse en distintos tipos de sistemas operativos debido a que trabaja en un nivel de **frame buffer** (que implica la representación de cada píxel de la pantalla de un sistema como ubicaciones en memoria), por lo que admite conexiones a sistemas **X11** típicas de UNIX/Linux, y también, de **Windows** y **Mac**. La implementación más popular de RFB es el llamado **Virtual Network Computing** (**VNC**) y sus derivados. ■



Como muchas otras aplicaciones informáticas, la administración remota se basa en el modelo cliente/servidor.



El **sistema X (X11)** cuenta con una arquitectura para llevar los píxeles a una ubicación remota.

Usos de la administración remota

Si bien en general la administración remota cubre necesidades de gestión de sistemas, en algunos casos admite otros usos alternativos.

La seguridad y la funcionalidad nunca han ido de la mano. En los comienzos de la tecnología, siempre se ha priorizado esta última frente a la primera, pero con el tiempo, el panorama ha cambiado.
El caso de la administración no escapa a este modelo, por lo cual sus usos también fueron atravesando etapas de madurez a medida que la tecnología avanzó.
Aunque parezca demasiado obvio que deben tomarse medidas de seguridad al conectarse remotamente a un sistema, los primeros programas solían ser bastante simples en cuanto al uso de las herramientas criptográficas. Esto se debía, en gran medida, a que el hecho de cifrar y descifrar tráfico en tiempo real, más los procedimientos iniciales de intercambio de claves, hacían aparentemente más lentos dichos programas, y la misma acción de agregar información de cifrado al flujo de datos implicaba, también, una mayor necesidad de ancho de banda, para lo cual se podría haber optado por la compresión, de no haber sido por el mismo tema anterior (la disminución del rendimiento).
Los diseños se realizaban para que fueran funcionales, sin tener en cuenta en absoluto la seguridad, que quedaba relegada a la confianza de quienes los utilizaban y administraban. Para contextualizar este escenario, hay que tener en cuenta la menor potencia de tecnología que se utilizaba hace unos diez o quince años, y el ancho de banda típico con el que se contaba en ese entonces.

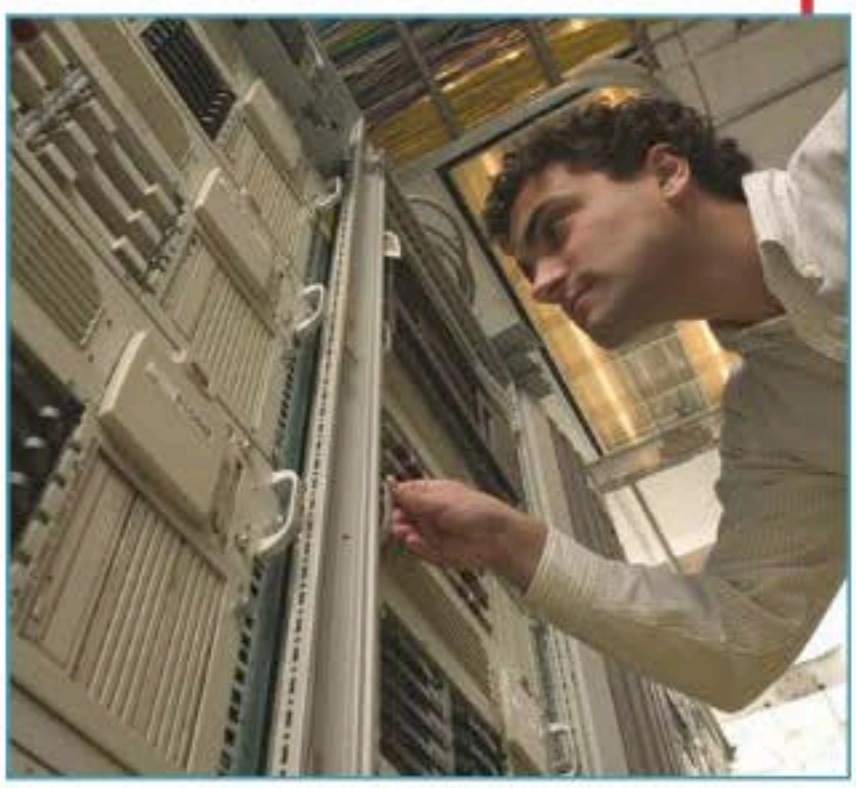
La administración remota se usa para monitorear el comportamiento de los menores en Internet.

UNO DE LOS PROBLEMAS MÁS DISCUTIDOS EN EL CAMPO DE LA ADMINISTRACIÓN REMOTA ES LA SEGURIDAD ASOCIADA.

Problemas

Uno de los problemas más discutidos en el campo de la administración remota ha sido siempre el de la seguridad asociada a ella. Esta preocupación se debe a que, lógicamente, el solo hecho de enviar los datos fuera de un equipo hace que aumente el riesgo de que esa información pueda ser interceptada, modificada o bloqueada por un intruso o atacante.
Por esta razón, los protocolos criptográficos utilizados suelen ser cuidadosamente seleccionados para esta tarea, e incluyen, por supuesto, un completo **criptosistema** que abarca el intercambio de claves públicas y certificados de autenticidad, el cifrado local utilizando claves privadas (empleando algoritmos del tipo asimétrico), el cifrado del flujo de datos por medio de algoritmos simétricos y, por último, el uso de **algoritmos de hash** para comprobación de la integridad y autenticidad de datos.
Si bien los sistemas criptográficos son diseñados para ser seguros, a esto debemos sumarle el riesgo asociado a su implementación en algún lenguaje de programación, lo cual, en general, es ciertamente más problemático que lo anterior. Es necesario considerar que aun los sistemas desarrollados para aumentar la seguridad podrían no ser suficientes.

Últimamente, el acceso a centros de cómputo se ha reducido con la administración remota.



Usos

Una vez resuelto y definido el tema de la seguridad, podemos enumerar y describir los usos que se les fueron dando a las tecnologías de conexión. Así, las acciones típicas que pueden tomarse al realizar conexiones a sistemas remotos son:

- Administración general.
- Apagado o reinicio.
- Acceso a los periféricos, como impresoras.
- Acceso a servicios de streaming o circuitos cerrados de televisión (**CCTV**).
- Configuración del Registro (de sistemas Microsoft Windows).
- Inicio, reinicio o detención de servicios.
- Instalación de software o cambio de configuraciones existentes.
- Visualización y monitoreo de acciones del usuario.

Considerando estas acciones tipicamente posibles, algunos de los escenarios donde suele aplicarse la administración remota son, por ejemplo, lo que mencionamos a continuación:

- Crear una conexión a la computadora propia desde la de la oficina donde se trabaja a diario; esto permite acceder a archivos y aplicaciones entre computadoras.
- Establecer una conexión a la computadora propia desde una ubicación donde se encuentre filtrado algún tipo de tráfico (podría ser un caso particular del ejemplo anterior).
- Realizar una conexión a un servidor ubicado en el centro de cómputos (también conocido como **data center**) desde la oficina donde se encuentra el equipo del administrador.
- Efectuar una conexión de un grupo de personas de soporte técnico a las computadoras de los usuarios distribuidos en distintos lugares del propio edificio y de otros alejados.
- Realizar una conexión de una computadora a otra dentro del mismo hogar para que los padres puedan supervisar el uso de Internet y aplicaciones por parte de los niños.
- Conectarse a la computadora propia desde una ubicación cualquiera de un enlace público a Internet (por ejemplo, una red inalámbrica en un bar o espacio público) para acceder a información, archivos o aplicaciones propias.
- Proceder a conectarse desde un **smartphone** u otro dispositivo móvil a un equipo remoto con mayor capacidad y funcionalidades para correr determinada aplicación.
- Establecer conexiones entre equipos informáticos para fines didácticos, con el objetivo de analizar la implementación de los diversos protocolos de comunicación.
- Realizar conexiones al equipo de un amigo o familiar para ayudarlo a resolver problemas con la computadora que no estén asociados a la conectividad.

Estos y otros escenarios típicos son los que suelen encontrarse cuando media una conexión de acceso remoto con fines que no sean ilegales. En caso de que la conexión no esté aprobada por el usuario y él no tenga conocimiento de que se está realizando, estaríamos hablando de un acto de **hacking**, que debió requerir previamente la búsqueda y explotación de una vulnerabilidad en el sistema remoto (por medio de la ejecución de un **exploit**) o bien la instalación de algún tipo de software malicioso (**malware**) que permita tener control sin que el usuario lo note. En esos casos, hablamos de **troyanización** de sistemas, y esto es parte de lo que se denomina seguridad ofensiva, que no busca proteger sino atacar un sistema. Los usos de este método suelen estar asociados a fines completamente maliciosos y, en algunos casos, hasta delictivos, aunque hay también excepciones que incluyen las tareas de investigación policial y otros objetivos que, aunque discutidos, son éticamente aceptables. ■

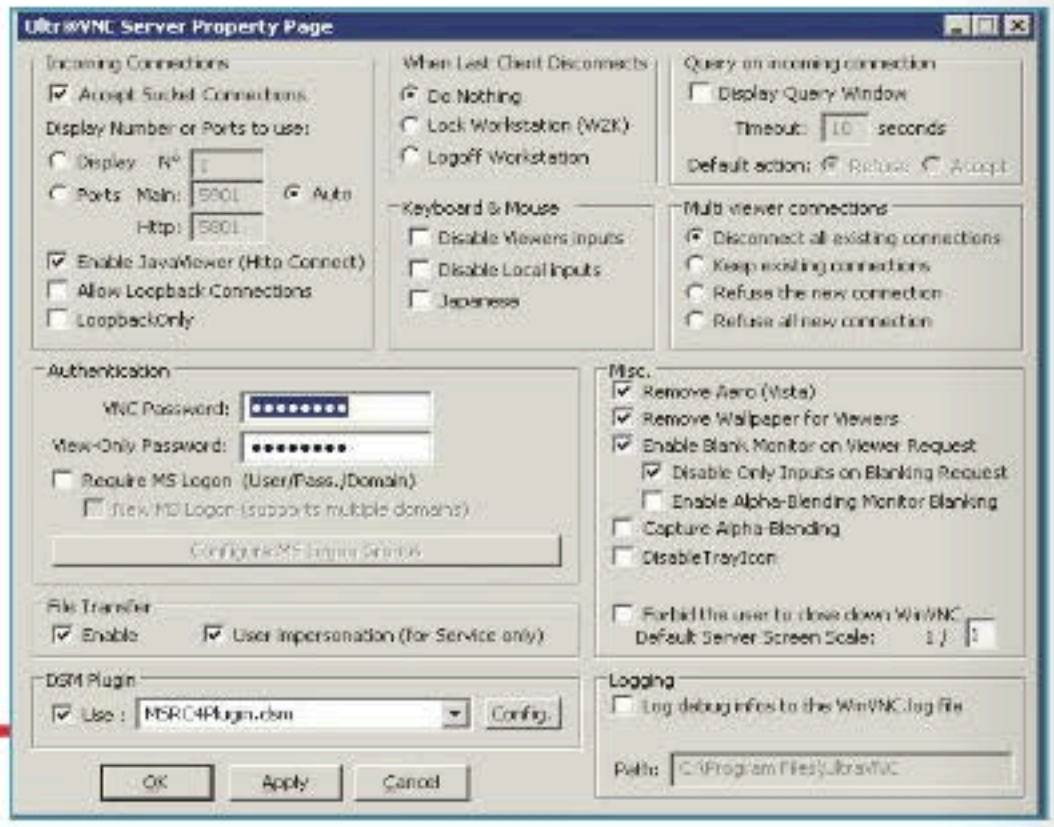
Administración remota y menores

Uno de los usos que han crecido recientemente en cuanto a la administración remota de sistemas es el monitoreo, por parte de los padres, de las computadoras que usan los niños. Esto, lejos de ser una actividad de espionaje o de abuso a la privacidad, es una de las medidas más recomendables para garantizar que las acciones de los menores de edad en Internet queden dentro de cierto margen, y se mantengan aisladas de los peligros principales que se presentan hoy en día, como el grooming.

