Conceptos de protección en la red local

1. Servicios de seguridad

Para responder a la solicitud de garantías necesarias en términos de seguridad de un Sistema de Información (SSI), estos servicios deben tener en cuenta los conocimientos y análisis efectuados.

Los distintos servicios de seguridad que se deben mantener son:

- Control de acceso al sistema.
- Gestión de permisos.
- Integridad.
- No denegación.
- Autentificación.
- Confidencialidad.

Esta protección se aplica tanto a la información como a los sistemas de soporte. Es muy importante que ninguno sea forzado ni olvidado. Aquí trataremos específicamente los dos principales que debe tener una red, la autentificación y la confidencialidad.

a. El control de acceso al sistema

Se trata, sobre todo, de proteger físicamente los dispositivos. Es necesario cerrar las salas de servidores, pero también las oficinas. De hecho, se puede robar dispositivos móviles que contienen información importante.

Los sistemas operativos y otras aplicaciones deben estar protegidos mediante la configuración e instalaciones regulares de parches que corrijan los posibles errores.

Las redes se pueden aislar y se deben filtrar las comunicaciones.

Se debe instalar y mantener software antivirus en todos los equipos. Se puede completar con la instalación de herramientas de detección de intrusión (IDS - *Intrusion Detection System*).

b. La gestión de permisos

El software, especialmente los sistemas operativos, utilizan su propio sistema de habilitación de accesos a los archivos o a los datos. Por ejemplo, Microsoft Windows utiliza los permisos NTFS, nombre tomado del sistema de archivos. Los sistemas Unix/Linux tienen una gestión basada en los accesos de lectura (*read*), de escritura (*write*) y de ejecución (*execute*). Los fallos en las distribuciones de estos permisos pueden aparecer rápidamente si no se utiliza una política conveniente.

Además, hay permisos no vinculados a los propios datos, pero sí a posibles acciones sobre aplicaciones, que deben administrarse complementariamente.

Para facilitar la gestión de los permisos, los usuarios se registran en bases de cuentas o directorios centralizados. Los derechos y permisos se asocian así a una cuenta, o a un grupo al cual pertenece esta. A continuación el usuario debe demostrar su identidad, dándose a conocer ante una cuenta conocida.

c. La integridad

Comprobar la integridad en las transferencias es asegurarse de que no tenga lugar ninguna modificación entre el emisor y el destinatario (hombre o máquina). Puede ser un muy buen complemento de la confidencialidad.

El CRC aún es falible y cualquier pirata lo puede manipular discretamente. Pero de todos modos sigue siendo conveniente para paliar los problemas de transmisión. La aplicación de tablas de *hash*, que calculan una huella digital, sigue siendo más fiable.

Las tablas de *hash* utilizan un algoritmo de criptografía que genera un texto de longitud fija, cualquiera que sea el tamaño del de entrada. El resultado de este cálculo se llama condensado, huella o *hash*. Esta función es de dirección única, puesto que no es posible encontrar el texto de origen a partir de la huella que se comunica al destinatario. Este puede efectuar el mismo cálculo a partir del contenido de la trama enviada. Basta solo una modificación para no encontrar el mismo resultado y considerar que se ha alterado el contenido.

Los dos principales algoritmos utilizados son:

- *Message Digest 5* (MD5), que genera huellas de 128 bits.
- *Secure Hash Algorithm 1* (SHA o SHA1), que genera resultados de 160 bits.

El servicio de integridad, en términos de almacenamiento y administración de los sistemas, lo pueden ofrecer los archivos históricos y las auditorías.

d. La no denegación

Este servicio lo proporciona la firma electrónica (que no es lo mismo que la autentificación). Su reconocimiento y, por tanto, su validación, implica la confianza de un tercero. Además, añade a esta validación de identidad un cálculo de integridad con tablas de *hash*.

La firma electrónica se puede utilizar en sitios web (validación de procedencia de los datos), en mensajes de correo electrónico, en el interior de un archivo...

2. Autentificación

Este servicio de seguridad es particularmente importante cuando un hardware se conecta a una red, es decir, cuando da acceso a otras máquinas. En realidad, incluye dos funciones. La primera es la identificación, es decir, el reconocimiento de la identidad. La segunda, la autentificación, comprueba la identidad declarada.

Se pueden utilizar cuatro formas de comprobación:

- «Lo que conozco», como contraseña.
- «Lo que tengo», como soporte físico.
- «Lo que soy», examinando una característica humana.
- «Lo que sé hacer», como una firma manuscrita.

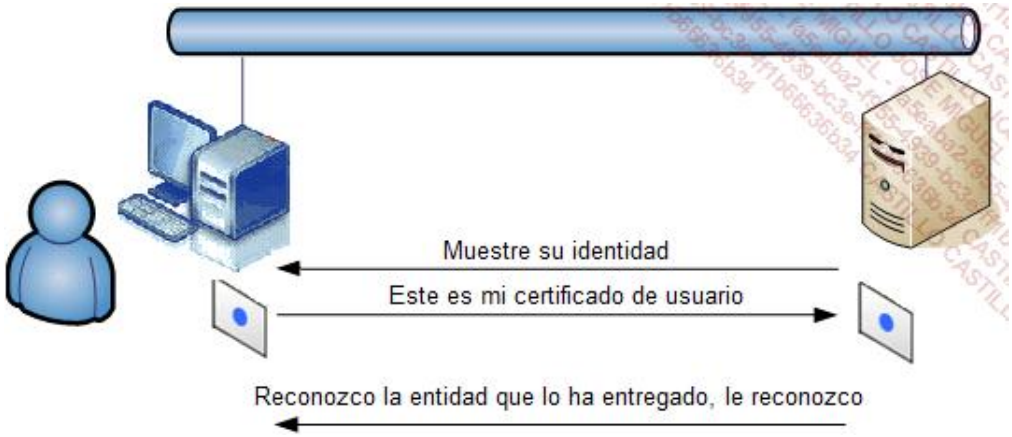
En la autentificación informática, este último caso requiere una pantalla táctil. Por lo tanto, no lo trataremos en esta obra.

Cuando el alcance de una red va más allá de los edificios controlados, a través de Internet o por las ondas hertzianas, hay que hacer una reflexión sobre la elección del medio de autentificación. Existen soluciones, más elaboradas que la habitual contraseña, y de bajo coste, que reducen los riesgos de suplantación de identidad.

a. La identificación

El principal medio de identificación es el «login». El usuario lo introduce y se controla en una base de datos o un archivo.

