SEGURIDAD INFORMATICA

ETHICAL HACKING

Ing. Luis Alberto Iquira Vargas

Curso de Actualización 2016

SEGURIDAD INFORMATICA

Hoy en día y ya desde hace varios años el Internet se ha consolidado como medio de interconexión global, y por otro lado los incidentes de seguridad relacionados con sistemas informáticos vienen incrementándose de manera alarmante. Este hecho, unido a la progresiva dependencia de la mayoría de organizaciones hacia sus sistemas de información, viene provocando una creciente necesidad de implantar mecanismos de protección que reduzcan al mínimo los riesgos asociados a los incidentes de seguridad.

La Seguridad Informática es el área de la informática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta y, especialmente, la información contenida o circulante, es decir; enfoca su atención en proteger el hardware, el software y la información.

Para ello existen una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información. La seguridad informática comprende software (bases de datos, metadatos, archivos), hardware y todo lo que la organización valore y signifique un riesgo si esta información confidencial llega a manos de otras personas, convirtiéndose, por ejemplo, en información privilegiada.

Debemos precisar el concepto de seguridad de la información como el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de la misma. Por lo que es perfectamente posible establecer la diferencia que existe entre Seguridad Informática y Seguridad de la Información.

Acorde a la breve introducción previa y conceptos detallados líneas arriba podemos abordar el concepto de Ethical Hacking, como el uso de técnicas de ataque para encontrar fallas de seguridad, con el permiso del dueño de la organización que es centro de estos ataques, con el objetivo de mejorar la seguridad. De este concepto, se deduce claramente que Ethical Hacking es parte de la Seguridad Informática.

Además, procurando evitar confusiones se aprovecha la definición de Wikipedia sobre Pen Testing: “Pen Testing es la abreviación de Penetration Testing, este conjunto de técnicas se enfoca en encontrar vulnerabilidades en un ambiente objetivo al cual un atacante podría penetrar, ya sean sistemas de redes o computadoras, y/o robar información. Pen Testing, refiere al uso de herramientas y/o técnicas, similares a las utilizadas por los criminales, para encontrar una vulnerabilidad donde el objetivo es penetrar o comprometer el sistema objetivo y obtener acceso a información para determinar el impacto al negocio.

OBJETIVOS DE LA SEGURIDAD INFORMATICA

El objetivo de la seguridad informática es proteger los recursos informáticos valiosos de la organización, tales como la información, el hardware o el software. A través de la adopción de las medidas adecuadas, la seguridad informática ayuda a la organización cumplir sus objetivos, protegiendo sus recursos financieros, sus sistemas, su reputación, su situación legal, y otros bienes tanto tangibles como inmateriales. Desafortunadamente, en ocasiones se ve a la seguridad informática como algo que dificulta la consecución de los propios objetivos de la organización, imponiendo normas y procedimientos rígidos a los usuarios, a los sistemas y a los gestores. Sin embargo debe verse a la seguridad informática, no como un objetivo en sí mismo, sino como un medio de apoyo a la consecución de los objetivos de la organización.

En general el principal objetivo de las empresas, es obtener beneficios y el de las organizaciones públicas, ofrecer un servicio eficiente y de calidad a los usuarios. En las empresas privadas, la seguridad informática debería apoyar la consecución de beneficios.

Para ello se deben proteger los sistemas para evitar las potenciales pérdidas que podrían ocasionar la degradación de su funcionalidad o el acceso a los sistemas por parte de personas no autorizadas. De igual forma, las organizaciones públicas deben proteger sus sistemas para garantizar la oferta de sus servicios de forma eficiente y correcta. En cualquier caso, los gestores de las diferentes organizaciones deberían considerar los objetivos de la propia organización e incorporar la seguridad de los sistemas desde un punto de vista amplio, como un medio con el que gestionar los riesgos que pueden comprometer la consecución de los propios objetivos, donde la cuantificación de los diferentes aspectos, muchas veces económica, debe ser central

Desde la perspectiva de la información, los objetivos de la seguridad informática son:

- Integridad: garantizar que los datos sean los que se supone que son.
- Confidencialidad: asegurar que sólo los individuos autorizados tengan acceso a los recursos que se intercambian.
- Disponibilidad: garantizar el correcto funcionamiento de los sistemas de información.
- Evitar el rechazo: garantizar de que no pueda negar una operación realizada.
- Autenticación: asegurar que sólo los individuos autorizados tengan acceso a los recursos.

¿SOBRE QUE MANTENER SEGURO?

Equipos: En cuanto a la seguridad física del equipamiento o hardware tenemos:

- Es fundamental que no se puedan sustraer, ni el equipo entero ni alguna pieza del mismo (principalmente el disco duro, pero también el dispositivo donde se hace la copia de seguridad de ese disco).

- En el caso de los portátiles no podemos evitar que salgan de la empresa, porque los trabajadores visitan las dependencias del cliente o se llevan trabajo a casa. Pero sí debemos vigilar que esos ordenadores apliquen cifrado en el disco duro y tengan contraseñas actualizadas, sobre todo en los usuarios con perfil de administrador.

- Es importante que no se puedan introducir nuevos equipos no autorizados. Un hacker no necesita romper la seguridad de un servidor si puede conectar a la red de la empresa un equipo suyo con el software adecuado para realizar el ataque. O si puede introducir un troyano en algún ordenador de un empleado.

- Aplicaremos mantenimiento preventivo para evitar averías. Por ejemplo, en cada ordenador, una vez al año, abrir la caja para limpiar los disipadores y los ventiladores, porque el polvo acumulado puede anular su función de rebajar la temperatura del sistema.

Aplicaciones: Los ordenadores de una empresa deben tener las aplicaciones estrictamente necesarias para llevar a cabo el trabajo asignado: ni más ni menos. Menos es evidente porque impediría cumplir la tarea; pero también debemos evitar instalar

software extra porque puede tener vulnerabilidades que puedan dañar al sistema completo.

Cuando una empresa adquiere un nuevo equipo, el personal de sistemas procede a maquetarlo: instala las aplicaciones utilizadas en esa empresa, cada una en la versión adecuada para esa empresa, con la configuración particular de esa empresa. Incluso puede llegar a sustituir el sistema operativo que traía el equipo por la versión que se utiliza en la empresa. El objetivo perseguido es múltiple:

- Ahorrar al usuario la tarea de instalar y configurar cada aplicación (y de paso evitamos darle demasiados privilegios).
- Asegurar que el software instalado responde a las licencias compradas en la empresa.
- Homogeneizar el equipamiento, de manera que solo tendremos que enfrentarnos a los problemas en una lista reducida de configuraciones de hardware. La solución encontrada se aplica rápidamente a todos los equipos afectados.

Pero debemos estar preparados porque otras aplicaciones intentarán instalarse:

- Intencionadamente. El usuario lanza un instalador del programa que ha descargado de Internet o lo trae de casa en un CD/USB.
- Inocentemente. El usuario entra en una página pirata que hace la descarga sin que lo sepa, o introduce un CD/USB que desconoce que está infectado por un virus.

En ambos casos, el antivirus será una barrera y la ausencia de privilegios de administración también ayudará. Pero conviene aplicar otras medidas para no ponerlos a prueba:

- A la hora de crear un usuario, evitar que tenga privilegios de administración del sistema. Aunque todavía puede instalar determinadas aplicaciones, solo afectarán a ese usuario, no a todos los de esa máquina.
- Desactivar el mecanismo de autoarranque de aplicaciones desde CD o USB (en algunas empresas, al maquetar los equipos de usuario, incluso quitan los lectores de CD y desactivan los USB de la máquina).

La primera garantía que debemos tener a la hora de instalar una aplicación es su origen: si ha llegado en un CD del fabricante o si la descargamos de su web, o si está incluida en el mecanismo de actualizaciones automáticas de la versión actual. Si el CD no es original, o si descargamos de la web de otro, debemos desconfiar.

Por ejemplo, en los teléfonos móviles y tabletas la mayoría de las aplicaciones procede de la aplicación oficial del fabricante (Google Play en Android, App Store en iPhone). Utilizamos su opción de búsqueda, miramos que el número de descargas sea elevado y la bajamos. Durante la instalación nos pide permiso para hacer algunas cosas en el equipo, aunque no tiene mucho sentido porque el 99 % de los usuarios no sabe qué le está preguntando y siempre acepta. En el fondo, confiamos en que la aplicación no es peligrosa porque la hemos encontrado en el sitio oficial, donde se supone que la prueban antes de colgarla.

Datos: En cuanto a la seguridad física de los datos tenemos que recordar que tienen una importancia adicional que el hardware y software respectivamente, puesto que las máquinas y las aplicaciones se compran; pero los datos de nuestra empresa son exclusivamente suyos. Hay que protegerlos por dos aspectos principales:

- Si desaparecen, la empresa no puede funcionar con normalidad.
- Si llegan a manos de la competencia, la estrategia empresarial y el futuro de la compañía están en riesgo.

Las empresas modernas responden al esquema de «oficina sin papeles»: están informatizados todos los datos que entran, los generados internamente y los que comunicamos al exterior. La infraestructura necesaria es amplia y compleja porque los niveles de seguridad son elevados:

- Todos los equipos deben estar especialmente protegidos contra software malicioso que pueda robar datos o alterarlos.
- El almacenamiento debe ser redundante: grabamos el mismo dato en más de un dispositivo. En caso de que ocurra un fallo de hardware en cualquier dispositivo, no hemos perdido la información.

- El almacenamiento debe ser cifrado. Las empresas manejan información muy sensible, tanto los datos personales de clientes o proveedores como sus propios informes, que pueden ser interesantes para la competencia. Si, por cualquier circunstancia, perdemos un dispositivo de almacenamiento (disco duro, pendrive USB, cinta de backup), los datos que contenga deben ser inútiles para cualquiera que no pueda descifrarlos.

Comunicaciones: Los datos no suelen estar recluidos siempre en la misma máquina: en muchos casos salen con destino a otro usuario que los necesita. Esa transferencia (correo electrónico, mensajería instantánea, disco en red, servidor web) también hay que protegerla. Debemos utilizar canales cifrados, incluso aunque el fichero de datos que estamos transfiriendo ya esté cifrado (doble cifrado es doble obstáculo para el atacante).

Además de proteger las comunicaciones de datos, también es tarea de la seguridad informática controlar las conexiones a la red de la empresa. Sobre todo con la expansión del teletrabajo, que permite aprovechar Internet para trabajar en la red interna como si estuviéramos sentados en una mesa de la oficina. Ahora las redes de las empresas necesitan estar más abiertas al exterior, luego estarán más expuestas a ataques desde cualquier parte del mundo.

El peligro también está en la propia oficina: no puede ser que cualquier visitante entre en nuestra red con solo conectar su portátil a una toma de la pared o a través del wifi de la sala de espera. Un hacker seguramente no conoce los usuarios y contraseñas de los administradores de cada máquina; pero puede introducir software malicioso que intente adivinarlo, aprovechar vulnerabilidades no resueltas en nuestras aplicaciones para desplegar gusanos que ralenticen el rendimiento de la red, etc.

Un segundo objetivo de la supervisión de las comunicaciones es evitar la llegada de correo no deseado (spam) y publicidad en general. Con ello liberamos parte de la ocupación de la conexión a Internet, reducimos la carga de los servidores de correo (así como la ocupación de disco), nuestros usuarios no sufrirán distracciones y finalmente evitamos ataques camuflados en esos correos.

La tendencia actual en las empresas es migrar sus sistemas a Internet. Es el llamado cloud computing. Las más atrasadas todavía se limitan a disponer del servicio de correo electrónico con su propio dominio (@miempresa.es) y colgar la página web en algún

servidor compartido (hosting); pero muchas ya utilizan el almacenamiento en web (por ejemplo, Dropbox y Google Drive para usuarios individuales; S3 de Amazon para empresas) y algunas están desplazando toda su infraestructura informática a servidores virtuales situados en algún punto del planeta con conexión a Internet (de nuevo Amazon con su EC2).

Realmente hace mucho que utilizamos cloud computing: todos los webmail (Gmail, Hotmail, etc.) son servicios de correo electrónico que no están en nuestros ordenadores, sino que nos conectamos a ellos mediante un navegador para enviar, recibir y leer los mensajes, sin importarnos cuántos servidores o equipos de red ha necesitado desplegar esa empresa para que todo funcione con normalidad.

Sea cual sea el grado de adopción de cloud computing en una empresa, la primera premisa debe ser la seguridad en las comunicaciones, porque todos esos servicios están en máquinas remotas a las que llegamos atravesando redes de terceros.

JUSTIFICACION DEL USO DE LA SEGURIDAD INFORMATICA

Habitualmente los usuarios finales no tienen en consideración la seguridad cuando hacen uso de un sistema, ya que, frecuentemente se ignoran los aspectos relacionados con la seguridad. De igual forma, estos aspectos a veces pueden considerarse una molestia, ya que la seguridad suele ir en el platillo opuesto de la comodidad y facilidad de uso en la balanza del diseño de un sistema. Es por esto que los usuarios a veces puedan tener una imagen negativa de la seguridad, por considerarlo algo molesto y que interrumpe su capacidad de realización de un trabajo determinado. En un entorno seguro, un usuario se encuentra con tareas que le pueden resultar incómodas (como por ejemplo, recordar contraseñas, cambiarlas periódicamente, etc.) y que pueden limitar las operaciones que puede realizar así como los recursos a los que se le permite acceder.

Sin embargo, la seguridad es fundamental a la hora de afrontar tareas que se realizan en sistemas informáticos ya que son las únicas medidas que pueden garantizar que éstas se realicen con una serie de garantías que se dan por sentado en el mundo físico. Por ejemplo, cuando se guardan cosas en una caja fuerte en un banco real, no se piensa que cualquier persona del mundo puede llegar a ésta de una forma inmediata como si se tratara, en lugar de un banco, de una estación de autobuses. En el mundo intangible de la

informática, tan cerca de un servidor están sus usuarios legítimos como los usuarios que hacen uso de la misma red de comunicaciones. Es más, estos usuarios, en el caso de una red global, se cuentan por millones. Algunos serán “buenos vecinos” pero otros serán agentes hostiles.

Los Delitos Informáticos

El avance de la tecnología que ha vivido y está viviendo la sociedad, ha generado que se observe una evolución tan grande en la forma de infringir la ley, debido a esta situación las respectivas autoridades se ven en la necesidad de tomar la decisión de diferenciar los delitos informáticos del resto de delitos y definir su tratamiento dentro del marco legal.

Rafael Fernández Calvo, define a los delitos informáticos como “el término genérico para aquellas operaciones ilícitas realizadas por medio de Internet o que tienen como objetivo destruir y dañar ordenadores, medios electrónicos y redes de Internet. Sin embargo, las categorías que definen un delito informático son aún mayores y complejas y pueden incluir delitos tradicionales como el fraude, el robo, chantaje, falsificación y la malversación de caudales públicos en los cuales ordenadores y redes han sido utilizados.

Con el desarrollo de la programación y de Internet, los delitos informáticos se han vuelto más frecuentes y sofisticados.” Muchos expertos y organismos a los delitos informáticos los denominan como delitos electrónicos, delitos relacionados con la computadora, delincuencia relacionada con la computadora, crímenes por computadora, por lo que denota que no existe una definición de carácter universal propia del delito informático.

El Delito Informático implica actividades criminales susceptibles a ser sancionadas, que en un primer momento los países han tratado de encuadrar en figuras típicas de carácter tradicional, tales como robo, hurto, fraudes, falsificaciones, perjuicios, estafa, sabotaje, sin embargo, debe destacarse que el uso indebido de las computadoras es lo que ha propiciado la necesidad de regulación por parte del derecho.

Como todo delito, el informático tiene un sujeto activo y otro pasivo:

- SUJETO ACTIVO: En este tipo de delitos, el sujeto activo debe tener conocimientos técnicos de informática, es decir, en cierto modo, una persona con nivel de instrucción elevado, para poder manipular información o sistemas de computación, también conocido como atacante.

- SUJETO PASIVO: en el caso del delito informático pueden ser: individuos, instituciones de crédito, gobiernos, en fin entidades que usan sistemas automatizados de información, también conocido como víctima.

Seguidamente se muestra algunos casos en los que se pretende mostrar alguno de los peligros, relativos a seguridad, de estar 'interconectados'. Para cada uno de ellos existen mecanismos de seguridad que permiten llevar a cabo las operaciones de manera satisfactoria.

- **Intercambio de información**

  Cuando se intercambia información con un ordenador remoto, esa información circula por una serie de sistemas intermedios que son desconocidos a priori (excepto en ámbitos muy específicos). Además, no sólo no se sabe cuales serán estos sistemas intermedios, sino que además no se dispone de ningún control sobre ellos o sobre lo que puedan hacer con nuestros datos al pasar por ellos. Quizá el propietario original es de fiar pero su sistema ha sido comprometido por un atacante que toma posesión de los datos enviados.

  Por otro lado tampoco se puede estar seguro de que el sistema al que uno se está conectando es quien dice ser. Existen diversos medios técnicos para suplantar la identidad de un sistema y engañar a un tercero cuando realiza la conexión.

  En definitiva, no existe una certeza absoluta de que aquellos sistemas a los que uno envíe información sean realmente los auténticos; además, en el caso de que lo sean no se sabe si les llegará la información que se les envía, o si llegará sin cambios o si, aún si llega sin modificaciones, será leída por terceras partes.

- **Instalación de software dañino involuntariamente**

  Otra posibilidad que no se debe descartar es que se instale software en un ordenador sin conocimiento del usuario o administrador. Esto puede ocurrir de muchas formas, algunas relacionadas con operaciones que se realizan todos los días. Algunos ejemplos son:

  - Introducción de virus o troyanos por la descarga y ejecución de ficheros en servidores, en principio, confiables, por parte del usuario. El efecto de distribución puede ser, incluso, involuntaria si se hace uso de sistemas de

archivos compartidos. En el caso de los virus el efecto destructivo se hará patente más pronto o más tarde. La instalación de troyanos puede, sin embargo, pasar desapercibida.

- Difusión de virus por correo electrónico. Lograda gracias a la malversación por parte del virus del programa utilizado como lector de correo (que lo ejecuta automáticamente sin intervención del usuario) o porque el usuario activa el virus inadvertidamente creyendo que se trata de otra cosa. Su efecto pernicioso es, además del destructivo habitual de un virus, la distribución a las direcciones conocidas convirtiendo su propagación en exponencial.

- Explotación de una vulnerabilidad de un servicio que se está ofreciendo a través de Internet. Como por ejemplo un servidor web. Un caso similar sería una carpeta compartida donde otros miembros de la red local (y quizá un virus que haya en sus ordenadores) pueden copiar archivos.

Este software dañino no sólo puede obtener o borrar información del sistema en el que se instala, también puede servir como plataforma de ataque a otros sistemas. Es por esto que todo ordenador, máxime cuando se encuentra expuesto a recibir información del exterior, debe protegerse con las medidas de seguridad adecuadas aunque se considere que no tiene información ni servicios de gran importancia.

- **Protección ante accesos no autorizados**

Cuando se ofrecen servicios o información en una red para sus usuarios legítimos, al mismo tiempo se abre la puerta a posibles intrusos en estos sistemas. Protegerse de esta posibilidad implica tener un especial cuidado con todo el software empleado, desde el sistema operativo hasta la última de las aplicaciones instalada, y cuidar en gran medida su configuración.