Plataformas VNC

El sistema de conexión remota VNC es uno de los más conocidos y utilizados por su simplicidad, y son varios los programas que lo implementan.

Para comenzar, debemos decir que **VNC** es la sigla en inglés de **Virtual Network Computing** (computación virtual en red), y representa hoy en día cualquier software de administración remota basado en dicha arquitectura, independiente del sistema operativo. La versión original fue desarrollada principalmente en el **Olivetti Research Laboratory**, en Cambridge (Reino Unido). **ORL** pertenecía en un principio a **Olivetti** y **Oracle Corporation**, pero en el año 1999, **AT&T** adquirió el laboratorio de investigaciones y lo cerró en 2002. Los principales desarrolladores de VNC en AT&T fueron **Tristan Richardson** (su creador), **Andy Harter** (director del proyecto), **James Weatherall** y **Quentin Stafford-Fraser**. Al cerrarse ORL, algunos de los que habían participado en el proyecto crearon **RealVNC**, de manera de continuar trabajando en su desarrollo y poder comercializarlo.



La ventana del visor de **UltraVNC** permite configurar rápidamente las opciones requeridas para establecer la conexión con otro equipo.

Código abierto

VNC comenzó siendo de código abierto, por lo que hoy existen implementaciones derivadas con licencia **GNU**. Hubo, además, otras versiones desarrolladas a partir del código original, que no provocaron inconvenientes de compatibilidad debido a las características del **RFB** y al hecho de que, entre cliente y servidor de VNC, se realiza un saludo inicial (**handshake**) para garantizar que se usarán las opciones más adecuadas soportadas por ambas partes.

Variantes

Existen muchas variantes de VNC, que además de sus funciones básicas, cuentan con características particulares, como la optimización para el sistema operativo o la transferencia de archivos (no nativa de VNC). Algunos, incluso, mantienen la compatibilidad con el sistema original, salvo por las funciones adicionales. Tal como se espera en los sistemas modernos de administración remota, es posible conectar varios clientes a un mismo servidor en simultáneo. El nombre de VNC tiene su origen en un **thin client** llamado **Videotile**, que así como lo hace VNC, utilizaba también el sistema **RFB** (**Remote Frame Buffer**), en ese momento desarrollado en el mismo laboratorio, y que constaba de una pantalla **LCD** con conexión por red **ATM**. VNC representaba al cliente **Videotile**

VNC en GNU/Linux

Para los fanáticos de plataformas del tipo **GNU/Linux** y derivados, los programas de servidor y cliente de VNC están disponibles en muchas de las principales distribuciones en su versión estable y en el formato propio del paquete para la distribución en cuestión, como **Red Hat** y **Fedora** (paquetes RPM) o **Debian** y **Ubuntu** (paquetes DPKG). Nunca está de más verificar cada tanto la existencia de nuevas versiones.

pero de manera virtual, solo en software. Su funcionamiento es muy sencillo, ya que se basa solo en un cliente que controla el servidor, un servidor que comparte su pantalla y un protocolo de comunicación (**RFB**) que utiliza sencillas órdenes gráficas y mensajes de eventos. Comúnmente emplea el puerto **5900/TCP** para su conexión de administración, aunque también admite la conexión por medio de un navegador utilizando el puerto **5800/TCP** (requiere algún tipo de **applet** de **Java** o similar) y la conexión en modo de escucha pasiva, por medio del puerto **5500/TCP**. Para evitar el consumo excesivo de ancho de banda, VNC trabaja con distintos tipos de codificación, que puede negociarse en el momento de la conexión. Por ejemplo, el envío de datos en crudo (**raw**), que manda los píxeles ordenados de izquierda a derecha (**scanline**), como en los televisores de tubo (**CRT**), y posteriormente, envía las modificaciones respecto de dicha pantalla y la ubicación de las ventanas.
En muchos casos, esta forma de codificar es muy eficiente; por ejemplo, cuando los cambios que se producen son progresivos y no muy numerosos, como el movimiento del puntero del mouse o la escritura de texto por teclado. En otros, no lo es tanto, como cuando se realizan muchos movimientos de ventanas o se transmite video.

una clave mayor, los sobrantes se quitan y se utiliza la cadena que ha sido recortada como contraseña. No obstante, para mayor seguridad, es conveniente tunelizar VNC a través de una conexión por **SSH** o, directamente, dentro de una **VPN**.
Para el caso particular de **UltraVNC**, este posee soporte de cifrado de sesión por medio de un **plugin** de código abierto, que incluye autenticación y transferencia de datos de forma segura y que, además, permite realizar la autenticación tomando cuentas de usuarios de **NTLM** y sistemas con **Active Directory**. El problema con este **plugin** es que pierde su compatibilidad con otras implementaciones de VNC. La gente de **Workspot** ha provisto parches para VNC que incorporan cifrado por medio del algoritmo criptográfico **AES**, el más robusto algoritmo simétrico en la actualidad.

Limitaciones

Entre las limitaciones de VNC podemos mencionar que las **versiones 3.x** y anteriores no son compatibles con **Unicode**; por lo tanto, no se permite transferir texto del Portapapeles si no es mediante el uso del juego de caracteres **Latin-1**. El hecho de que VNC esté basado en píxeles le da una gran flexibilidad, pero es menos eficiente que otros sistemas que incluyen compresión (como **X11** y **RDP**).

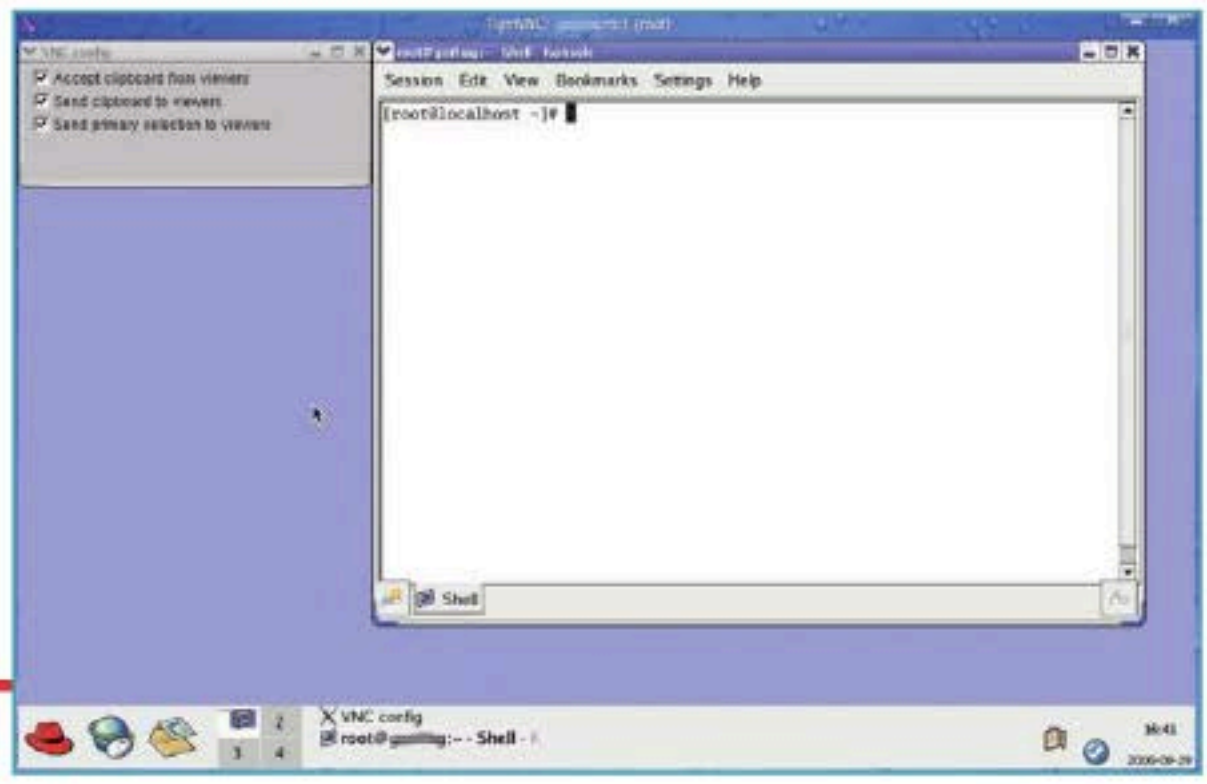
Demostración de funcionamiento del **VNC** original de AT&T sobre una Macintosh, en el año 1998.

Es importante destacar que con VNC no es necesario tener una pantalla físicamente conectada al equipo, basta con una conexión de red y una correcta configuración. Lo que el usuario está visualizando en el equipo servidor no necesariamente es lo mismo que lo que se muestra al cliente por medio de la conexión de VNC, ya que especialmente en sistemas GNU/Linux con soporte para múltiples sesiones, puede dirigirse el flujo de datos hacia otra sesión corriendo a la vez. En sistemas Windows, la sesión proporcionada es siempre la del usuario actual. ■

VNC ES UNA OPCIÓN FLEXIBLE PARA REALIZAR CONEXIONES REMOTAS QUE NO REQUIEREN UN ALTO NIVEL DE SEGURIDAD.

Seguridad

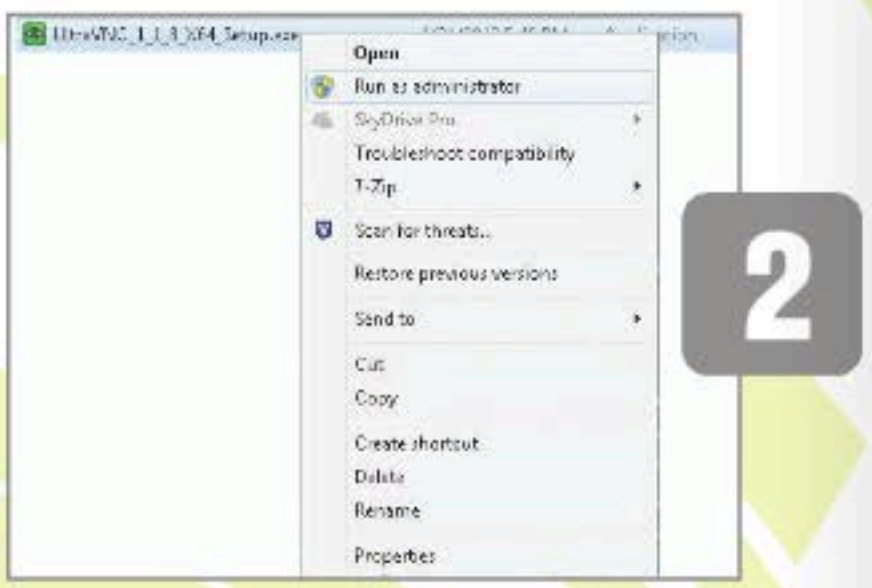
En cuanto a la seguridad, no puede decirse técnicamente que VNC es un protocolo seguro, al menos por defecto, ya que, por ejemplo, las claves se transmiten en texto plano, de la misma forma que lo hace Telnet. En algunas versiones, incluso, se presenta una limitación de 8 caracteres para la clave, de modo que si se manda



Aquí vemos una sesión de trabajo iniciada mediante el uso de TightVNC.

Instalación de un cliente y servidor UltraVNC

Examinamos en detalle la famosa suite UltraVNC para control remoto de equipos Windows y analizamos su instalación y configuración inicial.

