# Introducción

Jordi Serra Ruiz

PID_00200512

UOC
Universitat Oberta de Catalunya

# Índice

# 1. La seguridad en la empresa

Las personas responsables de administrar los sistemas informáticos de una empresa, ya sea una pequeña empresa o una muy grande, deben tener mucha práctica en resolver problemas derivados de la instalación de los equipos informáticos de sus empresas.

El material de esta asignatura muestra cómo se deben instalar y configurar estos sistemas informáticos, tanto el mismo sistema operativo que se decida instalar como las herramientas básicas de control y las diferentes aplicaciones típicas de los servidores, que en muchos casos ayudan a desempeñar las tareas diarias e, incluso, las esporádicas. En esta asignatura, se van a ver las siguientes herramientas y servidores:

- copias de seguridad,
- planes de riesgo,
- servidores de ficheros,
- servidor web,
- servidor de redes privadas virtuales (VPN),
- servidores de correo electrónico,
- servidores FTP, y
- virtualización.

## 1.1. Copias de seguridad

En muchos casos, lo más importante que tiene una empresa son los datos. Pongamos por ejemplo un banco, donde todos suponemos que dejamos nuestro dinero, pero en realidad no lo tiene físicamente, sino que tiene una base de datos con la cantidad de dinero que cada cliente tiene depositado en ese banco. Por lo tanto, lo más valioso que tiene ese banco, o en su caso una sucursal, son los datos. Si se pierde la base de datos no se perderá el dinero, pero sí se perderá la relación entre los clientes y el dinero. Por lo tanto, lo primero que hay que asegurar en una empresa es mantener los datos cueste lo que cueste. No podemos dejar a su suerte todos los datos que tiene una empresa, como en el ejemplo del banco, las transacciones económicas o los datos de clientes y proveedores.

Esto implica que se han de hacer copias de seguridad de los equipos informáticos, en especial de aquellos equipos que se dedican a ejecutar tareas de servidor, y toda la información que tienen en cada una de las bases de datos. Tener copias de los equipos de trabajo de los usuarios del sistema informático hará que una potencial recuperación del puesto de trabajo pueda ser mucho más rápida, pero ya será tan crítica como perder los datos de los servidores.

Es muy importante definir desde un principio una buena política de realización de copias de seguridad. Resulta imprescindible poder recuperar toda la información o la máxima a la que podamos optar con los recursos que se tengan en un periodo corto. En una empresa, el tiempo es dinero y, cuanto antes se recuperen los servidores, menos pérdidas habrá.

En general, puesto que dependerá mucho de los datos y sobre todo de la variación de estos y del tiempo máximo del que se disponga para poder recuperarlos, las buenas políticas de copias de seguridad señalan que hay que hacer una copia completa semanalmente, pero el hecho de decidir qué tipo de copia se hace a diario depende del tipo de datos y de la evolución que tengan estos datos. Por ejemplo, en el caso del banco, en el que los datos son críticos, podría decidir hacer una copia entera todos los días, puesto que es más rápida de recuperar que recuperar la copia entera del lunes e ir añadiendo las modificaciones de cada día. Pero también se debe tener en cuenta el tamaño de la copia, puesto que una copia entera es muy grande y, por lo tanto, en el caso de que no sea crítico usaremos alguna en la que no haya que guardar toda la información.

Dependiendo de la importancia de los datos, del tiempo que se tiene para hacer las copias y de los dispositivos físicos donde se almacenan los datos, podremos elegir entre varias opciones que nos aseguren que podremos recuperar todos los datos en un tiempo razonablemente corto para la empresa.

Las copias de seguridad se suelen hacer sobre el mismo sistema, ya sea en dispositivos de cinta, de DVD o sobre otro disco duro, entre otros. Dependerá mucho de los datos que se vayan a copiar y del presupuesto que se tenga para poder comprar un dispositivo más complejo. Una opción es llevar a cabo la copia de los datos a través de la red interna de la empresa o incluso a través de Internet. Actualmente, ya hay empresas que disponen de búnkeres en los que almacenan los datos de las empresas que gestionan las copias de seguridad, que durante la noche suben los datos hacia sus servidores.

Es importante mantener separadas las copias de seguridad de los dispositivos para que un fallo no destruya tanto el dispositivo del que hacemos copias como las mismas copias. Se han dado casos de empresas privadas que han tenido que cerrar e, incluso, instituciones públicas que han perdido tanto el servidor que contenía sus datos como la copia de seguridad debido a un incendio.

**Copias de seguridad en red**

En el caso de tener una base de datos con unos cuantos gigabytes o incluso terabytes de tamaño, si es una copia de seguridad de toda la base de datos, puede ocupar el sistema y la red durante muchas horas. Incluso nos podría pasar que en una noche no se pudiera realizar toda la copia y los datos ya no fueran los correctos.