Pero tampoco debería olvidarse la posibilidad de que existan intrusos que accedan físicamente al sistema. La evolución de las comunicaciones ha hecho que se preste una gran atención a la posibilidad de accesos remotos, pero de nada sirve evitar esta posibilidad si se permite el acceso físico al sistema a personas no autorizadas. Es por esto que, en algunos casos pueda ser necesario tomar las medidas de

seguridad adecuadas sobre el propio hardware para evitar robos, o pérdidas de información por estos accesos inadecuados.

En definitiva un buen sistema de seguridad debe proteger los sistemas vulnerables ante el posible acceso físico o remoto de intrusos no autorizados. Evidentemente, el nivel de seguridad establecido tendrá que ser consecuente con un análisis previo de los riesgos, considerando el impacto de dicho acceso no deseado contra las posibilidades de que este se produzca.

Algunas medidas de seguridad que se pueden implantar en estos casos van desde el cifrado de información sensible para impedir su acceso sin la clave adecuada, métodos físicos de destrucción de la información en caso de manipulación mecánica de la misma, etc.

- **Fallos de seguridad en la utilización del software**

  Se puede hacer un análisis agrupando los fallos de seguridad que se pueden dar en el software. Este análisis va a permitir enfocar, más adelante cómo distintos tipos de software ayudan a solventarlos. De una forma simplista, se pueden dividir en tres bloques:

  - Fallos debidos a errores desconocidos en el software, o conocidos sólo por terceras entidades hostiles.
  - Fallos debidos a errores conocidos pero no arreglados en la copia en uso del software.
  - Fallos debidos a una mala configuración del software, que introduce vulnerabilidades en el sistema.

  El primero de ellos se puede achacar a la calidad del código, el segundo a la capacidad y celeridad de arreglo de los errores descubiertos en el código por parte del proveedor del mismo y a la capacidad del administrador de recibir e instalar nuevas copias de este software actualizado. El tercer tipo de vulnerabilidades puede achacarse, sin embargo, a una falta de documentación del software o una falta de formación adecuada de los administradores para hacer una adaptación correcta del mismo a sus necesidades.

Los fallos pueden dar lugar a un mal funcionamiento del programa, siendo en el ámbito de la seguridad preocupantes por cuanto:

- Pueden implementarse algoritmos de forma incorrecta lo que puede llevar a una pérdida de seguridad (por ejemplo, un algoritmo de generación de claves que no se base en números totalmente aleatorios)
- Pueden diseñarse servicios que, en contra de sus especificaciones, ofrezcan funcionalidades no deseadas o que puedan vulnerar la seguridad del servidor que los ofrezca.
- Pueden no haberse tomado las medidas de precaución adecuadas para asegurar el correcto tratamiento de los parámetros de entrada, lo que puede hacer que un atacante externo abuse de ellos para obligar al programa a realizar operaciones indeseadas.

En el análisis previo se hace uso de algunos casos que evidencian los riesgos y/o peligros que existen de manera latente cuando se trata de software, de la misma forma; podría hacerse un análisis sobre que peligros existen cuando se trata de TICs o de Redes de Comunicación, en líneas generales tanto para la estructura física como para la lógica tenemos mucho por analizar sobre temas de vulnerabilidad, riesgos y/o peligros; y todo se centra sobre un punto: la información, que como se definió al inicio es un subconjunto dentro de la seguridad informática, pero quizás el de mayor importancia y complejidad no solo por lo que significa la información para las organizaciones sino también por dificultades como: definir exactamente qué tipo de información y en qué medida se desea proteger, por otro lado puede tenerse como inconveniente la necesidad de confidencialidad respecto a la información. Por todo ello se desarrollan las técnicas y herramientas que componen la seguridad informática ahondando en la investigación en favor de reducir esos riesgos y/o peligros latentes tratando de superar los inconvenientes que existen en este intento.

CRITERIOS DE SEGURIDAD

El Information Technology Security Evaluation Criteria (ITSEC) define los siguientes criterios de seguridad:

- **Confidencialidad:** la información debe estar disponible solamente para aquellos usuarios autorizados a usarla. La confidencialidad intenta que la información solo sea utilizada por las personas o máquinas debidamente autorizadas. Para garantizar la confidencialidad necesitamos disponer de tres tipos de mecanismos:
    - Autenticación. La autenticación intenta confirmar que una persona o máquina es quien dice ser, que no estamos hablando con un impostor.
    - Autorización. Una vez autenticado, los distintos usuarios de la información tendrán distintos privilegios sobre ella. Básicamente dos: solo lectura, o lectura y modificación.
    - Cifrado. La información estará cifrada para que sea inútil para cualquiera que no supere la autenticación.

  Veamos algunos ejemplos del mundo real:
    - Para entrar a un estadio de fútbol se necesita una entrada (autenticación); pero unos irán a tribuna y otros a un palco VIP (autorización).
    - Para sacar dinero de un cajero necesitas una tarjeta y el PIN de esa tarjeta (autenticación).
    - Al recoger un envío certificado necesitas llevar el DNI, para que comprueben que eres tú (autenticación).
    - En los parques temáticos hay que llevar una entrada (autenticación) y, si pagas un poco más, tienes un fast-pass para no hacer cola en las atracciones (autorización).
- **Integridad:** la información no se puede falsear. Los datos recibidos (o recuperados) son los mismos que fueron enviados (o almacenados), etc. El objetivo de la integridad es que los datos queden almacenados tal y como espera

el usuario: que no sean alterados sin su consentimiento. Un ejemplo sería el código identificador de la cuenta bancaria o el CCI.

- **Disponibilidad:** ¿quién y cuándo puede acceder a la información? La disponibilidad intenta que los usuarios puedan acceder a los servicios con normalidad en el horario establecido. Para ello se invierte en sobredimensionar los recursos, se tiene los siguientes ejemplos:

    - Una tienda tiene dos datáfonos con dos bancos distintos. Así siempre puede ofrecer el cobro por tarjeta.

    - Un equipo de fútbol tiene varios suplentes en el banquillo. Así siempre puede intentar mantener once jugadores cuando alguno se lesiona.

    - Los aviones llevan piloto y copiloto.

    - Cuando se hacen obras entre dos estaciones de metro, hay una línea de autobuses que lleva de una a otra por superficie, y el ticket es el mismo.

    - La falta de accesibilidad o disponibilidad produce una denegación de servicio, que es uno de los ataques más frecuentes en Internet.

- **No repudio:** cualquier entidad que envía o recibe datos no puede alegar desconocer el hecho. El no repudio se refiere a que, ante una relación entre dos partes, intentaremos evitar que cualquiera de ellas pueda negar que participara en esa relación. Hay muchos ejemplos de la vida real:

    - Los contratos se firman por las dos partes. Por ejemplo, la hipoteca de una casa.

    - Firmamos el impreso de matriculación en un ciclo formativo.

    - En algunas tarjetas de crédito hay que firmar un papel con los datos de la compra, y la tienda se queda una copia. Conservamos el ticket de compra para poder solicitar la devolución.

    - Cuando hacemos una reserva de vuelo obtenemos un localizador; a la hora de retirar el billete no pueden negar que hicimos la reserva.

Los dos criterios anteriores son especialmente importantes en el entorno bancario y de comercio electrónico.

IMPORTANCIA DE LA AUTENTICACION – AAA – e2e

La autenticación es especialmente importante en temas de seguridad. Debemos estar muy seguros de la identidad de la persona o sistema que solicita acceder a nuestra información.

Un esquema muy utilizado para analizar la autenticación es clasificar las medidas adoptadas según tres criterios:

- Algo que sabes. Para acceder al sistema necesitas conocer alguna palabra secreta: la típica contraseña.
- Algo que tienes. En este caso es imprescindible aportar algún elemento material: generalmente una tarjeta.
- Algo que eres. El sistema solicita reconocer alguna característica física del individuo (biometría): huella dactilar, escáner de retina, reconocimiento de voz, etc.

La autenticación será más fiable cuantos más criterios distintos cumpla:

- Para entrar en casa solamente nos hace falta una llave (algo que tienes). Pero en algunos países europeos los portales tienen un código (algo que sabes).
- Para entrar a un ordenador, generalmente necesitamos un usuario (algo que sabes) y una contraseña (algo que sabes).
- Para sacar dinero de un cajero necesitamos una tarjeta (algo que tienes) e introducir un PIN (algo que sabes). En cambio, en la web del banco solo necesitamos un usuario (que suele ser nuestro DNI, relativamente fácil de localizar) y un PIN (algo que sabes).

La sigla **AAA** se refiere a autenticación, autorización y accounting. Las dos primeras ya las hemos visto con anterioridad; la tercera se refiere a la información interna que los sistemas generan acerca de sí mismos. Concretamente, el uso que se hace de sus servicios. Esta información sirve para revisar el dimensionado de los equipos y,

debidamente asociada a cada departamento de la empresa, permite establecer limitaciones y penalizaciones.

Pero la información del accounting también permite comprobar la eficacia de las medidas de autenticación y autorización, sobre todo en un análisis forense tras un ataque.

Siguiendo el rastro podremos localizar por dónde ha entrado e intentar resolverlo. Por este motivo, es importante que el registro del accounting se haga en una máquina distinta: si el hacker ha conseguido entrar, puede fácilmente borrar sus huellas. Sin embargo, si el registro se hace simultáneamente en otra máquina, ya son dos las máquinas que debe atacar (y generalmente la máquina de registro se carga con el mínimo software posible, para reducir las opciones de entrada).

e2e significa extremo a extremo: la seguridad debe controlarse en el origen de los datos, en el destino de los datos y en el canal de comunicación utilizado entre origen y destino:

- En el origen y en el destino intentaremos que el equipo y las aplicaciones no hayan sido modificados. Si alguno no está bajo nuestro control, debemos desconfiar.

- En el canal intentaremos limitar quién accede y, sobre todo, cifraremos, porque nuestros datos atravesarán las redes de otras compañías. Sobre sus equipos y el personal que opera con ellos no tenemos ningún control, luego debemos desconfiar.

Con todos los criterios de seguridad se busca controlar en la medida de lo posible los siguientes dos aspectos negativos:

- **Vulnerabilidad:** punto o aspecto del sistema que es susceptible de ser atacado. Equivale al conjunto de debilidades del sistema. La vulnerabilidad es un defecto de una aplicación que puede ser aprovechado por un atacante. Si lo descubre, el atacante programará un software (llamado malware) que utiliza esa vulnerabilidad para tomar el control de la máquina (exploit) o realizar cualquier operación no autorizada.

  Hay tres tipos de vulnerabilidades:

- Vulnerabilidades reconocidas por el suministrador de la aplicación y para las cuales ya tiene un parche que las corrige. Si nuestra empresa utiliza esa aplicación, debemos aplicar el parche inmediatamente.

- Vulnerabilidades reconocidas por el suministrador, pero todavía no hay un parche. En algunos casos sí se proporciona una solución temporal (workaround), pero, generalmente, lo mejor es desactivar el servicio hasta haber aplicado el parche.

- Vulnerabilidades no reconocidas por el suministrador. Es el peor caso, porque podemos estar expuestos a un ataque durante un tiempo largo sin saberlo.

Los fabricantes de software intentan reaccionar rápidamente ante cualquier informe que demuestre una vulnerabilidad en sus programas. Gracias a Internet, de manera programada, los programas conectan con la web de su suministrador para comprobar si hay algún parche pendiente de aplicar (actualizaciones automáticas). Es decir, no esperan a que el administrador de la máquina compruebe uno a uno el estado de todos los programas instalados, porque puede pasar un tiempo precioso desde que se libera el parche hasta que el administrador se entera, lo descarga y lo aplica.

Es asi que existen muchos tipos de malware:

- Virus. Intentan dejar inservible el ordenador infectado. Pueden actuar aleatoriamente o esperar una fecha concreta (por ejemplo, Viernes 13).

- Gusanos. Van acaparando todos los recursos del ordenador: disco, memoria, red. El usuario nota que el sistema va cada vez más lento, hasta que no hay forma de trabajar.

- Troyanos. Suelen habilitar puertas traseras en los equipos: desde otro ordenador podemos conectar con el troyano para ejecutar programas en el ordenador infectado.

Realmente no es tan importante qué malware nos ha entrado: hay que eliminarlo de todas formas porque es una aplicación que no hemos querido instalar y que no nos traerá nada bueno (incluso puede mutar: un gusano convertirse en troyano, etc.).

Todos tienen en común su afán de replicación: intentan contaminar el máximo número de ordenadores posible para continuar la infección.

También hay que tener cuidado con los falsos antivirus. En algunas páginas web peligrosas (servicios de descargas ilegales, por ejemplo) aparece un mensaje que nos avisa de que estamos infectados y se ofrecen amablemente para descargar un antivirus que nos limpiará el ordenador.

Si pulsamos en el enlace y descargamos e instalamos ese programa, lo que realmente ocurre es que hemos dejado entrar un malware que, desde ese instante, puede hacer cualquier cosa: lanzar anuncios sin parar, instalar otros virus, abrir una puerta trasera para convertirnos en ordenador zombi en algún ataque organizado, robar datos personales (imágenes, vídeos), etc.

En algunos casos, el virus da la cara y directamente nos dice que ha secuestrado nuestro ordenador. Efectivamente: ya no podemos hacer nada con el teclado ni el ratón. Para recuperar la máquina hay que introducir una contraseña que solo nos la proporcionan tras efectuar un pago económico (es decir, piden un rescate).

Por supuesto, el primer aviso era falso; seguramente, al entrar de nuevo en esa página, seguirá apareciendo. Si bien es cierto que los navegadores pueden realizar análisis del disco duro buscando virus (los llamados antivirus on-line, como Panda Activescan), para ello necesitan la instalación previa de un software específico para esa tarea de buscar virus. Después podrán avisar o no, dependiendo de lo que encuentren; pero nunca aparecerá un aviso solo por entrar a una página.

Lo mismo puede ocurrir con programas que nos aseguran que acelerarán el rendimiento del ordenador, o el disco duro, o la conexión a Internet. Estos programas existen, pero debemos descargarlos desde fuentes de toda confianza, como las webs de los autores de ese software o un sitio con buena reputación (Softonic, CNET, etc.).

Para evitar que ocurra, lo mejor es tener siempre activado el antivirus (y tenerlo actualizado, claro). Y, si por cualquier razón, el ordenador ya está secuestrado, algunos antivirus tienen la opción de ejecutarse desde un LiveCD. Es decir, descargamos desde la web del fabricante del antivirus una imagen que grabamos en un CD. Esa imagen lleva un minisistema operativo y el programa del antivirus. Arrancamos el ordenador desde ese CD

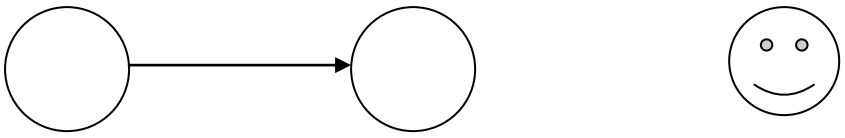
y podemos hacer una limpieza a fondo, con la tranquilidad de que el virus no se ha activado porque no está funcionando el sistema operativo del disco duro.

- **Amenazas o ataques(Threats):** Posible peligro del sistema. Pueden provenir de personas (hackers, crackers), de programas, de sucesos naturales. Equivalen a los factores que se aprovechan de las debilidades del sistema.

Para ambos aspectos deben existir las contramedidas, que serán las técnicas de protección del sistema contra las amenazas y la vulnerabilidad. Justamente si recordamos, la seguridad informática se encarga de identificar las vulnerabilidades del sistema y establecer las "técnicas, herramientas, etc" necesarias para intentar evitarlas. Estas "técnicas, herramientas, etc" vienen a ser las contramedidas a emplear para evitar los aspectos negativos descritos previamente. No debemos olvidar el siguiente axioma de seguridad: "No existe ningún sistema absolutamente seguro".

Tipos de Ataques o Amenazas

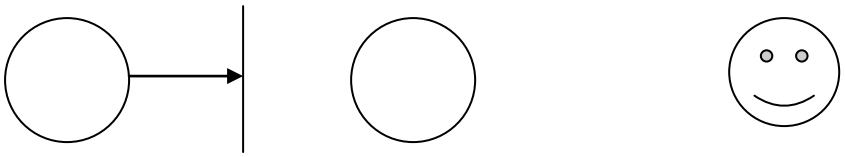
Dentro de un sistema que proporciona información, normalmente el flujo de información va desde la fuente hacia el destino, y lo que siempre se procura es que el intruso o amenaza se encuentre fuera de este flujo y sin poder alterar esta normalidad de funcionamiento.



FLUJO NORMAL DE INF.

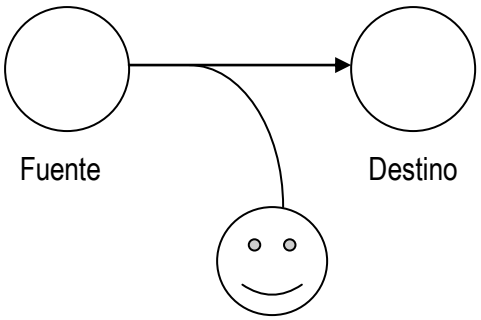
Lamentablemente existen ataques que alteran esta normalidad que pasamos a describir seguidamente:

- Interrupción: Destruye información o la inutiliza: Ataca la accesibilidad o disponibilidad. Aquí el intruso procura destruir algún dispositivo propio del flujo normal o también saturar la capacidad del procesador. El ataque consigue provocar un corte en la prestación de un servicio: el servidor web no está disponible, el disco en red no aparece o solo podemos leer (no escribir), etc.



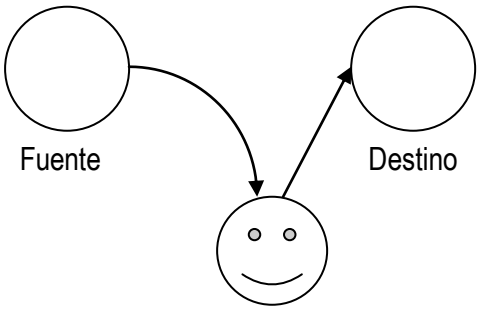
FLUJO INTERRUMPIDO DE INF.

- Interceptación: Una parte no autorizada gana el acceso a un bien. Ataca la confidencialidad. Intruso en la línea de información sin autorización, puede realizar copias de información. El atacante ha logrado acceder a nuestras comunicaciones y ha copiado la información que estábamos transmitiendo.



FLUJO INTECEPTADO DE INF.

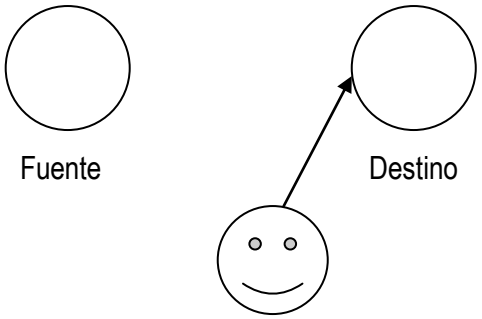
- Modificación: Una parte no autorizada modifica el bien. Ataque a la integridad. Cambiar contenidos de bases de datos, cambiar líneas de un programa, datos de una transferencia, etc. Ha conseguido acceder, pero, en lugar de copiar la información, la está modificando para que llegue alterada hasta el destino y provoque alguna reacción anormal. Por ejemplo, cambia las cifras de una transacción bancaria.



FLUJO MODIFICADO DE INF.