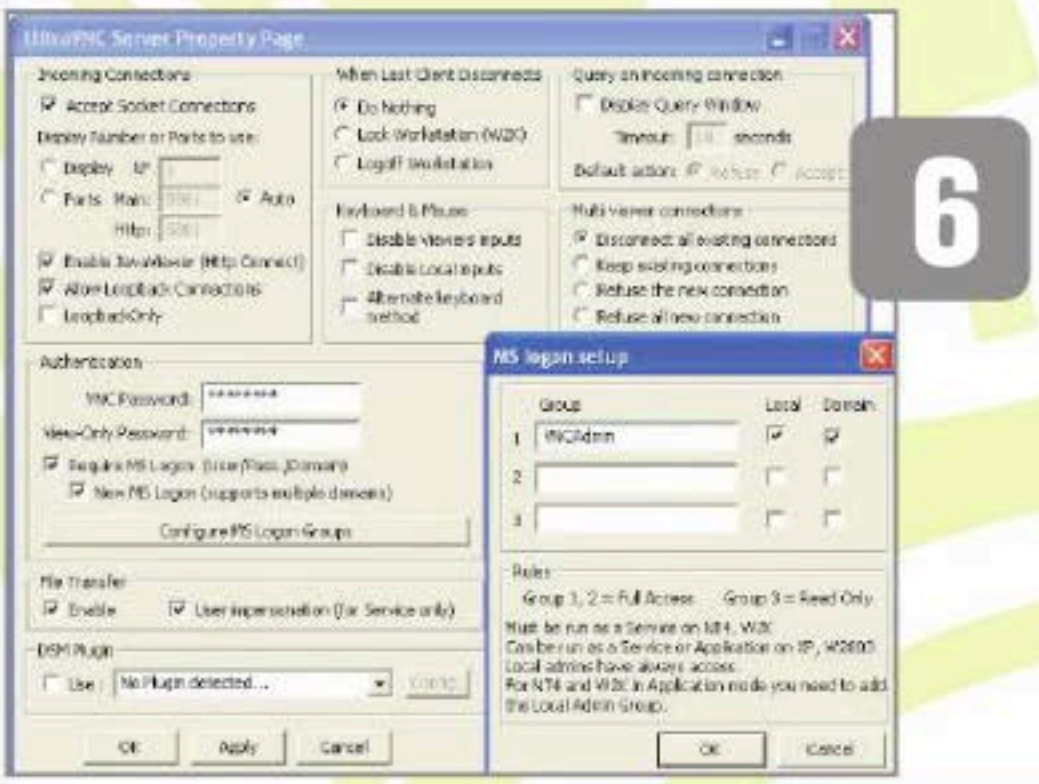


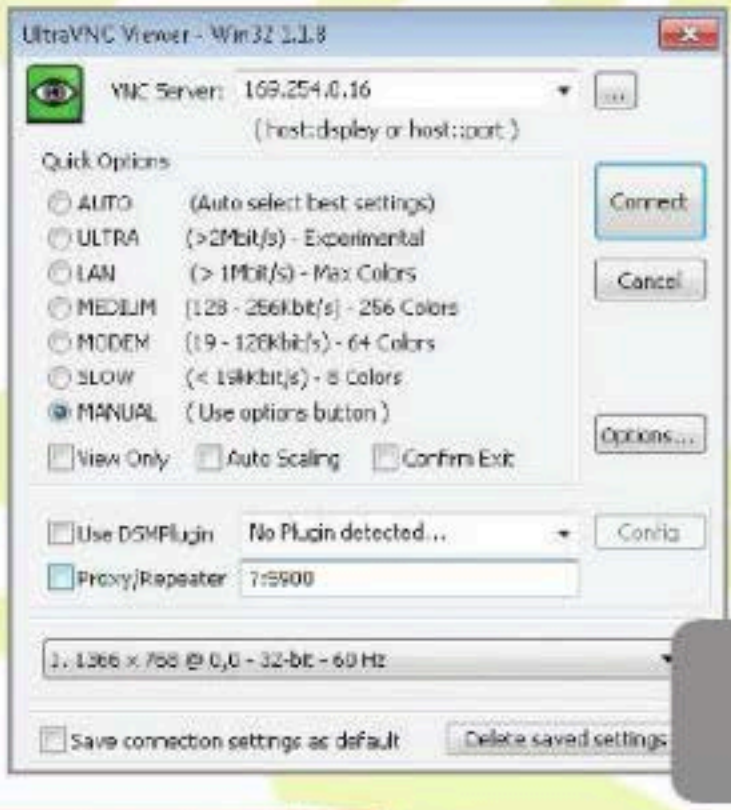
1 Vamos a descargar la última versión disponible para nuestro sistema, desde **www.uvnc.com/downloads**. Debemos verificar la versión de Windows que tengamos y la arquitectura (x86 o x64). También es posible descargar un paquete con los idiomas: francés, catalán, alemán, japonés, portugués, ruso y español.

2 Una vez descargado, ejecutamos el instalador. Es recomendable hacerlo como administrador, para lo cual utilizamos el botón derecho del mouse al seleccionar dicha opción. Este no cuenta con idioma español, solo con inglés, alemán y francés. Aceptamos el acuerdo de licencia GPL.

3 Luego de ver las mejoras de la versión que instalamos, seleccionamos la ruta de instalación y, a continuación, **Server** y **Client**. La opción **Silent** permite que el server se ejecute en modo oculto, en tanto que **Upgrade** se utiliza para actualizar una versión actualmente instalada.

4 Para conectarnos al equipo remoto apenas inicia aunque no esté logueado, activamos la opción **Register as a System Service**. La segunda opción inicia el servicio al finalizar la instalación. Recomendamos marcar la opción para asociar los archivos **.VNC**.





5 Descargamos el paquete de idiomas, que consiste en un archivo comprimido con 1 DLL por cada uno. Para instalar el español, copiamos el archivo **spanish.dll** a la ruta de instalación y lo renombramos. Para el servidor, renombramos a **vnclang_server.dll**, y para el cliente, a **vnclang.dll**. Se nos solicita reiniciar.

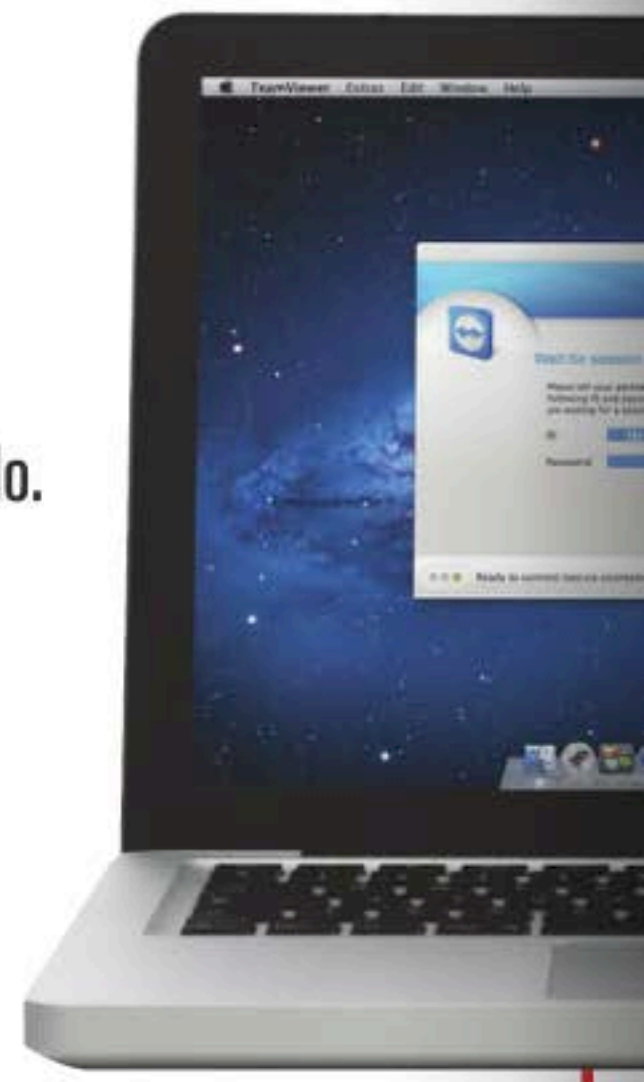
6 Desde el icono del **Server** seleccionamos la opción **Administrar propiedades** y configuramos la seguridad del servicio. Es necesario definir una contraseña de conexión robusta para evitar la conexión de usuarios no autorizados. También es posible activar el login empleando credenciales de Windows.

7 Para conectarnos al servidor abrimos **UltraVNCViewer**. Debemos introducir la **IP remota** y oprimir **Connect**. Es posible modificar las opciones gráficas para mejorar la respuesta en redes lentas. Además, podemos conectarnos con un navegador web utilizando el puerto **5800**.

8 Los antivirus suelen bloquear UltraVNC por considerarlo peligroso, ya que puede utilizarse para visualizar sin ser detectado. Si esto ocurre, veremos un error de instalación con el ejecutable **winvnc.exe**. Además, al instalar el idioma español, varios de los textos se superponen con otros.

TeamViewer

Veremos todo sobre el software multiplataforma para soporte remoto y reuniones online más utilizado. Sus ventajas, desventajas y características.



TeamViewer permite controlar a distancia cualquier computadora Windows, Mac o Linux; incluso, desde teléfonos o tablets iOS y Android. Se fundó en 2005, y sus oficinas centrales están ubicadas en Alemania. Posee subsidiarias en Australia y los Estados Unidos. Se dedica exclusivamente al desarrollo y la venta de software para colaboración basada en la Web.
En un corto período de tiempo, ha conseguido un rápido desarrollo y aceptación, con más de cien millones de instalaciones del software en más de 200 países alrededor del mundo.
El software está disponible en más de 30 idiomas, lo que le entrega una mayor flexibilidad y nos permite disponer de él en el idioma que necesitemos.

El acceso remoto y el control de equipos con sistemas Windows es sencillo gracias al uso de TeamViewer.

Características principales

TeamViewer es una aplicación intuitiva, rápida y segura para el control remoto y realización de reuniones. Como una solución todo en uno, puede utilizarse para:

- Proporcionar soporte remoto a colegas, amigos o clientes.
- Administrar servidores y estaciones de trabajo Windows. Es posible ejecutar TeamViewer como servicio del sistema de Windows y acceder al equipo, incluso, antes de iniciar sesión en Windows.
- Conectarse a equipos para brindar soporte técnico sin necesidad de realizar instalaciones en el cliente (por medio de la funcionalidad QuickSupport).
- Conectarse a otras plataformas, como Mac OS X y Linux.
- Realizar conexiones desde dispositivos iOS o Android a computadoras Windows, Mac o Linux.

TeamViewer admite la conexión remota a equipos con OS X, para administrarlos desde otro lugar.

- Compartir el escritorio para reuniones, presentaciones o trabajo en equipo.
- Conectarse a una computadora en nuestra casa en forma remota, y trabajar en documentos, revisar el correo electrónico o descargar imágenes y editarlas en forma sencilla y rápida.
- TeamViewer trabaja por detrás de firewalls, routers NAT y proxies sin necesidad de configuración, las cuales son las restricciones típicas que encontramos en las empresas.

Control a distancia

Es posible controlar equipos en forma remota a través de Internet, como si estuviésemos en frente de ellos. Para hacerlo, necesitamos conocer la dirección IP pública o bien utilizar algún sistema, como No-IP, para conseguir un registro DNS dinámico que nos permita conectarnos fácilmente cuando la IP brindada por el ISP cambie. También es posible guardar en el cliente el listado de equipos, para facilitar la conexión.

TeamViewer Management Console

TeamViewer Management Console es una nueva funcionalidad que ofrece una plataforma basada en la Web para administración de usuarios, reporting, y administración de computadoras y contactos. Esta consola es exclusiva para las licencias Premium y Corporate, por lo que su uso no es gratuito. Se trata de un servicio cloud hosteado en un data center propio de TeamViewer, que posee las certificaciones de seguridad ISO-27001 y HIPPA. Todo el tráfico es transmitido usando SSL (Secure Sockets Layer). Los datos se almacenan por medio de encriptación AES/RSA 2048 Bit. Para autorización y autenticación, se usa **Secure Remote Password Protocol** (SRP).