Teniendo en cuenta que hacer las copias de seguridad implica acceder a todos los datos en el espacio de tiempo más pequeño posible, hay que planificar las copias de acuerdo a los ritmos de cada empresa. Por otro lado, para los datos que tengan que disponer de un trato especial por las leyes de protección de datos, se tendrá que evitar hacerlos circular por la red innecesariamente y con las medidas suficientes para que terceras personas no

los puedan interceptar. En general, vale más llevar a cabo las copias por la noche y no en plena jornada laboral, puesto que los usuarios verán que el rendimiento del sistema informático quedará afectado seriamente y tanto la red como el acceso a los discos irán más lentos.

## 1.2. Planes de riesgo

Todas las empresas que tengan algún sistema informático un poco grande o cuyo funcionamiento sea crítico para la empresa, con el fin de mantener su negocio, deben tener un plan de riesgos para posibles emergencias. Las más comunes son la caída de la red eléctrica y los picos de tensión, que pueden dañar muy gravemente tanto las fuentes de alimentación de los equipos informáticos como las mismas placas base de los ordenadores que funcionan en aquel momento y dejar inservible por completo todo el sistema informático. Por ejemplo, una subida de tensión en un servidor de ficheros puede dejar a toda la empresa inoperativa, ya que, a pesar de que los ordenadores de las estaciones de trabajo funcionen, no podrán tener acceso a los documentos de trabajo. Es muy importante protegerse contra estas dos emergencias tan comunes (en el módulo de seguridad pasiva se mostrará cómo se debe hacer).

Otra posible emergencia es la subida de la temperatura a las salas donde se tienen ubicados los equipos informáticos que hacen los trabajos de servidores. Estas máquinas funcionan continuamente, en muchos casos las veinticuatro horas del día y los siete días de la semana (24 × 7). No se suele apagar un servidor aunque sea fin de semana, puesto que se aprovechan estas horas de bajo rendimiento para hacer las tareas de mantenimiento y las copias de seguridad.

Por lo tanto, los equipos emiten calor, de modo continuo, de las fuentes de alimentación y el resto de componentes del equipo, como el procesador, de manera que hay que disiparlo colocando algún sistema de refrigeración en la sala donde estén ubicados. Si este calor no se extrae, puede provocar que se paren automáticamente, que se reduzca la vida útil de los componentes e incluso un mal funcionamiento del equipo.

Por otro lado, si un servidor tiene que funcionar en régimen 24 × 7 –por ejemplo, se tiene que mantener en funcionamiento una base de datos en continuo–, hay que tener previsto qué pasa cuando este equipo se avería o deja de prestar servicio por cualquier anomalía. Hay que disponer de otro equipo con el que se pueda garantizar el servicio las veinticuatro horas del día de los siete días de la semana, de forma que hay que configurar los servidores para que se pasen información con el fin de que, si hay uno que deja de funcionar, el otro pueda ejercer de servidor principal, sin que la organización quede afectada por este hecho. Hay varias maneras de garantizarlo, por ejemplo, servidores de reserva, espejos de discos o RAID. Esto lo vamos a ver en los módulos siguientes.

### 1.3. Servidores de ficheros

Lo más usual es que las empresas medianas y sobre todo las grandes tengan un servidor, o más, para concentrar en un único punto todos los documentos y en otro, información de la empresa. De este modo, se tienen mucho más controlados los datos con el fin de hacer copias de seguridad, llevar a cabo los posibles planes de riesgo y controlar los accesos a la información. Se deben tener en cuenta las leyes de acceso a los datos personales, ya que una empresa puede tener datos personales de sus clientes o usuarios en las bases de datos, y no todo el mundo ha de tener acceso a estos datos.

Normalmente, solo se hacen las copias de los datos de estos servidores, así se evita hacer copias de seguridad de los equipos de los usuarios puesto que es mejor garantizar la disponibilidad de los datos más importantes colocándolos en un servidor y protegerlos como es debido, que tenerlos distribuidos por los equipos clientes y que se tengan que hacer copias de seguridad de todos los equipos. Los datos estarían distribuidos por muchos ordenadores y se haría mucho más difícil su tratamiento y control de acceso. Además, sería necesario tener planes de riesgo para cada uno de estos equipos. Por otro lado, con la creciente movilidad de los usuarios se complicaría todavía más la realización de copias de seguridad. Aun así, en algunos casos muy concretos sí se hacen copias de seguridad de los sistemas clientes, pero no para asegurar los datos, sino para poder recuperar el sistema con mucha más rapidez si es el caso de un ordenador crítico en su funcionamiento.