- Fabricación: Falsificar la información: Ataca la autenticidad. Añadir campos y registros en una base de datos, añadir líneas de un programa (virus), etc. El atacante se hace pasar por el destino de la transmisión, por lo que puede

tranquilamente conocer el objeto de nuestra comunicación, engañarnos para obtener información valiosa, etc.



FLUJO FABRICADO DE INF.

A su vez se pueden clasificar los tipos de ataques o amenazas como ataques de dos tipos: pasivos y activos. Como ataque pasivo tenemos a la interceptación, donde se consigue exponer la confidencialidad de la información. Ahora bien, tanto la interrupción, la modificación y la fabricación son ataques activos que atentan contra la disponibilidad e integridad de la información.

Los atacantes para poder conseguir su objetivo pueden aplicar una o varias de estas técnicas:

- Ingeniería social. A la hora de poner una contraseña, los usuarios no suelen utilizar combinaciones aleatorias de caracteres. En cambio, recurren a palabras conocidas para ellos: el mes de su cumpleaños, el nombre de su calle, su mascota, su futbolista favorito, etc. Si conocemos bien a esa persona, podemos intentar adivinar su contraseña. También constituye ingeniería social pedir por favor a un compañero de trabajo que introduzca su usuario y contraseña, que el nuestro parece que no funciona. En esa sesión podemos aprovechar para introducir un troyano, por ejemplo.

- Phishing. El atacante se pone en contacto con la víctima (generalmente, un correo electrónico) haciéndose pasar por una empresa con la que tenga alguna relación (su banco, su empresa de telefonía, etc.). En el contenido del mensaje intenta convencerle para que pulse un enlace que le llevará a una (falsa) web de la empresa. En esa web le solicitarán su identificación habitual y desde ese momento el atacante podrá utilizarla.

- Keyloggers. Un troyano en nuestra máquina puede tomar nota de todas las teclas que pulsamos, buscando el momento en que introducimos un usuario y contraseña. Si lo consigue, los envía al atacante.

- Fuerza bruta. Las contraseñas son un número limitado de caracteres (letras, números y signos de puntuación). Una aplicación malware puede ir generando todas las combinaciones posibles y probarlas una a una; tarde o temprano, acertará. Incluso puede ahorrar tiempo si utiliza un diccionario de palabras comunes y aplica combinaciones de esas palabras con números y signos de puntuación.

Contra los ataques de fuerza bruta hay varias medidas:

- Utilizar contraseñas no triviales. No utilizar nada personal e insertar en medio de la palabra o al final un número o un signo de puntuación. En algunos sistemas nos avisan de la fortaleza de la contraseña elegida.

- Cambiar la contraseña con frecuencia (un mes, una semana). Dependiendo del hardware utilizado, los ataques pueden tardar bastante; si antes hemos cambiado la clave, se lo ponemos difícil.

- Impedir ráfagas de intentos repetidos. Nuestro software de autenticación que solicita usuario y contraseña fácilmente puede detectar varios intentos consecutivos en muy poco tiempo. No puede ser un humano: debemos responder introduciendo una espera. En Windows se hace: tras cuatro intentos fallidos, el sistema deja pasar varios minutos antes de dejarnos repetir. Esta demora alarga muchísimo el tiempo necesario para completar el ataque de fuerza bruta.

- Spoofing. Alteramos algún elemento de la máquina para hacernos pasar por otra máquina. Por ejemplo, generamos mensajes con la misma dirección que la máquina auténtica.

- Sniffing. El atacante consigue conectarse en el mismo tramo de red que el equipo atacado. De esta manera tiene acceso directo a todas sus conversaciones.

- DoS (Denial of Service, denegación de servicio). Consiste en tumbar un servidor saturándolo con falsas peticiones de conexión. Es decir, intenta simular el efecto de una carga de trabajo varias veces superior a la normal.

- DDoS (Distributed Denial of Service, denegación de servicio distribuida). Es el mismo ataque DoS, pero ahora no es una única máquina la que genera las peticiones falsas (que es fácilmente localizable y permite actuar contra ella), sino muchas máquinas repartidas por distintos puntos del planeta. Esto es posible porque todas esas máquinas han sido infectadas por un troyano que las ha convertido en ordenadores zombis (obedecen las órdenes del atacante).

TIPOS DE ATACANTES

Se suele hablar de hacker de manera genérica para referirse a un individuo que se salta las protecciones de un sistema. A partir de ahí podemos distinguir entre:

- Hacker. Ataca la defensa informática de un sistema solo por el reto que supone hacerlo. Si tiene éxito, moralmente debería avisar a los administradores sobre los agujeros de seguridad que ha utilizado, porque están disponibles para cualquiera.

- Cracker. También ataca la defensa, pero esta vez sí quiere hacer daño: robar datos, desactivar servicios, alterar información, etc.

- Script kiddie. Son aprendices de hacker y cracker que encuentran en Internet cualquier ataque y lo lanzan sin conocer muy bien qué están haciendo y, sobre todo, las consecuencias derivadas de su actuación (esto les hace especialmente peligrosos).

- Programadores de malware. Expertos en programación de sistemas operativos y aplicaciones capaces de aprovechar las vulnerabilidades de alguna versión concreta de un software conocido para generar un programa que les permita atacar.

- Sniffers. Expertos en protocolos de comunicaciones capaces de procesar una captura de tráfico de red para localizar la información interesante.

- Ciberterrorista. Cracker con intereses políticos y económicos a gran escala.

BUENAS PRACTICAS DE SEGURIDAD INFORMATICA

Es muy dura la tarea del responsable de seguridad informática en una empresa grande: hay mucha información que proteger y múltiples puertas por donde sufrir intrusiones. Sus funciones son:

- Localizar los activos que hay que proteger: equipos, aplicaciones, datos y comunicaciones. Sobre todo, revisar la política de copias de seguridad: qué copiamos, cuándo copiamos, dónde lo copiamos, dónde guardamos de manera segura los dispositivos de copia, cómo verificamos que la copia se ha hecho bien, cuándo hacemos una prueba de recuperación de una copia, etc.

- Redactar y revisar regularmente los planes de actuación ante catástrofes, contemplando todas las posibilidades: ataque intencionado, desastre natural, arranque parcial de servicios (pocos servicios o todos los servicios pero con menor capacidad).

- No instalar nada que no sea estrictamente necesario, y revisar la configuración de los sistemas y aplicaciones por si estamos otorgando más permisos de los imprescindibles.

- Estar al día de todos los informes de seguridad que aparezcan. Para ello hay que registrarse en listas de correo sobre seguridad y, además, en las listas de nuestros proveedores (tanto de hardware como de software) para recibir sus noticias directamente.

- Activar los mecanismos de actualización automática de las aplicaciones que tenemos instaladas. Salvo sistemas delicados (tenemos que probar muy bien cada actualización antes de aplicarla), en general los fabricantes liberan actualizaciones que no dan problemas.

- Dar formación a los usuarios para que utilicen la seguridad y la vean como una ayuda, no como un estorbo.

- Revisar los log del sistema (el accounting que hemos visto antes). Algunas herramientas nos ayudan porque recogen los ficheros de log y aplican fácilmente muchos patrones conocidos (buscar la palabra error o warning, etc.).

- Considerar la opción de contratar una auditoría externa, porque si hemos cometido un error de concepto, es muy difícil que lo encontremos por nosotros mismos.

- Revisar la lista de equipos conectados: pueden haber introducido equipos no autorizados.

- Revisar la lista de usuarios activos: puede que algún empleado ya no esté en la empresa pero su usuario y todos los privilegios asociados siguen disponibles para él o para alguien de su confianza.

- En aquellos sistemas que lo permitan, configurar el aviso por SMS o correo electrónico para que nos enteremos los primeros de cualquier problema. Por ejemplo, los sistemas de baterías (SAI [sistema de alimentación ininterrumpida]) suelen tener esta funcionalidad.

Formalmente hay una serie de estándares sobre la seguridad informática. La normativa ISO/IEC 27002:2009 trata sobre la gestión de la seguridad de la información. En ella se propone implantar controles para afrontar los riesgos inherentes a los sistemas informáticos. Los controles incluyen políticas de empresa, estructura de la organización y procedimientos. Los controles se aplican a todas las partes afectadas: gestión de activos, seguridad sobre los recursos humanos (antes, durante y después de pertenecer a la empresa), seguridad física y ambiental, gestión de comunicaciones y operaciones, control de acceso, etc.

La segunda referencia mundial son las normas ITIL (Information Technology Infrastructure Library), que están orientadas a la gestión de servicios de tecnologías de la información, y uno de los aspectos que cubren es la seguridad.

SEGURIDAD PASIVA - EQUIPOS

UBICACIÓN DEL CPD

Las empresas colocan los equipos de usuario cerca del usuario (un ordenador sobre su mesa, un portátil que se lleva a casa); pero los servidores están todos juntos en una misma sala. Esa sala tiene varios nombres: CPD (centro de proceso de datos), centro de cálculo, DataCenter, sala fría, «pecera», etc. Centralizando se consigue:

- Ahorrar en costes de protección y mantenimiento. No necesitan duplicar la vigilancia, la refrigeración, etc.
- Optimizar las comunicaciones entre servidores. Al estar unos cerca de otros no necesitan utilizar cables largos o demasiados elementos intermedios que reducen el rendimiento.
- Aprovechar mejor los recursos humanos del departamento de informática. No tienen que desplazarse a distintos edificios para realizar instalaciones, sustituir tarjetas, etc.

Tan importante como tomar medidas para proteger los equipos es tener en cuenta qué hacer cuando esas medidas fallan. Todas las empresas deben tener documentado un plan de recuperación ante desastres, donde se describa con el máximo detalle (en una crisis no hay tiempo para reflexionar) qué hacer ante una caída de cualquiera de los servicios que presta el CPD. Este plan debe ser actualizado cuando se efectúe un cambio en el CPD (nuevo servicio, nuevo equipo). El plan debe incluir:

- Hardware. Qué modelos de máquinas tenemos instalados (tanto servidores como equipamiento de red), qué modelos alternativos podemos utilizar y cómo se instalarán (conexiones, configuración).
- Software. Qué sistema operativo y aplicaciones están instalados, con el número de versión actualizado y todas las opciones de configuración (permisos, usuarios, etc.).

- Datos. Qué sistemas de almacenamiento utilizamos (discos locales, armario de discos), con qué configuración y cómo se hace el respaldo de datos (copias de seguridad).

PROTECCIÓN

La informática es vital para la empresa: si los servidores se paran, la empresa se para. Sucede en todos los sectores: en una empresa de telefonía, en una compañía aérea, en unos grandes almacenes...

El CPD debe estar protegido al máximo:

- Elegiremos un edificio en una zona con baja probabilidad de accidentes naturales (terremotos, ciclones, inundaciones).

- También evitaremos la proximidad de ríos, playas, presas, aeropuertos, autopistas, bases militares, centrales nucleares, etc.

- Evitaremos ubicaciones donde los edificios vecinos al nuestro pertenezcan a empresas dedicadas a actividades potencialmente peligrosas: gases inflamables, explosivos, etc.

- Preferentemente seleccionaremos las primeras plantas del edificio.

    - La planta baja está expuesta a sabotajes desde el exterior (impacto de vehículos, asaltos, etc.).

    - Las plantas subterráneas serían las primeras afectadas por una inundación.

    - Las plantas superiores están expuestas a un accidente aéreo y, en caso de incendio iniciado en plantas inferiores, es seguro que nos afectará.

- Se recomienda que el edificio tenga dos accesos y por calles diferentes. Así siempre podremos entrar en caso de que una entrada quede inaccesible (obras, incidente, etc.).

- Es recomendable evitar señalizar la ubicación del CPD para dificultar su localización a posibles atacantes. La lista de empleados que entran a esa sala es muy reducida y saben perfectamente dónde está.

- Los pasillos que llevan hasta el CPD deben ser anchos porque algunos equipos son bastante voluminosos. Incluso conviene dotarlo de un muelle de descarga.

- El acceso a la sala debe estar muy controlado. Los servidores solo interesan al personal del CPD.

- En las paredes de la sala se deberá utilizar pintura plástica porque facilita su limpieza y se evita la generación de polvo.

- En la sala se utilizará falso suelo y falso techo porque facilita la distribución del cableado (para electricidad y comunicaciones) y la ventilación.

- La altura de la sala será elevada tanto para permitir el despliegue de falso suelo y falso techo como para acumular muchos equipos en vertical (Fig. 3.1), porque el espacio de esta sala es muy valioso.

- En empresas de alta seguridad, la sala del CPD se recubre con un cofre de hormigón para protegerla de intrusiones desde el exterior.

- Instalaremos equipos de detección de humos y sistemas automáticos de extinción de incendios, como los elementos del techo de la Figura.

- El mobiliario de la sala debe utilizar materiales ignífugos.

AISLAMIENTO

Las máquinas que situamos en el CPD utilizan circuitos electrónicos. Por tanto, hay que protegerlas ante:

- Temperatura. Los circuitos de los equipos, en especial los procesadores, trabajan a alta velocidad, por lo que generan mucho calor. Si además le sumamos la temperatura del aire, los equipos pueden tener problemas.

- Humedad. No solo el agua, también un alto porcentaje de humedad en el ambiente puede dañarnos. Para evitarlo utilizaremos deshumidificadores.

- Interferencias electromagnéticas. El CPD debe estar alejado de equipos que generen estas interferencias, como material industrial o generadores de electricidad, sean nuestros o de alguna empresa vecina.

- Ruido. Los ventiladores de las máquinas del CPD generan mucho ruido (son muchas máquinas trabajando en alto rendimiento), tanto que conviene introducir aislamiento acústico para no afectar a los trabajadores de las salas adyacentes.

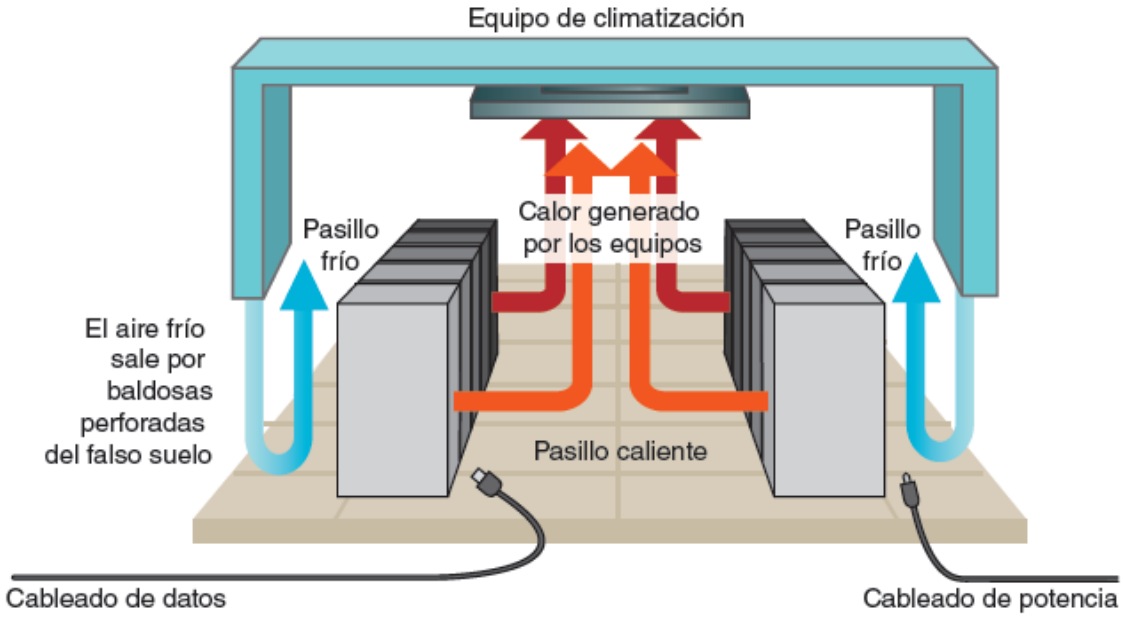
VENTILACIÓN

Los CPD no suelen tener ventanas. La ventilación que conseguiríamos con ellas sería mínima para todo el calor que se genera, y el riesgo de intrusiones desde el exterior (o simplemente la lluvia) no es admisible en una instalación de tanta importancia.

La temperatura recomendable en la sala estaría alrededor de los 22 grados. Las máquinas no lo necesitan, pero hay que pensar que ahí también van a trabajar personas. Para conseguirlo instalaremos equipos de climatización. Se suelen instalar por duplicado, para estar cubiertos ante el fallo de uno de los equipos.

En los CPD grandes se adopta la configuración de pasillos calientes y pasillos fríos. Las filas de equipos se colocan en bloques formando pasillos, de manera que todos los ventiladores que extraen el calor de la máquina (fuente de alimentación, caja de la CPU) apunten hacia el mismo pasillo. En este pasillo se colocan los extractores de calor del equipo de climatización. Ese mismo equipo introduce aire frío en los pasillos fríos, generalmente a través del falso suelo utilizando baldosas perforadas.

Si es posible, todo el cableado de potencia irá en los pasillos fríos (es peligroso sobrecalentarlos) y el cableado de datos en los pasillos calientes.



SUMINISTRO ELÉCTRICO Y COMUNICACIONES

Nuestro CPD no está aislado: necesita ciertos servicios del exterior. Los principales son la alimentación eléctrica y las comunicaciones. En ambos casos conviene contratar con dos empresas distintas, de manera que un fallo en una compañía suministradora no nos impida seguir trabajando.

El suministro eléctrico del CPD debería estar separado del que alimenta al resto de la empresa para evitar que un problema en cualquier despacho de ese edificio afecte a los servidores, porque están siendo utilizados por empleados de otros edificios, incluso por clientes y proveedores.

Para los sistemas críticos, en los que la empresa no puede permitirse ninguna interrupción del servicio, deberemos instalar generadores eléctricos alimentados por combustible.

En cuanto a las comunicaciones, conviene que el segundo suministrador utilice una tecnología diferente al primero. Por ejemplo, si tenemos una conexión ADSL, el segundo no debería ser ADSL también, porque comparten el mismo cable hasta llegar a la central: un fallo en ese cable nos desconectaría de los dos suministradores. En cualquier caso,

siempre conviene tener una tercera opción de conexión inalámbrica, por si el problema ocurre en la calle (obras en la acera, etc.).

CONTROL DE ACCESO

Las máquinas del CPD son vitales para la empresa y solo necesitan ser utilizadas por un reducido grupo de especialistas. El acceso a esta sala de máquinas debe estar especialmente controlado. No podemos consentir que alguien se lleve ninguna máquina o algún componente de ella (discos duros, cintas de backup) ni dejarle dentro intentando tener acceso desde las consolas de los servidores.

Las identificaciones habituales (contraseñas, tarjetas de acceso) se complementan con medidas más seguras, como la biometría. En instalaciones importantes, el CPD puede tener su propio equipo de vigilantes de seguridad. En la sala se suele instalar también una red de sensores de presencia y cámaras de vídeo para detectar visitas inesperadas.

CENTRO DE RESPALDO

A pesar de tanta protección, debemos pensar en la posibilidad de que ocurra una catástrofe en nuestro CPD y quede inservible (inundación, terremoto, sabotaje). La continuidad de la empresa no puede depender de un punto único de fallo; si disponemos de presupuesto suficiente, debemos instalar un segundo CPD.

Este segundo CPD, también llamado centro de respaldo (CR), ofrece los mismos servicios del centro principal (CP). Aunque, si la inversión en hardware resulta demasiado elevada, puede limitarse a los servicios principales, o a los mismos servicios pero con menos prestaciones. Por supuesto, debe estar físicamente alejado del CP; cuantos más kilómetros entre ambos, mejor.