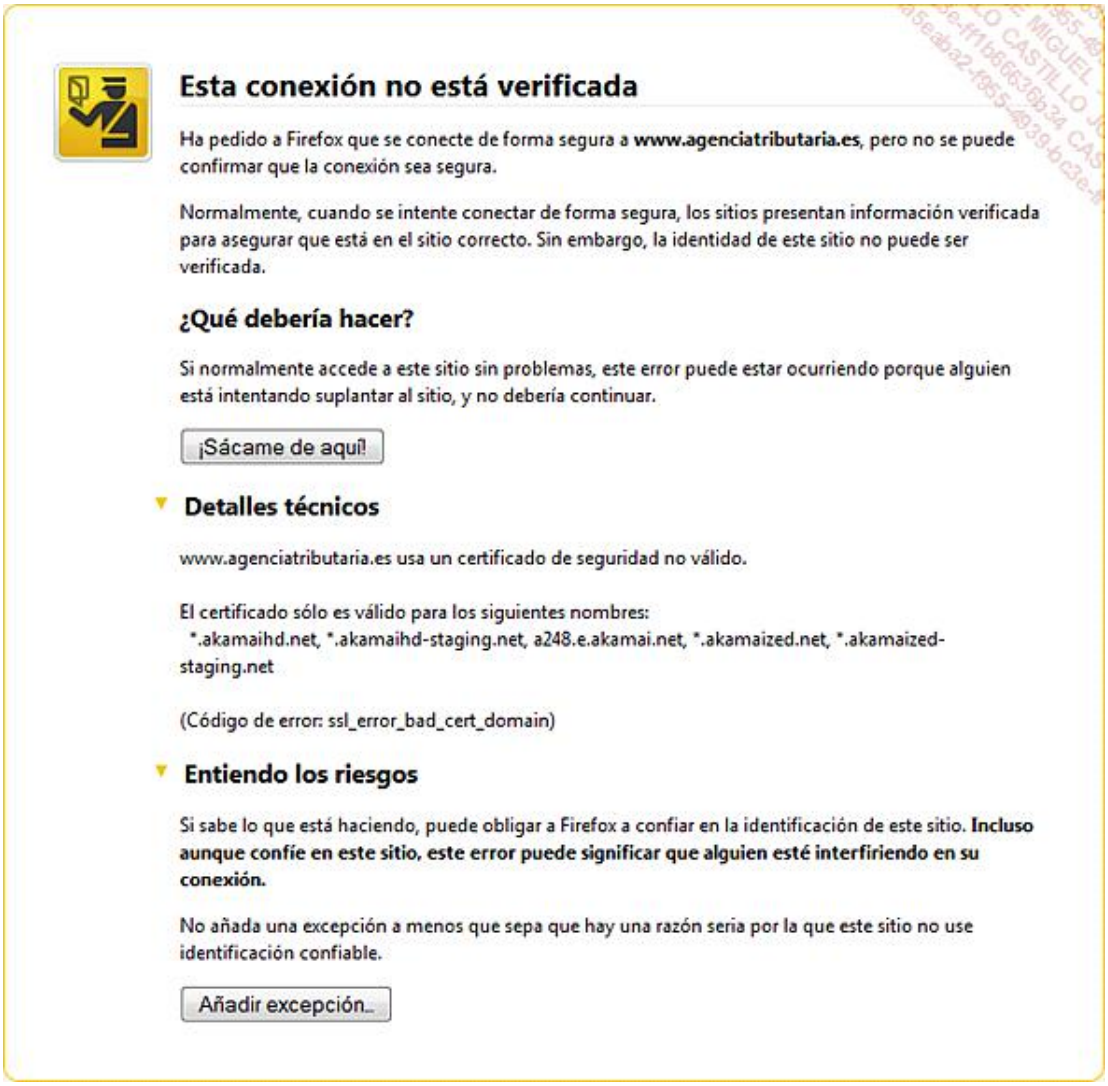
La informática permite, como en otros aspectos de la vida, el uso de una especie de carnet de identidad, el certificado electrónico, que debe ser reconocido por todos los sistemas, y, por tanto, su formato es estándar. El actual es X509, en su versión 3. A petición de uno de los extremos de la comunicación, el otro presenta su certificado para justificar su identidad.



Una entidad entrega un certificado electrónico: la autoridad de certificación (CA - *Certificate Authority*) o una de sus delegaciones. El ordenador que pide la comprobación debe conocer a esta entidad. Esta autoridad es la garantía de confianza.

Si no se reconoce la autoridad de certificación, aparece un mensaje explícito en el navegador (en los navegadores de nueva generación). En caso de no reconocimiento de la autoridad de certificación, esta página sustituye al cuadro de diálogo que conocemos.

Certificado no reconocido en Internet Explorer 11

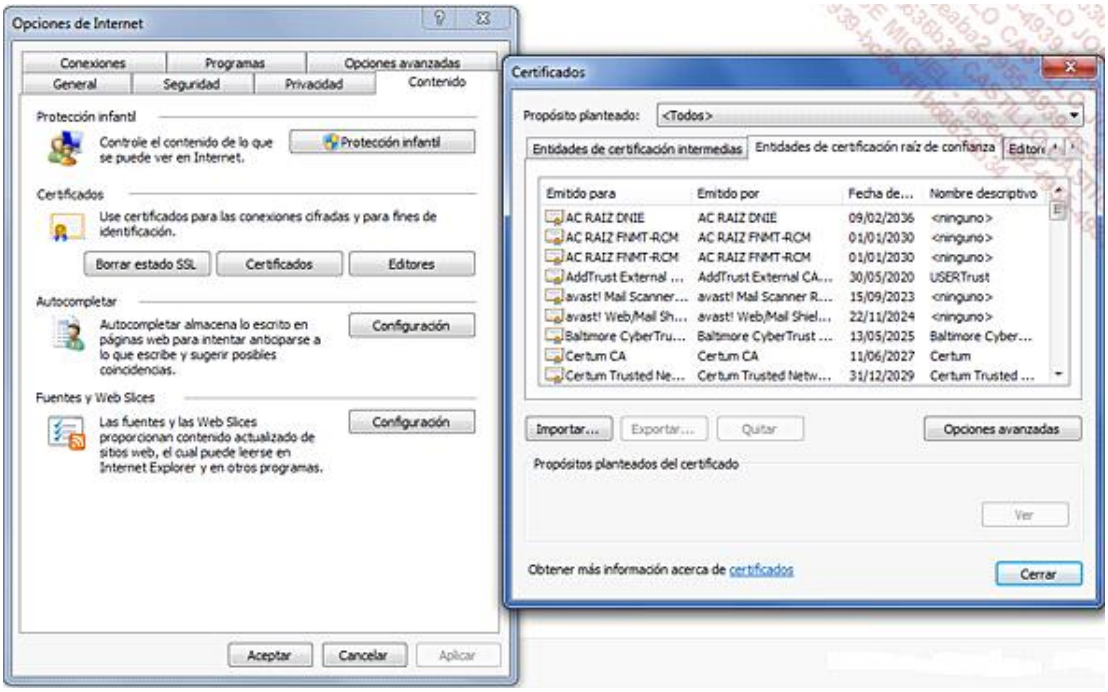


Certificado no reconocido en Firefox 37

Una empresa puede poner en marcha sus propios servidores de entrega y gestión de certificados. Este sistema es la infraestructura de gestión de claves (PKI - *Public Key Infrastructure*), ya que, y lo veremos más adelante, la gestión de las identidades solo es una de sus funciones.