Por lo tanto, con el servidor de ficheros se garantiza de manera centralizada la privacidad de los datos, así como el acceso a las aplicaciones y los datos específicos para cada tipo de usuario de la red. Por ejemplo, en una empresa de artes gráficas que tenga un departamento de edición gráfica y otro de contabilidad, los trabajadores que pertenezcan al departamento de artes gráficas no necesitan acceder a los datos del de contabilidad (no han de tener acceso a los datos de los presupuestos de la empresa, por ejemplo). En cambio, los trabajadores del departamento de contabilidad pueden tener acceso a las ediciones gráficas, a los productos finales, por si fuera necesario.

Por otro lado, también hay que configurar las aplicaciones: los dos grupos de trabajadores no tienen que ver las mismas aplicaciones, no es necesario que vean todas las aplicaciones instaladas en los servidores de ficheros, sino que basta con que cada departamento vea las aplicaciones que le son necesarias. Esto solo se podrá hacer con aquellas aplicaciones que estén preparadas para ser instaladas en servidores y los ordenadores de sobremesa se conecten como cliente a estos servidores para poder usar la aplicación.

**Ocultación de aplicaciones y ficheros**

Este procedimiento se puede hacer mediante perfiles o grupos de usuarios. Cada trabajador debe pertenecer a un grupo o a unos cuantos grupos de usuarios de aplicaciones. Cada grupo se tiene que definir con un acceso específico a un grupo de aplicaciones. De este modo, creamos una clasificación de aplicaciones y una de usuarios, lo que permite crear relaciones entre ellas.

Así pues, relacionando aplicaciones con grupos de personas tendremos mejor protegida la información dentro de la misma empresa. Muchos de los problemas de seguridad que tienen las empresas son dados por los mismos trabajadores internos, o externos, que puntualmente acceden a información impor-

tante, de modo que la pueden eliminar o modificar, de manera voluntaria o involuntaria, ya sea porque tienen permiso para acceder o simplemente porque la política de protección de datos está mal implementada y lo permite todo. Esto es importante tenerlo en cuenta en el momento de instalar el sistema, y tener muy claro qué tipo de usuario debe tener acceso a los datos más críticos, o simplemente a datos a los que no deben tener acceso, ya que no es parte de su trabajo. Cuando se dé de alta a un nuevo trabajador en la empresa, basta con asociarlo a un grupo de usuarios de los que ya se han creado para que tenga acceso tan solo a la información que sea necesaria para su trabajo.

**Ejemplo**

Siguiendo con el ejemplo anterior de la empresa de artes gráficas, se puede definir el grupo de contabilidad, al que se asociarán las aplicaciones de base de datos, contabilidad, hojas de cálculo y recursos humanos, entre otros; y el grupo de edición, al que se asociarán las aplicaciones de retoque fotográfico y edición de texto profesional, por ejemplo. Ambos grupos tendrán aplicaciones diferentes a partir de las tareas que tienen que desempeñar. A partir de estos grupos, se irán colocando en un grupo o en el otro en función de las tareas que tenga que desempeñar cada persona.

## 1.4. Servidor web

En la actualidad, es muy usual que las empresas tengan un sitio web en el que ofrecen sus servicios y dan información sobre la propia empresa. Algunas de las páginas web ofrecen una parte privada donde se tiene acceso a los datos más confidenciales de la empresa y que pueden ser necesarios para poder desempeñar alguna tarea fuera de la empresa. Para acceder a estas páginas web, se tiene que instalar en algún equipo informático un servidor de ficheros por Internet, más conocido como servidor web. Este servirá hacia Internet los ficheros de la página web a petición de los clientes remotos que quieren visualizarla.

Es evidente que, para acceder a la información de la empresa desde cualquier punto de Internet, se tiene que abrir el acceso al servidor, de modo que, como mínimo, ya habrá una puerta de acceso abierta al mismo. Por lo tanto, como mínimo, este sistema informático tendrá una puerta abierta directamente a la red Internet, cosa que es un peligro si no se configura de modo correcto el acceso a estos datos desde el exterior.

Se tiene que instalar el servidor de sitios web de manera segura, es decir, se tiene que hacer de modo que nadie tenga acceso al disco del servidor mediante el directorio de ficheros del servidor de sitios web para que, si es posible, el servidor de ficheros no sea el mismo que el servidor de sitios web. Hay maneras muy sencillas de proteger mínimamente los documentos y directorios a los que no queremos que se acceda desde el exterior; por ejemplo, se puede hacer que el usuario externo no se conecte al servidor de sitios web como administrador o superusuario del sistema. Y, aunque parezca extraño, no es raro que pase esto, puesto que la instalación del gestor de sitios web se hace desde el usuario administrador, de modo que, si no se cambia, se accede con ese perfil y se tiene acceso a toda la máquina. Siempre hay pequeños detalles que hay que cuidar para proteger correctamente el servidor. Aun así, las últimas

versiones de los servidores web ya han cambiado este proceso de instalación y una vez ha finalizado el proceso cambian el usuario con el que se va a ejecutar el proceso del servidor web.