Módulo cliente

Con el módulo cliente, **TeamViewer Quick Support**, es posible conectarse rápidamente sin necesidad de instalar programas adicionales. Las instalaciones permanentes (**TeamViewer hosts**) son completamente gratuitas para los dueños de licencias. Utilizando **file transfer**, se pueden copiar archivos o carpetas enteras fácilmente de un equipo a otro. También es posible utilizar la funcionalidad que nos permite tomar y mover, para una mayor simplicidad y velocidad.
TeamViewer permite utilizar la aplicación móvil para brindar soporte o conectarse a la computadora de la oficina o el hogar mientras se está en viaje. Por medio de la aplicación para iPhone, iPad o Android, es posible conectarse rápidamente y, de esa forma, administrar un equipo.

Sesión de trabajo

Al establecer una sesión, TeamViewer determina el tipo óptimo de conexión. Después de un **handshake** a través de los servidores centrales, puede establecerse una conexión directa a través de UDP o TCP (incluso, detrás de gateways, NAT y firewalls) o rutearse a través de la red de TeamViewer usando TCP o un túnel http. No es necesario abrir ningún puerto para trabajar con TeamViewer, ya que en la mayoría de los casos se usa el puerto 80.
Para conexiones espontáneas de soporte a clientes, TeamViewer Quick Support genera un password de sesión (**one-time password**) que tiene que ser informado por alguna persona que esté localmente frente al equipo.
Una vez que se reinicia el equipo, no es posible conectarse con el mismo password. Cuando se instala TeamViewer para soporte desatendido, se genera un password fijo que permite conectarse sin necesidad de intervención local.

No es posible conectarse en modo invisible; un usuario frente al equipo siempre podrá ver que estamos conectados mediante un panel que se observa sobre el **system tray**.

Cifrado

TeamViewer funciona con un cifrado basado en llaves públicas/privadas RSA y AES (256 bits) para codificación de la sesión. Este tipo de conexión puede considerarse segura mientras que la clave privada permanezca segura en el equipo cliente.
Cada cliente TeamViewer posee la clave pública del clúster principal y, por lo tanto, puede cifrar los mensajes que envía a este y verificar su firma. La PKI (*Public Key Infrastructure*) evita que haya ataques del tipo man-in-the-middle. La clave utilizada para conexión nunca es enviada en forma clara, sino encriptada, y solo es almacenada en el equipo cliente.

LOS ARCHIVOS DE PROGRAMA SE ENCUENTRAN FIRMADOS USANDO TECNOLOGÍA VERISIGN. ESTO PERMITE VERIFICAR SU ORIGEN.

Ataques

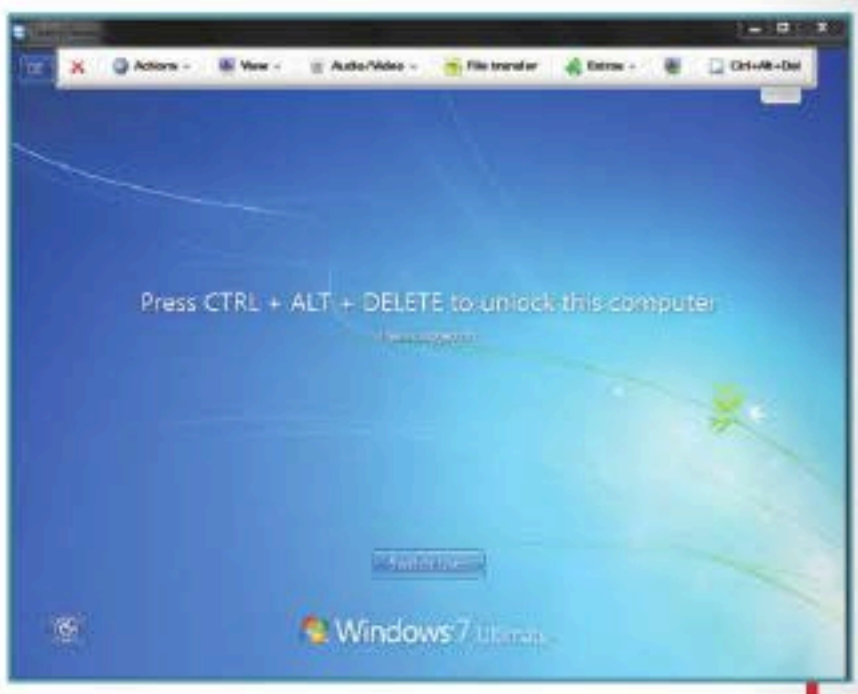
La validación de los ID se basa en varias características de hardware y software, y es generada automáticamente por TeamViewer. Los servidores de TeamViewer comprueban la validez del ID antes de cada conexión, de manera que se controlan los intentos de conexión con identidades falsas.
En el contexto de la seguridad informática, un ataque de fuerza bruta es un método de prueba y error con la intención

TeamViewer permite conectarse en forma remota a tablets con Android, para administrarlas a distancia.

de adivinar una contraseña. Con la creciente potencia de cálculo de los equipos actuales, el tiempo necesario para adivinar contraseñas se vuelve cada vez más reducido. Como defensa contra ataques de fuerza bruta, TeamViewer aumenta exponencialmente la latencia entre los intentos de conexión. Por lo general, realizar 24 intentos lleva 17 horas.

TEAMVIEWER POSEE MECANISMOS PARA PROTEGER EL EQUIPO DE LOS LLAMADOS ATAQUES DE BOTNETS.

Consideremos que la latencia solo se restablece después de que hayamos introducido la clave correcta. TeamViewer tiene un mecanismo para proteger los ataques no solo de un equipo específico, sino también de varios de ellos, conocidos como ataques de botnets, tratando de acceder a un determinado equipo de TeamViewer. También es posible generar listas blancas y negras para enumerar los equipos que pueden conectarse y los que no pueden hacerlo. Aunque TeamViewer es una excelente opción para la administracion remota, existen algunas alternativas interesantes; a continuación mencionaremos algunas de ellas. **Logmein (https://secure.logmein.com/ES)** es uno de los sistemas de acceso remoto más utilizados, ya que nos ofrece la posibilidad de acceder a nuestro equipo desde cualquier lugar, solo utilizando un navegador web. Su sitio web es accesible y fácil de usar, lo que nos entrega una mayor comodidad pues no debemos ejecutar aplicaciones o abrir puertos en el cliente. Otra de las opciones dignas de comentar es **RealVNC**, cuyo sitio web se encuentra en la dirección **www.realvnc.com**. Este programa nos ofrece una completa y funcional aplicación para controlar equipos en forma remota. También dispone de una versión gratuita que, aunque no ofrece todas las características de la versión comercial, es perfectamente utilizable para usuarios sin muchas exigencias. Por otra parte, RealVNC se compone de varias aplicaciones desarrolladas para distintos sistemas, con lo que será posible controlar la computadoras desde dispositivos tales como un iPhone o un equipo móvil con sistema Android. ■



Aquí vemos un equipo Windows de soporte conectándose a otro equipo Windows.

Seguridad en TeamViewer

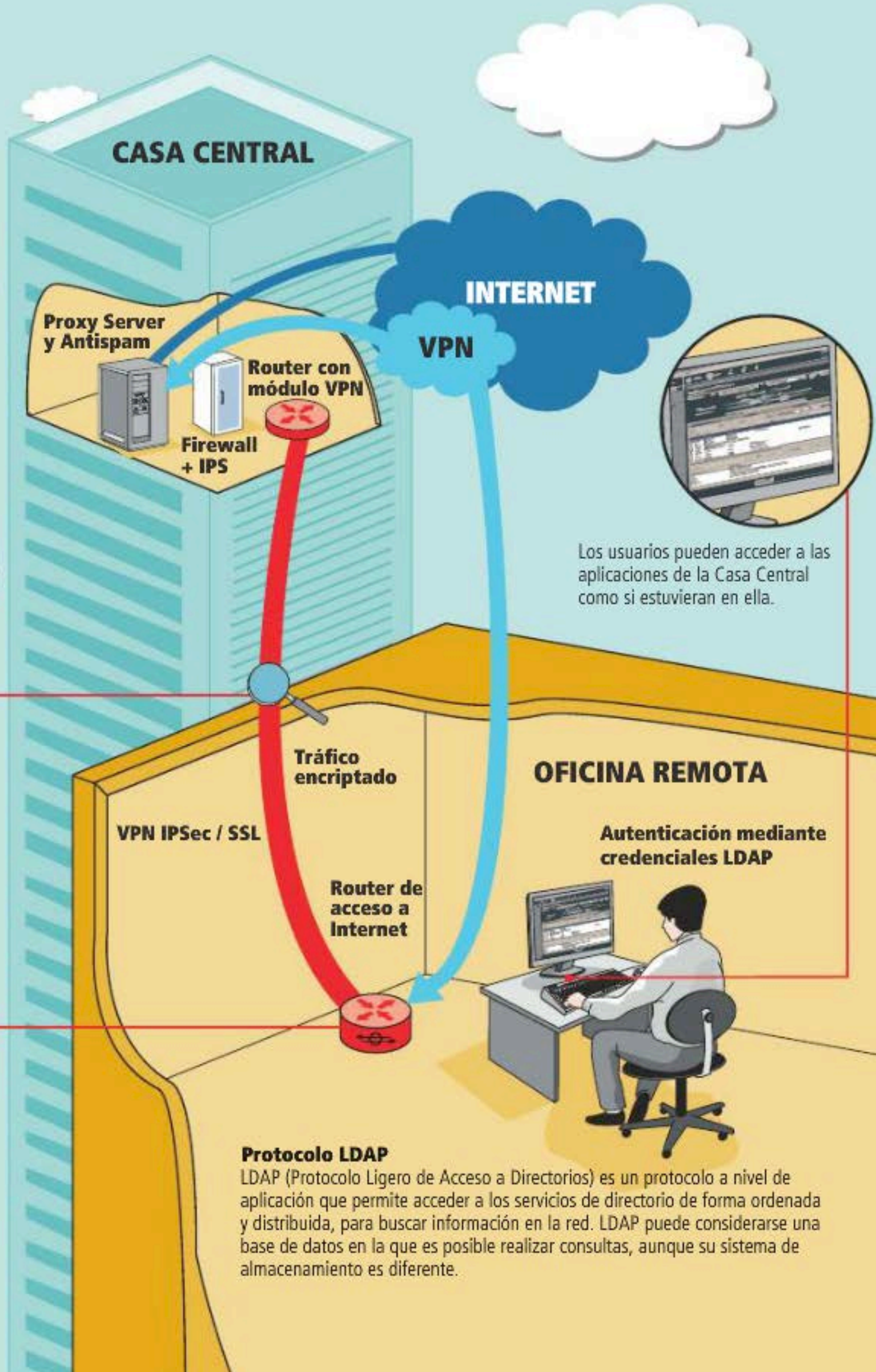
TeamViewer ofrece un nivel de seguridad muy elevado para las conexiones remotas que se realizan mediante su uso. De esta forma, encontramos que las sesiones remotas con esta aplicación están codificadas mediante infraestructura de clave pública RSA (1024-bit) y AES (256-bit). Luego de instalar TeamViewer, vemos que, en su configuración predeterminada, se utiliza uno de los servidores de TeamViewer.com para conectar el equipo local y el remoto, aunque después del protocolo inicial se establece una conexión directa a través de UDP o TCP.

La oficina remota

Los usuarios en una oficina remota pueden acceder a los recursos de la Casa Central en forma transparente, es decir, sin saber que son servicios que residen en otra locación. Incluso, la navegación por Internet se realiza desde el enlace de la Casa Central, pasando por el proxy,que verifica los permisos del usuario e implementa las políticas definidas. Los e-mails entrantes y salientes son analizados por el antispam en la Casa Central.