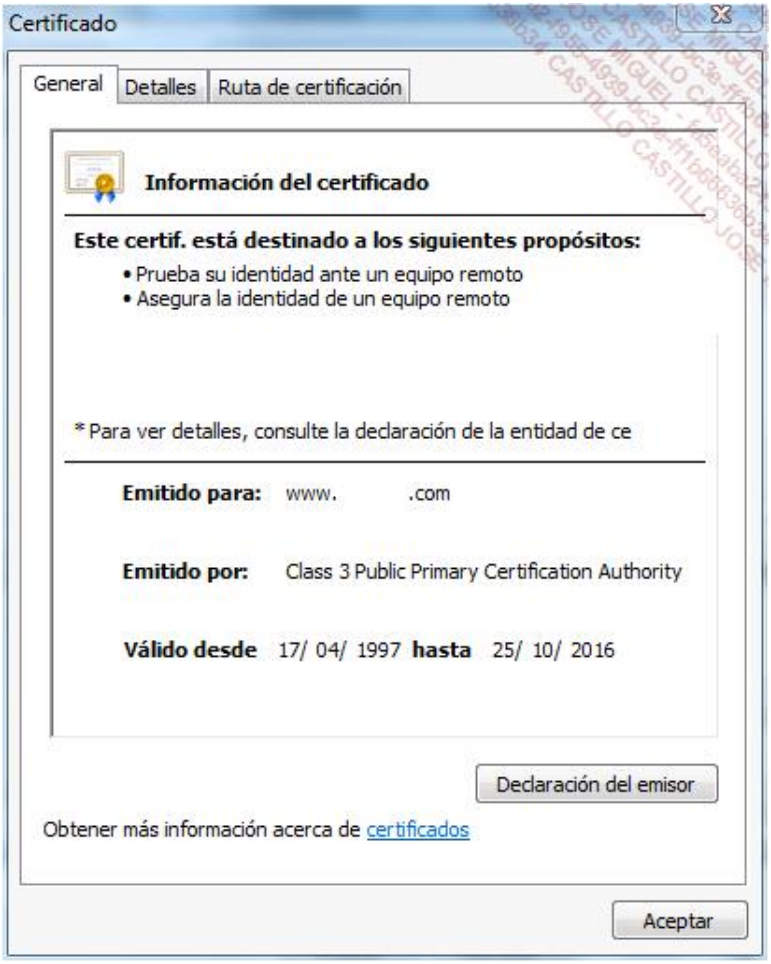
Para evitar el despliegue y la administración de esta infraestructura, los certificados se pueden comprar a empresas especializadas. Están reconocidas a nivel mundial.

Se debe reconocer la identidad justificada por el certificado. Para esto, es necesario, en primer lugar, que la autoridad que entrega el certificado esté reconocida por el sistema que la comprueba. En los sistemas Windows, por ejemplo, están enumeradas en las propiedades de Internet Explorer, en la ficha **Contenido**. Si se despliega una infraestructura de gestión de claves para la empresa, es necesario que todos los equipos y servidores interesados la reconozcan.



Raíces de confianza en IE11

Los certificados electrónicos pueden justificar la identidad de un usuario o de un servidor. También tienen otras aplicaciones.



Ejemplo de certificado

b. La autentificación por contraseña

La contraseña actualmente representa el medio de autentificación más común.

La primera categoría es la contraseña estática. Se trata de una simple secuencia de caracteres alfanuméricos y especiales, elegidos por el usuario, y por un periodo que puede ser limitado o ilimitado. Para comprobar su introducción, se almacena en un archivo o una base de datos en el ordenador o en un servidor. Esta contraseña puede ser objeto de diversos ataques para intentar obtenerla, por ingeniería social, diccionario o fuerza bruta.

El uso de contraseñas dinámicas reduce la debilidad de la autentificación. Entre las técnicas utilizadas, la más usual combina el conocimiento del código de autentificación con un soporte físico. Cada contraseña, también llamada testigo (*Token*), se puede usar una sola vez (OTP - *One Time Password*). Se ofrece al usuario por medio de un generador, la tarjeta de testigo, que la calcula aleatoriamente. Se incluye un factor temporal para hacerla única. También es necesario el correspondiente componente informático en el servidor para que valide esta contraseña. La solución más conocida de este tipo es RSA, de Secure ID, cuyo modelo de tarjeta de testigo es el que se ve a continuación:

En cuanto a su implementación, esta solución es un poco más compleja que la anterior. Además, requiere la sincronización regular de la tarjeta de testigo con el servidor. Es muy difícil que falle, mientras no roben el componente físico o no se pierda. El acceso a este se puede proteger con un código.

c. La autentificación con soporte físico

Ya hemos visto que las soluciones de contraseña dinámica pueden recurrir a un soporte físico. Pero este dispositivo se puede utilizar en una sola solución de autentificación. En este caso, es necesario el reconocimiento del objeto a distancia o por inserción en un lector. Este medio es mucho más seguro que el uso de una contraseña estática y resulta más sencillo que la solución con contraseña dinámica.

El soporte físico puede ser una tarjeta inteligente. Su accesibilidad lógica requiere además el conocimiento de un código, el *Personal Identification Number* (PIN). Muy utilizado en tarjetas de crédito, o en el *Subscriber Identity Module* (SIM) de la telefonía móvil.

Una tarjeta inteligente requiere un lector específico. Ofrece una pequeña capacidad de memoria y puede contener contraseñas, o incluso el certificado de identidad de su dueño.

Un segundo soporte puede ser una llave USB especial. Al contrario que la solución anterior, el conector, presente en todos los ordenadores modernos, permite leer su contenido. Este medio también ofrece más capacidad de memoria para el almacenamiento de información personal. Su acceso puede estar protegido por una contraseña o incluso por reconocimiento de la huella dactilar.

d. La autentificación por biometría

Una huella dactilar es una característica biométrica. Permite comprobar directamente la identidad de la persona y no requiere nada más, ni código PIN, ni contraseña. Se trata del medio más sencillo y seguro para el usuario. De hecho, ¡el usuario siempre lleva el identificador con él y es muy difícil de robar!

En contraposición, el acceso biométrico es un poco más complejo y requiere dispositivos más costosos. La huella dactilar es el mecanismo más sencillo, más utilizado que soluciones como el reconocimiento de voz o la lectura del iris.

La comprobación de la singularidad de las características del dedo es muy accesible; para ello se utilizan lectores específicos o incorporados al teclado, al ordenador portátil o al dispositivo móvil.

En contrapartida, esta autentificación no permite una disponibilidad permanente a determinada información, que se almacena en tarjetas inteligentes y llaves USB.

Ejemplos de dispositivos de autentificación

Los dispositivos generalmente no permiten la lectura de la huella dactilar poniendo el dedo encima. De hecho, la huella se podría recuperar si se marcase así sobre el lector. Como vemos en las fotografías anteriores, los dispositivos necesitan que se deslice el dedo sobre un escáner.

3. Confidencialidad

Hacer secreto un mensaje es la primera función de los sistemas de criptografía. Para esto se realiza una transformación, llamada codificación, de la información confidencial, el texto sin protección. El resultado es un texto cifrado o criptograma. El texto original se encuentra normalmente a través de una operación de descifrado.

Con frecuencia se utiliza la expresión encriptación en lugar del término cifrado.

En informática, las funciones matemáticas, los algoritmos criptográficos, generan claves que pueden servir para los cálculos de cifrado o descifrado.

Realizar un desencriptado es intentar encontrar el texto desprotegido a partir de un criptograma, sin conocer la clave de descifrado. Esta acción se cataloga como análisis criptográfico.

La necesidad de confidencialidad en el intercambio de información es aún más importante en las redes abiertas. Si el paquete no debe leerse cuando viaja entre el emisor y el receptor, es necesario cifrarlo, para que circule transparente. Esto se puede realizar en las capas bajas, medias o altas del modelo de red.

En términos de almacenamiento, si una información se considera confidencial, se debe cifrar el archivo que la contiene. Esta acción de cifrado se recomienda particularmente en dispositivos portátiles y móviles.

Se utilizan dos familias de sistemas criptográficos para hacer confidenciales las comunicaciones de red. Emplean:

- Claves simétricas, utilizadas a la vez para el cifrado y el descrifrado.
- Claves asimétricas (privadas/públicas), utilizadas cada una para una de las dos tareas.

a. El cifrado con claves simétricas

Este método es el más antiguo. Se utiliza una sola y única clave generada por un algoritmo. Es necesaria tanto para la operación de cifrado como para la de descifrado.

Esta clave, que tiene que ser secreta, debe transmitirse siempre entre el emisor y el destinatario. Se trata del principal problema del uso de este sistema.

La fiabilidad del intercambio de mensajes cifrados por clave simétrica depende de dos factores:

- El tamaño de las claves.
- Su frecuencia de renovación.