Otro problema del servidor web son los accesos al directorio de archivos: hay que protegernos de los accesos en busca de documentos, puesto que si no desactivamos la posibilidad de ver el contenido del directorio, cualquier persona puede ver los ficheros que tiene almacenados el servidor de sitios web. Así, se puede llegar a obtener información de la empresa que no se quiere que sea pública. Muchas veces, una estructura de ficheros y carpetas puede mostrar los diferentes departamentos o incluso nombres de usuarios del sistema y ayudar a atacantes que quieran obtener datos privados de la empresa.

Cabe señalar que en los directorios donde están los archivos de los sitios web no se tiene que almacenar nada que no sea estrictamente necesario para visualizar de manera correcta la información pública de la empresa. No se tiene que colocar información no querida en los directorios públicos de la web de la empresa. O, tal como ha pasado alguna vez, comentarios que revelan información en el código fuente de las páginas web.

### 1.5. Servidor de redes virtuales privadas

En algunos casos concretos, aunque cada vez más, los trabajadores de la empresa se tienen que conectar desde otro emplazamiento, desde el ordenador del cliente, por ejemplo, situado incluso en otro país. En estas empresas, habrá que usar estas redes privadas virtuales o VPN para dar servicio a los comerciales o trabajadores que necesitan tener acceso de modo seguro a los datos de la empresa desde el exterior. Incluso poder dar servicio al llamado teletrabajo, en el que los trabajadores ya no van a la oficina, sino que trabajan desde casa o desde cualquier otra parte del mundo. Estos trabajadores se deben poder sentir seguros a la hora de usar redes inseguras para poder subir o bajar ficheros de los servidores de la empresa.

Necesitamos instalar un canal seguro por el que el ordenador cliente se conecte al servidor de manera segura. Se tiene que cifrar la información que circula en ambos sentidos para que nadie pueda acceder a ella. Es evidente que este tipo de conexión es mucho más seguro que la que se puede hacer mediante los famosos Telnet o FTP. Estas conexiones no ofrecen ningún tipo de seguridad, de manera que no se recomienda el uso en servidores en los que la seguridad es primordial. Vale más la pena utilizar cualquier otro protocolo de comunicación seguro como, por ejemplo, el *secure shell* (*SSH*).

### 1.6. Servidores de correo electrónico

Del mismo modo que en el caso de los servidores de sitios web, y en especial del SSH, el correo electrónico es una puerta de entrada para cualquier persona al servidor, ya que debe tener algún puerto abierto para recibir y enviar

los correos electrónicos. Hay que tener cuidado con los servidores de salida de correo, los SMTP, ya que si no lo configuramos correctamente y se cierra solo al correo de salida de la empresa, se puede convertir en una puerta de salida de correos externos que utilizarán el servidor de salida del correo como servidor SMTP propio. Es decir, que terceras personas mediante Internet usen el servidor de envío de correos de la empresa como servidor propio de e-mail. Esto puede hacer que la empresa tenga innumerables problemas, como por ejemplo el envío mediante el servidor de la empresa de correo peligroso (como correo basura o pornografía infantil) sin que los correos electrónicos que se envían sean de la empresa misma.

El servidor de salida de correo se tiene que configurar para que solo lo puedan utilizar las personas que están dadas de alta en la organización, mediante el simple hecho de instalar el servidor de correo saliente seguro, con autenticación del usuario que accede al servicio. Esto se consigue enviando los correos del cliente al servidor de correo saliente por el puerto 25 (puerto por defecto de las aplicaciones SMTP) con cifrado de la información. Antes era usual que el servidor SMTP no hiciera ningún tipo de comprobación y solo había que mandar un e-mail con el formato correcto al puerto 25 para que este servidor lo encaminara hacia Internet y, evidentemente, esto hacía que el servidor SMTP lo pudieran usar terceras personas ajenas a la empresa.

Para el servidor de correo entrante también está la posibilidad de activar un canal seguro entre el servidor de correo y el cliente que consulta el correo que ha recibido. Eso también es importante, ya que permite que la circulación de datos entre los dos puntos sea segura. Si el cliente de correo (por ejemplo, Thunderbird, Kmail, Outlook o Eudora) accede al servidor de correo entrante por el puerto 110, recibirá los mensajes en formato normal, de modo que cualquier intruso que esté "detectando[1]" la red podrá obtener los datos que se están recibiendo, ya que viajan en texto plano por la red interna o incluso por Internet.

(1) *Detectar una red* significa acceder a esta mediante algún sistema físico y obtener los paquetes de información que pasan por esta red.

