Curso práctico aplicado de protección, privacidad y seguridad de la información (C.A.P.P.S.)

Por Guillermo García Núñez (guillermogn@gmail.com)

Ingeniero Superior de Informática de Sistemas

Noviembre del 2007. Versión 2.2b

Prólogo

A lo largo de los años y después de prestar mis servicios a usuarios de distintas empresas, he visto la necesidad que tienen éstos de proteger su privacidad y por ende, de aplicar medidas de seguridad para lograrlo.

Este libro va orientado a la privacidad, a la gestión y protección de los datos que los usuarios medios almacenan en sus estaciones de trabajo, no importa si trabajan en oficinas, son autónomos, pequeñas empresas familiares o grandes corporaciones; todos deberían proteger sus datos personales, así como la información que es esencial en sus empresas y que suele descansar en ordenadores personales y no en servidores con las medidas de seguridad adecuadas.

La seguridad de la información la podemos vulnerar de muchas maneras, y la tecnología y el desconocimiento suelen aportar bastante a ello.

Este libro-guía de cerca de ciento cincuenta páginas está indexado por temáticas, donde cada capítulo intenta cubrir un área o problema y aportar soluciones y herramientas que puedan ser útiles, además de links a bibliografía en inglés y también en castellano.

He procurado aportar un poco de mi experiencia, y la de otros, que se han tomado la molestia de publicar artículos, sobretodo en Internet, con la intención de mejorar los conocimientos de todos nosotros. Este manual es un poco obra de la comunidad internauta, más que mía, por eso lo devuelvo a Internet para que siga creciendo (si es que así ha de ser).

Esta obra, cuya versión es la 2.1, puede ser modificada y completada. Bastará añadir los nombres de las personas que sigan haciéndola crecer junto al mío, ya sea al principio del documento o mediante un anexo al final del mismo, explicando los cambios que se han ido haciendo a la misma, y sin que cambien las condiciones de la licencia que actualmente acompaña al libro.

No responderé consultas técnicas sobre el libro, ni me comprometo a mantenerlo más allá de lo que he presentado ahora.

Espero que sea útil a muchos, y que pueda servir de apoyo, como a mí me han servido las aportaciones de otras personas, profesionales o no, del mundo de la informática.

Todas las críticas CONSTRUCTIVAS serán bienvenidas. Se que las cosas siempre pueden hacerse mejor, pero no siempre disponemos del tiempo para hacerlo.

Guillermo García

Valencia a 6 de noviembre del 2007

Trabajo actual:

Universidad Politécnica de Valencia (UPV)
Analista-Programador de Sistemas y Redes
Dpto. de Sistemas Informáticos y Computación (DSIC).
Europa – España - Valencia

Capítulo 1. La información debe ser protegida.

1.1. Introducción

No es cierto que un ordenador sea un electrodoméstico más, como tampoco es cierto que pueda ser considerado un mueble más de la casa, o una herramienta más de la oficina.

Los utilizamos en nuestro despacho, en los momentos de ocio, e incluso cuando nos desplazamos. Casi todo el mundo tiene al menos uno a su disposición, y no importa si se trata de un sobremesa, un compacto, un portable o un portátil.

Lo fundamental es que se han convertido en algo valioso en lo que depositamos nuestra confianza. Esa confianza genera una cadena de valor, por la cual él nos sirve y nosotros a cambio, llenamos su disco duro de proyectos, estudios de mercado, bases de datos de clientes, información sobre proveedores o personal de la empresa, agendas, emails, documentos, acuerdos comerciales y un sin fin de cosas más que nos hacen dependientes de la máquina.

En tan solo uno o dos años, puede atesorar la mayor parte del conocimiento que para nosotros es valioso y se convierte en un ente importante. Sin embargo, puede ser robado [1], destruido [2], averiarse o no estar disponible cuando realmente sea necesario.

Al principio, todos le damos una dosis de confianza limitada, y lo empleamos para tareas concretas, luego vamos confiando más en él, hasta que se convierte en nuestra memoria (agenda, emails, Web History, recordatorios, fechas importantes, reuniones, convenciones, conferencias), nuestra máquina de escribir, en quien nos informa de lo que pasa en el mundo (blogs, periódicos, sitios web, noticias RSS [3]), de cómo organizamos las vacaciones (vuelos, viajes, hoteles, mapas), es nuestro representante legal (acceso a la banca online, certificados digitales para acceder a las Administraciones Públicas), cuida las relaciones con familia y amigos (Messenger, emails, VoIP[4], redes sociales[5]), nos pone en contacto con empresas o servicios, nos hace sentirnos parte de algo más grande (Google Maps), nos permite trabajar desde casa, acceder a formación online, compartir conocimiento, estudiar tendencias o nuevos productos, gestionar proyectos y un largo etcétera.

Son muchas las funciones que le vamos otorgando y muy poco lo que hacemos para protegerlo. Es cuestión de tiempo que nos encontremos en un aprieto.

Los ordenadores están expuestos a todo tipo de fallos, sabotajes, robos, espionaje industrial, desastres naturales y errores nuestros.

Cuando hablamos del valor de un ordenador o del servicio que nos presta, siempre pensamos en términos de la información que contiene. Lo valioso es la información y su pérdida en ocasiones, puede ser traumática por lo difícil de recuperarla o por el daño que causa no poseerla. El ordenador en sí siempre es reemplazable, es solo cuestión de dinero y de tiempo. Pero la información, una vez perdida, puede que nunca pueda recuperarse, o peor aún, puede caer en manos de competidores y ser incluso causa

de despido o de demandas por daños y perjuicios con fuertes indemnizaciones si datos sensibles de clientes o proveedores han ido a parar a manos de terceros.

Por si fuera poco, la capacidad para almacenar información en los ordenadores ha crecido exponencialmente en los últimos tiempos, y ahora podemos almacenar años de trabajo, sin que nos veamos en la necesidad de tirar nada, lo cual resulta contraproducente a nivel de privacidad y dificulta la tarea de realizar copias de seguridad, por el elevado espacio que se llega a necesitar para las mismas.

1.2. Las copias de seguridad como solución.

Es común la creencia de que teniendo una copia de los datos por si se pierden, y haciendo copias de seguridad con regularidad, es suficiente. Estudiemos esa afirmación hecha tan a la ligera.

Si nos roban un bien tan intangible como es la información de nuestro ordenador de la oficina o de casa, la pregunta es: ¿Alguien puede sacarle partido?, ¿podrían usarlo contra los intereses de mi empresa o los míos propios?, ¿iría ese aprovechamiento en detrimento de un futuro prometedor? Casi siempre la respuesta es que sí.