El Firewall y el IPS analizan el tráfico denegando lo que no está autorizado.

Si el router de la oficina remota soporta establecimiento de VPNs "site to site", los usuarios pueden acceder en forma transparente a las aplicaciones de la Casa Central. De lo contrario, desde las teminales deben establecer una VPN utilizando un cliente o mediante un sitio web.

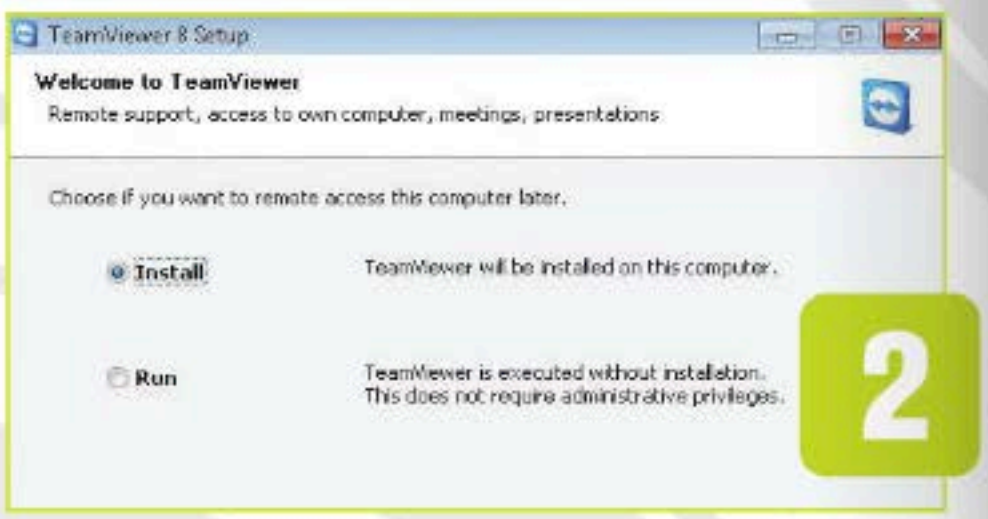


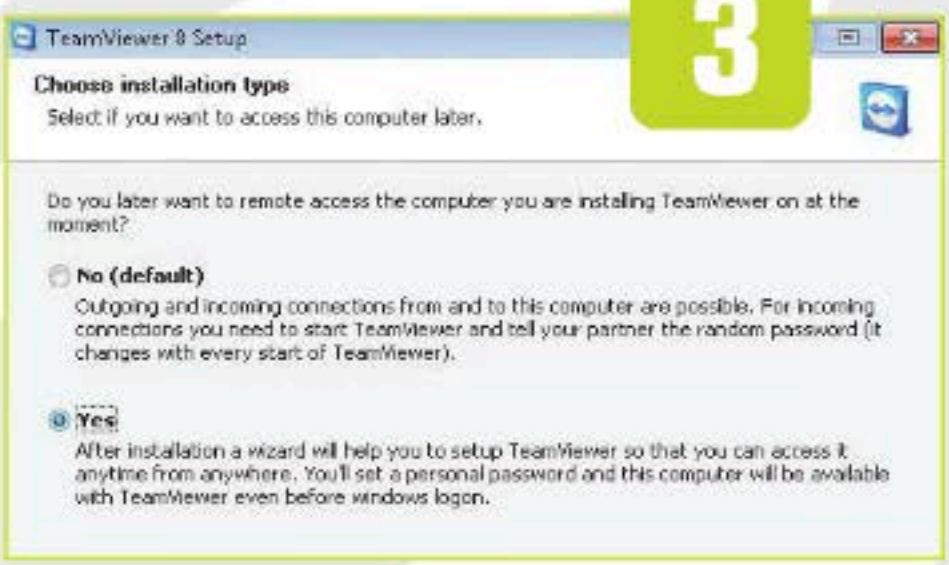
Protocolo LDAP

LDAP (Protocolo Ligero de Acceso a Directorios) es un protocolo a nivel de aplicación que permite acceder a los servicios de directorio de forma ordenada y distribuida, para buscar información en la red. LDAP puede considerarse una base de datos en la que es posible realizar consultas, aunque su sistema de almacenamiento es diferente.

Cómo poner en marcha TeamViewer

TeamViewer permite visualizar la pantalla y controlar un equipo remoto utilizando la red. Aquí veremos la manera de ponerlo en marcha.





1 Descargamos la última versión disponible de TeamViewer para nuestro sistema operativo, desde **www.teamviewer.com**. También es posible obtener una versión MSI para distribuir de forma automatizada utilizando **Políticas de grupo** (**GPO**).

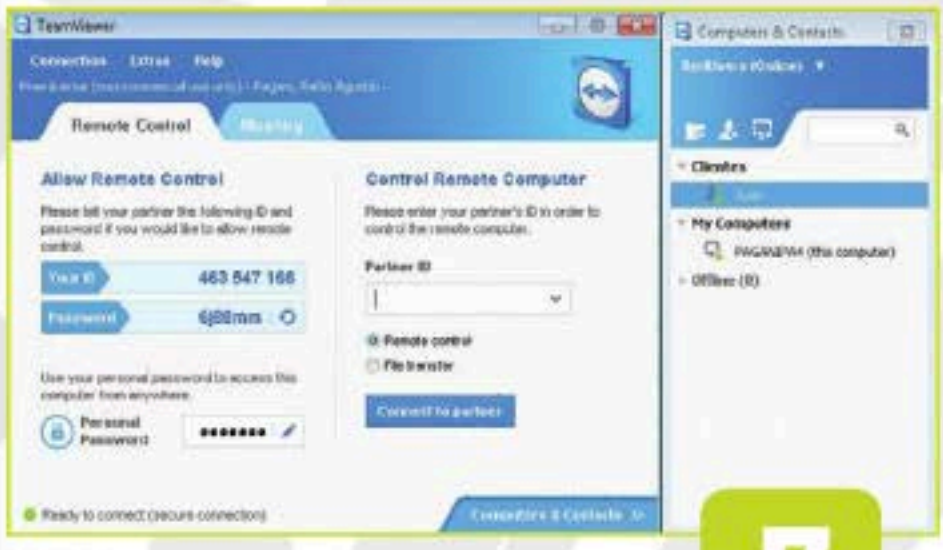
2 Una vez descargado, debemos ejecutar el instalador; es recomendable hacerlo como **Administrador**. Seleccionamos la opción **Install** para instalar el servidor. La aplicación es gratuita siempre que la usemos con un fin no comercial, por lo que indicamos que la usaremos en forma personal.

3 Para conectarnos en forma remota sin necesidad de que una persona nos indique el password aleatorio, debemos seleccionar la opción **Yes**. La opción **Default** requiere de un usuario frente al equipo. A continuación, seleccionamos **Full Access** para realizar todas las acciones.

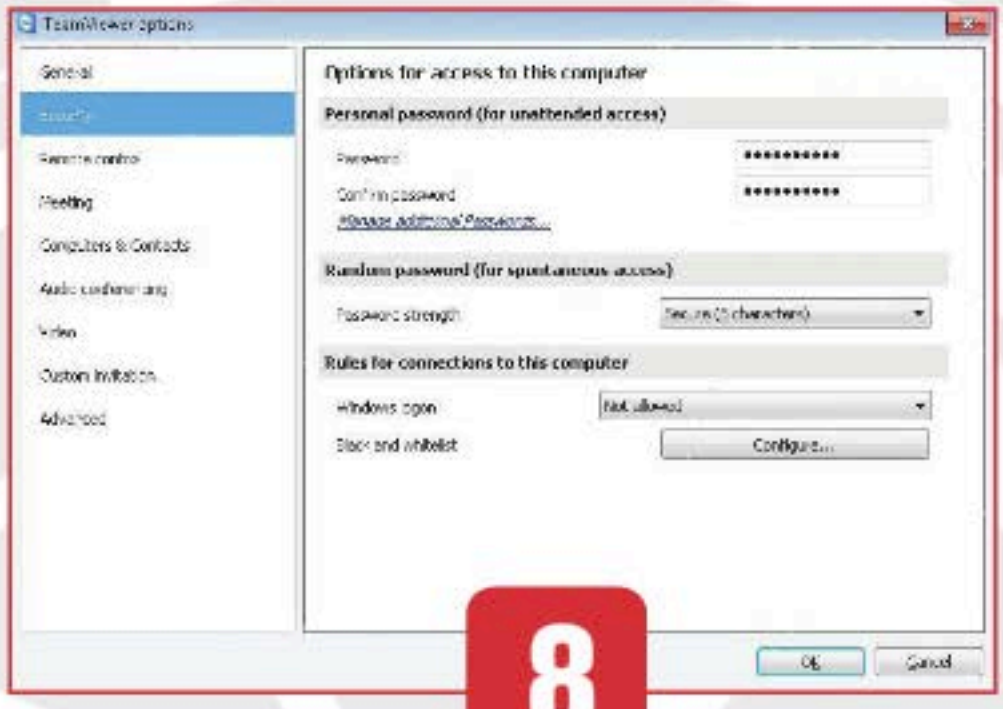
4 **Remote Print** permite imprimir en una impresora definida en el host remoto. La función TeamViewer VPN establece una conexión entre los equipos para acceder a la red. El **Meeting Add-in** para Outlook se usa para agendar reuniones incluyendo la información de conexión.

5

6



7



8

5 Una vez finalizada la instalación, se abrirá automáticamente el asistente de configuración del servidor. En esta pantalla establecemos el acceso desentendido, para lo cual ingresamos el nombre del equipo tal como se mostrará cuando vayamos a conectarnos y la contraseña requerida.

6 En esta pantalla podemos identificarnos si ya poseemos un usuario de TeamViewer, o creamos uno. Esta información permite que el equipo quede registrado en nuestra lista. De esta manera, se facilita el acceso a él desde un listado de máquinas que se mostrará en el cliente.

7 Una vez finalizada la instalación, abrimos el cliente y, luego, nos identificamos en él desde la opción **Computers & Contacts**, que nos permite llevar un registro de los equipos que administramos. Es posible, además, chatear con los contactos que definimos y que están identificados en su cliente.

8 Desde las opciones de TeamViewer es posible definir las configuraciones de seguridad para conectarse al equipo, la calidad de la imagen, las configuraciones para reuniones y enviar invitaciones a conectar. La persona que recibe la invitación debe descargar TeamViewer Quick Support.

Aplicaciones similares a TeamViewer

Existen numerosas aplicaciones que permiten controlar equipos; cada una cuenta con características particulares para distintas necesidades.

Así como TeamViewer ofrece la posibilidad de conectarse y controlar remotamente un equipo, hay otras aplicaciones que pueden realizar la misma tarea de manera similar. Cada una cuenta con características particulares. TeamViewer permite instalar el software servidor y conectarse de manera desatendida, pero también existe la posibilidad de que un usuario que precisa soporte ejecute una versión que no requiere instalación para obtener asistencia.