Es necesaria una correspondencia equilibrada entre la longitud de la clave y la potencia de cálculo solicitada. De hecho, si la clave es demasiado pequeña, se puede descubrir fácilmente y los paquetes pierden su confidencialidad. Si es muy grande, los cálculos de cifrado/descifrado pueden necesitar una capacidad de procesador incompatible con las necesidades de otras comunicaciones simultáneas o la utilización de dispositivos poco potentes (PDA, smartphone...).

Se asigna manualmente una clave estática, tanto en el emisor como en el receptor. En este caso, se puede determinar que no se renueve la clave. Esto aumenta las oportunidades que tiene un pirata de encontrarla. Es preferible el uso de métodos de utilización de claves dinámicas, es decir, renovadas regularmente.

Los algoritmos de cifrado simétricos más utilizados son:

- *Rivest's Cipher* n°4 (RC4), que utiliza claves de diferentes tamaños, generalmente hasta 256 bits.
- Triple DES, variante del algoritmo anterior, que calcula sucesivamente con 3 claves DES, dos de ellas diferentes.
- *Advanced Encryption Standard* (AES), el más reciente, con claves de 256 bits.


El algoritmo Data Encryption Standard (DES), cuyas claves son de 56 bits, ya es obsoleto porque se consideraba demasiado inseguro.

b. El cifrado de claves asimétricas

Complementaria a la técnica de clave simétrica, esta utiliza dos claves distintas:

- La primera, privada, tan solo la conoce su propietario.

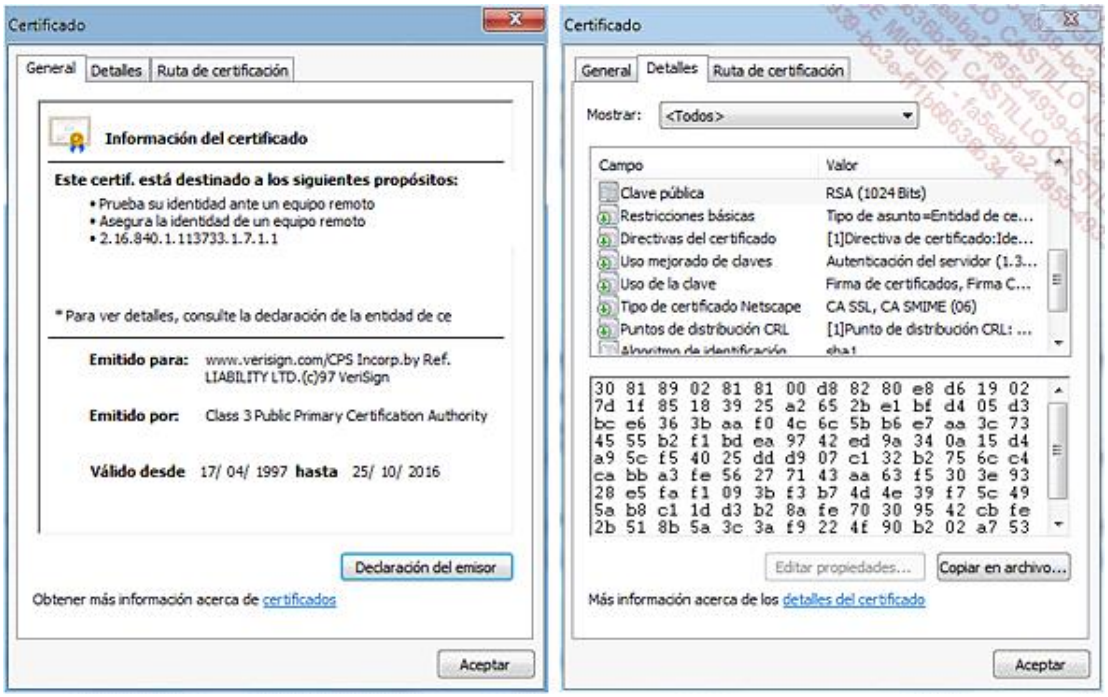
- La segunda, pública, que es la que se transmite.

Estas dos claves están relacionadas matemáticamente, lo que hace una solo puede deshacerlo la otra. En cambio, no es posible encontrar una por medio de la otra. Si se hace un cifrado con la clave pública, solo la clave privada correspondiente, que está protegida permanentemente, puede descifrar el mensaje.

Este método asimétrico implica no tener que generar sistemáticamente un nuevo par de claves. Eso implicaría complicaciones de administración y gestión de claves. Se prefiere que la clave tenga una vida más larga, lo que conlleva unos tamaños de clave más grandes que antes.

La utilización de cifrados asimétricos generalmente requiere la implementación de una infraestructura de gestión de claves (PKI - *Public Key Infrastructure*), como la que se utiliza para la identificación. De hecho, hay que identificar al dueño de la clave pública. Por eso se añaden las características al certificado, que igualmente tiene la clave pública que se ha de utilizar.

En la siguiente impresión de pantalla, vemos que al fabricante se le asocia una clave pública.



Las claves privadas se almacenan en una parte no pública del certificado.

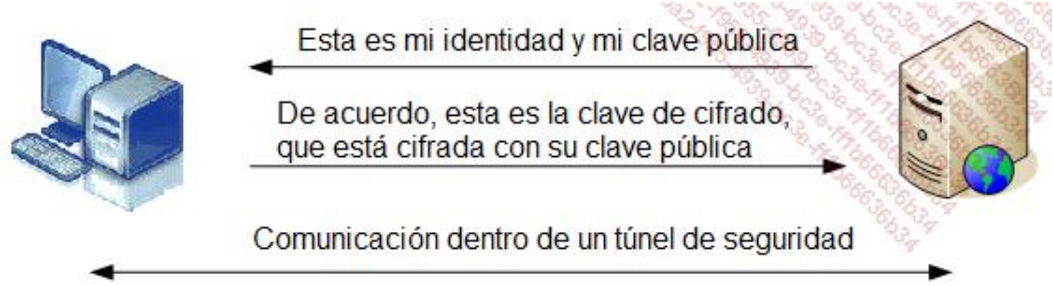
Los certificados electrónicos también proporcionan en su parte pública el algoritmo de tabla hash utilizado para comprobar la integridad de los paquetes entregados.

El algoritmo de cifrado asimétrico más utilizado es Rivest, Shamir, Adelman (RSA), del nombre de sus tres creadores, que compite con el Diffie-Hellman. Las claves utilizadas tienen generalmente tamaños de 1024 o 2048 bits, o incluso superiores.

Para las comunicaciones de red, el cifrado con estas claves de todos los mensajes implicaría potencias de cálculo muy importantes. Es más bien la clave simétrica de cifrado la que se protege al viajar con un sistema asimétrico. A partir del momento en que cada entidad posee una clave, se puede implementar un túnel de cifrado. De hecho, la comunicación no será comprensible para cualquier otro sistema.

Secure Socket Layer (SSL), cuya versión 3 se estandariza como *Transport Layer Security* (TLS), funciona así. Este protocolo de protección de transacciones se utiliza, por ejemplo, en las comunicaciones web efectuadas por *HyperText Transfer Protocol Over TLS* (HTTPS). La implementación de esta seguridad se desarrolla del siguiente modo.

El servidor web proporciona en primer lugar su certificado, que el cliente debe reconocer. Este último genera una clave de cifrado simétrico, cifrada a su vez con la clave pública proporcionada por el certificado. Luego, esta información se reenvía al servidor, que puede encontrar la clave simétrica gracias a su clave privada. A continuación, toda la comunicación está cifrada dentro de un túnel seguro.