Hace un par de años, se hizo un estudio[6] sobre los riesgos a los que se someten los ciudadanos al no saber cuidar, proteger y/o destruir la información adecuadamente. Dos estudiantes del MIT adquirieron por Internet y en tiendas de segunda mano discos duros a bajo precio. Luego intentaron recuperar la información con herramientas especiales. En muchos casos, sus anteriores propietarios no habían borrado los discos duros, y en el resto, que sí lo había hecho, el proceso se había efectuado de forma inadecuada.

El resultado fue que obtuvieron desde datos de cuentas bancarias, hasta información sobre tarjetas de crédito, declaraciones de renta, y un sinfín de cosas más. Algunas de ellas comprometedoras en aspectos de carácter privado y personal; y otras, peligrosas desde el punto de vista de la entidad a la que había pertenecido la persona propietaria del ordenador en cuestión.

Con esto vemos, que no basta con protegernos de la pérdida de la información, sino que en caso de pérdida, debemos asegurarnos que otros no puedan acceder a ella. Y siempre que un equipo quede obsoleto, debemos asegurarnos que todos los datos han sido, no borrados, sino destruidos, porque en caso contrario, pueden ser recuperados[7].

1.3. Medidas del riesgo.

Lo primero que tendemos a averiguar siempre que roban a alguien, es dónde ha sucedido y a qué hora, si no coincide con nuestros hábitos, entonces nos relajamos y nos sentimos más seguros. A nosotros no nos pasará porque no vivimos o trabajamos en ese barrio. Tal vez fue porque iba solo o hizo gala de opulencia, lo cual llamó la atención de personas indeseables. Intentamos así creer que nosotros estamos fuera del alcance de esos individuos.

Forma parte de la naturaleza humana alejar los peligros y los malos pensamientos de nuestra mente rodeándonos de una falsa seguridad que en ocasiones resulta en un peligro mayor. Existe un artículo muy interesante sobre ese tema y el optimismo que aplicamos al riesgo (leer artículo en inglés).

Por otra parte, artículos como éste, pueden hacernos ver la realidad más cercana.

1.4. Las Herramientas.

Si tenemos claro lo importante que es proteger la información y garantizar nuestra privacidad, hemos de conocer las herramientas que hay a nuestro alcance. Algunas, son las mismas que otras personas pueden emplear para acceder a nuestros datos.

Internet es hoy en día una gran biblioteca donde se puede aprender y encontrar casi de todo. Con tiempo y dedicación cualquiera puede aprender lo suficiente, como para que proteger la información de nuestro negocio, trabajo, proyecto o clientes, sea esencial. Por ejemplo, un psicólogo que atiende a sus pacientes, les prepara ejercicios, les enseña técnicas y estudia y describe su evolución a través de informes, dispone de mucha información personal que queda registrada en el historial del paciente. La Ley Orgánica de Protección de Datos (LOPD), obliga a proteger esos datos adecuadamente.

Un asesor fiscal tiene que asegurarse que los datos de las empresas con las que trabaja y las declaraciones de renta que lleva a cabo, están protegidas y no puedan ser fácilmente accedidas por medios fraudulentos.

En la página de El Mundo, podemos ver el valor que se le da a la información personal por parte de las empresas. Además de varias notas interesantes de lo que está pasando en Estados Unidos en nombre de la seguridad del país, podemos acceder a una curiosa calculadora, donde veremos el valor que se le da a cada dato personal nuestro (es necesario tener instalado el plugin de Flash).

Hay información más completa sobre el tema en el siguiente artículo, escrito por Horacio M. Lynch y Mauricio Devoto, en concreto, la parte más interesante del tema sería ésta, relacionada directamente con lo que estamos hablando.

La información es pues, un bien que debe protegerse porque la ley exige a esas empresas de pequeño o mediano tamaño que lo hagan, y la mayoría no lo hace debidamente[9].

Es tal la importancia que posee en la sociedad actual que existen estándares sobre como debe ser tratada y gestionada. La primera normal referente a la seguridad de la información es la ISO 7799, a la que luego le sucedió la 17999, ahora englobada en la ISO 27000 (ISO 27000).

Podemos leer más del tema aquí:

- ISO 17999:
  - http://www.enterate.unam.mx/Articulos/2005/febrero/seguridad.htm
  - http://www.virusprot.com/Art41.htm
  - http://www.iso-17799.com/
- ISO 27000:
  - http://www.security.kirion.net/seguridad/
  - http://seguridadit.blogspot.com/2006/01/norma-iso-17799-vs-iso-27001.html
  - http://www.molemag.net/
  - http://www.pc-news.com/detalle.asp?sid=&id=10&Ida=2544
  - http://sociedaddelainformacion.wordpress.com/tag/seguridad/iso-27000/

Bibliografía

[1]. General Electric ha revelado recientemente el robo de un ordenador portátil de la compañía con los nombres y datos de la Seguridad Social de 50.000 empleados.
El ordenador, en manos de un directivo de General Electric autorizado a tener esos datos, fue sustraído de la habitación de un hotel que estaba cerrada con llave, dijo la empresa.
La compañía tuvo que enviar cartas electrónicas a todas aquellas personas cuyos nombres y datos de la Seguridad Social estaban en el portátil para notificarles el fallo y ofrecerles acceso gratuito durante un año a un servicio de vigilancia de crédito.
La empresa declinó dar más detalles sobre dónde y cuándo tuvo lugar el robo o si el ejecutivo sigue trabajando en General Electric.
Sin embargo, apuntó que las pruebas indicaban que el ladrón estaba más interesado en el ordenador que en los datos que contenía, y aseguró que no había indicios de que la información hubiese sido usada inadecuadamente.

[2]. En los últimos meses han explotado, quemado y ardido unos cuantos portátiles por todo el mundo. Parece ser que la responsabilidad viene de las baterías que han resultado ser defectuosas. Fabricantes como IBM, Lenovo, Toshiba, Apple o Dell están retirando millones de baterías del mercado. El denominador común de estos incidentes parece ser Sony, que es quien suministró las baterías a todas estas marcas. En los aeropuertos empiezan a plantearse marcarlos como equipaje peligroso. El problema de estas partidas defectuosas parece tener su origen en la presencia de partículas metálicas microscópicas en las celdas de ion de litio que forman las baterías. En determinadas circunstancias, aún por determinar, estas partículas podrían ser capaces de producir cortocircuitos. Lo que parece indudable es que el problema que nos ocupa ahora empeora con el tiempo, ya que los incidentes aparecen cuando ha transcurrido un año o más de la venta del equipo.