En condiciones normales, el CR está parado (stand-by) esperando que, en cualquier momento, la empresa pueda necesitar detener el CP y activar el CR como nuevo CP. Los usuarios (empleados, clientes, proveedores) no deberían notar el cambio. Para ello, la información del CP también está en el CR. Esto incluye la configuración de los servicios; pero, sobre todo, los datos que han sido modificados en el último instante, antes de la conmutación de centros. Por tanto, no es suficiente con recuperar la última copia de seguridad del CP (sobre todo, porque la configuración puede ser distinta): debemos habilitar mecanismos especiales de réplica, en especial para las bases de datos, que son

más complejas que los sistemas de ficheros. Pero esto necesita de muy buenas comunicaciones entre el CP y el CR, con lo que la distancia que los separa puede ser un problema.

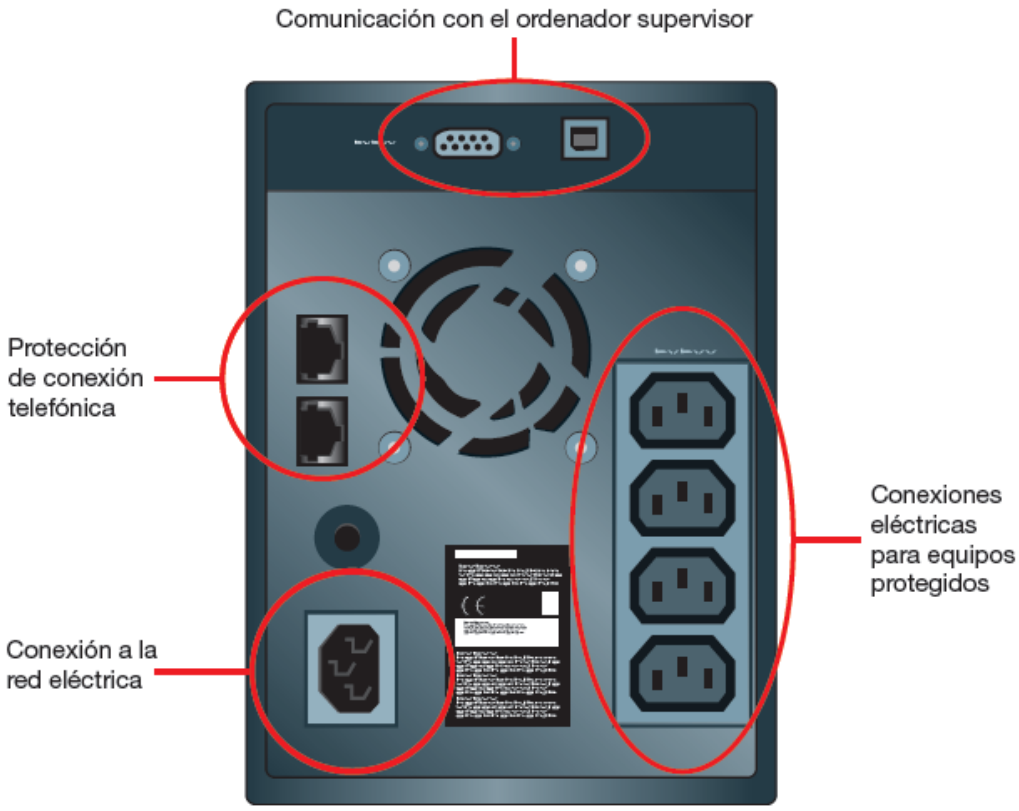
Como hemos señalado con anterioridad en el plan de recuperación ante desastres, puede que las circunstancias que nos lleven a conmutar el CR al CP sean muy urgentes y no haya tiempo para descubrir cómo se hace: todo el procedimiento de conmutación debe estar documentado con el máximo detalle, así como la posterior recuperación del CP, asumiendo los cambios ocurridos mientras estaba inactivo. Incluso conviene probarlo una vez al año para confirmar que los pasos están bien descritos y el personal está capacitado para ejecutarlos bien.

Los equipos del centro principal y el centro de respaldo constituyen los centros de producción de la empresa: están en funcionamiento para dar servicio a los empleados, clientes y proveedores de la misma. Pero no son las únicas salas con servidores y equipamiento de red. Cualquier cambio en las aplicaciones corporativas o la nueva web de la empresa no puede instalarse directamente en las máquinas de producción, porque un fallo no detectado puede bloquear algunas áreas de la empresa. Primero se prueba en un entorno controlado, llamado maqueta de preproducción, donde el personal de la empresa aplica el cambio. En esta fase hay un contacto directo con el suministrador del software para resolver inmediatamente cualquier contingencia.

SAI/UPS

La corriente eléctrica es vital en cualquier ordenador. Como no podemos confiar en que nunca va a fallar la empresa con la que hemos contratado el suministro eléctrico, tenemos que pensar en alternativas. En esta misma unidad hemos sugerido contratar un segundo suministrador o disponer de un generador propio (grupo electrógeno). Sin abandonar estas soluciones, en un CPD nunca debe faltar un SAI (sistema de alimentación ininterrumpida), en inglés UPS (Uninterruptible Power Supply).

Un SAI es un conjunto de baterías que alimentan una instalación eléctrica (en nuestro caso, equipos informáticos). La Figura siguiente corresponde a la vista trasera de un SAI. Lo enchufamos a la corriente eléctrica por la toma de la izquierda y ofrece cuatro enchufes en la derecha.



En caso de corte de la corriente, los equipos conectados al SAI siguen funcionando porque consigue electricidad de las baterías. La capacidad de estas baterías es reducida depende del SAI elegido y del consumo de los equipos, aunque el mínimo garantizado suele ser diez minutos. Este es el factor más importante a la hora de adquirir un SAI: cuántos vatios consumen los equipos que debe proteger y cuánto tiempo necesitamos que los proteja.

Al igual que ocurría con los equipos de climatización, si el presupuesto lo permite, conviene aplicar redundancia e instalar un doble juego de equipos SAI, para estar cubiertos en caso de que uno fallara. Esto es posible porque la mayoría de los servidores vienen con doble fuente de alimentación y conectaríamos una fuente a cada grupo de SAI.

Cuando ocurre un corte de luz, el SAI procede de esta manera:

- Espera unos minutos por si el corte ha sido puntual y el suministro se recupera inmediatamente por sí solo. Si no es así, ejecuta una parada ordenada de los equipos conectados al SAI. Siempre es mejor solicitar una parada al sistema

operativo y las aplicaciones que ejecuta que perder la corriente y confiar en que no se genere ninguna inconsistencia.

Conectar los equipos al SAI tiene otras ventajas:

- Suelen llevar un estabilizador de corriente que quita los picos, que también pueden ser muy dañinos.

- En algunos SAI también se incluye una entrada y salida de cable telefónico (conectores a la izquierda del ventilador en la Figura 3.10), que sirve para proteger nuestra conexión, porque las comunicaciones por línea telefónica también utilizan corriente eléctrica, luego también estamos expuestos a picos de tensión.

Tipos de SAI

Tradicionalmente, se han considerado dos tipos de equipos SAI:

- SAI en estado de espera (stand-by). Los equipos informáticos toman corriente del suministro principal, mientras el SAI se limita a vigilar que ese suministro fluya. Cuando ocurre un corte, el SAI activa inmediatamente sus baterías para que los equipos no se vean afectados (el tiempo de respuesta suele ser suficiente). A partir de ese momento, el SAI aplica los tiempos de espera señalados en el punto anterior. Cuando vuelve la corriente, desactiva la generación de corriente propia y empieza a cargar las baterías.

- SAI en línea (on-line). Los equipos siempre están tomando corriente de las baterías del SAI. Cuando ocurre un corte, el SAI se limita a aplicar los tiempos de espera. Cuando vuelve la corriente, empieza a cargar las baterías. La ventaja del SAI en línea es que no dependemos del tiempo de respuesta para activar las baterías; en cambio, la ventaja del SAI en espera es que podemos sustituir las baterías sin detener el suministro a los equipos conectados.

Monitorización de SAI

Cuando tenemos un SAI confiamos en que está bien y que responderá cuando sea necesaria su intervención. Pero conviene revisar regularmente el estado del SAI. Estos

equipos suelen incorporar unos indicadores luminosos en el frontal: si está cargando o descargando las baterías, porcentaje de batería restante, etc.

Sin embargo, es una información puntual y solo disponible si se está delante del equipo. Para mejorar su gestión, los SAI suelen incorporar un puerto de conexión con un ordenador.

En la Figura previamente mostrada vemos dos: un puerto serie y un USB. En ese ordenador instalaremos el software adecuado para comunicarse con el SAI y conocer no solo el estado actual, sino todas las veces que ha actuado en el pasado reciente. Por supuesto, ese ordenador debe estar protegido, sea por este SAI o por cualquier otro.

Triggers

El software del SAI, además de la monitorización, incluye la configuración de los comandos para responder ante un corte de corriente. En general, la respuesta consistirá en realizar la parada ordenada de los equipos protegidos. Son opciones principales de este tipo de software:

- Cuándo hacerlo: en un instante concreto (cuando se alcance Battery Backup Time) o cuando detecte que la carga de la batería está baja.
- Qué hacer con el sistema: suspenderlo o apagarlo.
- Qué comando ejecutar antes de empezar el apagado (Run Command File Before Shutdown). En este apartado aprovecharemos para apagar las otras máquinas conectadas a este SAI.
- Además de la opciones previas, se puede configurar un aviso por correo a los administradores del sistema desde el software del SAI.

SEGURIDAD PASIVA - ALMACENAMIENTO

ESTRATEGIAS DE ALMACENAMIENTO

Para una empresa, la parte más importante de la informática son los datos: sus datos.

Porque:

- El hardware es caro, pero se puede volver a comprar.
- Un informático muy bueno puede despedirse, pero es posible contratar otro.
- Si una máquina no arranca porque se ha corrompido el sistema de ficheros (el típico BSOD), puedes instalar de nuevo el sistema operativo y las aplicaciones desde los CD o DVD originales.

En todos los casos anteriores se recupera la normalidad en un plazo de tiempo razonable. Sin embargo, los datos de esa empresa son únicos: no se pueden comprar, no se pueden contratar, no hay originales. Si se pierden, no los podemos recuperar (por lo menos, ni fácil ni rápidamente).

Bien, puesto que los datos son tan importantes, hay que esforzarse especialmente en mejorar su integridad y disponibilidad:

- Podemos comprar los mejores discos del mercado en calidad (MTBF) y velocidad; aunque nunca debemos olvidar que son máquinas y pueden fallar (salvo los SSD, todos los discos tienen partes móviles). En un puesto de usuario nos lo podemos permitir (lo cambiamos y listo): en un servidor hemos visto que no.
- Podemos concentrar los discos en unos servidores especializados en almacenamiento.
- Podemos replicar la información varias veces y repartirla por ciudades distintas.
- Podemos contratar el servicio de respaldo de datos a otra empresa, conectados por Internet, para no depender de nuestros equipos y personal.

Cada empresa elegirá implementar una o varias, según sus necesidades y posibilidades.

RENDIMIENTO Y REDUNDANCIA. RAID EN WINDOWS Y LINUX

Los ordenadores pueden conectar varios discos internos porque las placas base suelen traer integrada una controladora de discos para dos o tres conexiones. Pero ¿para qué queremos varios discos en un ordenador? Por la misma razón por la que compramos CPU de varios núcleos o placas base con varias CPU.

Podemos aprovechar varios discos de un ordenador para:

- Crear unidades más grandes. Dos discos de 500 GB juntos nos pueden dar una unidad de 1 TB. Con tres discos tenemos 1,5 TB, etc. Por ejemplo, si queremos ripear un Blu-ray de 25 GB y solo tenemos discos de 20 GB, necesitamos juntar dos en una unidad de 40 GB. O, si queremos darle al /home 2 TB y solo tenemos discos de 640 GB, podemos juntar tres.

- Crear unidades más rápidas. Si tenemos dos discos de 500 GB y configuramos el sistema para que, en cada fichero, los bloques pares se escriban en un disco y los impares en otro, después podremos hacer lecturas y escrituras en paralelo (en el mejor caso, ahorramos la mitad de tiempo). Con un único disco de 1 TB tenemos la misma capacidad, pero cada lectura o escritura debe esperar que termine la operación anterior. La diferencia es más notable si ponemos tres discos, cuatro, etc.

- Crear unidades más fiables. Si configuramos los dos discos anteriores para que, en cada fichero, los bloques se escriban a la vez en ambos discos, podemos estar tranquilos porque, si falla un disco, los datos estarán a salvo en el otro.

Pues una de las tecnologías que lo consigue se llama RAID. Hay varios niveles de RAID.

Los más importantes son:

- RAID 0. Agrupamos discos para tener un disco más grande, incluso más rápido. Desde ese momento, los bloques que lleguen al disco RAID 0 se escribirán en alguno de los discos del grupo. Por supuesto, para el usuario este proceso es transparente: él solo ve un disco de 1 TB donde antes había dos discos de 500 GB. En el RAID 0 podemos elegir entre spanning y striping (que es lo más común). En cualquier caso, si falla uno de los discos, lo perdemos todo.

- RAID 1. Se le suele llamar mirror o espejo. Agrupamos discos por parejas, de manera que cada bloque que llegue al disco RAID 1 se escribirá en los dos discos a la vez. Si falla uno de los discos, no perdemos la información, porque estará en el otro. A cambio, sacrificamos la mitad de la capacidad (el usuario ha conectado dos discos de 500 GB y solo tiene disponibles 500 GB, en lugar de 1 TB) y no ganamos rendimiento.

- RAID 5. Hemos visto que el RAID 0 es más rápido que cada uno de los discos, pero tan seguro como cualquiera de ellos. El RAID 1 es más seguro que los discos por separado, pero con el mismo rendimiento. El RAID 5 consigue ambas cosas aplicando dos mecanismos:

    - Para cada dato que el sistema quiere almacenar en el RAID, este aplica un procedimiento matemático (en general, la paridad) para obtener información complementaria a ese dato, de tal manera que se puede recuperar el dato en caso de perder cualquier disco (sea disco de datos o paridad).

    - Una vez obtenida la paridad, se hace striping para repartir el dato y su paridad por los discos conectados al RAID.

ALMACENAMIENTO EN RED: NAS Y SAN. CLÚSTERS

Hemos visto que podemos mejorar el rendimiento y la fiabilidad del almacenamiento de un ordenador conectando varios discos y configurándolos en RAID.

Pero en las empresas se suele trabajar en equipo, compartiendo ficheros entre varios ordenadores.

Tenemos que pensar cómo compartir ficheros y cómo hacerlo con seguridad (quién puede leer esos ficheros y quién puede modificarlos, borrarlos o incluir nuevos).

Aunque en el caso práctico 4 veremos cómo se hace en un ordenador de un puesto de trabajo, no es la solución más recomendable porque:

- Hacer de servidor de ficheros afectará al rendimiento de sus aplicaciones (Office, Chrome), y viceversa.

- Estaríamos pendientes de si la otra persona lo ha apagado al salir de la oficina (y puede que estemos en edificios diferentes).

- Es un ordenador personal, luego es probable que no disponga de RAID ni copias de seguridad.

- Estamos expuestos a que un virus entre en ese ordenador y borre todo.

Por tanto, lo mejor es ponerlo en un servidor dedicado y, a ser posible, especializado en almacenamiento. De esta manera:

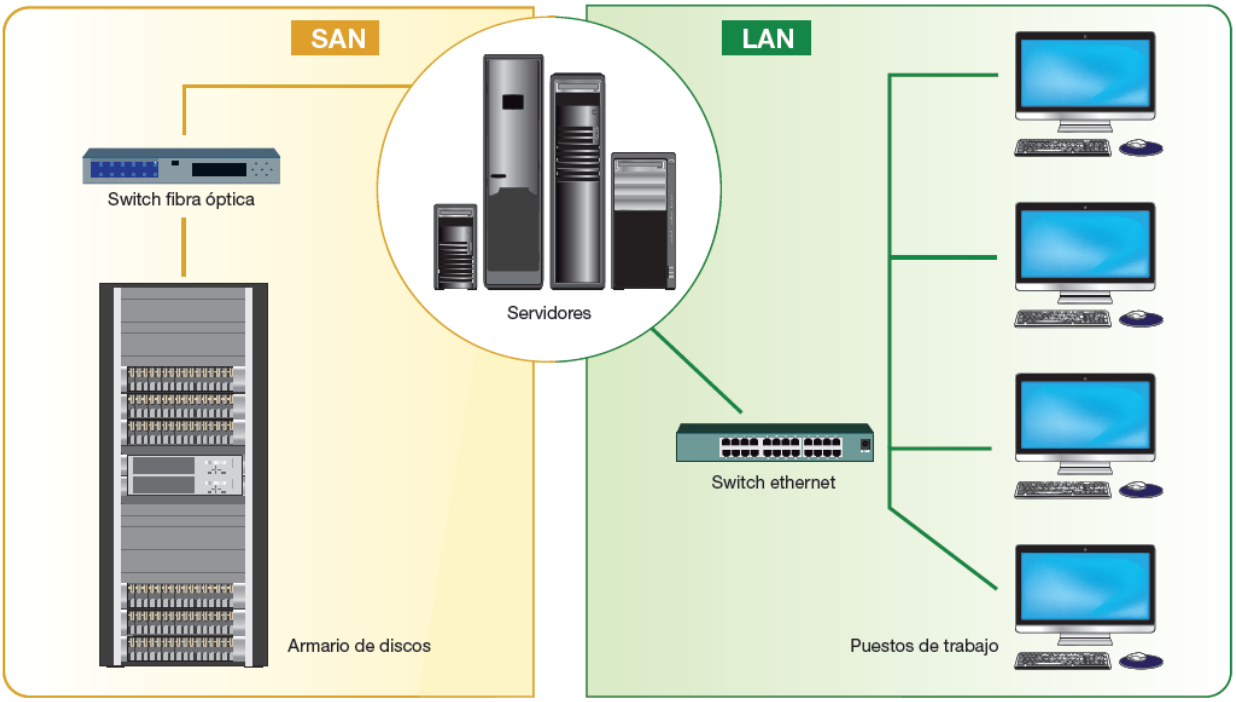
- Podemos instalar el software estrictamente necesario y tenerlo actualizado (menor riesgo de infecciones).

- Estará bajo la supervisión del personal del CPD (centro de proceso de datos), lo que garantiza estar encendido todo el tiempo, formar parte de la política de copias de seguridad de la empresa, detectar cuando el disco está próximo a llenarse, etc.

- Si, además, es un servidor especializado en almacenamiento, dispondrá de hardware suficiente para desplegar configuraciones RAID, una memoria caché de alto rendimiento, etc.

En un entorno privado puede ser suficiente con un pequeño equipo que haga de servidor NAS; pero en un entorno empresarial necesitamos mucho más rendimiento y seguridad, por lo que el equipo servidor necesitará potencia de procesamiento, amplia memoria caché, tarjetas de red de alta capacidad y configuraciones RAID.

Si otros servidores también lo necesitan, seguramente optaremos por una solución SAN (Storage Area Network). En un SAN los discos están en lo que se llama un «armario», donde se realiza la configuración RAID. El armario dispone de cachés de alto rendimiento para reducir los tiempos de operación. Los servidores se conectan al armario mediante conmutadores de fibra óptica (por eso hablamos de network). La configuración de los armarios es flexible: para cada equipo se pueden asignar unos discos concretos y reservarle cierta cantidad de caché. Y cambiarlo cuando sea necesario.