4. Protección de los datos de usuario

Uno de los principales problemas en materia de seguridad es la protección de los datos sensibles de la empresa. Estos datos están en manos de los usuarios.

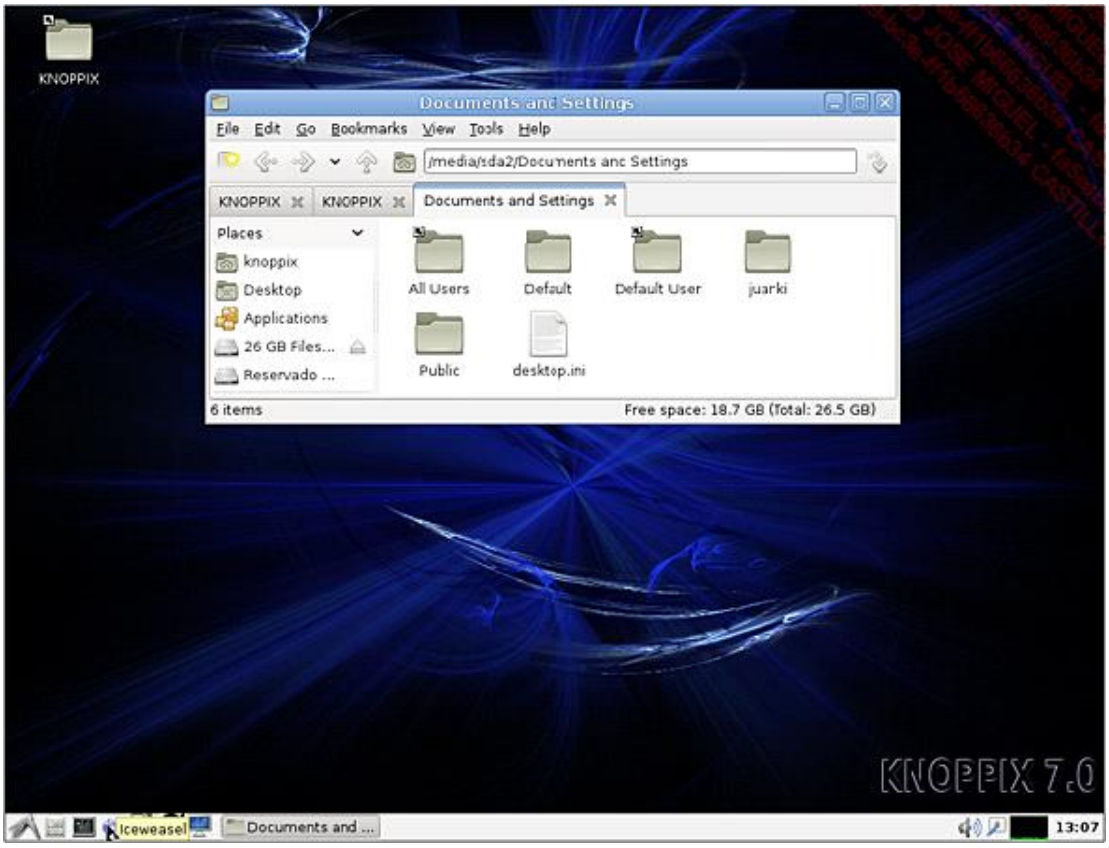
A menudo, la empresa no tiene otra opción que permitir al usuario trabajar localmente con estos datos en dispositivos móviles como ordenadores portátiles.

Casi siempre, la primera protección del equipo es únicamente una contraseña de administrador que nadie conoce.

Desafortunadamente, si el acceso como administrador a menudo no es posible cuando se arranca el equipo de manera normal, no sucede lo mismo cuando se utiliza algún otro sistema de tipo «Live CD» para arrancar el ordenador. Es entonces cuando se toma conciencia de que la seguridad de los datos del ordenador es mínima.

Un «Live CD» es un sistema operativo en un soporte removible que arranca completamente sin instalar nada en el disco duro del ordenador.

De este modo, si se arranca un equipo con Windows formateado en NTFS, con una versión de Knoppix de Linux, se accede fácilmente al contenido del disco Windows:



Acceso a una partición de Windows a partir de un Live CD Linux

Dispone de información complementaria sobre Knoppix en la URL: http://knoppix.net/

Atención, no se trata de juzgar aquí tal o cual sistema operativo. Es muy fácil recuperar una contraseña de administrador en un sistema UNIX/Linux que tenga una seguridad normal. Sin embargo, es necesario acceder físicamente a la máquina. Es por esta razón por lo que una sala de servidores tiene que estar protegida como una caja fuerte.

Por tanto, es fácil imaginar un robo de datos, a partir a partir del momento en que le roben su portátil.

Existen igualmente otros «Live CD» que ofrecen dar otro paso más y crear un nuevo acceso como administrador.

Veamos qué ofrece Microsoft por su parte.

a. Protección de la inicialización del disco

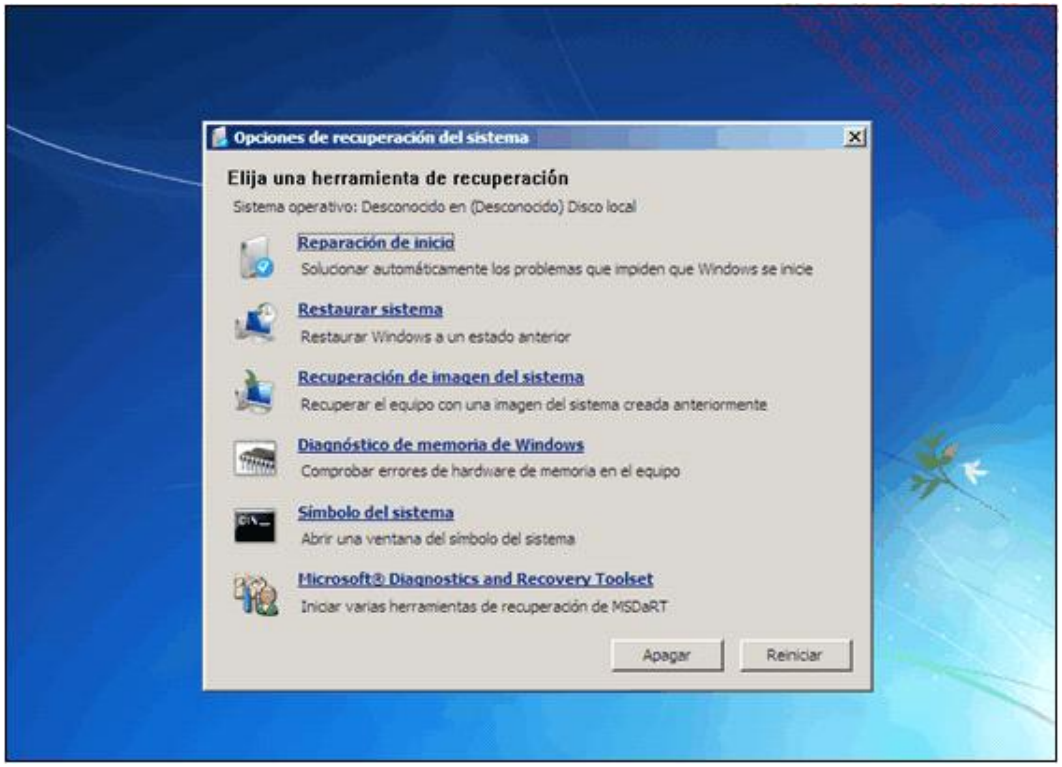
Acceso como administrador a un ordenador

Microsoft ofrece MDOP (*Microsoft Desktop Optimization Pack*), un conjunto de herramientas para empresas que han suscrito un contrato de licencias para sus equipos: este pack de optimización de los equipos integra numerosas herramientas y permite acceder a funcionalidades bajo licencias complementarias.