[3]. RSS es parte de la familia de los formatos XML desarrollado específicamente para todo tipo de sitios web que se actualicen con frecuencia y por medio del cual se puede compartir la información y usarla en otros sitios web o programas. A esto se le conoce como redifusión o sindicación.
El RSS no es otra cosa que un sencillo formato de datos que es utilizado para sindicar (redifundir) contenidos a suscriptores de un sitio web. El formato permite distribuir contenido sin necesidad de un navegador, lo cual también puede verse como desventaja ya que necesita de la instalación de otro software. Algunos adelantos han permitido utilizar el mismo navegador para ver los contenidos RSS. El acrónimo se usa para los siguientes estándares:

* Rich Site Summary (RSS 0.91)
* RDF Site Summary (RSS 0.9 y 1.0)
* Really Simple Syndication (RSS 2.0)

[4]. Voz sobre Protocolo de Internet, también llamado Voz sobre IP, VoIP, Telefonía IP, Telefonía por Internet, Telefonía Broadband y Voz sobre Broadband es el enrutamiento de conversaciones de voz sobre Internet o a través de alguna otra red basada en IP.

[5]. Redes Sociales. En 2002 comienzan a aparecer sitios web promocionando las redes de círculos de amigos en línea cuando el término se empleaba para describir las relaciones en las comunidades virtuales, y se hizo popular en 2003 con la llegada de sitios tales como Friendster, Tribe.net, MySpace, Ecademy, openBC, Soflow y LinkedIn. Hay más de 200 sitios de redes sociales, aunque Friendster ha sido uno de los que mejor ha sabido emplear la técnica del círculo de amigos. La popularidad de estos sitios creció rápidamente y grandes compañías han entrado en el espacio de las redes sociales en Internet. Por ejemplo, Google lanzó Orkut el 22 de enero de 2004. Otros buscadores como KaZaZZ y Yahoo crearon redes sociales en 2005.

[6]. Durante dos años, un par de estudiantes del MIT han adquirido discos de segunda mano a través de subastas en Internet y tiendas de segunda mano. De un total de 129 discos adquiridos y operativos, fue posible recuperar archivos en un total de 69. Y de éstos, en 49 había información "privada": datos médicos, cartas de amor, pornografía y más de 5.000 números de tarjetas de crédito.
Esto puede poner los pelos de punta al indicar que, según algunas estimaciones, durante el año 2002 un total de 150.000 discos duros fueron "jubilados". Si bien la mayoría de estos discos retirados acaban en la papelera, un porcentaje significativo de los mismos pasa al mercado de segunda mano.
Hoy en día los en los discos duros de todos nosotros tenemos almacenada una gran cantidad de información altamente sensible, que bajo ningún concepto deseamos pueda llegar a manos de cualquier otra persona.

[7]. El problema fundamental es que los ordenadores de los que se deshacen particulares y empresas contienen a veces información confidencial, que puede ser aprovechada por chantajistas, pederastas o timadores, según ha publicado el diario británico 'The Times'. La mayor parte de los discos duros fueron adquiridos a través de eBay. Como elemento de control, otros 10 se compraron en LCS Remploy, una empresa dedicada a la destrucción de datos, que garantizó que estaban 'limpios'.
Entre los datos almacenados había información extremadamente personal, como números de la seguridad social, pruebas de una aventura extramatrimonial e información biográfica muy detallada sobre menores (perfiles psicológicos incluidos), dado que, por ejemplo, analizaron discos duros de equipos provenientes de una escuela primaria de la Iglesia de Inglaterra situada en East Yorkshire.
El caso de los expedientes de los menores es especialmente delicado. 'The Times' explica que en ese caso se da un claro incumplimiento del Acta de Protección de Datos del Reino Unido. El director del grupo de estudio aseguró al rotativo que había encontrado información muy comprometedora, incluso cuando sólo habían visto una parte muy pequeña de la información recuperada.

[8]. En un artículo publicado en Hispasec, nos cuentan el caso de un padre de familia que se presentó in situ, cara desencajada, portando un ordenador debajo del brazo. Había recibido una carta de Telefónica donde le informaban que habían detectado que su ordenador estaba enviando spam y que debía ponerle remedio, ya que de continuar la situación podrían tomar medidas judiciales. Lo calmaron y le explicaron que no lo iban a encarcelar, al mirar el ordenador (un Windows XP), lo encontraron cargado de troyanos, virus, gusanos y otros especimenes. Tenía antivirus instalado y actualizado, aunque no había detectado nada. Le limpiaron el ordenador y le cambiaron la configuración de seguridad del navegador.

[9]. Pocas organizaciones inscriben sus ficheros en la Agencia de Protección de Datos. La sustracción de información en España es cada vez más frecuente - El motivo del robo es obtener datos de la competencia - La ley española castiga hasta con 600.000 euros la pérdida de datos médicos.
Los casos destapados muestran que la mayoría de empresas ven comprometidas sus bases de datos de tres formas: por la pérdida de discos de back-up, que suele gestionar una tercera empresa, por la entrada de intrusos o los empleados en el sistema informático, y por el robo de ordenadores.
Para Daniel Cruz, responsable del Departamento de Planificación de Seguridad de ESCERT / Inet Secur, "los robos de datos con información personal suceden también en España, donde siempre ha existido un mercado de datos. Muchas veces no son robos de terceros, sino que las fugas provienen de la propia organización, por errores voluntarios o no".
La Ley Orgánica de Protección de Datos (LOPD) española es considerada una de las más estrictas del mundo. "Hemos investigado pérdidas de bases de datos durante un transporte, su aparición en la vía pública, robos de un ex socio o empleado, en entidades financieras, hospitales, empresas y administraciones", relata Jesús Rubí, adjunto al director de la Agencia de Protección de Datos. Las multas son ejemplares: entre 60.000 y 300.000 euros, por no tener medidas de protección, y entre 300.000 y 600.000 euros por pérdida de datos de nivel alto, como la información médica.
Hay un conocimiento creciente de la normativa. Las grandes corporaciones, que tienen las bases de datos más grandes y complejas, ya cuentan con políticas al respecto. El problema son las pymes y los pequeños y medianos ayuntamientos.

Capítulo 2. Sin privacidad

2.1. Introducción

La privacidad se define en el diccionario de la Real Academia de la Lengua (RAE) como:

Ámbito de la vida privada que se tiene derecho a proteger de cualquier intromisión.