El almacenamiento compartido es especialmente importante en los clústers. Un clúster es un conjunto de máquinas (llamadas nodos) coordinadas para realizar una tarea en común. Puede ser una base de datos, un servidor web, un sistema de gestión de redes, búsqueda de vida extraterrestre (SETI), almacenamiento compartido en Internet (P2P, como eMule, que veremos en el siguiente apartado), etc.

Cada máquina ejecuta una parte de la funcionalidad y está coordinada con el resto de las máquinas. Para ello necesitan un determinado software de clúster instalado en todas ellas y, sobre todo, un almacenamiento fiable y de alto rendimiento, porque los nodos intercambian mucha información.

ALMACENAMIENTO EN LA NUBE Y P2P

Supongamos que nuestra empresa ya tiene en sus instalaciones NAS (disco en red) y SAN (discos de alto rendimiento, capacidad y seguridad). Pero hay más necesidades:

- Queremos colgar ficheros para nuestros clientes y proveedores.
- Cuando estamos fuera de la oficina podemos necesitar algún fichero (un presupuesto, un contrato).
- Vamos a continuar en casa un trabajo que tenemos a medias.

- Simplemente queremos una copia de unos documentos importantes en otro lugar que no sea la oficina.

Para un empleado, una solución simple es guardarlo todo en un pendrive USB. Pero se pierden con demasiada facilidad (y la información que va puede ser muy importante: conviene haberla cifrado) y además no podríamos trabajar simultáneamente con otros compañeros (aunque cada uno lleve su pendrive, los siguientes cambios no estarían sincronizados). La solución habitual era abrir un acceso directo desde Internet hasta los discos de la empresa. Funciona, aunque es delicado, porque al final es una «puerta trasera» por donde pueden intentar entrar hackers, y llegar hasta esos discos o cualquier otro servidor nuestro.

Como alternativa, en los últimos años han aparecido multitud de servicios de Almacenamiento en la nube:

- La primera generación (Megaupload, FileServe, etc.) consiste en que un usuario sube un fichero a una web para que lo descarguen otros usuarios conectados a esa web. Pero resulta incómodo, primero porque solo almacena ficheros, sin una estructura de carpetas; y, segundo, porque si queremos todos los ficheros de una carpeta, hay que ir uno por uno, o comprimirlos en un zip y subirlo.

- La segunda generación (Dropbox, iCloud, Box.net, Skydrive, GoogleDrive) es más simple: directamente sincronizan carpetas de los dispositivos (ordenador personal, móvil, tableta) entre sí y con los servidores del proveedor (Fig. 4.57). Cualquier cambio que hagas en cualquier dispositivo automáticamente ocurre en los demás dispositivos y en el disco del proveedor, sin necesidad de acordarse de conectar a una web y hacer la descarga (aunque también está disponible).

Todos estos servicios tienen ventajas e inconvenientes:

- Nuestros datos están fuera de nuestras instalaciones, por lo que podemos acceder a ellos a cualquier hora, sin estar allí, y con la tranquilidad de que cualquier desastre que ocurra en la oficina no les afectará.

- La empresa proveedora del servicio de almacenamiento en la nube se preocupa por hacer copias de seguridad de los datos que subimos; incluso suelen conservar versiones anteriores de cada fichero que modificamos.

- La conectividad a Internet de estas empresas suele ser muy superior a la nuestra, por lo que el acceso es rápido. Y al mismo tiempo no ocupamos ancho de banda de nuestra conexión.

- Sin embargo, perdemos el control sobre el acceso a nuestra información. Tenemos que confiar en la capacidad técnica y humana del proveedor de almacenamiento en la nube para evitar ataques sobre sus servidores (de nuevo, conviene cifrar los archivos que subimos a la nube). Y confiar también en que no incurre en prácticas delictivas, como el caso Megaupload, que cierra el servicio a todos los clientes, inocentes o no.

Las soluciones P2P (peer to peer) están muy extendidas entre particulares (eMule, Torrent); las empresas no suelen recurrir a ellas para información confidencial porque, si en almacenamiento en la nube teníamos que desconfiar de un proveedor, en P2P son miles. Pero sí son interesantes para difusión de contenidos, como hace PandoNetworks.

BACKUP DE DATOS

Ni el RAID 1 ni el RAID 5 nos permiten dormir tranquilos. Estamos protegidos ante el fallo de uno de los discos, pero no si fallan dos. O si se incendia la sala y arde el servidor. O si alguien accede a la máquina y la formatea. Podemos ver el RAID como una forma de seguir funcionando, aunque haya fallecido uno de los discos. Pero nuestros datos son más importantes y hay que seguir protegiéndolos. Por eso haremos copias y las llevaremos lo más lejos posible. Primero vamos a distinguir entre:

- Backup de datos. Copia de seguridad de los datos del usuario o empresa que están almacenados en un ordenador.

- Imagen del sistema. Copia de seguridad de los programas (sistema operativo y aplicaciones) que están instalados en un ordenador.

Normalmente se hace una imagen del sistema justo después de instalarlo y configurarlo, o después de la instalación de una aplicación importante. En cambio, el backup de datos hay que hacerlo diariamente, incluso con más frecuencia, dependiendo de la actividad de la empresa.

El segundo paso es identificar los datos que tenemos que salvar. Aquí tenemos que distinguir entre:

- Ficheros. Pueden ser unidades enteras, la típica carpeta Mis Documentos, etc. Existe la complicación de detectar los ficheros que están siendo modificados precisamente cuando se ha lanzado la copia.

- Sistemas complejos, como las bases de datos, donde la concurrencia de cambios suele ser mucho más alta que con ficheros, porque una operación afecta a varias tablas. Por este motivo, los servidores de base de datos tienen sus propios mecanismos de exportación del contenido de las tablas.

Finalmente, para cada tipo de información identificada en el paso anterior, hay que acordar la frecuencia de respaldo. En un supermercado, para la base de datos de empleados puede ser suficiente efectuar una copia diaria o semanal; pero la base de datos de ventas no puede esperar tanto.

TIPOS DE DISPOSITIVOS LOCALES Y REMOTOS

Una vez hemos confirmado qué información del disco duro queremos conservar y con qué frecuencia, hay que decidir dónde hacemos la copia: soporte físico y ubicación de este soporte físico. En cuanto al soporte físico, podemos pensar en:

- Usar otra partición del mismo disco duro. No es buena idea, porque si falla el disco, lo perdemos todo. Por cierto, esta es la solución de los ordenadores personales para evitar entregar DVD de instalación del sistema operativo.

- Usar otro disco de esa máquina; pero si se destruye la máquina, lo perdemos todo.

- Pasarlo a un disco duro extraíble para llevárnoslo, o quizá el disco duro de otra máquina al que accedemos por FTP. Sería aceptable, pero los discos duros son relativamente caros; por lo menos, mucho más que otras tecnologías de almacenamiento, como las cintas o los discos ópticos (CD/DVD/BR), que además son fáciles de transportar y realmente no necesitamos las elevadas prestaciones de un disco duro (no vamos a estar leyendo y escribiendo continuamente; solo durante la copia).

- Si podemos elegir entre cintas y discos, mejor las cintas porque tienen más capacidad y son más fiables y reutilizables. Las cintas más usadas son las LTO (Linear Tape- Open).

En cualquier caso, y sobre todo si vamos a utilizar soportes extraíbles, que se pueden extraviar, debemos preocuparnos por cifrar el contenido. Esto ya lo hace la mayoría de los programas de backup, incluso se puede hacer en el hardware, en el dispositivo de escritura.

La facilidad de extraer un soporte y poner otro es vital. Primero porque evitamos estar siempre utilizando el mismo elemento, lo que acelera su deterioro, y sobre todo porque las copias de seguridad, si podemos, hay que conservarlas lo más alejadas posible del disco copiado, para evitar que un desastre en la sala de ordenadores también termine con las copias. Por ello:

- Si nuestra empresa tiene dos sedes, conviene que las cintas de una sede se intercambien con las cintas de la otra por mensajería.

- Si solo hay un edificio, en la parte opuesta al CPD.

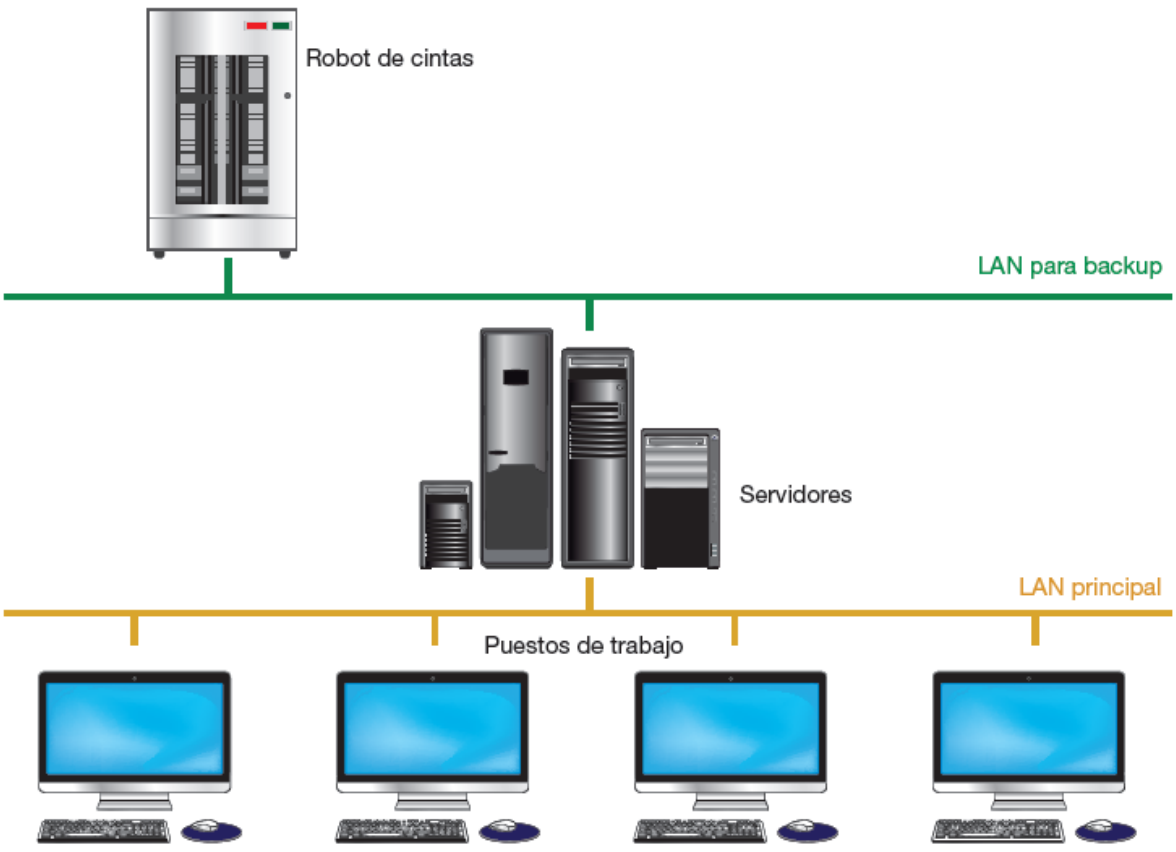
- Deben estar siempre en una sala con control de acceso, para evitar que cualquiera llegue hasta nuestros datos.

- Dentro de la sala, hay que meterlas en un armario ignífugo.

Una vez elegido el soporte, hay que decidir dónde ponerlo. Podríamos comprar uno para cada servidor como dispositivo local (Fig. 4.65), pero resulta caro y laborioso, dado que vamos a utilizar varias cintas (por ejemplo, una para cada día de la semana) y alguien debería ir máquina por máquina cambiando las cintas, y etiquetando perfectamente de

qué máquina son y a qué día corresponden. Interesa centralizar estas tareas repetitivas y que las hagan máquinas, no personas. En las empresas se suele instalar una librería de cintas (robot de cintas), donde se hace el backup de todos los servidores de la empresa y también aquellos puestos de trabajo que lo necesiten. Cada cinta está etiquetada y el robot mantiene una base de datos donde registra qué cinta utilizó en cada momento. Las etiquetas suelen ser códigos de barras y también RFID.

Este dispositivo remoto está conectado a la LAN de la empresa o directamente a los servidores mediante SAN. Ejecuta un software servidor que conecta con un software cliente instalado en cada equipo seleccionado. Normalmente, la red que utiliza es una LAN o VLAN distinta a la LAN de trabajo (los ordenadores con función de servidor suelen llevar dos interfaces de red). Al utilizar una LAN diferente, la actividad de la empresa no se ve afectada por el tráfico de backup, y viceversa.



TIPOS DE COPIAS

Como hemos visto antes, cada empresa debe identificar qué datos quiere proteger mediante copia de seguridad. Hay tres tipos de copia:

- Completa. Incluye toda la información identificada. Si era una unidad de disco, todos los archivos y carpetas que contiene; si era una base de datos, la exportación de todas sus tablas.

- Diferencial. Incluye toda la información que ha cambiado desde la última vez que se hizo una copia de seguridad completa. Por ejemplo, si el lunes se hizo una completa y el martes solo ha cambiado el fichero a.txt, en la cinta del martes solo se escribe ese fichero. Si el miércoles solo ha cambiado el fichero b.doc, en la cinta del miércoles se escribirán a.txt y b.doc.

- Incremental. Incluye toda la información que ha cambiado desde la última copia de seguridad, sea completa o incremental. En el ejemplo anterior, la cinta del martes llevará el fichero a.txt, pero la cinta del miércoles solo b.doc.

Una empresa podría decidir hacer todos los días copia completa. Pero, si hay muchos datos, es un proceso lento y algo arriesgado, porque hay que vigilar que se esté haciendo una copia consistente de la información (mientras se hace la copia, el sistema sigue funcionando y en cualquier momento alguien puede introducir cambios). Con la copia diferencial o incremental tenemos las mismas garantías, porque recuperamos la información aplicando la última cinta completa y la última diferencial (o la última completa y todas las incrementales).

En una empresa mediana es habitual el esquema de diez cintas:

- Una para un backup completo (los viernes).

- Cuatro para un backup parcial diario (diferencial o incremental) de lunes a jueves.

- Cinco para backups completos anteriores: quincenal, mensual, trimestral, semestral y anual.

Elegir entre diferencial o incremental para el backup diario depende de cada empresa. Si hay poca actividad diaria, se puede permitir el diferencial, porque aporta la ventaja de que

cada cinta diaria tiene toda la información necesaria para recuperar ese día (en el incremental, si perdemos la cinta de un día, puede que tenga ficheros que no estén en las cintas siguientes). Pero si hay mucha actividad, estamos de nuevo ante el problema de mantener la consistencia de la copia.

IMAGEN DEL SISTEMA

La imagen del sistema no es tan importante como los datos, porque en último extremo podríamos instalar desde cero, con el CD/DVD del sistema operativo y las aplicaciones necesarias, y después aplicaríamos a ambos las opciones de configuración que tenemos documentadas. Pero este proceso es lento y generalmente necesita que un técnico esté presente (y también se puede equivocar); una imagen nos ayudará a recuperar el sistema rápidamente y sin errores.

La imagen de un sistema es un volcado del contenido del disco duro. Con todo: ejecutables y datos del sistema operativo, ejecutables y datos de las aplicaciones instaladas y datos personales de los usuarios. Generalmente se comprime en un único fichero que ocupa muchos gigabytes, dependiendo del tamaño del disco, la ocupación y el tipo de contenidos. Ese fichero suele estar cifrado y se almacena lejos del sistema original, como hacemos con las cintas del backup.

Como hemos explicado antes, la imagen no es un método adecuado de hacer copias de seguridad en una empresa. Es cierto que copiamos todo, programas y datos, pero es un proceso lento durante el cual el sistema no está operativo, lo que es incompatible con la misión crítica que la informática desempeña en una empresa.

Creación y recuperación. LiveCD

Existen varias herramientas en los distintos sistemas operativos para crear y recuperar imágenes (Norton Ghost, Acronis True Image), pero presentan el inconveniente de ser formatos propietarios, de manera que para recuperarlas necesitas el mismo programa (incluso la misma versión), lo cual puede ser un problema en determinadas circunstancias.

Nosotros vamos a estudiar una solución sencilla y genérica, disponible para cualquier plataforma hardware habitual. Consiste en la utilización de un LiveCD Linux, con el cual arrancaremos el ordenador cuyo disco queremos clonar. Una vez dentro, elegiremos el

dispositivo local o remoto donde almacenar la imagen (generalmente, un disco USB) y procederemos a ejecutar la copia.

Por supuesto, una solución alternativa es apagar el ordenador, extraer el disco duro, ponerlo en otro ordenador y hacer la copia allí. El LiveCD nos ahorra esas manipulaciones. Las ventajas del LiveCD son:

- Es una solución válida para clonar sistemas Windows o Linux en cualquiera de sus versiones, porque trabajamos directamente con el disco, sin importar qué hay dentro.

- Es una solución válida para cualquier hardware convencional, porque Linux funciona en casi todas las plataformas.

- Es una solución interoperable: el formato del fichero es estándar, de manera que un fichero creado con un LiveCD se puede recuperar con otro LiveCD diferente.

Los inconvenientes son:

- Como cualquier imagen, hay que recuperarla entera, no hay opción de elegir carpetas o ficheros.

- Durante la recuperación estamos escribiendo en todo el disco; un error en un sector puede interrumpir la operación.

- El tamaño del disco donde recuperamos debe ser el mismo o superior al del disco original.

- No incluye opciones avanzadas, como dejar la imagen en el mismo disco e instalar un gestor de arranque que permita recuperarla fácilmente, como ocurre en los ordenadores actuales. Aunque es una opción poco fiable, porque el daño del disco que nos lleva a recuperar la imagen le puede haber afectado a ella.

Por muchas medidas de control de acceso que pongamos, un hacker puede sentarse delante de un equipo de nuestra empresa. O directamente robar un portátil a uno de nuestros directivos. Vamos a intentar ponérselo difícil para que su «trabajo» sea una carrera de obstáculos y, seguramente, ante alguna barrera, desista.

LA CAJA DEL ORDENADOR

Lo primero es evitar que pueda abrir la caja del ordenador para llevarse el disco duro y «destriparlo» tranquilamente en casa. La mayoría de las cajas de los ordenadores de sobremesa llevan un par de anclajes donde colocar un candado normal. También está la opción de cambiar un tornillo normal por un tornillo con llave.

Para los portátiles tenemos el famoso candado Kensington, que tiene una cabeza que se introduce por una ranura especial de la caja del portátil. La cabeza continúa en un cable de acero para que lo enrollemos en alguna parte fi ja (la mesa o algún anclaje especial). La cabeza puede utilizar una llave o una combinación de números.

Los candados son poco efectivos, pero por lo menos obligamos al ladrón a traer alguna herramienta más y le hacemos perder un tiempo precioso. Incluso si lo abre, la mayoría de las cajas de ordenador profesionales llevan un detector que graba en la memoria de la BIOS la fecha y hora en que se ha producido la apertura. Al día siguiente, cuando el empleado encienda el ordenador, aparecerá un mensaje en pantalla avisándole.

LA BIOS DEL ORDENADOR

Con el candado, el hacker ya no se podrá llevar el disco. Pero en la Unidad 4 hemos visto que, utilizando la técnica del arranque con LiveCD, montábamos tranquilamente el disco duro local y hacíamos una copia del mismo en un dispositivo externo.