Para aumentar la seguridad de la empresa y el servidor de correo, se instala de manera segura, mediante el uso del protocolo SSL, la aplicación de correo que tenga el cliente, y tiene que hacer las consultas por el puerto 995 y dar el nombre de usuario de la red. Mediante este simple cambio en la instalación del servidor de correo nos podemos ahorrar muchos problemas de seguridad en la red, puesto que cada día más se envía todo tipo de información (alguna importante y confidencial) mediante el correo electrónico. Por el mero hecho de enviar continuamente información por la red, llega un momento en el que ya no somos conscientes de que el correo se envía en abierto, es decir, sin cifrar o codificar, de modo que todo lo que se envía como correo electrónico es susceptible de que lo lean fácilmente otras personas.

## 1.7. Servidores FTP

Tal como ya se ha comentado en los apartados anteriores de servidores de sitios web y redes virtuales, para maximizar la seguridad lo mejor es trabajar siempre con el protocolo SSL, es decir, que en vez de instalar el servidor FTP vale más instalar el servidor SFTP (SecureFTP), que usa el protocolo SSL para cifrar la comunicación entre los dos puntos de la conexión. Esto nos asegura, además de una buena política de claves de acceso de los usuarios, que el canal por el que circula la información entre el servidor de ficheros y el cliente que accede a este servidor mediante FTP sea seguro, es decir, que una vez establecido el canal no se pueda acceder a los datos que circulan por la red.

## 1.8. Virtualización

Las empresas optan cada vez más por la instalación de servidores virtualizados, ya que ofrecen muchas ventajas y pocos inconvenientes. La virtualización consiste en tener un único servidor con unas prestaciones más elevadas de lo que sería necesario para un servidor convencional, pero que en lugar de tener un único servidor tiene unos cuantos de forma virtual. Mediante un software específico se crean máquinas ficticias que se configurarán como servidores, de este modo se dispondrá de una única máquina física, pero de más de un servidor dentro de esa máquina.

Esto permitirá tener tantos servidores como sea necesario con la única inversión en hardware inicial, con un solo equipo informático. Por lo tanto, el ahorro en hardware es muy grande, además de tener en cuenta que el grado de disipación del calor ahora solo viene dado por una única máquina en lugar de tener muchas. Evidentemente, el consumo de electricidad también se verá reducido por el mismo concepto.

Otra ventaja muy importante es que, si se configura correctamente, las máquinas virtuales son independientes del hardware, por lo tanto, en el caso de que un servidor real dejara de funcionar, solo habría que copiar los ficheros de la máquina virtual en otro servidor para tener en pocos minutos otra vez en funcionamiento el sistema informático virtualizado. Ahora es mucho más fácil hacer una copia de seguridad de todo el sistema, ya que solo será necesario hacer la copia de los ficheros del software de virtualización.

## 2. Cortafuegos

**Ejemplo de cortafuegos**
Fuente: (CC). lindztrom.

Uno de los temas más importantes que debemos tener en cuenta en la seguridad de un servidor es el de los cortafuegos o *firewalls*. Los hay de dos tipos, los cortafuegos de hardware y los de software.

Los primeros son un dispositivo físico, normalmente pequeño, que conectamos a la entrada de la red de la compañía, de modo que toda la información que quiere entrar o salir de la red interna tiene que pasar por este aparato. En realidad, es como si el cable Ethernet de la red de la compañía, en lugar de conectarse directamente al *router* del proveedor de los servicios de Internet, se pusiera este aparato justo en medio y cortara todas las comunicaciones que van de los ordenadores hacia la red y solo dejara pasar aquellas que se hayan configurado previamente como permitidas.

Es decir, en el punto de salida de la red interna (LAN) a la red Internet (WAN), y de entrada de la WAN a la LAN, está el cortafuegos, que nos para todas las tramas de datos de entrada de la red que no vayan precedidas de una trama interna, es decir, tramas de datos que no se han solicitado desde dentro de la propia LAN a partir de una aplicación permitida o de un puerto abierto.

En cambio, los cortafuegos implementados mediante software son programas que se ejecutan en las máquinas clientes, tanto si son los servidores mismos como los equipos informáticos de los trabajadores. Este último caso es el más habitual en empresas pequeñas y en entornos más domésticos, a pesar de que existen muchos modelos de *firewall* pequeños que dan muy buen rendimiento a unos precios muy bajos.

Por el hecho de ser programas que no dejan de estar hechos por personas, estos últimos cortafuegos son más vulnerables a ataques y a malas configuraciones que los cortafuegos físicos, en los que, a pesar de poder haber vulnerabilidades y malas configuraciones, es más difícil saltarse las reglas establecidas. No dejan de ser programas que se ejecutan en máquinas que tienen acceso libre a Internet. Un mal funcionamiento del software del cortafuegos o de la máquina misma hace que el cortafuegos no sea efectivo.