Podemos perderla, y lo hacemos cada día de muchas formas:

1. Cuando se recopilan datos sobre nosotros sin que lo sepamos y sin nuestro permiso.
    - Es el caso de la navegación web.
    - De las búsquedas por Internet.
    - De las compras en Internet.

2. Cuando tiramos documentos, informes o datos nuestros sin destruirlos.
    - Al borrar datos del disco duro sin hacerlo adecuadamente.
    - Al tirar las cartas a la basura sin triturarlas.
    - Al no destruir cds y dvds antes de tirarlos.
    - Al deshacernos de viejas agendas, papeles, notas, apuntes, fotos, carnets identificativos (DNI, tarjetas de socio, clubes, carnets de conducir, etc.).

3. Cuando damos más información de la necesaria al adquirir o comprar algún servicio.
    - Direcciones, número de miembros en la familia, ingresos, número de tarjetas de crédito, etcétera.
    - Datos personales y/o familiares al darnos de alta en las tarjetas de compra de centros comerciales, supermercados, hipermercados o tiendas.

4. Cuando respondemos a preguntas sobre estadísticas de lo que pensamos, queremos, aspiramos, nuestros hobbies, etc.
    - Al responder a cuestionarios por la calle.
    - A análisis estadísticos y consultas efectuadas por teléfono.
    - A consultas sobre destinos vacacionales.
    - Al comprar coche nuevo y rellenar el cuestionario de opinión.

5. Cuando damos información sin que nos sea pedida sobre nuestra vida privada.
    - Problemas en la familia.
    - Disputas con la pareja.
    - Preocupaciones sobre nuestros hijos.
    - Apreturas económicas.

6. Cuando las empresas que disponen de datos nuestros los intercambian o ceden a otras sin nuestro permiso.
    - Los bancos para ofrecer servicios a clientes VIP.
    - Ofertarnos viajes o productos relacionados con otros que ya adquirimos anteriormente.
    - Cuando una empresa que posee nuestros datos es comprada o absorbida por otra, con una política de privacidad distinta a aquella con la que los dimos.

7. Cuando nuestros datos son robados o extraviados por empresas a las que se los dimos voluntariamente.
    - Números de la Seguridad Social.
    - Tarjetas de crédito.
    - Datos sobre cuentas bancarias.
    - Informes médicos.

¿Qué hace todo esto tan distinto en el ámbito informático? Muchas de estas cosas las hacíamos ya cuando no había ordenadores, y entonces no eran tan graves.

Hoy, los ordenadores sintetizan, procesan, ordenan, reorganizan y entrecruzan los datos de miles o decenas de miles de personas a velocidades que antes no se podían plantear. Ese cruce de información o el espacio tan reducido que hace falta para almacenarla, es lo que la hace peligrosa. Cruzando decenas de bases de datos se puede obtener mucha información de alguien.

Supongamos una encuesta telefónica sobre productos, gustos, poder económico, etc. Aparentemente es anónima, o eso nos dicen. Ahora esa información se almacenará en una base de datos, asociada al número de teléfono al que se llamó, para que se pueda comprobar si fuera necesario que la persona que te encuestó es verdad que te llamó e hizo su trabajo.

Si esa base de datos se cruza con la de tu operador telefónico, ya han enlazado la persona con todos los datos que diste por teléfono. Si tu operador telefónico es el mismo que te conecta a Internet, y cruzando esas dos bases de datos con una tercera, salen todos tus datos sobre Internet, que pueden relacionarse a su vez con los datos que Google pueda tener sobre tus búsquedas.

Ya no eres anónimo, estás registrado, y se sabe todo sobre ti.

Es el espacio tan ínfimo que ocupan y la capacidad para cruzar los datos, lo que convierte a la informática y los ordenadores en una potente herramienta que pulveriza la seguridad y la privacidad. Pero es culpa nuestra. Nosotros tenemos que saber que información dar y a quien darla. La respuesta es sencilla, dar la información justa, preguntarnos siempre si lo que se nos requiere es necesario para el servicio que se nos presta, y no sentirnos incómodos por no dar aquella que no sea necesaria, ni sentir vergüenza al decir cosas como: “Esa información no tengo porqué darla” o simplemente mentir y falsear los datos que no sean esenciales para adquirir el servicio.

2.2. Ordenadores Privados vs. Ordenadores de Oficina.

Durante mucho tiempo se ha hablado de seguridad informática, sin discernir dónde, cuando o para qué se utilizan los ordenadores en cuestión. Sin embargo, los riesgos de los que son susceptibles no son los mismos y dependen de varios factores.

Un ordenador que esté en una oficina o en casa de un particular, donde la persona que utilice el ordenador siempre sea la misma, asegura su privacidad, ya que nadie, excepto él o ella, lo usa [1].

Al problema de que alguien acceda ilegalmente al contenido del PC sin nuestro permiso (falta de seguridad), se añade en las oficinas, el hecho de que un ordenador puede ser usado por distintas personas en momentos diferentes o turnos de trabajo consecutivos.

Por tanto, en este último caso, no basta con proteger el ordenador de un acceso externo, sino que los usuarios deberían aprender a proteger sus datos, su correo, y toda la información que pueda ser confidencial, privada o de carácter personal del resto de compañeros.

Aunque se supone que en la empresa se trabaja y que nadie navega por Internet, juega, chatea o hace la compra, lo cierto es que se hace. Y toda esa información queda acumulada en el PC. Según las estadísticas del INE en el segundo semestre del 2005, el 51% de la población tiene acceso a Internet desde el trabajo[2]. Los riesgos pues, de que alguien pueda acceder a esa información, son mayores al usarlo varias personas.

Según IDC, las estadísticas también indican que al menos el 30% del tráfico en la red de las empresas, no se corresponde con trabajo propiamente dicho, sino con participaciones en subastas, búsquedas de nuevos empleos, juegos de azar, comercio electrónico a distancia y pornografía, entre otros.

Los ordenadores de la oficina suelen tener un mantenimiento y cada cierto tiempo se reinstalan completamente para que su rendimiento, prestaciones o estado no se deterioren y puedan mermar su eficacia. Eso, no sucede en un hogar o empresa pequeña donde existe uno, o a lo sumo dos ordenadores. En estos casos el mantenimiento suele ser escaso, y siempre derivado de problemas que ya se han producido.

Desde el punto de vista de la privacidad, los ordenadores de la oficina están más expuestos, aunque desde el punto de vista de la seguridad son los otros los que presentan mayores riesgos por su escaso mantenimiento.

El principal problema que se presenta a la hora de proteger la información privada de cada persona es que los distintos programas que se usan en un PC, tienden a guardar los datos del usuario que lo utiliza en sitios distintos del disco duro.