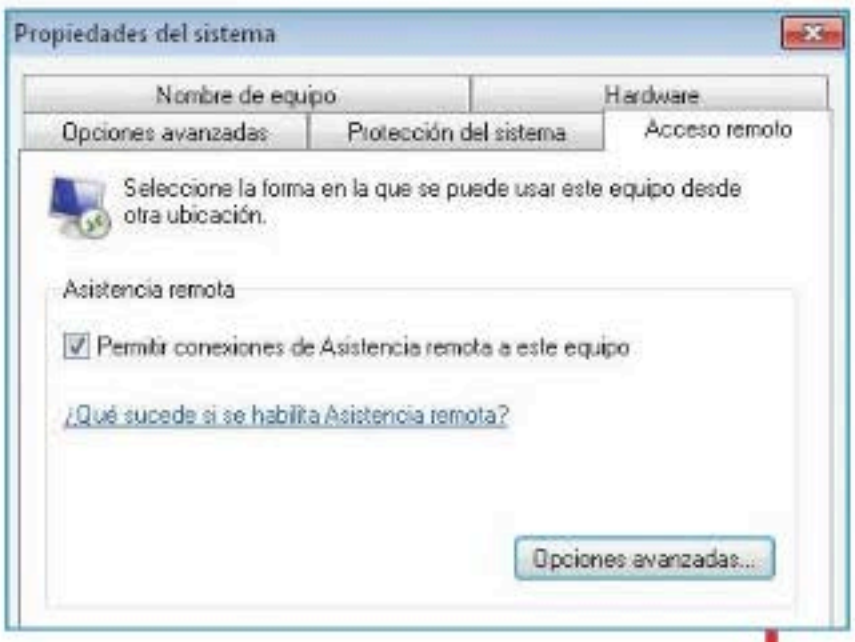
TeamViewer permite visualizar o controlar un dispositivo Android o iOS desde una computadora.

LogMeIn

LogMeIn (https://secure.logmein.com/ES) se inició como una aplicación para control remoto de equipos personales a través de Internet, pero se fue desarrollando hasta convertirse en una suite muy completa. Cuenta con las mismas funcionalidades que TeamViewer. Permite brindar soporte a usuarios utilizando la aplicación **Rescue**, que no requiere de instalación. Soporta PC, Mac y dispositivos móviles. Utilizando la consola **Central**, es posible realizar numerosas tareas administrativas, como administrar de manera centralizada y distribuir el software a los clientes, automatizar actualizaciones de Windows, monitorear los antivirus, generar una gran variedad de reportes y obtener alertas sobre el uso del procesador y la memoria, entre otras.
La versión gratuita de LogMeIn brinda la funcionalidad básica para administrar uno o más equipos a distancia. La versión **Pro** (comercial) incluye algunas funcionalidades adicionales, como transferencia de archivos, impresión remota, alta calidad de imagen, y más. La aplicación **Ignition** puede instalarse en un pen drive para controlar equipos sin necesidad de acceder mediante un navegador web. Tal como TeamViewer, LogMeIn permite controlar equipos Windows y Mac desde dispositivos iOS y Android. La aplicación **join.me** se usa para iniciar reuniones virtuales. Es posible realizar llamadas por Internet, compartir pantalla, compartir el control de la presentación, chatear y enviar archivos. Posee software que permite la visualización desde iOS y Android.

GoToMyPC

GoToMyPC (www.gotomypc.eu/remote_access/remote_access) tiene una funcionalidad similar a la de TeamViewer y LogMeIn. A diferencia de esos programas, no posee una versión gratuita y solo ofrece un período de prueba de 30 días, luego del cual es necesario adquirir un plan para poder utilizar el servicio. La versión **Inicial** permite que un único usuario se conecte a varios equipos, en tanto que la versión **Pro** permite un administrador y de dos a cincuenta usuarios conectados.
La versión **Corporate** permite tener muchos administradores y usuarios. Soporta conexiones a Windows y Mac OS X



Asistencia remota de Windows. Es posible configurar sus opciones desde **Group Policy Objects (GPO)**.

y también da la posibilidad de conectarse desde teléfonos o tablets con Android o iOS. Permite transferir archivos entre los equipos e imprimir en forma remota, así como también copiar y pegar archivos entre los equipos. Soporta múltiples monitores y transfiere el sonido de un equipo al otro.

Ammyy

La aplicación **Ammyy** (**www.ammyy.com/es**), creada en 2007, posee una funcionalidad y un aspecto muy similares a los de TeamViewer. Tiene una versión gratuita para usuarios hogareños. Tanto el cliente como el servidor no requieren instalación; solo es necesario que el usuario final informe el ID y la IP para que un administrador puede conectarse a distancia. Para brindar soporte de forma desatendida, solo se debe instalar el servicio y definir un password de conexión. También permite realizar presentaciones en forma remota.

WRA

La forma tradicional de brindar soporte remoto a usuarios utilizando equipos Windows es a través de **Windows Remote Assitance**. **WRA** permite conectar dos equipos para obtener asistencia. Posee un asistente que detecta algunos de los problemas más comunes e intenta repararlos. Si la detección o solución falla, es posible enviar una solicitud de soporte a un administrador. Este debe introducir el archivo de invitación recibido o la contraseña **EasyConnect** brindada por el usuario. Este programa ofrece una funcionalidad básica para usuarios finales, sin tener demasiados requisitos.

Otras opciones

Existen numerosas aplicaciones que implementan el protocolo VNC, como **RealVNC**, **TightVNC** y **UltraVNC**. Estas ofrecen una gran funcionalidad a un bajo costo, ya que están basadas en tecnología Open Source. RealVNC posee tres versiones: la **Free** solo permite conectarse remotamente a equipos particulares; la **Personal** posee una encriptación AES de 128 bits, permite utilizar autenticación del sistema operativo, imprimir en el equipo remoto, transferir archivos y chatear, y cuenta con servicio de soporte dedicado; la **Corporativa** añade una encriptación más robusta de 256 bits, la funcionalidad de single sign-on y una herramienta de rápido despliegue del cliente en la red. También cuenta con versiones para iOS y Android, además de Windows, UNIX, Linux y Mac OS X. **VNC Viewer Plus** permite realizar conexiones *Out of Band* (fuera de línea) en equipos con procesadores **Intel vPro**. De esta manera, es posible controlar el equipo aun cuando este se encuentre apagado o su sistema operativo no esté instalado. De esta manera, es posible ingresar en el menú de configuración BIOS o cambiar el orden de booteo de una computadora, entre otras acciones.

EXISTEN MÁS DE CIEN PRODUCTOS QUE PERMITEN COMPARTIR LA PANTALLA EN FORMA REMOTA.

Tightvnc ofrece la funcionalidad de administración remota de equipos de manera gratuita y Open Source, tanto para particulares como para empresas. Cuenta con el programa **TightProjector**, para compartir la pantalla del presentador con muchos otros equipos y dictar entrenamiento o hacer reuniones. **VNC Reflector** permite conectarse a equipos en distintas redes no visibles entre sí actuando como proxy. UltraVNC, por su parte, ofrece la herramienta denominada **Single Click**: un servidor VNC que no requiere instalación ni modificaciones en el Registro del sistema para ejecutarse. La conexión hacia el equipo de soporte es iniciada por el usuario para facilitar la salida a través de firewalls o proxy. ■

Citrix Online Software

Citrix **ha adquirido distintas empresas para formar uno de los portfolios más completos relacionados con el mercado de compartir pantallas. Posee la propiedad de las aplicaciones** GoToMyPC, GoToAssist, GoToMeeting, GoToWebinar, GoToTraining, HiDefCorporate, ShareFile **y** PODIO. **Todas ellas integran una suite de colaboración y soporte muy poderosa orientada, principalmente, a empresas. No cuenta con aplicaciones gratuitas, pero es posible descargar software de prueba por tiempo limitado. Su gran ventaja es que no es necesario instalar servidores, ya que se ejecuta desde la nube.**

Protocolos SSH y Terminal Server

Entre los protocolos más comúnmente utilizados para la administración remota, se encuentran SSH y Terminal Server, que luego fue renombrado como RDP. En estas páginas conoceremos su funcionamiento.

Algunos protocolos de conexión remota para administración de sistemas se han destacado más que otros, ya sea por su uso masificado, por su facilidad o por su potencia. Uno de ellos es el conocido **SSH** (acrónimo de **Secure Shell**), que podría traducirse como consola segura. SSH sirve, justamente, para conseguir conexiones seguras a sistemas remotos, contando con las funcionalidades de una consola local, a la vez que es el nombre del protocolo y del software que lo ha implementado. Pese a que suele usarse en línea de comandos, tiene la capacidad de redirigir el tráfico de un **servidor X** (sistema gráfico de entornos **UNIX/Linux**) para correr programas que requieran interfaz gráfica.

Puede realizar la gestión automática de **claves RSA**, de modo que no sea indispensable escribir a mano las contraseñas al realizar conexiones. SSH fue creado para reemplazar otro modo de conexión, ya que en esa época, la forma de operar acciones sobre sistemas remotos era con el uso de los llamados **comandos r** de sistemas del tipo UNIX, basados en el comando **rlogin**, de funcionamiento similar al de Telnet. Dadas las limitaciones de seguridad y las debilidades que poseía Telnet, el finlandés **TatuYlönen**, de la **Universidad Tecnológica de Helsinki**, escribió SSH en 1995 utilizando varias piezas de software libre, como GNU **libgmp**, y comenzó a distribuirlo de manera gratuita. Luego, la licencia fue

Características

SSH también permite realizar transferencia segura de archivos con el comando **SCP** (**Secury Copy**) y simular sesiones de **FTP** seguras (con el comando **SFTP**, **Secure FTP**).

La herramienta de conexión a **Escritorio Remoto** viene incluida con los sistemas Windows.

KDRDC es una implementación del protocolo **RDP** para los entornos KDE de GNU/Linux.

modificada, y al crearse la empresa **SSH Communications Security**, se comenzó a ofrecer una versión gratuita para uso doméstico y académico, y una diferente, con más opciones, para uso comercial. En 1997, SSH se propuso en **IETF** como primer borrador del estándar. En 1999 comenzó a escribirse la implementación libre por excelencia, perteneciente al sistema operativo **OpenBSD**, que sería llamada **OpenSSH**. La primera versión de SSH hizo uso de una serie de algoritmos de cifrado patentados (en la actualidad, algunas de las patentes ya expiraron), por lo que debieron ser reemplazados con posterioridad. Además, en 1998, los investigadores argentinos **Ariel Futoransky** y **Emiliano Kargieman** encontraron una grave vulnerabilidad que permitía a un posible atacante insertar datos en el flujo de la comunicación, basada en una insuficiente protección del algoritmo **CRC-32** usado hasta la **versión 1.5**. En 2001 se descubrió otra seria vulnerabilidad, que permitía modificar el último bloque de una sesión cifrada con el algoritmo **IDEA**, y casi simultáneamente, se detectó otra que permitia a un servidor malicioso redirigir la autenticación efectuada por un cliente a otro servidor.

NO ES RECOMENDABLE UTILIZAR LA VERSIÓN 1 DE SSH, YA QUE POSEE ALGUNOS PROBLEMAS DE SEGURIDAD.

Debido a esos problemas, la versión 1 de SSH es considerada completamente obsoleta en la actualidad, y debe deshabilitarse, incluso, en caso de que pueda ser usada por la implementación que se emplee de software, en favor de la versión 2 (no compatible con la anterior). El nombre para la versión 2 fue **Secsh**, y se aplicó en 2006 cuando la IETF la adoptó como estándar. En 2008 se descubrió una vulnerabilidad teórica en todas las versiones, que permitía recuperar hasta 32 bits de texto plano de un bloque de texto cifrado, pero no ha podido ser explotada hasta la fecha.

```
C:\WINDOWS\system32\cmd.exe
PsExec v1.98 - Execute processes remotely
Copyright (C) 2001-2010 Mark Russinovich
Sysinternals - www.sysinternals.com

PsExec executes a program on a remote system, where remotely executed console
applications execute interactively.

Usage: psexec [\\computer[,computer2[,...] | @file]][-u user [-p psswd][-n s][-l
][-s|-e][-x][-i [session]][-c [-f|-v]][-w directory][-d][-<priority>][-a n,n,...
] cmd [arguments]
      -a          Separate processors on which the application can run with
                  commas where 1 is the lowest numbered CPU. For example,
                  to run the application on CPU 2 and CPU 4, enter:
                  "-a 2,4"
      -c          Copy the specified program to the remote system for
                  execution. If you omit this option the application
                  must be in the system path on the remote system.
      -d          Don't wait for process to terminate (non-interactive).
      -e          Does not load the specified account's profile.
      -f          Copy the specified program even if the file already
                  exists on the remote system.
      -i          Run the program so that it interacts with the desktop of the
                  specified session on the remote system. If no session is
                  specified the process runs in the console session.
      -h          If the target system is Vista or higher, has the process
                  run with the account's elevated token, if available.
      -l          Run process as limited user (strips the Administrators group
                  and allows only privileges assigned to the Users group).
                  On Windows Vista the process runs with Low Integrity.
      -n          Specifies timeout in seconds connecting to remote computers.
      -p          Specifies optional password for user name. If you omit this
                  you will be prompted to enter a hidden password.
      -s          Run the remote process in the System account.
      -u          Specifies optional user name for login to remote
```

El ejecutable **PsExec** de **Sysinternals**, perteneciente a Microsoft, permite ejecutar comandos remotos de manera individual.