Dispone de más información sobre Microsoft Desktop Optimization Pack en http://technet.microsoft.com/es-es/windows/microsoft-desktop-optimization-pack.aspx

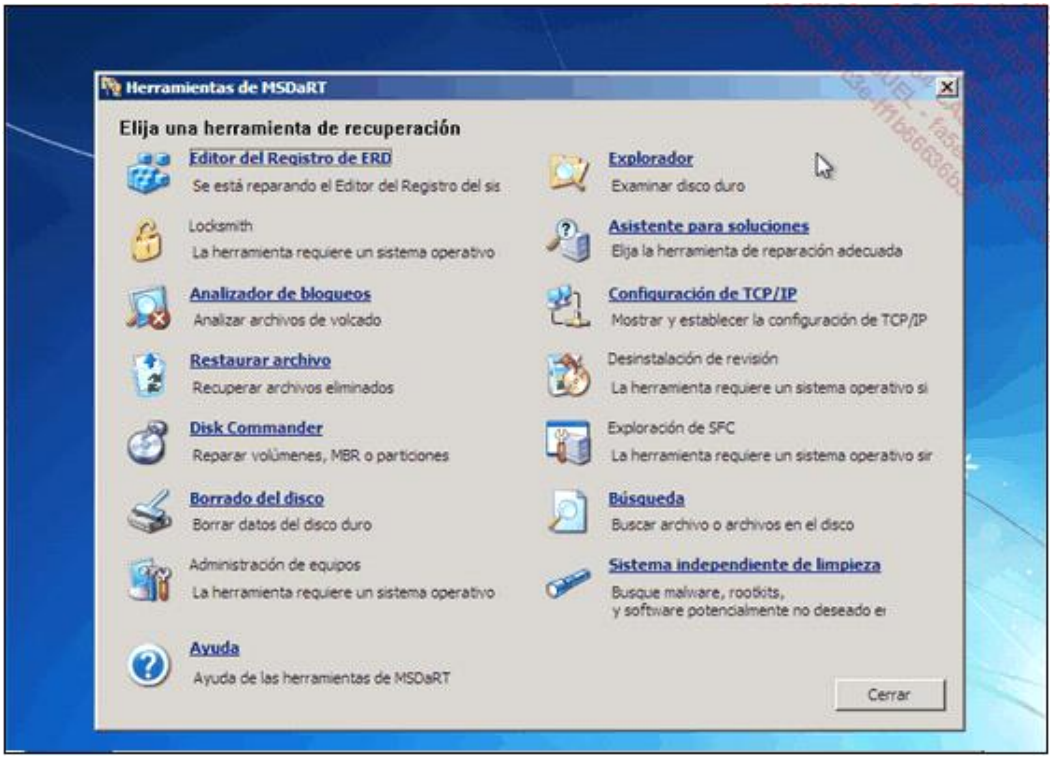
Así, usted puede crear discos autónomos que permiten reparar problemas en los equipos de trabajo.

Cuando arranque con el disco del sistema operativo utilizado, se le ofrecen diversas opciones:



Acceso a diferentes herramientas de reparación

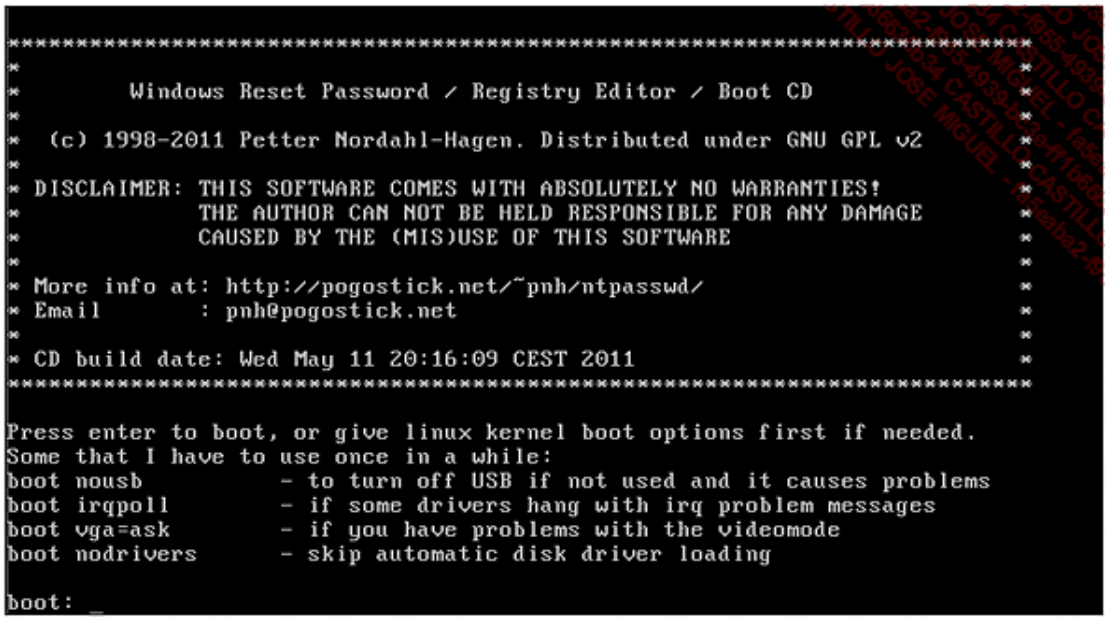
Entre estas herramientas, encontramos **MSDaRT** o **Microsoft Diagnostics and Recovery Toolset**, que integra **Emergency Repair Disk Comander**.



Se proporcionan numerosas herramientas interesantes, entre las que destaca **Locksmith**, que permite crear una nueva contraseña de administrador.

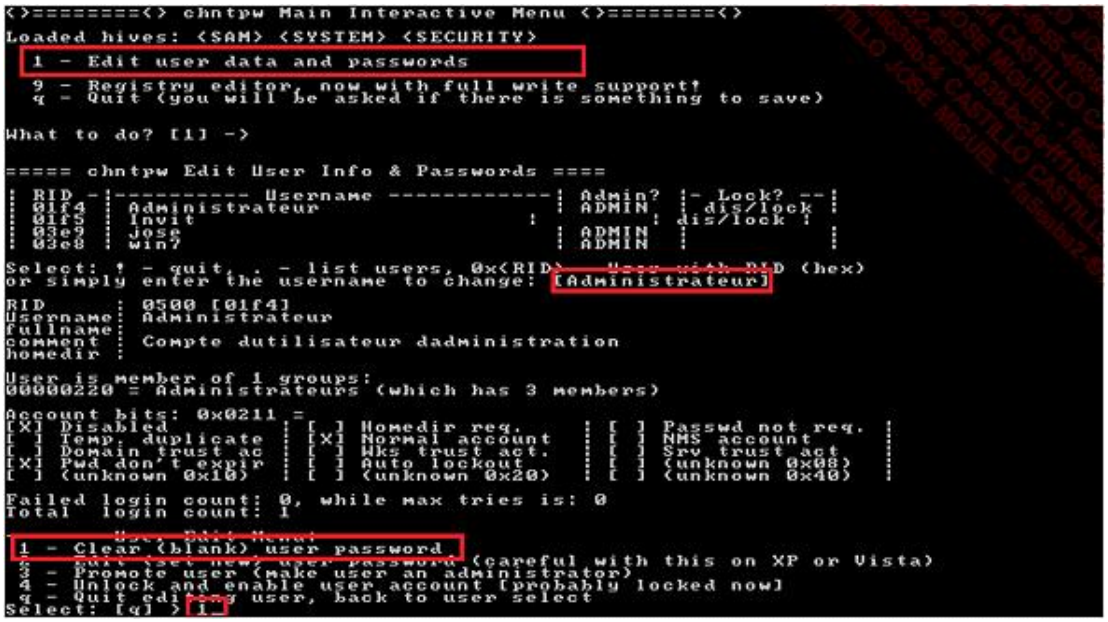
Ejecución de Locksmith

Del mismo modo, existen herramientas de Linux que permiten reiniciar la contraseña de administrador local. La interfaz no es siempre muy amigable.