A eso se añade el hecho de que los usuarios usan determinadas carpetas para guardar el correo electrónico, otras para los documentos, para la agenda, etc., y discernir qué es válido de que no lo es, cuando toda la información que afecta a un usuario está

tan fragmentada y en muchos casos no es más que basura que puede ser borrada, se convierte en algo bastante dificultoso.

En Windows, es bien conocido que toda la información del usuario se almacena por defecto en C:\Documents and Settings\nombre_usuario. Sin embargo el contenido de esta carpeta crece exponencialmente en poco tiempo y un usuario sin demasiados conocimientos puede llegar un momento que no sepa que puede ser considerado de utilidad y qué simplemente ocupa espacio y no vale para nada.

Esto nos revela ya un hecho, los ordenadores acumulan datos y basura simplemente por el hecho de usarlos y cuanto más los usamos más datos se almacenan, algunos de ellos especialmente sensibles. Esto nos obliga a realizar cada cierto tiempo una tarea de eliminación de toda aquella información que pudiendo ser sensible, no nos interesa conservar.

Incluso sin ver los contenidos de aquello a lo que accedemos, Windows almacena los nombres de los documentos que redactamos, las búsquedas realizadas por el disco duro, las páginas web visitadas, el correo electrónico leído (incluso cuando a veces lo hayamos borrado), la agenda electrónica y un sinfín de datos más, aparte de los documentos que se almacenan en la carpeta “Mis Documentos”.

Sin embargo, existen aplicaciones que pueden y de hecho hacen limpieza sistemática por el disco duro de todos esos archivos temporales que dejan rastro de lo que hacemos, leemos, o compramos.

Ejemplos potentes y bastante fiables de estas herramientas serían por ejemplo: CCleaner y IE Privacy Keeper que veremos durante este curso.

Existe otro tipo de utilidades que permiten interceptar todo lo que hacen programas como el Internet Explorer, el Mozilla Firefox y Opera sobre el disco duro, tomando nota de ello, para que nada más cerremos el navegador web, se eliminen todos los cambios que se han hecho en el disco duro. En la práctica, esto equivale a no haber navegado, porque el ordenador queda en el mismo estado en que estaba. Ejemplos de este tipo de aplicaciones son SandieBox.

Y si lo que deseamos es navegar desde un pc por Internet sin dejar rastro existen otras maneras de hacerlo, como usar Windows PE para lanzar el navegador o utilizar un navegador portable.

Podemos también emplear herramientas de rastreo que nos dirán dónde almacenamos los archivos más voluminosos del disco duro, donde están nuestros datos, permiten localizar archivos agrupándolos por categorías (todos los documentos de Excel, por ejemplo), muestran gráficas, etcétera. Ejemplos de estos programas serían el Tree Size Profesional o el WindirStat.

2.3. Los portátiles en el mundo.

Según el INE, casi la mitad de los españoles tiene al menos un ordenador en su casa, y de ellos, el 13,5 % dispone de un portátil. En definitiva, que la tasa de penetración de los ordenadores portátil en España, es todavía escasa, aunque se espera que se acelere a lo largo del 2006.

La privacidad alcanza su mayor exponente de peligro cuando alguien tiene la posibilidad de robarnos el ordenador y dedicar tiempo para inspeccionarlo. En ese preciso momento dispone incluso de la posibilidad de intentar recuperar información que alguna vez estuvo en el disco duro y nosotros borramos.

Si la información fue simplemente eliminada con la tecla suprimir y luego vaciamos la papelera de reciclaje, o si la borramos con las teclas suprimir y mayúsculas, existen grandes posibilidades de que aún esté en el disco duro y puede ser recuperada.

Solo mediante técnicas profesionales de eliminación, que deben ser aplicadas cada cierto tiempo al disco, podemos garantizar que aquello que ya no está, no puede ser recuperado. En inglés, el término para referirse al proceso de borrado de estos espacios de disco que aparentemente están vacíos, es wiping.

Y aun así, se ha demostrado que todavía existe el riesgo de que pueda ser recuperado, aunque cuantas más veces sobrescribamos la misma área del disco, el riesgo disminuye, hasta llegar a un número de sobre escrituras donde se considera prácticamente imposible cualquier recuperación de la información previa.

Los portátiles suelen ser los ordenadores más vulnerables, porque:

- Son fáciles de robar (pequeños, ligeros, se dejan en cualquier lugar).
- La gente que viaja, acaba almacenando toda la información que es esencial para su trabajo, con lo que suelen tenerla bastante organizada y bien sintetizada, además de centralizada en algún sitio del disco duro.
- Pertenecen a ejecutivos, comerciales, etc. y llevan siempre información confidencial y secreta de la propia empresa[3].

Algunos hechos que deberíamos tener en cuenta y que deberían hacernos reflexionar sobre la seguridad de nuestros ordenadores portátiles son estos:

- En EEUU desaparece un portátil cada minuto.
- En Europa, dos tercios de las pymes que operan con portátiles han sufrido robo de alguno de ellos.
- En el 2005 se robaron 750.000 portátiles en el mundo y la tasa de robos crece al 20% anual.
- El 97% de los portátiles robados nunca fue recuperado.
- Más de 93 millones de registros de información personal fueron perdidos en esos robos.

En principio, hemos de tener claro que aunque podemos minimizar el número de causas de pérdida del portátil, y la posibilidad de que sucedan, nunca podremos garantizar al 100% que no nos será robado, no se extraviará o no se averiará. Es por eso que la redundancia de la información y la protección de la misma, son dos aspectos clave. Para la mayoría de nosotros, como particulares, seguramente será más importante lo primero que lo segundo; pero para mucha gente y para la actividad de las empresas, es tan importante lo primero como lo segundo.

Hasta hace poco las empresas no se planteaban que el robo de un portátil de estas características podía afectarles competitivamente hablando. Ahora comienzan a tomarse medidas como:

- Fijar el portátil a algún sitio mediante un cable de acero (montaje), y si no tiene donde engancharlo siempre se puede recurrir al sistema del puerto de video (montaje).
- Instalarles un sistema de localización que permitirá sabe donde está si es robado (localización a partir de la IP).
- Cifrar todos los datos del portátil, dejándolo así bloqueado en caso de pérdida o sustracción (veremos esto en detalle más adelante).
- Instalarles un software que hará que la primera vez que el ordenador se conecte a Internet posteriormente al robo, se ponga en contacto con el fabricante del software o inutilice el portátil. Ejemplos son Computrace de Absolute Software y Cyber Angel de Computer Sentry Software.
- Instalarles una alarma sobre el cable de seguridad, que también puede ser de fibra óptica o un detector de movimiento.
- Emplear servicios integrales de los fabricantes, o soluciones específicas como EasyGuard de Toshiba o Drivelock de HP.
- Y desde luego, vigile su portátil, manténgalo a la vista y cerca de usted.
- No abandone ni aunque sea por unos instantes su pc si tiene aplicaciones con datos confidenciales a las que entra con login y password abiertas, ya sean transacciones con el banco, correo electrónico basado en webmail, o documentos cifrados con su paquete ofimático preferido. O al menos, si lo hace, bloquee su sesión antes de irse.