Es evidente que cada uno tiene ventajas e inconvenientes. Los primeros son complicados de instalar y configurar y, además, son considerablemente más caros que los segundos, que son muy baratos, los hay que son completamente gratuitos, para los equipos de los usuarios y resultan fáciles de instalar y configurar. En cambio, como ventaja de los cortafuegos hardware podemos señalar la robustez, ya que si no se está conectado directamente al equipo real no se

puede configurar, o no es aconsejable permitir que se pueda configurar directamente desde la red WAN, aunque es evidente que sí se tendría que permitir hacerlo mediante la red LAN de la empresa.

# 3. Comparativa Windows respecto a GNU/Linux

En general, la seguridad informática en los servidores que se instalan en las empresas que quieren ofrecer algún tipo de servicio por Internet, o simplemente que quieren tener almacenados en un lugar seguro sus datos, parece evidente que es un concepto que no entiende de marcas, ni de filosofías de licencias, ni de términos legales. La seguridad informática en los servidores tiene que estar por encima de todo, incluso del sistema operativo que se decide instalar.

Aquí nos vamos a centrar únicamente en los dos sistemas operativos más utilizados en la instalación de servidores, la familia de servidores de Microsoft Windows y GNU/Linux.

Entraremos en detalle en la manera como se configuran algunas de las diferentes herramientas de seguridad de los dos sistemas y, por lo tanto, no veremos en este material los demás sistemas operativos, tan válidos como estos dos que hemos seleccionado. Un ejemplo de sistema corporativo que también cuida mucho la seguridad es el AS400 de IBM, así como el Solaris de SUN, que está basado en Unix, igual que Linux.

Es evidente que la marca Microsoft, para algunos, representa seguridad e imagen de empresa solvente y competente, mientras que, para otros, es una empresa que solo trata de hacer dinero a expensas de crear productos con muchos errores o *bugs* y muchos agujeros de seguridad. Tanto los primeros usuarios como los segundos tienen su parte de razón; la verdad siempre es relativa en estos casos. Lo que no se puede negar es que actualmente los productos de Microsoft son los más utilizados en los ordenadores personales, tanto los domésticos como los de los clientes terminales de las empresas, y que como imagen de empresa tiene una muy buena presencia en el sector; otra cosa es lo que piensan de la empresa las personas que están más vinculadas al mundo del software libre. Sin embargo, no se puede negar que Microsoft es un estándar *de facto*.

En cambio, GNU/Linux es visto por las empresas grandes como un producto hecho por mucha gente, sin un liderazgo serio, y como un producto que seguramente les traerá problemas, ya que la compañía Microsoft ha dado la imagen de que su sistema operativo solo lo tenemos que conectar y ya lo tenemos a punto para trabajar, aunque, en realidad, en algunos casos también se producen problemas. No obstante, esta visión ya no se ajusta a la realidad.

En la actualidad, el sistema operativo GNU/Linux se desarrolla constantemente, se sacan nuevas versiones y se arreglan las vulnerabilidades mucho más rápido que otras compañías de sistemas operativos. Incluso hay empresas dedicadas a proporcionar soporte técnico y montar la estructura del sistema in-

formático basado en este sistema operativo libre. Las mejoras en el sistema operativo que proponen los programadores siempre las tiene que supervisar el equipo de personas que se encargan de cada distribución. No es un sistema operativo que se base en las aportaciones de personas distribuidas en todo el mundo, sino que hay organizaciones que se encargan de mejorar y validar las sucesivas versiones del sistema operativo GNU/Linux.

Podríamos comparar los dos sistemas operativos en dos puntos, en cuanto a seguridad y en cuanto a costes, por ejemplo. La seguridad en GNU/Linux es una de las primeras cosas que se tuvo en cuenta a la hora de crear el sistema operativo, ya que desde un principio se pensó como un sistema operativo multiusuario, de forma que la seguridad entre usuarios era muy importante, no se permitía que los datos de los usuarios fueran públicos entre ellos. Otro tema que se debe considerar en cuanto a la seguridad son los virus. Actualmente, son casi incontables los virus que atacan de una manera u otra el sistema operativo de Microsoft, ya sea a un modelo en concreto o a toda la familia de sistemas operativos de Microsoft; en cambio, para GNU/Linux se conocen muy pocos virus que ataquen el sistema o parte de él. También hay que tener en cuenta que los ataques aprovechando las vulnerabilidades pueden venir también por las aplicaciones de terceros, que pueden dejar de alguna manera el sistema desprotegido, pero de esto no se puede culpar directamente al sistema operativo, ya que no es culpa de él, aunque en muchos casos acaba recibiendo las consecuencias de los ataques y los agujeros de seguridad de las aplicaciones.