Ejemplo de herramienta de Linux para reiniciar una contraseña Windows

Basta con elegir las opciones que se ofrecen por defecto para reiniciar la contraseña de administrador:



Reinicio de una contraseña de administrador

Ahora se entiende bien que nuestro sistema operativo, a día de hoy, es vulnerable.

Afortunadamente existen soluciones para fortalecer la seguridad.

En primer lugar, el hecho de poder arrancar el ordenador desde una unidad removible es un fallo de seguridad evidente.

Conviene, pues, proteger con contraseña la BIOS del ordenador para impedir cualquier modificación del arranque y configurar el arranque solo a partir del disco duro local.

Algunas empresas bloquean la utilización de dispositivos USB o solo autorizan algunos que estén homologados.

Vemos que se puede actuar a diferentes niveles:

- Protección del acceso a la BIOS.
- Control de acceso o de utilización de dispositivos móviles.
- Control del arranque del ordenador.
- Protección de datos o, lo que es lo mismo, la protección de las particiones que tienen los datos para convertirlas en inexpugnables si se arranca con otro sistema.

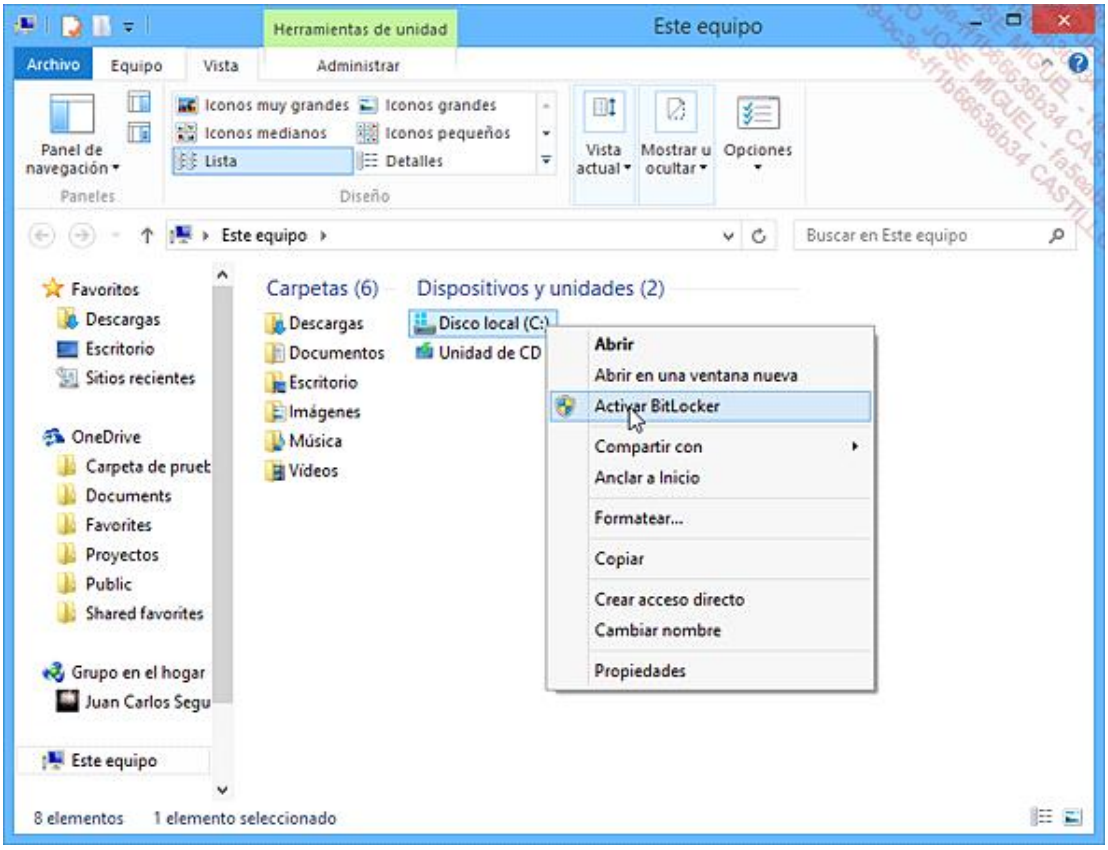
b. Cifrado de los discos locales

Ahora, examinemos las posibles soluciones para proteger los datos sensibles de la empresa.

Cifrado nativo de Windows

Actualmente, la mayoría de los equipos ejecutan Windows. Desde Windows Vista y la siguiente versión ofrecida (solo en Ultimate y Enterprise), es posible activar el cifrado de unidad BitLocker (*BitLocker Drive Encryption*) si el ordenador dispone de una tarjeta TPM (*Trusted Platform Module* o módulo de plataforma de confianza).

Esto va a permitir cifrar todo el disco de sistema e igualmente los discos de datos (locales o removibles).



Activación de BitLocker en la partición de sistema en Windows 8.1

BitLocker permite cifrar todo el disco, asegurando así protección para el sistema y los datos que están almacenados. Asimismo, garantiza la integridad del sistema.

Una vez se ha activado la protección, cualquier archivo grabado se cifra automáticamente. En modo de funcionamiento normal, los archivos se descifran sobre la marcha de manera transparente. Además, si el sistema se modifica, el equipo se bloquea automáticamente.

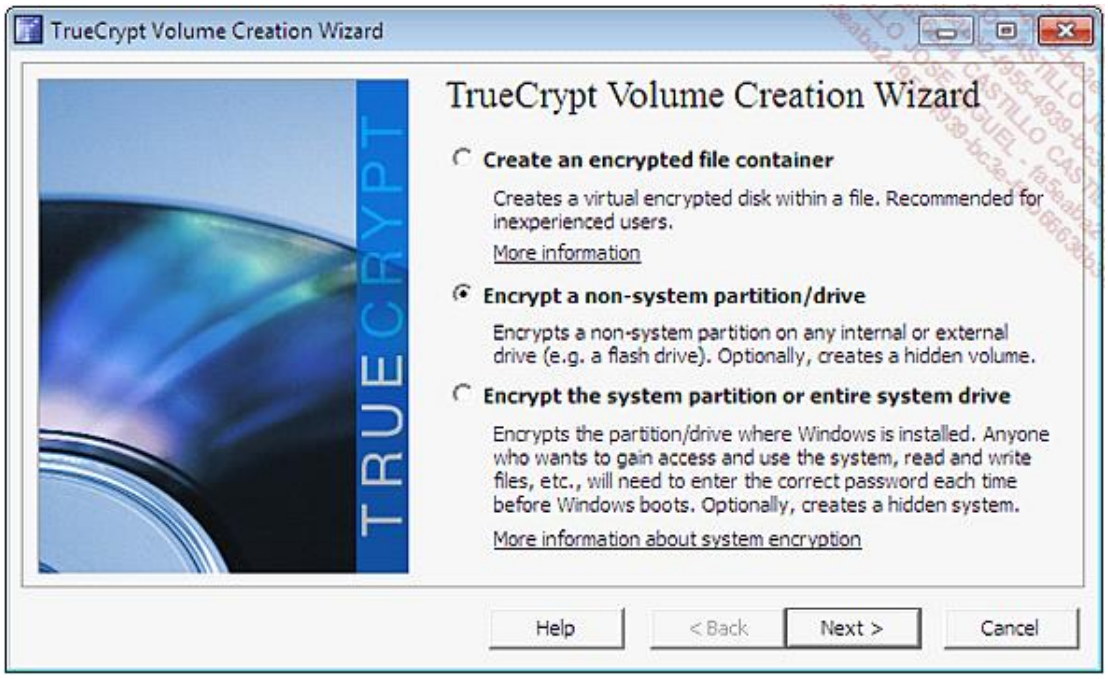
Cifrado con una solución de terceros

Existen muchas soluciones que permiten implementar el cifrado de disco.