2.4. Los ordenadores de acceso público.

Podemos definir en esta categoría los ordenadores que están disponibles en cibercafés, salas de juego, de carácter informativo a modo de kiosco virtual, para consulta en las bibliotecas, o para la lectura de correo electrónico o navegar por Internet. En ocasiones son máquinas dedicadas a un fin, pero que no estando protegidas, nos permiten abrir sitios web distintos al que está por defecto, o hacer otras cosas.

La clasificación puede ser aun más amplia y puede englobar todos aquellos computadores utilizados por decenas de personas al día, con acceso restringido a

determinados servicios, y configurados para que no puedan ser manipulados más allá de lo imprescindible de la funcionalidad a la que han sido asignados.

Estos ordenadores son los más oportunos para cometer actos delictivos, ya que son visitados o usados por mucha gente diariamente, y aunque cualquier fechoría pueda saberse que nació de él, todavía habría que identificar al causante.

Podemos conectarnos a ellos para navegar, pero nunca deberemos acceder al correo, el banco o dar los datos de la tarjeta de crédito desde ellos. Estos consejos son aún más firmes si la red en cuestión es inalámbrica y no cableada.

En muchos casos, no podremos acceder a la configuración del navegador, casi siempre el Internet Explorer. Siempre debemos comprobar nada más abrir el navegador que en el menú de Herramientas, en Opciones de Internet, podemos borrar el Historial de Navegación, y que en Auto completar, podemos evitar que complete o recuerde datos de los formularios o contraseñas.

Si no podemos acceder a las Opciones de Internet, lo mejor es que paguemos por el servicio aunque no lo hayamos utilizado y nos marchemos. No tiene sentido emplear esos servicios, sobretodo cuando estamos de viaje, arriesgando nuestras tarjetas de crédito o cuentas bancarias.

El correo electrónico es otro servicio que si, como la mayoría de la gente, tenemos configurado por pop y smtp (luego veremos algo más sobre esto), no deberíamos usar en una red que no conozcamos. Nuestras contraseñas y los correos que leemos o enviamos pueden ser capturados fácilmente. Solo deberíamos acceder a leer y/o enviar emails si lo hacemos con protocolos seguros como https, pop seguro y smtp seguro.

Del mismo modo, solemos conectar a estos ordenadores nuestros discos duros portátiles, la memoria USB, el reproductor de música, o cualquier aparato que tengamos para enviar información, fotos, y demás datos a algún amigo o familiar. No deberíamos hacerlo, por lo menos no sin tomar antes algunas precauciones como son verificar que la máquina tiene un antivirus y que está actualizado, y si podemos, conectar nuestro dispositivo USB en formato solo lectura. Algunos dispositivos llevan una pestaña que permite que el ordenador lea su contenido, pero no que pueda borrarlo, sobrescribirlo o añadir nada nuevo. Esto protege nuestros datos. Y desde luego, ese lápiz USB no debería contener datos sensibles que un programa espía en el ordenador pueda leer o capturar.

De nuevo, es una mala idea conectar nuestro portátil a la propia red, si no tiene el antivirus actualizado, y está al día en cuanto a parches de seguridad pues puede resultar infectado. Aun así, acceder a Internet desde esa red, con nuestro portátil es la opción que representa menos peligro para nuestros datos. Sin embargo, los riesgos relacionados con el email siguen siendo los mismos. Mejora eso sí la fiabilidad que tenemos respecto a acceder al banco, o comprar cosas en Internet, pues cualquier información que de esas operaciones almacenemos, quedan en nuestro PC y no en otro ajeno. En cualquier caso, en una operación de compra por Internet, deberíamos asegurarnos de que la página web usa https.

2.5. Redes inalámbricas.

La mayor parte de la gente que hoy tiene redes inalámbricas en casa, es porque tienen un router que comunica a través de la línea telefónica con la centralita (línea ADSL) y luego, tiene uno o varios equipos informáticos en casa que conectan con ese router sin necesidad de emplear cables, sino por ondas electromagnéticas que se emiten por el aire.

Hace no mucho un técnico de determinada compañía telefónica decía que en una finca residencial donde había estado instalando routers y configurando líneas ADSL, había ya tantos vecinos con ese servicio, que había vecinos que en vez de conectarse a su router, estaban usando el del vecino. Lo bueno del caso es que no se había hecho intencionadamente, sino que a lo mejor la señal del router del vecino, llegaba al PC de otro con más fuerza que la del propio router, y el PC se cogía automáticamente a la red en la que percibía mejor señal.

Esto sucedía porque ningún vecino tenía protección de ningún tipo frente a usos fraudulentos que otros vecinos pudieran hacer de su red. Veamos las causas.

- **La password.**
  - Sin password: Muchas empresas de telecomunicaciones proporcionan a sus clientes kits de auto instalación, donde en apenas unos instantes el cliente tiene configurado el router y listo para ser usado. Normalmente el router queda sin contraseña (o una típica), lo que quiere decir que desde Internet alguien puede conectar con el router y cambiar la configuración para adecuarla en su beneficio.
  - Password por defecto: También puede suceder que para una determinada marca, todos los routers de un determinado modelo, vengan con la misma contraseña y que como nadie la cambia, cualquiera que sepa la contraseña de ese router y marca por defecto, puede acceder a él.
  - Password adecuada: La mejor manera de garantizar que el router tiene password, es leerse el manual y cambiarla por una lo suficientemente larga y compleja, Naturalmente hemos de elegir una que seamos capaces de recordar.