Desde un punto de vista de la seguridad parece que es mejor GNU/Linux, pero desde hace unos cuantos años Microsoft ha mejorado mucho sus sistemas, ahora ya no permite tener un sistema nuevo en el mercado que no haya pasado por todas las pruebas de calidad y que no haya buscado las vulnerabilidades que se hayan podido probar.

El coste de las licencias es uno de los temas más importantes para las empresas. En el caso de las empresas grandes, pueden tener miles de puntos de trabajo y por lo tanto también trabajadores, lo que hace incrementar considerablemente el presupuesto de las licencias y formaciones. En cambio, en las empresas pequeñas en las que pueden tener pocos puntos de trabajo y personal, las licencias representan muchas veces un esfuerzo considerable.

Aunque la filosofía del sistema operativo GNU/Linux es que sea libre, eso no quiere decir que sea gratuito, de modo que hay empresas que se dedican a instalar y configurar los sistemas GNU/Linux. Todas las aplicaciones que se ejecutan en este sistema operativo tienen que ofrecer el código fuente para que los usuarios de estos programas los puedan personalizar según sus necesidades. Aun así, el software es gratuito.

En cambio, el sistema operativo de Microsoft tiene licencias que hay que pagar para instalarlo y utilizarlo y, además, es propietario, es decir, que no se ha hecho público el código fuente, excepto en algún caso muy concreto, para que los usuarios lo puedan personalizar según las características propias de cada empresa.

Casi todas las aplicaciones que se ejecutan en el sistema operativo de Microsoft son propietarias y tienen algún coste, ya sea en licencias únicas o anuales, que se tienen que pagar para seguir trabajando, o no se tiene el código fuente para mejorar o localizar el software a medida. Aunque cada vez más hay software libre que se puede usar sobre el sistema operativo Windows. Navegadores, gestores de correo, editores de textos y de fotos son varios ejemplos de ello.

Microsoft ha optado desde hace muchos años por una política de incluir su sistema operativo con los nuevos ordenadores personales que se venden. Llegó a acuerdos, y todavía los conserva, para que los grandes fabricantes de ordenadores (como HP, Compaq o Dell) incluyeran su sistema operativo en los ordenadores personales que se vendían y que todavía se venden. De este modo, los usuarios finales tienen la sensación de que solo hay que comprar el ordenador y que, cuando lo enciendan, este ya funcionará. Y de hecho es así. Por otro lado, también llegó a acuerdos con el fabricante de chips (Intel) para disponer de más información entre las dos empresas con el fin de mejorar el rendimiento del sistema operativo con un procesador en concreto.

Esto les ha dado una ventaja muy importante en cuanto al número de sistemas operativos instalados, ya sea en las casas particulares o en las empresas. Ahora hay alguna marca de equipos informáticos que vende sus ordenadores con los dos sistemas operativos, y el usuario es quien decide con cuál se queda; o incluso hay quien los vende sin ningún sistema operativo y, entonces, el usuario, o el administrador de sistemas en el caso de las empresas, es quien opta por comprar el sistema operativo de Microsoft, por instalar GNU/Linux con un contrato con alguna empresa del estilo de Suse o REDHat o por bajar gratis de Internet la última distribución de GNU/Linux e instalarla.

Es evidente que los costes de las licencias del software son una buena parte de los costes que tienen las empresas, y muchas veces los jefes no ven como una inversión rentable los gastos en seguridad, puesto que por sí solos no generan beneficios para la empresa. Por eso, hoy en día hay muchas empresas que instalan en los equipos informáticos el sistema operativo GNU/Linux, ya que tiene una buena cantidad de aplicaciones que hacen lo mismo que las aplicaciones propietarias.

Pero en contrapartida, las empresas que optan por usar el sistema operativo GNU/Linux se encuentran con la dificultad de que los empleados desconocen en su mayoría el sistema y, por lo tanto, tienen que dedicar mucho dinero a

los costes de formación y a organizar o contratar cursos para que los usuarios de los ordenadores puedan trabajar en un entorno que no han visto nunca o casi nunca.

En cambio, gracias a la política de Microsoft de incluir el sistema operativo desde hace muchos años en los ordenadores personales, y de la facilidad con la que hasta ahora se ha hecho la copia pirata de este sistema, cuando las empresas contratan nuevo personal, no le tienen que hacer ningún cursillo de formación para utilizar el ordenador. Hoy en día, es muy conocido el sistema operativo Windows, y Microsoft lo que hace es no apartarse de esa línea para que los empresarios opten por este sistema operativo con el fin de reducir costes de formación en los trabajadores.

A pesar de todo, en la actualidad la diferencia de funcionamiento para un usuario final de un ordenador entre los dos sistemas operativos es muy pequeña. Visualmente los dos sistemas son muy parecidos, e incluso las aplicaciones tienen interfaces gráficas muy parecidas, como por ejemplo Microsoft Office y OpenOffice.