En particular, TrueCrypt, que es una aplicación de código abierto ampliamente reconocida.

Dispone de más información en: http://www.truecrypt.org

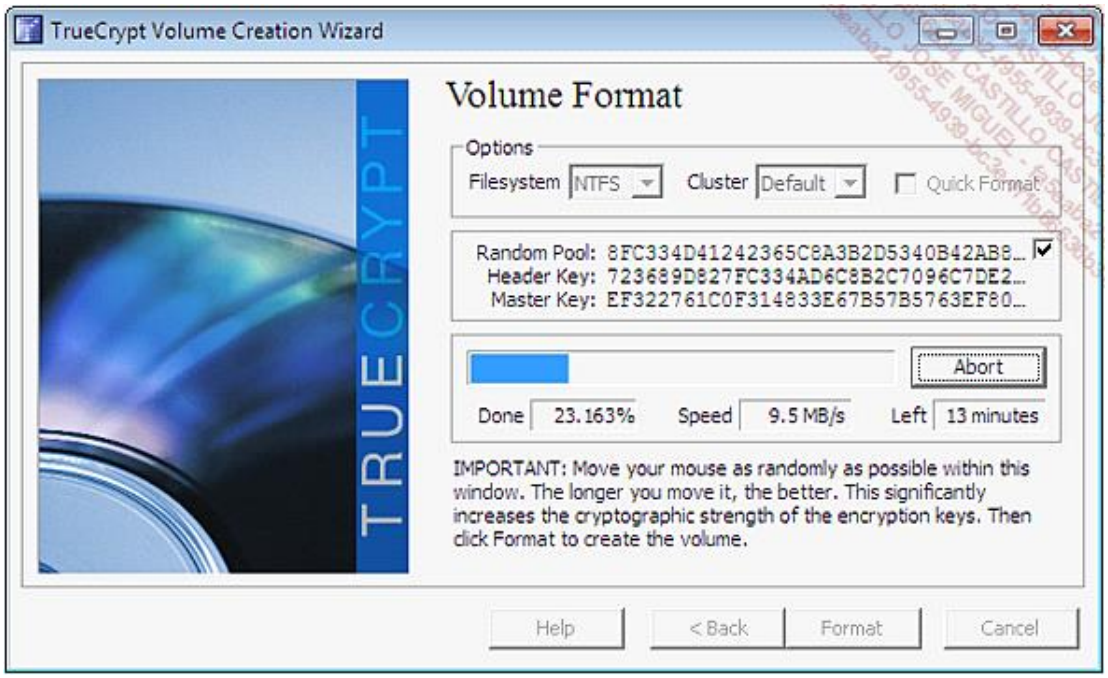
Por ejemplo, para activar el cifrado de una partición del sistema, después de haber instalado TrueCrypt y haber creado la estructura inicial de almacenamiento de las claves (el contenedor), vamos a proceder de la siguiente manera:



Cifrado de un disco de datos con TrueCrypt

Ahora hay disponibles varias opciones. Elegimos activar el cifrado al mismo tiempo que el formateo de la partición, que está en blanco.

Igualmente podríamos activar el cifrado en segundo plano para conservar los datos existentes en la partición de datos.



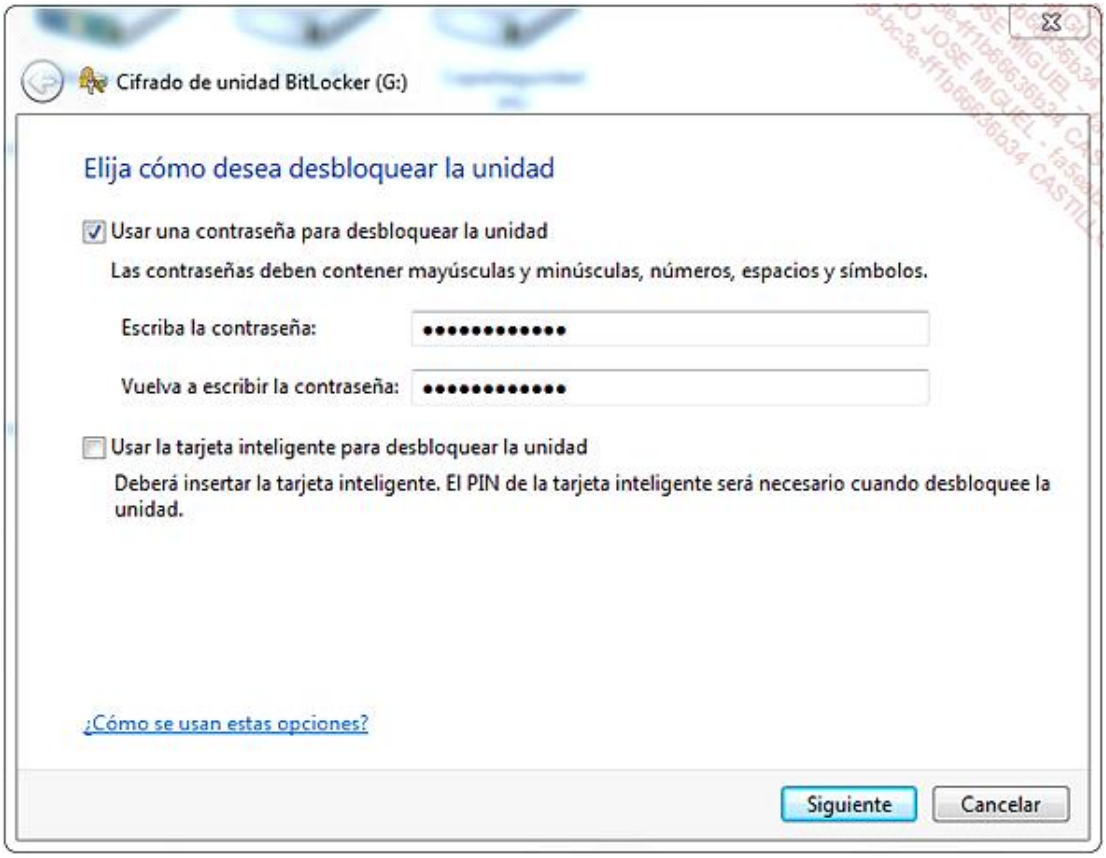
Formateo de una nueva partición con activación del cifrado TrueCrypt

Una vez se ha cifrado la partición, la debemos montar con TrueCrypt para poder utilizarla.

c. Cifrado de discos USB

El cifrado de discos USB se puede implementar con la tecnología *BitLocker To Go* o «cifrado BitLocker portable».

Cifrado de un disco USB externo en Windows



Definición de una contraseña para el cifrado BitLocker

El cifrado de la totalidad del disco se ejecuta como tarea en segundo plano:

Cifrado de un disco con BitLocker To Go