- **La configuración.**
  - El DHCP. Cuando un ordenador quiere acceder a Internet necesita una IP, que no es más que un número que le permite identificarse delante de otras máquinas. La IP la da el router. Si nuestro router no sabe a quien debe darle IP, se la dará a cualquier PC que se la pida. Esto significa, que otros PCS pueden acabar conectados a nuestra red, y usando nuestro ancho de banda, es decir, nuestra ADSL irá más lenta porque dará servicio a más clientes y no solo a nosotros. Esto se soluciona especificando al DHCP que solo debe dar IP a nuestros ordenadores. Los ordenadores para conseguir la IP le envían al DHCP (un programa que funciona en el router) la MAC que es el identificador previo a recibir la IP. Podemos decirle al router que MACs son las de nuestros PCS y por tanto, las únicas que debe

aceptar. También podemos desactivar el DHCP y poner las IPs a mano en nuestros PCS.

- **El cifrado.**
  - Si no queremos que el vecino de al lado "oiga" nuestros emails enviados por el aire, averigüe nuestras contraseñas del correo y pueda leer un documento de Word que estamos enviando a un colega, necesitamos encriptar los datos que enviamos por el aire que hay entre nuestro PC de casa y el router. Esto se puede hacer con distintos protocolos de seguridad. Los más conocidos son WEP, WPA y WPA2. El más fácil de vulnerar es WEP. Hoy en día deberíamos comprar routers que soporten al menos WPA y deberíamos asegurarnos que los PCS que compramos sean compatibles al menos con WPA. Si no usamos el cifrado, todo lo que transmitamos entre nuestros PCS, todos nuestros datos, estarán viajando por el aire en texto claro y pueden ser capturados.

- **La potencia de la señal.**
  - Mucha gente se compra antenas especiales que se conectan al router después de anular la que traen por defecto para que la señal llegue más lejos y con más fuerza. Eso está bien si es necesario. Pero cuando más potente sea el alcance del router, más personas pueden intentar conectarse a nuestra red "por la cara" para usar nuestra línea ADSL o para intentar acceder a nuestros pcs.

En cualquier caso, y usemos WEP o WPA, deberíamos cambiar la contraseña de cifrado del router y del PC cada cierto tiempo. También podemos mirar en las estadísticas del router y averiguar cuantas máquinas hay conectadas a él normalmente.

Los routers suelen por defecto admitir conexiones desde Internet hacia ellos. Para eso los programas que intentan conectar a él, usan lo que se denominan puertos. Es una buena idea que si solemos conectarnos desde el PC a Internet, pero no desde Internet a nuestro PC (por ejemplo desde el trabajo queremos acceder a nuestro PC) cerremos todos los puertos, para que desde fuera de nuestra red, no se pueda atacar nuestro ordenador.

Servicios de descarga de videos, música, conexiones remotas por Terminal Server al PC, etcétera, requieren que el router acepte conexiones desde Internet a determinados puertos. Por eso deberíamos dejar abiertos solo los puertos concretos que necesitemos y deberíamos cerrar los demás.

2.6. Búsquedas en Internet.

La mayoría de la gente piensa que cuando busca cosas por Internet mediante Yahoo o Google o cuando navega no está siendo identificado y que su identidad permanece anónima. En ciertos aspectos es así, pero muchas veces se puede acabar identificando a la persona, donde vive y quien es.

Por ejemplo, cuando yo accedo a Amazon u otras webs comerciales y busco precios de determinados libros, la siguiente vez que me conecto a esa web, lo primero que se me ofrece son cosas relacionadas con las que ya compré la otra vez.

La pregunta que surge en seguida es: ¿Y como sabe que soy yo? Existen varias maneras, veamos las más importantes.

Las cookies: Una cookie no es más que un pequeño archivo de texto con un número muy largo que la web que estamos visitando deja en nuestro disco duro. En concreto, la web le solicita al navegador que guarde ese archivo, al que le pone una fecha de caducidad que casi siempre suele ser nunca o algo parecido a 31 de diciembre del 2100.

La siguiente vez que conectas con el mismo navegador a esa web, la web solicita al navegador web la cookie asociada. Si no existe, el sitio web, no te reconoce y te abre una página general donde te ofrece sus artículos. Si el navegador envía la cookie o número muy largo, la web que estamos visitando, busca ese número o identificador en la base de datos y averigua cuales son tus gustos, cuando te conectaste por última vez y demás datos que guardó la primera vez que generó la cookie y le pidió al navegador que la dejara en el disco duro. Naturalmente ahora que te ha reconocido, seguirá almacenando tus gustos y preferencias en la base de datos y acabará conociendo todos tus gustos y preferencias para saber qué quieres, que te gusta, cuando te gastas normalmente y cuando sueles comprar.

Puede ser también que tú borres de vez en cuando las cookies manualmente de cada navegador web que usas, sea el Internet Explorer, el Mozilla, el Firefox, Opera o cualquier otra variante. O incluso puedes especificar en el navegador que no acepte cookies. El único problema a esta decisión es que hay páginas web, que no funcionan si el navegador no admite cookies.

Aún borrándolas, el sitio web puede almacenar también la IP de tu ordenador. Si tienes una ADSL en casa, la IP de tu ordenador no será lo que almacene, sino la del router que es quien establece las conexiones con Internet para tu PC. La IP del router, hay empresas telefónicas que te la cambian cada cierto tiempo, pero otras no lo hacen.

Si siempre usas la misma IP, o siempre te conectas a Internet desde tu lugar de trabajo, donde las IPs suelen ser siempre las mismas, eso significa que Google, Yahoo, Amazon y otras empresas comerciales te tienen identificado. Porque una vez tienen la IP, se puede saber a qué empresa corresponde y tu empresa sabe que IP tiene cada máquina, a no ser que sean asignadas cada cierto tiempo a ordenadores distintos.

En definitiva, que pueden identificarte, saber quien eres y qué te gusta. El problema es más grave que todo eso, porque puede que en los últimos meses estés buscando cambiar de empleo, o información sobre divorcios porque no soportas a tu marido/mujer, o sobre tus derechos como trabajador.

¿Qué pasaría si esa información se filtrara? ¿Y si todo lo buscado por ti en los últimos diez años quedará registrado en una base de datos, ocupando miles de líneas con las fechas cuando sucedió, con la IP que te asocia al mismo puesto de trabajo donde llevas diez años?

¿Crees que no puede pasar? Ya ha pasado. Y puedes leerlo aquí. Este otro artículo es más general pero también da una idea clara sobre el tema.

Y naturalmente aceptar la tecnología con preocupaciones nos evitará cosas como ésta.

Soluciones.

Navega con un PC que no sea el tuyo habitualmente. Si estás en una empresa donde existen PCS que se usan por muchas personas, y no solo por una y concreta, conéctate a él para navegar por Internet. Para leer el correo y comprar cosas sigue usando tu PC.