Para evitar que un hacker haga lo mismo, hay que entrar en la BIOS para modificar el orden de arranque. Por defecto suele estar puesto primero el CD/DVD y después el disco duro local HDD (Hard Disk Drive). Debemos cambiarlo para que el primero y único sea el HDD (si algún día hace falta otra cosa, siempre podremos volver aquí).

Esta tarea se suele hacer cuando llega un nuevo equipo a la empresa. Tampoco hay que olvidar cambiar las contraseñas del administrador, porque si no ponemos ninguna o dejamos los valores por defecto, el hacker puede entrar a la BIOS y modifi car el orden de arranque.

En algunas empresas incluso activan una contraseña de uso del ordenador. Es decir, al arrancar la BIOS siempre pide una contraseña, no solo cuando queremos acceder a su configuración.

Si hemos olvidado las contraseñas de la BIOS, la solución típica es retirar la pila que mantiene esos valores en memoria. En las placas base modernas directamente hay un jumper que, si está cerrado cuando el ordenador arranca, borra esos valores. Por ambos motivos (pila o jumper) hay que seguir evitando el acceso al interior de la caja del ordenador.

EL BOOT MANAGER

Ya hemos conseguido que el hacker no se pueda llevar nada y solo arranque la máquina desde nuestro disco local. En este disco puede ocurrir que tengamos instalados varios sistemas operativos (o varias versiones del mismo sistema, como suele ocurrir en Linux), de manera que, al arrancar, un programa llamado boot manager (gestor de arranque) nos permite elegir uno de ellos. Ahora hay que establecer quién accede a cada opción.

CIFRADO DE PARTICIONES

Con las barreras que hemos puesto hasta ahora, el hacker no se puede llevar nada; solo puede arrancar desde el disco local y solo puede elegir alguna de las entradas del boot manager. Pero si alguna de estas medidas falla, todavía podemos evitar que acceda a nuestros datos: vamos a cifrar el contenido, de manera que sea ilegible.

AUTENTICACIÓN EN EL SISTEMA OPERATIVO

Hemos conseguido que nuestro hacker no pueda evitar que la máquina arranque con un sistema operativo instalado por nosotros. Comparado con lo que hemos visto hasta ahora (BIOS, boot manager), los sistemas operativos permiten incluir mucho más software de autenticación y más complejo. Veremos múltiples mecanismos para asegurarnos de que nuestro sistema solo lo usa quien está autorizado para ello.

USUARIO/PASSWORD

Es el mecanismo más típico. Aplicando la estrategia «algo que sabes», la pantalla inicial del sistema espera que la persona introduzca el nombre de un usuario y la contraseña asociada a ese usuario. Mientras lo teclea, el nombre del usuario es visible pero la contraseña no (se suele sustituir por asteriscos, guiones, etc.), para evitar que la vea alguien que se encuentre a nuestra espalda.

Si nos equivocamos, bien porque el usuario no existe, bien porque la contraseña no es la correcta, el sistema nos impide la entrada y nos deja intentarlo de nuevo. En algunos sistemas nos ofrece una pista sobre la contraseña (si la pusimos la última vez que cambiamos la contraseña), y la mayoría tiene un límite de intentos. Alcanzado ese límite, el sistema se puede bloquear durante un tiempo o defi nitivamente (por ejemplo, los móviles tienen un límite de tres intentos para introducir el PIN). Con este límite evitamos ataques de fuerza bruta que prueben una a una todas las combinaciones de letras, números y caracteres especiales.

TARJETAS

En algunas ocasiones, el mecanismo de usuario y contraseña no es sufi ciente: es inseguro (alguien puede espiar qué teclas pulsamos) o simplemente molesto (por ejemplo, en los tornos de acceso a la entrada de la empresa no podemos perder el tiempo tecleando).

Para estos casos aplicaremos la estrategia «algo que tienes» y repartiremos tarjetas entre los usuarios. Por ejemplo, los cajeros automáticos de los bancos aplican una seguridad doble: la tarjeta más un número PIN.

Las tarjetas son de dos tipos: sencillas (magnéticas, RFID) o complejas (chip). Las magnéticas van desapareciendo porque las RFID son igual de baratas y no sufren borrados accidentales (en Londres y Madrid ya se utilizan para el abono de transporte).

Las tarjetas con chip son más seguras pero más caras, por lo que se utilizan en ocasiones especiales. Hay dos tipos:

- Las que son simplemente un dispositivo de almacenamiento: contienen nuestras claves para que las lea el dispositivo donde introducimos la tarjeta.

- Las que constituyen un dispositivo de procesamiento: contienen nuestras claves, pero nunca salen de la tarjeta. El chip se limita a cifrar con ellas algún desafío que lanza el dispositivo por donde introducimos la tarjeta.

BIOMETRÍA

La seguridad del mecanismo usuario/contraseña es sufi ciente para la mayoría de las aplicaciones. La tarjeta es cómoda. Pero cualquiera podría sentarse en nuestro ordenador, insertar nuestra tarjeta (robada o duplicada), introducir nuestro usuario y contraseña (nos puede haber espiado, o se la dijimos al irnos de vacaciones) y acceder al sistema como si fuéramos nosotros mismos. Si la información que manejamos es importante, aplicaremos la estrategia «algo que eres», para complementar el mecanismo usuario/contraseña con un control más: la biometría.

La biometría consiste en identificar alguna característica física del sujeto: la huella dactilar, el ojo, la voz. La persona o personas autorizadas deben grabar primero su característica física. Por ejemplo, en la huella se graban dedos de las dos manos, por si se sufre un accidente en una de ellas. Después, cada vez que quieran utilizar el ordenador, deberán situar el dedo encima del sensor.

Como hemos dicho antes, el control biométrico no es sustitutivo del usuario/contraseña, sino complementario: conviene tener los dos para aumentar la seguridad (estrategia «algo que sabes, algo que eres»). Aunque en algunas ocasiones sí se utiliza individualmente para ahorrar la molestia de estar pulsando teclas: por ejemplo, para acceder a alguna zona vip de la empresa.

ELEVACIÓN DE PRIVILEGIOS

Ya estamos autenticados en el sistema operativo y podemos trabajar con él, pero siempre limitados a los privilegios asociados al usuario con el que nos hemos presentado.

En las empresas, la mayoría de los empleados utilizan usuarios que no tienen permiso para realizar tareas de administración de la máquina (usuarios limitados, no administradores); así se reduce el daño que puedan causar, ya sea por error o porque se ha colado un virus.

Pero hay determinadas situaciones (instalación de nuevos programas, modificación de parámetros del sistema) para las que sí necesitamos ser administradores.

Una solución es salir del usuario actual y entrar como administrador, pero es más sencillo solicitar, de manera puntual, una elevación de privilegios. Consiste en pedirle al sistema ejecutar un determinado programa con permisos de administrador. Se aplica solo a ese programa y solo a esa ejecución: no afecta a las aplicaciones abiertas antes o después, ni siquiera cuando abramos ese mismo programa más adelante.

En cuanto al usuario, dependiendo de la configuración del sistema, simplemente aparecerá una ventana de confi rmación o nos pedirá una nueva autenticación.

CUOTAS

Hasta ahora hemos protegido nuestros sistemas evitando el acceso de personas no autorizadas; ahora vamos a protegerlos de las personas que sí están autorizadas. Porque nuestros usuarios, con intención o no, también pueden dañar el sistema. Por ejemplo, pueden descargar muchos archivos pesados, de manera que llenan el disco y el sistema empieza a fallar porque siempre necesita escribir en algunos fi cheros (el típico error fi lesystem full); también pueden lanzar procesos muy pesados, que ralentizan la CPU y no permiten trabajar a los demás usuarios.

Para evitarlo, los sistemas se confi guran para aplicar cuotas. Para el disco, se establece que cada usuario puede ocupar un número determinado de bytes (megabytes, gigabytes).

Cuando excede ese límite, podemos confi gurar de modo que el sistema no le permita extenderse más.

Hay que asignar las cuotas con cuidado:

- Si son muy bajas, tendremos a los usuarios quejándose todos los días porque no les dejamos trabajar. Hay que tener especial cuidado con los usuarios que se crean porque son necesarios para arrancar una aplicación, como el www-data del servidor web Apache: si exceden la cuota, la aplicación se parará.

- Si son muy altas, no tendrán el efecto disuasorio que se espera de ellas y, al final, terminaremos comprando más disco.

ACTUALIZACIONES Y PARCHES

Ya tenemos el sistema protegido contra el acceso de extraños y contra el mal uso de los propios. Pero estamos hablando de software: hecho por humanos y, por tanto, sujeto a errores.

El CD/DVD que hemos utilizado para instalar Windows contiene una versión concreta liberada en una fecha concreta; desde entonces, los programadores de Microsoft han seguido trabajando. El resultado son las actualizaciones: paquetes de software donde se introducen mejoras y, sobre todo, corrigen defectos.

Como administradores responsables del sistema, debemos instalar esas actualizaciones. Por suerte, no hace falta esperar a que nos llegue otro CD con cada actualización: se descarga automáticamente desde Internet.

Microsoft libera actualizaciones de forma rutinaria, y Service Pack, cada dos semanas, los martes por la noche; pero si encuentran la solución a un problema urgente, lo liberan inmediatamente, sin esperar al siguiente martes. Las actualizaciones se configuran desde el panel de control.

Podemos elegir entre:

- No buscar actualizaciones ni instalarlas (no recomendable).
- Comprobar si hay actualizaciones, pero no descargarlas ni instalarlas. Esto solo tiene sentido en equipos con poco disco o acceso limitado a Internet.
- Descargar actualizaciones, pero no instalarlas. En algunos sistemas podemos tener una configuración muy sensible a cambios en el sistema operativo.
- Descargar e instalar siempre. Es lo más habitual en los puestos de usuario.

Este comportamiento no es único de Microsoft; todos los fabricantes de aplicaciones necesitan actualizar su software porque desde que lo descargamos han seguido trabajando. Esto nos ocurre con Adobe Reader, Adobe Flash Player, Dropbox, los antivirus, etc.

Los parches son parecidos a las actualizaciones, pero se utilizan solo para corregir defectos y suelen necesitar que el usuario lo descargue y lo instale. Es decir, cuando alguien (el propio fabricante o algún cliente) detecta un problema en una aplicación, el fabricante avisa a todos los clientes afectados, les describe un workaround (si lo hay) y, cuando tiene el parche que lo arregla, les avisa para que lo descarguen de su web. Por este motivo es importante tener copias originales de las aplicaciones y registrarse en la web del fabricante para estar al día de los problemas que aparezcan.

ANTIVIRUS

Podemos tener el sistema actualizado, pero hay mucho programador malicioso que quiere instalar software en nuestro sistema para su provecho (diversión, espionaje industrial, etc.). Son los llamados virus informáticos, que son de muchos tipos (gusanos, troyanos, etc.), pero, en cualquier caso, estamos hablando de malware (software maligno) y hay que evitarlos.

Los virus pueden instalarse en nuestra máquina sin que lo sepamos, aprovechando algún defecto del sistema operativo o las aplicaciones instaladas (defectos que todavía no se han resuelto, o se han resuelto y no nos hemos enterado). Pero también les podemos «abrir la puerta» porque estamos haciendo la instalación de una aplicación que hemos conseguido de algún sitio no oficial. Para combatir ambos casos tenemos que instalar un antivirus.

El antivirus es un programa que está vigilando continuamente lo que ocurre en nuestra máquina. Concretamente, cualquier software que se intenta ejecutar (ejecutables .exe, librerías .dll) primero pasa por el antivirus. Él lo compara con su base de datos de virus y, si lo encuentra, impide que se ejecute y avisa al usuario.

Aunque el antivirus siempre va por detrás del virus, es importante tenerlo actualizado. La actualización afecta tanto a la base de datos de virus conocidos como al software del propio antivirus.

MONITORIZACIÓN

Hemos evitado el acceso de externos, hemos aplicado cuotas a los internos, tenemos activadas las actualizaciones automáticas del sistema operativo y todas las aplicaciones instaladas, tenemos antivirus actualizado… ¿Estamos tranquilos? Pues no. Hemos visto

que cualquiera de las medidas aplicadas es imperfecta. Nuestra labor es instalarlas, formar a los usuarios y, todos los días, vigilar que todo esté normal.

Esta vigilancia consiste en:

- Revisar los log del sistema y las aplicaciones. Cualquier suceso anómalo quedará anotado en alguna parte. Para cada aplicación hay que saber dónde lo hace (fichero, base de datos).

- Si el sistema lo permite, activar la copia sincronizada del log en otra máquina. Es decir, cada aviso se escribe a la vez en nuestra máquina y en otra. De esta forma podremos analizar un desastre, evitaremos que un hacker borre sus huellas, etc.

- Revisar la ocupación del sistema, principalmente el disco y la CPU. Lo habitual es programar una tarea para revisarlo regularmente (cada cinco minutos, por ejemplo) y generar una alarma que alerte al administrador cuando se supere algún límite (90 % del disco, por ejemplo).

- Suscribirse a las newsletters de los fabricantes de nuestro hardware y software para tener a mano la información oficial: actualizaciones, parches, nueva funcionalidad, workarounds, etc.

- Participar en foros de usuarios de las mismas aplicaciones que nosotros, para estar al día de los problemas que aparecen (puede que nos pase lo mismo) y para poder pedir ayuda si algo nos sobrepasa (en paralelo con la consulta al soporte oficial).

La monitorización de los log consiste primero en diferenciar qué es un problema y qué no lo es. El texto de log ayuda porque suele tener un indicador de gravedad (crítica, alto, medio, bajo o simple aviso), aunque es la clasificación del fabricante: solo nosotros conocemos nuestro sistema y sabemos las consecuencias de cada aviso.

Para conocer la ocupación de recursos de una máquina podemos entrar en ella y lanzar herramientas locales. Pero si tenemos a nuestro cargo la monitorización de muchos equipos, no podemos estar todo el día entrando en cada uno de ellos cada cinco minutos.

Conviene instalar una herramienta de inventario y monitorización. El inventario es la lista de equipos y conexiones y la configuración de ambos; la monitorización es la supervisión

en todo momento del estado de los elementos del inventario. Estas herramientas facilitan mucho el trabajo del administrador porque:

- Rastrean la red periódicamente buscando nuevas altas y bajas de equipos en el inventario.
- Son capaces de identificar distintos tipos de equipos, no solo ordenadores, sino también equipamiento de red. Para ello es necesario que los equipos ofrezcan interfaces estándar, como SNMP (Simple Network Management Protocol).
- Obtienen la configuración para todos los equipos del inventario y la registran en una base de datos para generar informes, avisar de cambios, etc.
- Incorporan alertas sobre ocupación de disco, inactividad de una interfaz, etc.
- Podemos monitorizar en directo la actividad de las interfaces de red, uso de CPU, etc.

La implantación de una de estas herramientas representa la frontera entre una administración artesanal de la red y sistemas, y una administración moderna y profesional.

El punto de inflexión suele ser un límite en la proporción entre el número de equipos y el número de integrantes del departamento de soporte informático. Cuando el personal ya está desbordado de trabajo, introducir estas herramientas permite automatizar las tareas rutinarias y así dejar tiempo libre a las personas que atienden los problemas complicados. Por ejemplo, localizar los equipos de la red que tienen un determinado software instalado, detectar nuevos equipos conectados pero no autorizados, etc.

APLICACIONES WEB

La arquitectura de aplicaciones ha evolucionado con el tiempo:

- En los años sesenta y setenta eran monolíticas: toda la funcionalidad, tanto la interfaz de usuario como la lógica de proceso, estaba en la misma máquina. Los usuarios utilizaban terminales «tontos» conectados al ordenador principal. La protección de una aplicación monolítica se centraba en proteger la máquina donde ejecutaban todos los programas.

- En los años ochenta y noventa aparecen los ordenadores personales y las redes de comunicaciones dentro de las empresas. Estos dos avances permiten implementar las aplicaciones siguiendo la arquitectura cliente-servidor: la interfaz de usuario y parte de la lógica de proceso están en el ordenador del usuario, y el resto de la lógica de proceso está en un ordenador central, al que conectan los ordenadores de usuario mediante la red local. La protección se complica: ahora hay que proteger a cada cliente, el servidor y la red local de la empresa.

- A partir de los años noventa, el éxito de Internet permite extender las aplicaciones web (que siguen el modelo cliente-servidor) a cualquier punto de conexión del planeta.

Hay un par de diferencias con los años ochenta: el cliente suele ser siempre el mismo (el navegador) y la comunicación utiliza redes públicas, sobre las que la empresa tiene nulo control. La protección es más difícil que nunca.

Nadie duda de las ventajas de implementar una aplicación mediante tecnologías web:

- No necesitamos instalar nada en el cliente: solo se necesita el navegador (que se incluye con el sistema operativo y que tiene otros usos, como navegar por Internet).

Con esto evitamos instalar un cliente nuevo que pueda entrar en conflicto con otras aplicaciones de la máquina, el usuario no necesita privilegios especiales para instalar programas, etc.

- Cualquier actualización generada por nuestros programadores (más funcionalidad, parches que arreglan defectos) está inmediatamente disponible para los usuarios porque siempre descargan la página actualizada de la última versión. No hay que esperar a que todos los usuarios sean avisados de la actualización, la descarguen, instalen, etc.

Por esta razón están ampliamente extendidas en Internet (Google Apps, ZoHo, Twitter, WordPress YouTube, etc.), y también dentro de las empresas, las intranets. Pero debemos tener cuidado con:

- La máquina que aloja el servidor web y sus aplicaciones accesorias (base de datos y otras). Si un hacker toma esta máquina, tiene acceso a toda la información y

todas las conexiones de los usuarios. Hay que aplicar las medidas de protección que hemos estudiado en este tema.

- Si la máquina del servidor web no es nuestra, sino alquilada (hosting web), no tenemos control sobre las medidas de protección. Debemos confiar en la profesionalidad del proveedor y repasar el contrato, en especial el apartado de los niveles de servicio (SLA [Service Level Agreement]). Por ejemplo, podemos exigir al proveedor que si el servidor web está caído más de dos horas al año, nos haga un descuento del 25 % en la siguiente cuota.

- La transmisión entre el cliente web (navegador) y el servidor web. Muchas aplicaciones todavía utilizan el protocolo HTTP, donde todo viaja en texto en claro. En algún tramo de red puede estar escuchando un hacker y conocer qué hacemos, incluso modificarlo para su provecho. Debemos optar por HTTPS.

- La máquina de un usuario conectado puede haber sido hackeada y su navegador también. Por ejemplo, se ha instalado un keylogger que envía todas las contraseñas fuera de nuestro control. En este punto es importante el antivirus.

CLOUD COMPUTING

Después de las aplicaciones web, la siguiente evolución de las aplicaciones en Internet es el cloud computing (computación en la nube). Conviene diferenciar entre computación en la nube y almacenamiento en la nube (cloud storage: iCloud, Dropbox, Amazon S3).

El almacenamiento también aporta fl exibilidad (número variable de GB reservados, backup automático), pero se limita a guardar archivos y carpetas; la computación es más amplia porque ejecuta programas que trabajan con archivos, bases de datos, otros servidores, etc. Sin embargo, se complementan porque la computación en la nube puede trabajar con archivos de almacenamiento en la nube.