RDP

Si bien existen implementaciones de SSH que corren sobre Windows, no son demasiado utilizadas debido a la existencia de un protocolo propio de administración remota, basado en el **estándar ITU-T T.128**, para compartir aplicaciones: **RDP** (**Remote Desktop Protocol**). RDP fue introducido por **Microsoft** en **Windows NT 4.0** y es un protocolo propietario. Su objetivo, tal como todos los protocolos de esta especie, es permitir la comunicación remota entre sistemas para la ejecución de aplicaciones, presentando la información procesada que se recibe del servidor al cliente. Es justamente en RDP que se basó en un principio la tecnología **Terminal Services** de Microsoft, que luego se renombró como **Remote Desktop Services**. En RDP, la información gráfica generada por el servidor es transformada en un formato propio y enviada al terminal, que la interpreta para mostrarla del otro lado. Tanto las teclas presionadas como los movimientos del mouse se redirigen al servidor luego de ser cifrados y comprimidos, y se utiliza por defecto el puerto **3389/TCP**. Cuando se inicia la sesión remota, lo que se muestra es la pantalla de bienvenida de Windows y no, las acciones remotas del usuario. Si bien esta herramienta se utiliza para administración remota, también se la encuentra en entornos con **thin clients**.

Seguridad

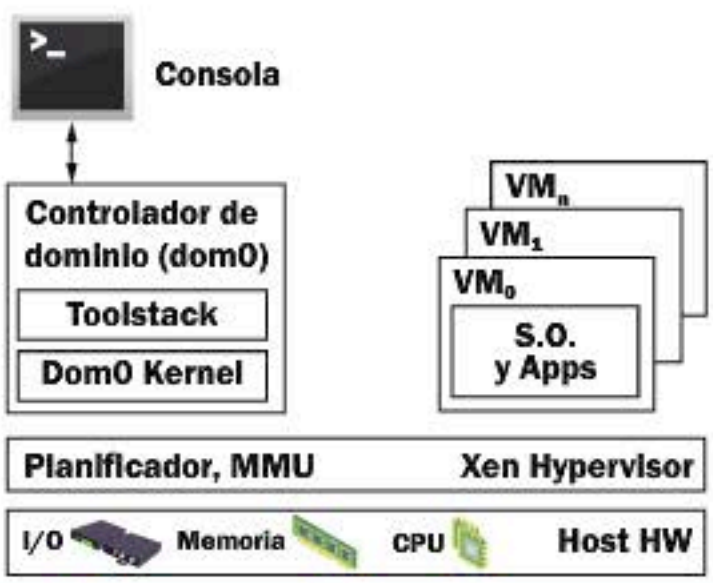
En cuanto a la seguridad estándar, realiza el cifrado de datos por medio del algoritmo **RC4 de 128 bits** y permite también aplicar seguridad a nivel de capa de transporte con **TLS** (**Transport Layer Security**). Además de soportar el redireccionamiento de puertos serie y paralelo, y del sistema de archivos, también soporta el redireccionamiento del audio y el uso de impresoras instaladas localmente, de forma remota. Desde la versión 6 (2006), se permite el uso de aplicaciones con archivos del lado del cliente, y el funcionamiento de aplicaciones que, a su vez, están provistas por una conexión remota. Otras características técnicas incluyen que los servicios sean configurables vía **Windows Management Instrumentation**, que se permita el ajuste de ancho de banda para clientes, y el soporte para varios monitores. Pese a ser propietario de Microsoft, existen implementaciones de terceros, como **rdesktop** y su **forkFreeRDP**. ■

Plataforma Citrix

Citrix es conocido en el universo de la virtualización y la presentación de aplicaciones gracias a las diferentes tecnologías que ha provisto al mercado. Veamos las alternativas que nos ofrece.

Si bien suele referirse a **Citrix** como un software, lo cierto es que es más bien un conjunto de aplicaciones, tanto de virtualización de servidores, como de conexión de redes, **Software as a Service** (**SaaS**) y procesamiento en la nube. Estas tecnologías son desarrolladas por **Citrix Systems, Inc.**, una empresa multinacional nacida en el año 1989, con sede en **Fort Lauderdale**, **Florida**. Los primeros años fueron muy duros, ya que entre 1989 y 1995 la empresa no tuvo beneficios, y de hecho, en 1989 y 1990 no obtuvo ingresos, por lo que entre 1991 y 1993, recibió dinero de otras firmas, como Intel y Microsoft, y de inversores privados, a fin de sobrevivir en la industria. En 1993, Citrix adquirió a **Novell** su producto **Netware Access Server**, una aplicación de acceso remoto para DOS que ofrecía aplicaciones del servidor a los usuarios y que la empresa comercializó como **WinView**; fue un exitoso producto. Como parte de su relación con **Microsoft**, Citrix obtuvo una licencia del código fuente de **Windows NT 3.51** y lanzó en 1995 una versión de Windows NT con acceso remoto, llamada **WinFrame**, orientada a grandes corporaciones. Con Windows NT 4, Microsoft decidió no proveer licencia del código fuente, pero como resultado de las negociaciones posteriores, adquirió la tecnología de Citrix para **Windows NT Server 4.0** y derivó en lo que, finalmente, fue **Windows Terminal Server**.

Las oficinas centrales de la empresa **Citrix Systems Inc.** se encuentran en la ciudad de Fort Lauderdale, Florida, en los Estados Unidos.



La **arquitectura XEN** trabaja sobre el hardware para ofrecer virtualización de múltiples sistemas operativos.

En el año 2007, Citrix adquirió la empresa **XenSource**, dueña del proyecto de código abierto del **hipervisor Xen**, que a partir de 2009 lo ha puesto gratuitamente a disposición de todos los usuarios y sin límites de implementación.
En 2010 surgió **Citrix Receiver**, un cliente universal para la entrega de servicios virtuales que ofrece conexión desde **tablets** y **smartphones**, basado en la arquitectura **Independent Computing Architecture** (**ICA**), protocolo antiguamente diseñado por Citrix para servidores de aplicaciones, que establece especificaciones para la transmisión de información entre clientes y servidor, sin estar asociado a ninguna plataforma específica.

Productos

Las familias de productos más importantes de Citrix son:

- **Citrix Delivery Center**: incluye **XenDesktop**, **XenApp**, **XenServer** y **NetScaler**, y permite virtualizar servidores, estaciones de trabajo y aplicaciones, centralizados en el **data center** y luego distribuidos como servicios bajo demanda en el momento en que se requieran. Por su parte, **XenDesktop** es un cliente ligero (**thin client**) que provee acceso remoto

a aplicaciones y estaciones de trabajo, tanto con plataforma **PC**, **Mac** o **smartphones**. **XenServer**, en cambio, es un monitor de máquinas virtuales que permite la ejecución de distintos sistemas operativos simultáneamente sobre el mismo equipo. Por último, **NetScaler** brinda optimización de la disponibilidad para aplicaciones sobre la base del balanceo de cargas y la gestión del tráfico, con el objetivo de mejorar su rendimiento.

- **Citrix Cloud Center**: un conjunto de productos que provee a las empresas la capacidad de crear nubes híbridas, y también permite a los proveedores de servicios brindar soluciones corporativas basadas en la nube (cloud as a service). Cuenta con funciones de virtualización, conexión en red y entrega de aplicaciones, así como también federación de redes y dominios, de modo que se mejore sustancialmente la seguridad en los entornos basados en la nube.

- **Citrix Online Services**: una suite de soluciones para servicios remotos que cuenta con productos como **GoToMeeting**, un software de videoconferencias web; **GoToAssist**, que sirve para manejar remotamente estaciones de trabajo, orientado a soporte técnico; y **GoToView**, destinado a la grabación y compartición de un sistema en red.

EL PRODUCTO MÁS RECONOCIDO DE CITRIX ES XENAPP, QUE OFRECE VIRTUALIZACIÓN Y TAMBIÉN ENTREGA DE APLICACIONES.

Asimismo, cuenta con productos dedicados a **mobile**, como **Zenprise** (empresa adquirida a fines de 2012), y otros relacionados con compartir archivos entre estaciones de trabajo y dispositivos móviles (**ShareFile** y **StorageZone**). Como toda gran empresa del sector informático, Citrix ha combinado y modificado sus distintos productos en función de las necesidades del mercado, por lo cual también ha concretado la compra de compañías relacionadas con su rubro. En general, los productos de administración remota y publicación de aplicaciones de Citrix han sido muy bien aceptados en el mercado, dadas sus variadas funcionalidades y la facilidad de uso por parte de los administradores de sistemas, para los cuales la complejidad es, en sí, un problema que puede reducir drásticamente la eficiencia de su trabajo. Otros administradores, en función del presupuesto de su departamento de sistemas y su propia área de expertos, han optado por soluciones abiertas o con alguna licencia del tipo libre, lo que puede, en principio, reducir los costos, pero requiere de mayor dominio de las tecnologías.

Actualidad

Dado que hoy en día Citrix es un jugador fundamental en la industria, algunos gigantes de la talla de **Cisco** han celebrado

El sitio web de **Citrix** en español cuenta con explicaciones detalladas sobre sus tecnologías y líneas de productos.

alianzas con ella. Quizás la lucha más clara de mercado la ha librado contra la apliocación **VMWare**, ya que su hipervisor **Xen** ha encontrado un claro nicho en un segmento en que el anterior ya se encontraba sólidamente posicionado.
No obstante, la combinación entre los avances en la virtualización y las tecnologías de administración remota desarrolladas durante la última década ha logrado acercar funcionalidades a entornos que, hasta el momento, requerían de sistemas operativos específicos, soportes y librerías particulares, y contaban con una creciente dificultad para liberarse masivamente al mercado.
Tal es el ejemplo de dispositivo como tablet PC y teléfonos inteligentes o smartphones, los cuales permitieron comprobar que la experiencia de funcionalidad del usuario no necesariamente debe estar limitada a los equipos tradicionales, como computadoras de escritorio o notebooks. Estos dispositivos, en conjunto con las nuevas tecnologías, nos permiten aprovechar al máximo las posibilidades de virtualización y acceso remoto. ■