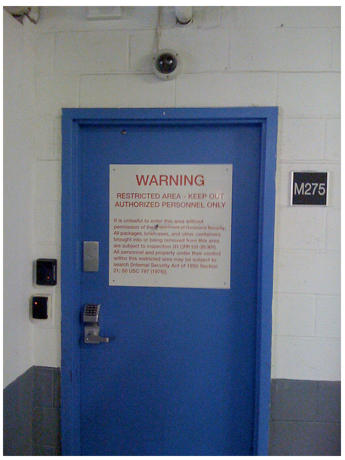
# 4. Seguridad física

Uno de los temas más importantes en cuanto a la seguridad de una empresa es la seguridad física. No sirve de mucho tener un cortafuegos muy potente y caro, vigilar las entradas en la red, hacer copias de seguridad de todos los datos, tener instalado y muy bien configurado un buen sistema operativo, por ejemplo, si no se tiene en cuenta la seguridad física.

Un simple ordenador en un despacho que sea fácil de acceder para los ladrones nos puede causar problemas graves, puesto que si entran a robar y se lo llevan, pueden acceder a muchos datos de la empresa que tiene guardados o que simplemente están en el perfil de usuario que se guarda en local. En ese ordenador se pueden guardar, por ejemplo, números de cuentas corrientes, datos personales o direcciones.

No sería la primera vez que en una empresa entran unos ladrones en horario laboral y se llevan un equipo informático mientras los trabajadores están en una reunión o en otra sala. Por lo tanto, un aspecto que debemos tener muy en cuenta es que los equipos informáticos no sean muy accesibles para personas no autorizadas, y sobre todo aquellos equipos que desempeñan las tareas de servidor. Ya no solo porque los puedan robar personas externas a la empresa, sino porque por descuido o error algún trabajador los pueda apagar o entrar en el sistema operativo y desconfigurar alguna aplicación.

Por norma general, los equipos que se destinan a ejecutar las tareas de servidores se tienen que instalar en habitaciones separadas de los trabajadores, cerradas con llave y con sistema de refrigeración todo el año. Así se evitarán problemas con el acceso de personas que no están autorizadas o que no están familiarizadas con estos equipos y que, por lo tanto, pueden tocar el sistema sin saber exactamente lo que están haciendo.




**Puerta de seguridad con código de entrada**
Fuente: (CC). Salim Virji.

Otra cuestión importante en cuanto a la seguridad física es el almacenamiento de las copias de seguridad o *backups*. No sirven de mucho las cintas, los DVD o cualquier otro sistema de almacenamiento de estas copias de seguridad guardadas en la misma oficina si se declara un incendio en el edificio y se queman todos los servidores y las cintas donde estaban las copias de seguridad. Imaginemos los millones de dólares que se podrían haber perdido en los casos de las torres gemelas del World Trade Center, en Nueva York, o en la torre Windsor, en Madrid, en la que el fuego lo destruyó absolutamente todo, si las empresas grandes no hubieran tenido un buen sistema de copias de seguridad guardado en otro edificio o incluso en otra ciudad.

**Ejemplo**

Recordemos un caso más reciente, donde un ayuntamiento de España perdió todos los datos informáticos cuando se quemó todo el edificio y no tenían guardadas las copias de seguridad fuera del edificio. Perdieron todos los datos y los históricos.

Debido a esos posibles accidentes se tiene que guardar con regularidad un juego de copias de los servidores fuera de las instalaciones de la empresa, bastante lejos y protegidos con sistemas ignífugos para asegurar que en un incendio no se pierdan los datos por las llamas o por el elevado calor que se alcanza en un gran incendio. En el mercado hay cajas de seguridad ignífugas en las que no entra el fuego, pero otro tema que debemos tener en cuenta es cómo puede quedar una cinta de copia de seguridad si una caja de hierro eleva la temperatura interior a 1.000 ºC a causa de un gran incendio.

# 5. Contenido del material

En este material se va a ver la instalación de dos servidores más o menos completos, con casi todas las funcionalidades que se pueden necesitar. Se va a mostrar la configuración de GNU/Linux y un servidor de la familia de Microsoft, el gestor de correo electrónico, el servidor de sitios web, el servidor de ficheros e impresión, el servidor de copias de seguridad, el servidor FTP, los planes de riesgo, la instalación de la red y los clientes de esta red, entre otros.

No se quiere sobreponer un sistema operativo sobre otro y, por lo tanto, se ha optado por explicar el funcionamiento de ambos, de forma que para cada apartado, y después de explicar el concepto teórico, se explicará cómo se instala y se configura cada una de las aplicaciones en los dos sistemas operativos. El administrador de sistemas tiene que decidir en cada caso qué se tiene que instalar, tanto para el servidor como para las estaciones de trabajo. No es extraño encontrar servidores con GNU/Linux instalados y clientes Windows en la misma red.