A las empresas ya no les interesa conectar a Internet un servidor web de su CPD porque necesitan dedicar recursos a proveer QoS (Quality of Service, calidad de servicio), buena conectividad, servidores potentes, administradores efi caces, etc. Además, abrir al exterior las conexiones del CPD es una fuente de problemas por la cantidad de ataques que nos pueden llegar.

Tampoco convence ya alquilar espacio en un hosting porque, si es un servidor web compartido, el rendimiento es bajo; si es un hosting dedicado, suelen ser máquinas individuales de potencia media.

IaaS: Infrastructure as a Service

Un primera solución de cloud computing es el IaaS (Infrastructure as a Service). Nuestra empresa quiere poner una máquina entera (un Linux, por ejemplo) en un proveedor, pero con una diferencia frente al hosting dedicado: esa máquina ejecutará en un entorno virtualizado, de manera que podemos regular la potencia. Si la aplicación está ralentizándose por un exceso de carga, contratamos temporalmente más CPU y más RAM (y asumimos el incremento de coste asociado); cuando ya no lo esté, volvemos a la confi guración básica. Incluso se puede solicitar que arranquen más máquinas (se llaman instancias).

El procedimiento es similar al de las máquinas virtuales: generamos un disco virtual (fi chero vdi, por ejemplo), instalamos lo que necesitamos (generalmente Linux RedHat o Ubuntu, pero también Windows Server) y lo subimos a la web del proveedor. Desde un panel de control en esa web modifi camos la ejecución de la máquina según nos convenga en cada momento.

Pero en esta opción seguimos necesitando personal especializado para administrar esas instancias, generarlas, actualizarlas, confi gurar la seguridad, vigilar la virtualización, etc.

SaaS: Software as a Service

Las empresas que no quieren incurrir en ese gasto (una fábrica de quesos sabe de quesos, no de software) eligen SaaS (Software as a Service), aplicaciones completas donde el mismo proveedor se encarga del desarrollo de la aplicación, su mantenimiento y también pone las máquinas y la conectividad (o en las máquinas de un IaaS, pero nunca en las nuestras).

Por ejemplo, para el correo de la fábrica de quesos, en lugar de utilizar una máquina nuestra (lo que supone contratar una buena conexión a Internet y asumir los recursos humanos necesarios para realizar la confi guración, administración, monitorización 24 x 7…), podemos simplemente contratar el servicio Google Apps de Google.

De cara a la protección de las aplicaciones, en los dos casos (IaaS, SaaS), como ya ocurría con el hosting, perdemos el control sobre la seguridad de la máquina y el software que ejecuta en ella: tenemos que confiar en la profesionalidad del proveedor y redactar muy bien los SLA del contrato del servicio.

CRIPTOGRAFIA

¿POR QUÉ CIFRAR?

La información es poder: los planos de un nuevo motor de coche eléctrico, la estrategia electoral de un partido político o la fórmula de un nuevo medicamento. Todos son ejemplos de información que interesa a terceras personas: una empresa de la competencia, un partido rival.

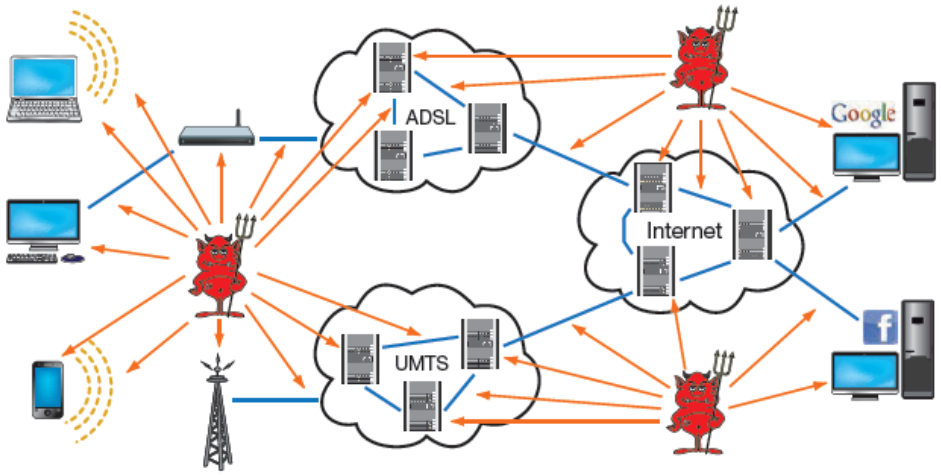
Para sacar el máximo partido de una información hay que compartirla con otros individuos: el plano del motor o la fórmula deben llegar a la fábrica, y la estrategia electoral se discutirá en algún comité regional. En todos estos casos, el autor del documento (emisor) debe transferirlo a algún soporte (disco duro, CD, pendrive USB, impresión en papel, cuenta de correo electrónico, upload a un servidor web, etc.) y hacer llegar ese soporte hasta el destino (receptor) mediante algún canal de comunicación (empresa de mensajería, fax, Internet, etc.).

En ese canal pueden estar acechando terceras personas con la intención de interceptarlo: sobornarán al mensajero para hacer una copia del disco duro/CD/USB o una fotocopia del papel, «hackearán» el servidor de correo, capturarán el tráfico de red en el servidor web. Es imposible asegurar que nunca conseguirán el documento. Nuestra esperanza es que, aunque lo tengan y lo puedan leer, no entiendan nada porque el contenido estará cifrado. Aquí nos ayuda la criptografía.

Nuestra era de la información y las comunicaciones necesita el cifrado más que nunca, porque cada vez existen más medios de almacenamiento (memorias portables de todo tipo) y, sobre todo, más mecanismos de comunicación:

- Voz mediante teléfono (fijo/móvil) con tecnología analógica (fijo) y digital (GSM, UMTS, RDSI, VoIP), así como el aumento constante de videoconferencias.
- Mensajería electrónica breve (SMS, Skype, WhatsApp) o completa (correo electrónico, burofax).
- Datos por línea digital (ADSL, fibra, HFC) o inalámbrica (wifi, UMTS, LTE).

- Apertura de las redes internas de las empresas para que puedan trabajar sus trabajadores (VPN de teletrabajo), sus clientes (acceso web) y otras empresas (VPN de empresas), todo a través de Internet.



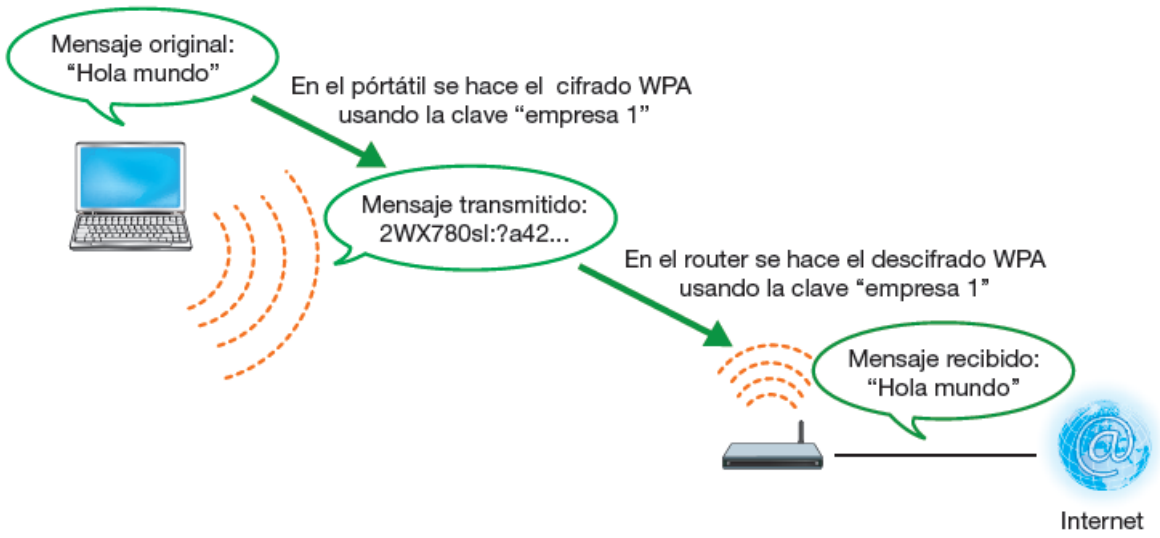
Todas esas conversaciones utilizan redes compartidas con otros usuarios que no somos nosotros y administradas por otras empresas que no son la nuestra. Las operadoras de telecomunicaciones pueden darnos confianza utilizando protocolos seguros; pero para las empresas no es suficiente (las operadoras de telecomunicaciones también son sobornables y «hackeables») y por eso aplican cifrado en todas partes (incluso dentro: podemos tener empleados «traidores»); también los usuarios particulares deberían preocuparse de hacerlo porque su privacidad les pertenece (llamadas personales, correos intercambiados con sus contactos, movimientos bancarios, etc.).

CONCEPTO CRIPTOGRAFIA

La palabra criptografía viene del griego cripto (que significa «ocultar») y graphos (que significa «escribir»). Se podría traducir por: cómo escribir mensajes ocultos. En la antigüedad se utilizaba sobre todo durante las guerras, para comunicar estrategias, de manera que, aunque el mensajero fuera interceptado por el enemigo, el contenido del mensaje estaba a salvo.

La criptografía consiste en tomar el documento original y aplicarle un algoritmo cuyo resultado es un nuevo documento. Ese documento está cifrado: no se puede entender nada al leerlo directamente. Podemos, tranquilamente, hacerlo llegar hasta el destinatario, que sabrá aplicar el algoritmo para recuperar el documento original.

Realmente, hace falta algo más que el algoritmo, porque el enemigo también puede conocerlo (incluso lo utiliza en sus propias comunicaciones). Por ejemplo, nosotros tenemos una red wifi con cifrado WPA, pero el vecino también. La privacidad la conseguimos gracias a la clave del algoritmo (Fig. 2.2): un conjunto de valores que, combinados con el documento original tal y como se indica en el algoritmo, generan un documento cifrado de tal forma que, solo con ese documento, es imposible deducir ni el documento original ni la clave utilizada. Por supuesto, debemos evitar que el enemigo pueda llegar a conocer nuestra clave.



Las claves son combinaciones de símbolos (letras, números, signos de puntuación, etc.). Por tanto, nuestra seguridad está expuesta a los ataques de fuerza bruta: probar todas las combinaciones posibles de símbolos. Para evitarlo tomaremos estas medidas:

- Utilizar claves de gran longitud (512-1024-2048-4096 bytes), de manera que el atacante necesite muchos recursos computacionales para cubrir todo el rango rápidamente.

- Cambiar regularmente la clave. De esta forma, si alguien quiere intentar cubrir todo el rango de claves, le limitamos el tiempo para hacerlo.

- Utilizar todos los tipos de caracteres posibles: una clave compuesta solo de números (diez valores posibles) es más fácil de adivinar que una con números y letras (36 valores posibles).

- No utilizar palabras fácilmente identificables: palabras de diccionario, nombres propios, etc.

- Detectar repetidos intentos fallidos en un corto intervalo de tiempo. Por ejemplo, la tarjeta del móvil se bloquea si fallamos tres veces al introducir el PIN.

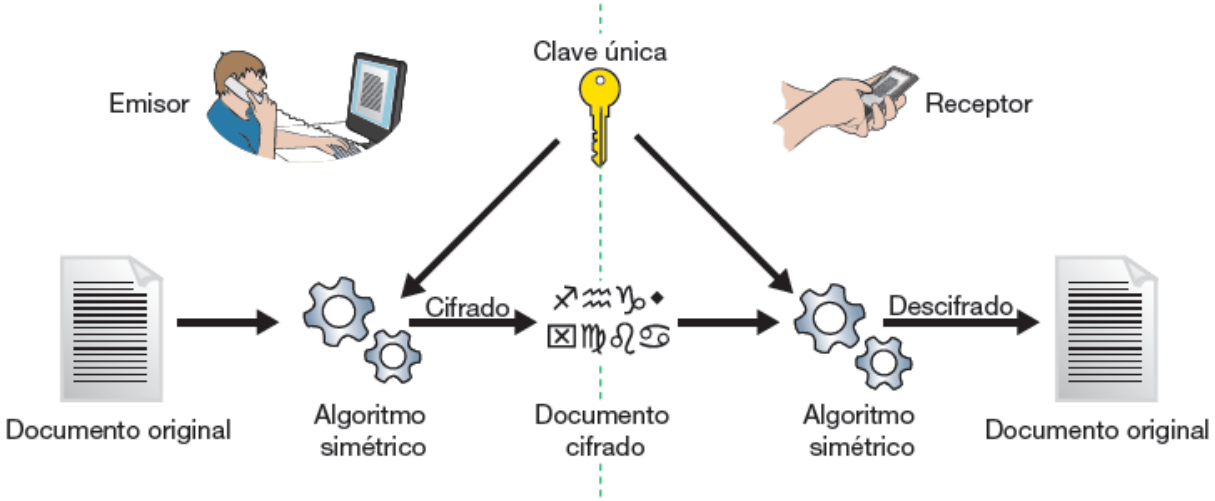
Las claves no son el único punto débil de la criptografía; pueden existir vulnerabilidades en el propio algoritmo o en la implementación del algoritmo en alguna versión de un sistema operativo o un driver concreto. Estas vulnerabilidades las estudia el criptoanálisis.

CRIPTOGRAFÍA SIMÉTRICA Y ASIMÉTRICA

Los algoritmos de criptografía simétrica utilizan la misma clave para los dos procesos: cifrar y descifrar. Son sencillos de utilizar y, en general, resultan bastante eficientes (tardan poco tiempo en cifrar o descifrar). Por este motivo, todos los algoritmos, desde la antigüedad hasta los años setenta, eran simétricos. Los más utilizados actualmente son DES, 3DES, AES, Blowfish e IDEA.

El funcionamiento es simple: en la siguiente figura el emisor quiere hacer llegar un documento al receptor. Toma ese documento y le aplica el algoritmo simétrico, usando la clave única, que también conoce el receptor. El resultado es un documento cifrado que ya podemos enviar tranquilamente.

Cuando el receptor recibe este documento cifrado, le aplica el mismo algoritmo con la misma clave, pero ahora en función de descifrar. Si el documento cifrado no ha sido alterado en el camino y la clave es la misma, el resultado será el documento original.



Un ejemplo de criptografía simétrica es la autenticación de un móvil GSM: por qué sabe que es nuestro número, aunque metamos la tarjeta SIM en otro teléfono. El procedimiento es el siguiente:

- Nuestra tarjeta SIM contiene un identificador T y una clave K.
- Ese identificador T y la clave K aparecen asociados a nuestro contrato en los servidores de autenticación de la operadora de la que somos clientes.
- Cuando encendemos el teléfono, se conecta a la red de la operadora y solicita entrar con el identificador T. Su servidor de autenticación recibe la petición y genera un número aleatorio A (llamado desafío), que nos lo envía.
- Una vez recibido, en nuestro teléfono aplicamos un determinado algoritmo simétrico sobre ese número A, utilizando la clave K. El resultado es el número B. Enviamos el número B al servidor de autenticación.
- Cuando lo recibe, él también aplica el mismo algoritmo con la misma clave. Si el resultado es igual a B, se confirma que somos los dueños del identificador T. Nos asigna nuestro número 6XX, y ya podemos hacer y recibir llamadas.
- Si cambiamos de teléfono, no importa porque el número va asociado a la SIM.

Con esta solución estamos protegidos de una posible captura de tráfico inalámbrico mediante un sniffer de red:

- Podría capturar el número A. Pero es un simple número aleatorio: sin el algoritmo y la clave, el atacante no podrá generar la respuesta correcta B.

- Podría capturar también el número B y ya tendría la respuesta correcta cuando el servidor envía el número A. Pero la probabilidad de que el servidor repita el mismo número A para este abonado es muy baja. Es decir, si el atacante elabora una tarjeta SIM preparada para responder B cuando le pregunten A, es muy poco probable que tenga éxito.

El problema principal de la criptografía simétrica es la circulación de las claves: cómo conseguimos que el emisor y el receptor tengan la clave buena. No podemos utilizar el mismo canal inseguro por el que enviaremos el mensaje (la inseguridad nos ha llevado a cifrar).

Hay que utilizar un segundo canal de comunicación, que también habría que proteger, y así sucesivamente. Por ejemplo, en el correo de bienvenida a una empresa puede aparecer la contraseña de la wifi de la oficina; cuando se cambie, se envía otro correo, etc.

El segundo problema es la gestión de las claves almacenadas. Si en una empresa hay diez trabajadores y todos tienen conversaciones privadas con todos, cada uno necesita establecer nueve claves distintas y encontrar nueve canales seguros para actualizarlas cada vez (en total 81 claves y 81 canales). Si aparece un trabajador nuevo, ahora son 100 claves y 100 canales. Y las empresas pueden tener muchos trabajadores: 500, 5 000, 50 000... ¿Cada vez que cambie mi clave tengo que avisar a 49 999 compañeros? Es poco manejable.

En los años setenta, los criptógrafos Diffie y Hellman publicaron sus investigaciones sobre criptografía asimétrica. Su algoritmo de cifrado utiliza dos claves matemáticamente relacionadas de manera que lo que cifras con una solo lo puedes descifrar con la otra.

Comparado con la clave simétrica, ahora el emisor no necesita conocer y proteger una clave propia; es el receptor quien tiene el par de claves. Elige una de ellas (llamada clave pública) para comunicarla al emisor por si quiere enviarle algo cifrado. Pero ya no hace

falta buscar canales protegidos para enviarla porque, aunque un tercer individuo la conozca, todo lo que se cifre con esa clave solo se podrá descifrar con la otra clave de la pareja (la clave privada), que nunca es comunicada. Y matemáticamente es imposible deducir la clave privada conociendo solo la clave pública.

Como se ilustra en la siguiente figura, cuando el emisor quiere hacer llegar un mensaje confidencial al receptor, primero consigue la clave pública del receptor. Con esa clave y el documento original, aplica el algoritmo asimétrico. El resultado es un documento cifrado que puede enviar al receptor por cualquier canal. Cuando el mensaje cifrado llega al receptor, él recupera el documento original aplicando el algoritmo asimétrico con su clave privada. Si el receptor quiere enviar al emisor una respuesta cifrada, debería conseguir la clave pública del emisor y seguir el mismo procedimiento.

La criptografía asimétrica resuelve los dos problemas de la clave simétrica:

- No necesitamos canales seguros para comunicar la clave que utilizaremos en el cifrado. Podemos adjuntarla en nuestros correos, añadirla al perfil de nuestras redes sociales, «postearla» en un blog, incluso repartirla en octavillas por la calle.

- No hay desbordamiento en el tratamiento de claves y canales. Si somos nueve empleados, solo necesitamos nueve claves y un solo canal: la intranet de la empresa, un correo destinado a toda la empresa, etc. Y si aparece un empleado nuevo, serán diez claves y el mismo canal.

Sin embargo, los algoritmos asimétricos tienen sus propios problemas:

- Son poco eficientes: tardan bastante en aplicar las claves para generar los documentos cifrados, sobre todo porque las claves deben ser largas para asegurar la independencia matemática entre ellas.

- Utilizar las claves privadas repetidamente es arriesgado porque algunos ataques criptográficos se basan en analizar paquetes cifrados. Estos paquetes serían capturados en la red o directamente el atacante podría elaborar un software malicioso que generase paquetes de tamaño y contenido elegidos cuidadosamente y conseguir enviarlos a nuestro servidor para que los devolviera cifrados con su clave privada.