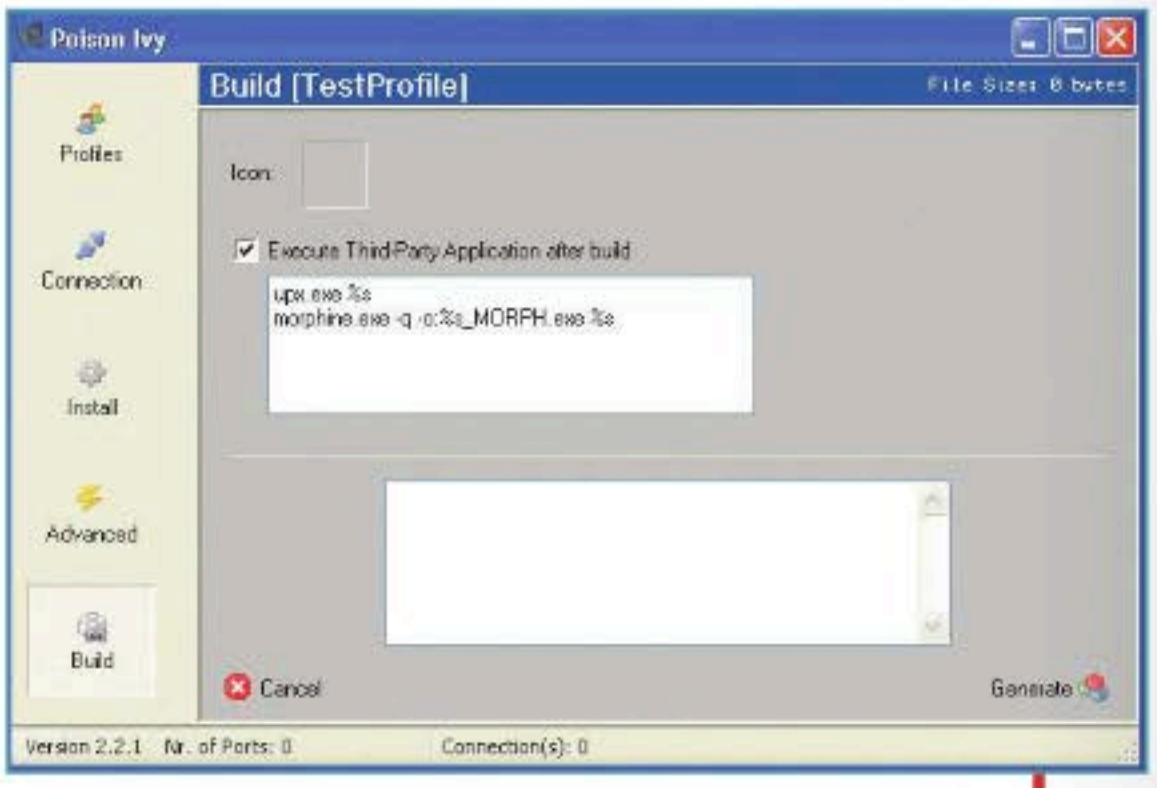
Fundación de Citrix

El antiguo desarrollador de IBM **Ed Iacobucci**, que deseaba incluir soporte multiusuario en OS/2, renunció cuando a IBM no le interesó la idea, y entonces fundó Citrix con el nombre Citrus. Pero tuvo problemas de derechos con otra marca comercial y lo cambió a Citrix, una palabra compuesta entre Citrus y UNIX. Muchos de los fundadores habían trabajado también en OS/2. De hecho, su primer producto fue **Citrix Multiuser**, basado en OS/2, cuya licencia de código fuente había adquirido de Microsoft para evadir a IBM.

Administración remota silenciosa

En muchos casos, un administrador de sistemas prefiere evitar la colaboración y aprobación del usuario. En ese caso, también hay alternativas de software para realizar la administración.

A fines de los años 90, cuando las redes comenzaban a difundirse en entornos corporativos, gobiernos y organizaciones, el software también acompañó ese desarrollo, atendiendo a las necesidades de los profesionales que manejaban, administraban y mantenían los sistemas. Teniendo en cuenta el perfil de estas personas, en general altamente técnico, y debido también a la dificultad de encontrar usuarios que tuvieran apenas conocimientos de computadoras y redes, las posibilidades de resolver problemas a distancia dependía fuertemente de la capacidad de conversación telefónica del administrador, algo que, en muchos casos, no era sencillo de encontrar.



PoisonIvy presenta una herramienta de creación del servidor que se ejecuta del lado del usuario que se quiera monitorear.

Aplicaciones no profesionales

Paralelamente, en el submundo del **hacking** proliferaba el software creado por no profesionales, entusiastas y estudiantes, quienes también comenzaron a encontrar ventajas en la posibilidad de realizar tareas remotas desde una computadora a otra, pese a que en entornos hogareños era prácticamente imposible hallar escenarios en los que hubiera más de una sola máquina. Así fue como, especialmente entre **hackers** y **programadores**, empezó a gestarse la idea de administrar los sistemas en forma remota. Claro que aún no eran tan sofisticados como para contar con las facilidades de **drivers**, librerías, **APIs**, y todo lo que tenemos en la actualidad. En ese contexto, nacieron las primeras herramientas de control remoto de sistemas, que básicamente trabajaban en una modalidad **cliente/servidor**, utilizando algún protocolo simple que corría sobre **TCP-IP**, y estaba orientado a algún sistema operativo en especial, en general, plataformas Windows. Dado que el ancho de banda no podía desperdiciarse en ese entonces, las aplicaciones eran completamente minimalistas y eficientes, y estaban construidas en lenguajes de bajo nivel, como **C** o **Assembler**. Así nacieron algunos programas cuyos fines no quedaba del todo claro si eran maliciosos o no, pues el hecho de ejecutarlos no implicaba que el usuario lo supiera, y en efecto, comenzaron a usarse para hacer bromas entre amigos e instalar el ejecutable que hacía las veces de servidor, para luego asustarlos abriendo y cerrando la lectora de CDs, o cambiando el fondo de pantalla.

Administración remota

Con el correr de los años, la administración remota pasó de ser un lujo de programadores **underground**

LogMeIn ofrece una consola que facilita el control remoto de un equipo, aun detrás de una conexión de banda ancha con IP dinámica.

y **hackers**, a convertirse en una necesidad comercial que surgía de la comodidad que proveía la administración centralizada de sistemas, especialmente en empresas grandes, que comenzaban a crecer en cuanto a su parque informático y equipos en los **data centers**. Fue entonces cuando algunas compañías y grupos de desarrolladores orientaron más aún sus esfuerzos hacia la creación de aplicaciones que tuvieran la posibilidad de gestionar y operar remotamente un sistema operativo, incluyendo modos sigilosos de uso que no requirieran la intervención del usuario, y que de hecho, pudieran operar en simultáneo con él. De esta forma, en 1999, **Dmitry Znosko** (hoy CEO de la empresa **Famatech**) creó **Radmin**, uno de los programas de administración remota más populares, con características que fueron creciendo con los años hasta transformarse en una completa aplicación de gestión remota en la actualidad. **Radmin** utiliza el **mirror driver** como driver de pantalla, y sus mecanismos de seguridad, de hecho, han mejorado mucho en las últimas versiones, al incorporar sistemas de cifrado optimizados. No obstante, siempre tuvo el perfil de un software de administración, y no, de una herramienta de **hacking**. Para obtener más información, el sitio oficial es **www.radmin.com**. Otro de los programas de administración remota más populares es **TeamViewer**, creado en el año 2005 en Alemania, y hoy producido y comercializado por el gigante de la seguridad **GFI Software**. **TeamViewer** cuenta con una versión **freeware** y otra para uso comercial en empresas, lo que hace que mucha gente lo conozca por haberlo utilizado en entornos hogareños. Si bien para funcionar debe ser instalado en el equipo remoto, cuenta con un modo de operación denominado **Quick Support**, que se ejecuta sin necesidad de instalación. El nivel de seguridad de las conexiones que establece es muy alto, ya que utiliza una infraestructura de clave pública con los algoritmos **RSA** y **AES**. Su sitio es **www.teamviewer.com**.

Otras opciones

A diferencia de las dos últimas, existen programas menos pensados para su uso oficial, y más librados a la conciencia del operador, ya que sus funciones están optimizadas para actuar de manera subrepticia en el sistema y operarlo a distancia, con todas las opciones que se podrían requerir, desde captura de pantallas, manejo de ventanas, instalación y ejecución de programas, hasta la discutida captura de teclas (**keylogging**). Algunos ejemplos de este tipo de aplicaciones son **PoisonIvy** y **ProSpyRAT**. El primero ha detenido su desarrollo hace algunos años, por lo que, al no haber ninguna empresa detrás de él, no puede garantizar su continuidad, ya que no es un software comercial. ■

TEAMVIEWER ES UN PROGRAMA ALEMÁN, QUE FUE CREADO EN 2005.

Tecnología Intel vPro

Considerando que muchas funciones de software se incorporan también en el hardware, Intel creó la familia vPro que aquí conoceremos.

Intel **vPro** es un conjunto de tecnologías que proveen características como el acceso remoto a computadoras de manera independiente del estado en el que se encuentre el sistema operativo y la propia máquina. Se pensó, principalmente, para cubrir las necesidades corporativas de administración, monitoreo y mantenimiento. Algunas acciones que se pueden realizar con vPro incluyen el encendido y apagado remoto, la modificación de la secuencia de arranque, el arranque remoto y la redirección de consola.

Implementación de contraseña de un solo uso.

Seguridad

Desde el punto de vista de la seguridad, vPro propone la protección contra **rootkits** y otros tipos de malware, y permite la virtualización basada en hardware mediante una tecnología de virtualización para administración centralizada de imágenes y almacenamiento en red, independientemente del **firewall**. Así, las computadoras que cuentan con procesadores de la familia **Intel CorevPro** de tercera generación y **Xeon E3-1200 v2** simplifican y agilizan algunas funciones importantes en el aspecto de la administración de sistemas, y ofrecen un mayor nivel de protección al ser combinados con software de seguridad. A pesar de que vPro es una tecnología que viene integrada directamente, requiere de instalación y configuración, que se realiza mediante el programa **Setup and Configuration**.

Intel Identity Protection

Una importante tecnología incorporada en la familia vPro es **Intel Identity Protection** (Intel **IPT**), que ofrece algunas defensas adicionales integradas, como, por ejemplo:

- Contraseñas integradas de un solo uso, que permiten eliminar el costo y mantenimiento de generadores de claves físicos, mientras que permite el acceso a **VPN** y sitios web.
- Infraestructura de clave pública (**PKI**) integrada, que implica la existencia de un segundo factor de autenticación almacenado en el **firmware** de la placa.
- Pantalla de transacción protegida, una tecnología de cifrado para entrada y salida de datos que pretende evitar el robo de identidad, y reduce el riesgo de los **keyloggers**.

Adicionalmente, vPro acelera el cifrado y descifrado de datos mediante **AES New Instructions**, que aumenta cuatro veces la velocidad de cifrado; y con **Secure Key**, que genera más números aleatorios, para mejorar la seguridad. ■

Procesadores con vPro

Si deseamos contar con la posibilidad de acceder a todas estas funciones que provee la tecnología **vPro** de Intel, debemos pensar en adquirir un equipo de escritorio o una laptop de gama media o alta, en general, orientado a entornos corporativos, que incorporan procesadores como **Core 2** (**Duo** o **Quad**) y **Centrino 2** de portátiles y algunos dispositivos móviles, aunque es probable que con el tiempo se vaya incorporando como una tecnología común en todos los equipos.

PRÓXIMA ENTREGA

18

SERVIDORES WEB Y FTP

En el próximo numero aprenderemos sobre los servidores utilizados para alojar sitios web y transferir archivos mediante el protocolo FTP. Además, conoceremos la manera de configurarlos y administrarlos correctamente.

Técnico en
REDES &SEGURIDAD

PROFESORES EN LÍNEA
profesor@redusers.com

SERVICIOS PARA LECTORES
usershop@redusers.com

SOBRE LA COLECCIÓN

CURSO VISUAL Y PRÁCTICO QUE APORTA LOS SABERES NECESARIOS PARA FORMAR TÉCNICOS EXPERTOS EN REDES Y SEGURIDAD. INCLUYE UNA GRAN CANTIDAD DE RECURSOS DIDÁCTICOS COMO INFOGRAFÍAS, GUÍAS VISUALES Y PROCEDIMIENTOS REALIZADOS PASO A PASO.

Con la mejor metodología para llevar adelante el montaje y mantenimiento de las redes informáticas y con los aspectos clave para brindarles la protección necesaria, esta obra es ideal para aquellos aficionados que deseen profundizar sus conocimientos y para quienes quieran profesionalizar su actividad.

REDES &SEGURIDAD 00017
9 789871 857784

CONTENIDO DE LA OBRA