- Hay que proteger la clave privada. No basta con dejarla en un fichero de una carpeta del disco duro en la cuenta de nuestro usuario; cualquier otro usuario con permisos de administrador podría llegar hasta él. Por este motivo, las claves privadas se guardan todas juntas en un fichero llamado keyring (archivo de llaves, llavero), y este fichero está protegido mediante cifrado simétrico. Es decir, para poder usar la clave privada, hay que introducir una clave que descifra el llavero y permite leerla.

  Necesitamos una segunda medida de protección de la clave privada: la copia de seguridad del llavero. Si el disco duro se estropea, perderemos el fichero que contiene la clave privada y no podremos volver a utilizarla. Por tanto, debemos incluirlo en la política de backup de la empresa, y confiamos en que, aunque alguien más tenga acceso al backup (cintas, discos, etc.), la clave simétrica todavía protege el llavero.

- Hay que transportar la clave privada. En cifrado simétrico, si hemos enviado el fichero cifrado a otra máquina y queremos descifrarlo, basta con recordar la clave e introducirla. Pero en la clave privada esto es imposible (son cientos de símbolos sin sentido). Debemos transportar el llavero, con el riesgo que supone (si lo perdemos, podrían intentar un ataque de fuerza bruta contra el cifrado simétrico).

La solución más común a los problemas de proteger y transportar la clave privada es la tarjeta inteligente.

Es una tarjeta de plástico que contiene un chip electrónico. Hay dos tipos:

- Tarjeta de memoria. Es equivalente a una memoria Flash y se limita a almacenar el llavero. Cuando se introduce en el lector, el ordenador hace una copia temporal del llavero y trabaja con él introduciendo la clave simétrica, etc.

- Tarjeta procesadora. La tarjeta de memoria es peligrosa porque hemos expuesto nuestro llavero. En cambio, en las tarjetas procesadoras las claves también están almacenadas, pero nunca salen de la tarjeta. Cualquier cifrado que necesite nuestra clave privada es realizado por el propio chip porque incluye una CPU, memoria RAM, etc.

Por supuesto, sigue siendo necesario introducir la clave simétrica que abre el llavero. El ejemplo más sencillo es la tarjeta SIM de los teléfonos móviles: para poder usarla necesitamos introducir el número PIN. Aunque la usemos en otro teléfono, el PIN es el mismo porque está asociado a la tarjeta. En la sección final de esta unidad veremos otro ejemplo de tarjeta inteligente: el DNI electrónico.

Las tarjetas inteligentes también se pueden clasificar por su tipo de interfaz:

- Tarjeta de contacto. El lector necesita tocar los contactos metálicos del chip para interactuar con él. Son las más utilizadas, sobre todo en entornos de alta seguridad, como el sector bancario, Administración electrónica, etc.

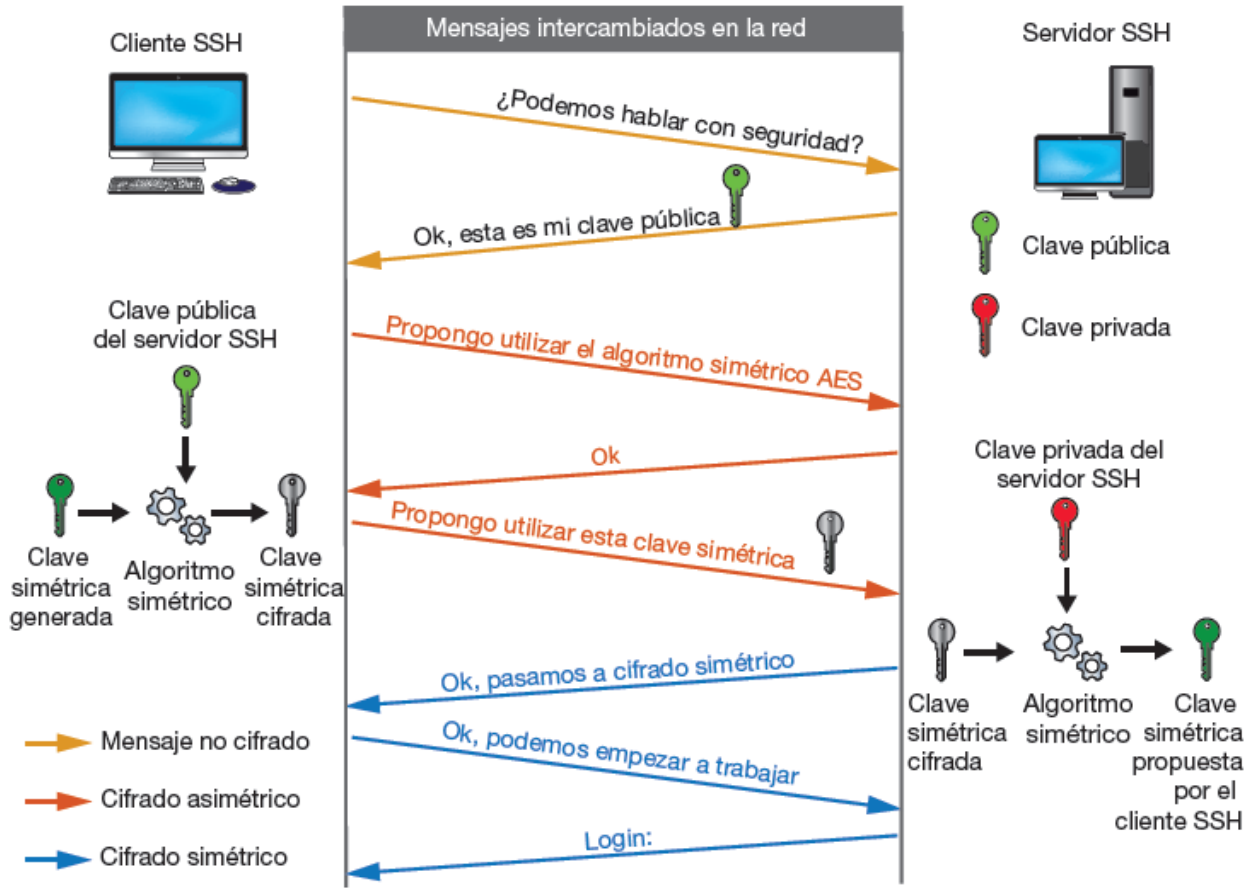
- Tarjeta sin contacto. El lector utiliza tecnologías inalámbricas para interactuar con el chip. Se utilizan en situaciones donde se necesitan transacciones rápidas, como el acceso al transporte público.

El cifrado asimétrico no se puede utilizar para cifrar todos los paquetes intercambiados en una red local porque el bajo rendimiento del algoritmo ralentizaría el tráfico. En su lugar se adopta un esquema híbrido:

- Criptografía asimétrica solo para el inicio de la sesión, cuando hay que generar un canal seguro donde acordar la clave simétrica aleatoria que se utilizará en esa conversación.

- Criptografía simétrica durante la transmisión, utilizando la clave simétrica acordada durante el inicio de sesión. Generalmente se suele cambiar la clave simétrica cada cierto tiempo (minutos) para dificultar más el espionaje de la conversación.

Es decir, cuando A quiere establecer una conversación con B, en A se genera en ese instante una nueva clave simétrica (CS). Para enviársela a B de modo seguro, A la cifra utilizando un algoritmo asimétrico con la clave pública de B. Cuando B recibe la CS cifrada, la descifra con su clave privada y desde ese momento pueden seguir el diálogo cifrando con el algoritmo simétrico acordado y la CS recibida.



CIFRAR Y FIRMAR

La primera utilidad de la criptografía es ocultar el mensaje para aquellos que no son destinatarios del mismo. Es decir, garantizar la confidencialidad de la comunicación cifrando el documento original.

La segunda utilidad es conseguir determinar la autenticidad del emisor. ¿Cómo podía estar seguro el general romano de que ese mensaje con las nuevas órdenes venía de otro general romano, y no de algún enemigo? Si el enemigo conocía el algoritmo de cifrado y la clave actual, podía intentar engañarle mediante un mensaje falso pero correctamente cifrado.

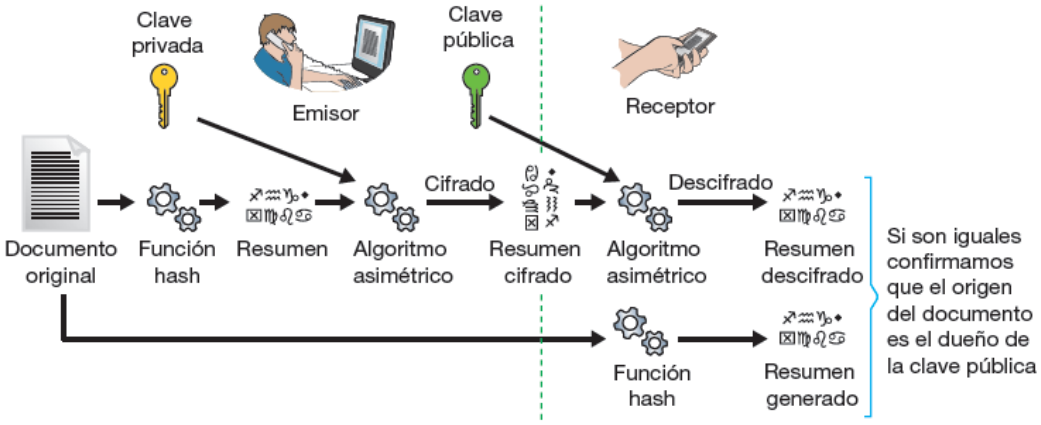
En el paso 18 del caso práctico 3 nos ha ocurrido lo mismo: hemos tenido que recurrir a una comprobación más (entrar al usuario alumno para comparar la huella de su clave) para estar seguros de que estábamos cifrando el mensaje para el destinatario correcto.

En criptografía asimétrica, el mecanismo de firma garantiza que el emisor es quien dice ser. Supongamos que vamos a enviar un documento y queremos que el receptor confíe en que somos nosotros. Para conseguirlo, el emisor aplica al documento una función resumen (función hash, no olvidar que una función hash se utiliza también para comprobar que un fichero no ha sido alterado. Es importante sobre todo si el fichero es un ejecutable, que puede haber sido modificado por un virus para intentar replicarse. Las funciones más utilizadas son MD5 y las distintas versiones de SHA.). El resultado de esta función es una lista de caracteres, el resumen, que la función garantiza que solo se pueden haber obtenido con el documento original (el algoritmo de la función hash no necesita una clave extra como los algoritmos de cifrado). Ahora el emisor cifra ese resumen con su clave privada y lo envía al destino, junto con el documento original.

En el destino se hacen dos operaciones:

- Aplicar la misma función hash al documento para obtener su resumen.
- Descifrar el resumen recibido, utilizando la clave pública del emisor.

Si ambos resúmenes coinciden, el destino puede estar seguro de que el emisor del documento es el mismo que el dueño de la clave pública que acaba de aplicar para descifrar el resumen recibido.



Por supuesto, si queremos que el documento original no pueda ser interceptado en la transmisión desde el emisor al receptor, debemos cifrarlo. Para ello usaremos la clave pública del receptor. El procedimiento completo sería:

- El emisor aplica la función hash al original para generar el resumen.
- El emisor toma su clave privada para aplicar el algoritmo asimétrico al documento resumen. El resultado es un documento resumen cifrado.
- El emisor toma la clave pública del receptor para aplicar el algoritmo asimétrico al documento original y al documento resumen. El resultado es un documento conjunto cifrado que se envía al receptor.

En el receptor, utiliza su clave privada para descifrar los documentos y la clave pública del origen para comprobar la firma.

PKI. DNIe

Hasta ahora hemos aprendido a enviar documentos a un destinatario de manera que solo él pueda aprovecharlos (cifrado), y garantizando que el documento es nuestro (firmado). Pero en todos los casos hemos necesitado una comprobación extra sobre la clave pública: comparar la huella de esa clave importada con la huella de la clave original, para estar seguros de que vamos a comunicarnos con la persona correcta.

En nuestros casos prácticos ha sido sencillo porque estamos trabajando en la misma máquina o, como mucho, en la máquina del compañero. Pero la mayoría de las comunicaciones seguras ocurren entre máquinas muy alejadas entre sí que seguramente

pertenecen a otras empresas. Por ejemplo, las oficinas virtuales de los bancos o el correo web (Gmail, Hotmail, etc.). No podemos entrar en sus máquinas para ver las huellas ni negociar con cada uno otro canal seguro donde poder consultarlas.

La solución a este problema es la implantación de una PKI (Public Key Infrastructure, infraestructura de clave pública). Ahora, en la comunicación segura entre cliente y servidor aparecen nuevos interlocutores:

- La Autoridad de Certificación (CA [Certificate Authority]), cuya misión es emitir certificados.

Hasta ahora los generábamos nosotros mismos con una herramienta en el ordenador.

- La Autoridad de Registro (RA [Registration Authority]), que es la responsable de asegurar que el solicitante del certificado es quien dice ser. Por ejemplo, en los certificados necesarios para presentar la declaración de la renta, la solicitud se puede hacer por Internet, pero para recogerlos hay que presentarse con el DNI en una oficina de la Administración.

- La Autoridad de Validación (VA [Validation Authority]) es la responsable de comprobar la validez de los certificados digitales emitidos. En la práctica suele coincidir con la CA.

- Los repositorios. Son almacenes de certificados. Los principales son el repositorio de certificados activos y el repositorio de listas de revocación de certificados (certificados que, por cualquier motivo, fueron expresamente desactivados antes de caducar).

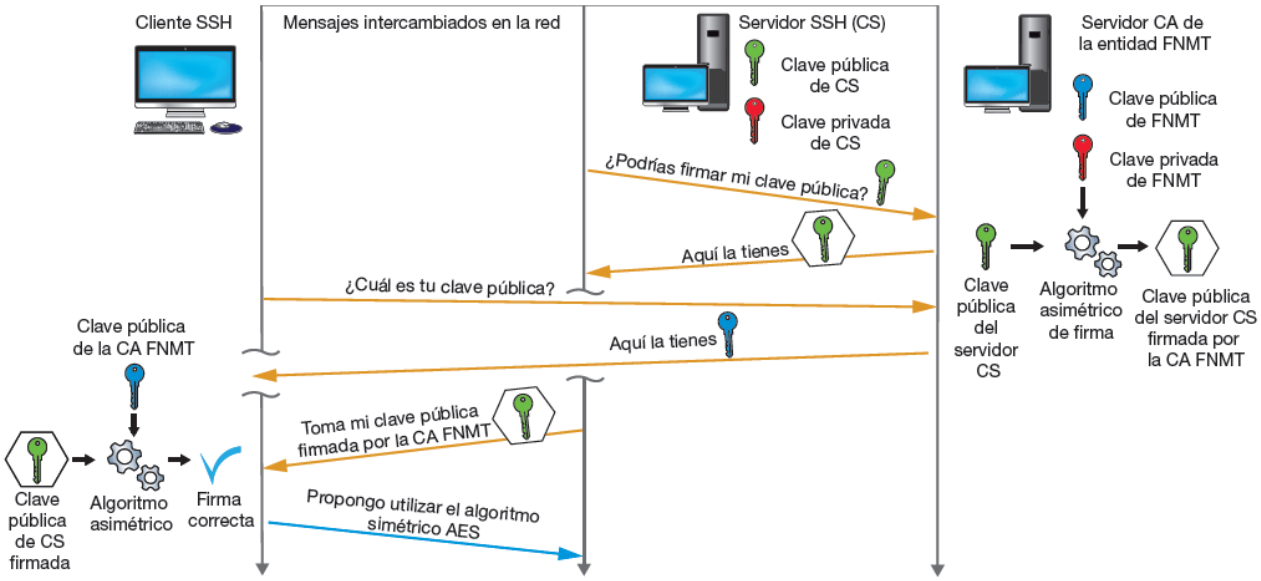
El funcionamiento es el siguiente: Durante el inicio de la sesión, el servidor envía su clave pública al cliente para que cifre el diálogo que van comenzar (autenticación usuario/contraseña, etc.); pero el cliente, antes de utilizarla, desconfía: necesita comprobar que el servidor es quien dice ser. Luego el servidor lo ha supuesto y ha enviado, junto con su clave pública, la firma digital de esa clave. Esa firma digital ha sido realizada por una CA oficial utilizando la clave privada de esa CA. El cliente puede verificar la firma recibida utilizando la clave pública de la CA (en este punto puede necesitar conectar con la VA). Si la firma es correcta, la clave pública del servidor también lo es y podemos iniciar la sesión segura con toda confianza.

Por tanto, para que funcione la autenticación de una clave pública mediante PKI, se necesitan dos pasos previos:

- El servidor ha conseguido que una CA le firme su clave pública. Por ejemplo: Veri-Sign, FNMT, etc.
- El cliente dispone de la clave pública de esa CA dentro de su llavero de claves asimétricas.

En la figura siguiente hemos añadido estos dos pasos al ejemplo de la figura acerca del protocolo SSH. En algún momento el servidor SSH consigue que una CA le firme la clave pública, y en algún momento el cliente SSH instala la clave pública de esa CA.

Desde ese instante ya pueden establecerse conversaciones seguras entre cliente y servidor SSH, porque el cliente puede autentificar la clave pública ofrecida por el servidor.



Realmente, las CA no emiten un simple fichero con la firma, como hemos visto hasta ahora en los casos prácticos (ficheros .gpg o .asc); ni encontramos suelta la clave pública de una CA para importarla. Es importante la información complementaria: quién firma, para quién firma, qué usos tiene la clave (cifrado y firmado, solo firmado, etc.), en qué fecha se firmó, cuándo caduca esa firma, qué algoritmos se han utilizado, etc.

Esta información se recoge en una estructura que constituye el certificado digital, según el estándar X.509. Por tanto, en el funcionamiento de una PKI los usuarios importan

certificados de CA y los servidores envían sus claves públicas dentro de certificados. Ahora bien, ¿cómo podemos estar seguros de que la clave pública de la CA es auténtica? Porque se ha instalado en nuestro ordenador de manera segura: bien porque forma parte de la instalación del sistema operativo, bien porque en algún momento la hemos importado voluntariamente. Se suelen llamar certificados raíz (root certificates).

Hay muchas empresas públicas y privadas que disponen de una PKI y se dedican a emitir certificados. Los usuarios que desean un certificado de esa empresa visitarán solo una vez su RA y su CA para obtenerlo, aunque después usarán muchas veces la VA y los repositorios.

Solo volverán a la CA para renovar el certificado cuando esté próximo a caducar. Además de las comunicaciones por Internet, las empresas también necesitan cifrar la información interna que circula por sus sistemas y sus redes. Para reducir el coste que supone contratar los certificados con una empresa externa, suelen crear una PKI propia que no emita certificados al público en general, sino solo a sus empleados y sus sistemas. La instalación consiste en configurar un servidor de la empresa con el software necesario para ejercer las funciones de CA y VA, y poner la clave pública de la CA en todos los equipos, uno a uno. La RA es asumida por el departamento de informática.

Como casi todo en seguridad informática, la PKI no es perfecta. Todavía tenemos dos vulnerabilidades:

- Un virus en nuestro ordenador puede alterar el depósito de claves, e importar sin nuestro consentimiento claves públicas de CA fraudulentas. Una conexión segura a servidores respaldados por esas CA no es fiable.

- Un ataque a los servidores de una CA podría robar su clave privada. Desde ese momento, el atacante puede firmar las claves públicas de servidores peligrosos y los clientes se conectarían a ellos confiando en que es una firma legal.