Utiliza proxies gratuitos que te permiten leer páginas web en Internet sin que quede registrado que eres tú quien las accede o que utilizas el servicio en cuestión.

Asegúrate que borras toda la información que genera tu navegador después de que termines de usarlo. Lo puedes hacer manualmente o mediante herramientas o plugins que se integran con tu navegador. Pero hazlo.

Nota: Recientemente Google ha desarrollado una nueva herramienta para poder revisar el historial de las búsquedas que hemos realizado durante los últimos meses. Es necesario registrarse con el correspondiente usuario de gmail para poder emplearla, lo que aun nos identifica más si cabe. La citada herramienta se llama Google Web History y puede mostrarnos todas las búsquedas y navegación realizada, aunque no haya sido por medio de Google, esto se debe a que se apoya en la Google Toolbar.

El hecho de que Google haya comprado recientemente doubleclick, quien también almacena información sobre los clientes en base a cookies, hace parecer cada vez más a Google a Gran Hermano.

2.7. Navegadores Web.

2.7.1. Introducción

Los navegadores web son los programas o aplicaciones que usamos para visitar las webs o portales disponibles en Internet. La mayoría de nosotros accedemos a páginas web para ver el estado de nuestras cuentas bancarias, realizar compras, leer nuestro mail mediante webmail, descargar archivos por ftp o http y para acceder a otros muchos servicios.

Por defecto, los navegadores almacenan las páginas que visitamos, es decir, al acceder a ellas, las cachean o almacenan en el disco duro. La siguiente vez que accedemos a la misma página web, los elementos que no hayan cambiado, pueden ser cargados del disco duro. Del mismo modo, usando el modo de navegación offline (sin conexión a Internet) el navegador nos permitirá recorrer las páginas visitadas con anterioridad.

Los navegadores pueden registrar los enlaces o páginas web que visitamos más a menudo, es lo que se conoce como los favoritos. Los favoritos pueden organizarse por categorías, identificarse mediante descripciones que los hagan más fáciles de recordar que una URL y también, pueden borrarse cuando dejamos de necesitarlos.

Cuando rellenamos formularios en Internet, o accedemos a nuestro banco o email, e introducimos nuestros datos, los navegadores pueden recordarlos, para ayudarnos a rellenarlos la próxima vez.

Del mismo modo, cuando nos conectamos a un portal de Internet, los navegadores envían información sobre la versión del navegador que empleamos y el sistema operativo que tenemos instalado.

A veces, los portales web, envían al navegador una cookie o archivo que el navegador normalmente acepta (se puede configurar que no sean aceptados, pero muchos sitios web dejarán de funcionar adecuadamente) y que permite al portal reconocernos la próxima vez que entremos. Puede incluso que la primera vez nos tengamos que dar de alta, e introducir nuestros datos. Sin embargo, al quedarnos con la cookie, la próxima vez que nos conectemos al sitio web, éste preguntará al navegador si tiene alguna cookie y si es así, será enviada para ahorrarnos el proceso de identificación o simplemente para ser reconocido como un usuario que se ha conectado con anterioridad.

Todos estos datos se almacenan en el disco duro y deberían ser borrados para proteger nuestra privacidad y salvaguardar nuestros intereses. Veámoslo con más detalle:

- El histórico de páginas visitadas hoy o en la última semana, puede decir mucho sobre cuales son nuestros hábitos, cual es nuestro banco o a qué portal pertenece nuestra cuenta de email. Más fácil es todavía desplegar el cuadro de direcciones web, para ver que hemos visitado recientemente.

Debemos por tanto borrar tanto el histórico de páginas visitadas, como la caché utilizada por el navegador, como la lista de urls que hemos visitado hoy y que aparecen en el desplegable.

- Los datos introducidos en formularios. Comentarios que hemos hecho en foros, login y passwords en distintos servicios como chat, webmail, compras por Internet (tarjetas de crédito, número seguridad social, direcciones, teléfonos). Los navegadores permiten marcar la opción de NO recordar estos datos que hemos tecleado anteriormente. Es cómodo que sean recordados, pero NO es seguro. Es mejor teclearlos en cada ocasión. Además deberemos borrarlos cada vez que terminemos de usar el navegador si decidimos que sean.

- La lista de programas descargados en el gestor de descargas. Una vez hemos descargado algún programa y lo hemos instalado, no necesitamos que el gestor de descargas recuerde su nombre y de donde lo descargó. Este pequeño programa que acompaña a algunos navegadores tiene opciones también para borrar esta información.

Si usamos un ordenador que no sea el nuestro, tenemos que asegurarnos que las opciones de borrado están disponibles y que podremos usarlas cuando terminemos de emplear el navegador. Son fundamentales, pues garantizan nuestra privacidad y evitan que otros puedan utilizar nuestras credenciales o datos de identificación para acceder a servicios de Internet en nuestro nombre.

Si visitamos el sitio web http://snoop.cdt.org/snoop_on_me.shtml, veremos en pantalla cual es la información que el navegador envía de nosotros a los portales o webs que visitamos.

En principio, el navegador web más utilizado en el mundo es el Internet Explorer en todas sus variantes: IE 5, IE 6 e IE 7. Detrás de él, están el Mozilla Firefox y el Opera.

Los tres navegadores permiten borrar toda la información de carácter privado o confidencial, aunque en el Internet Explorer y en Opera, es necesario seleccionar la opción adecuada del navegador para hacerlo. Mientras que en el Mozilla Firefox, el propio navegador puede hacerlo solo al cerrarse, e incluso, puede pedirnos confirmación.

En el mercado existen infinidad de navegadores, aunque los tres más usados son los citados anteriormente. El IE es utilizado casi por el 90% de personas que se conectan a Internet, le sigue Firefox con un 10% aproximadamente de utilización (en Europa llega al 20%), y en último lugar está Opera, con un porcentaje muy reducido del mercado. Todos los demás tienen un uso casi testimonial.

Existen navegadores para Windows, Linux y Mac OS. Algunos de los navegadores fueron desarrollados para los tres sistemas operativos, pero la mayoría de ellos hoy en día tienen como mucho soporte para Windows y Linux simultáneamente. No es de extrañar tampoco que los usuarios de ordenadores de Apple tengan navegadores propios como Shiira o Safari.

Existen incluso antiguos navegadores que permiten recorrer Internet en modo texto, sin imágenes, fotos o videos. También están desapareciendo.

Los navegadores han sido desarrollados de acuerdo a las necesidades que se han ido creando con el tiempo y en ocasiones han evolucionado compitiendo entre ellos, pero a veces, de un proyecto abandonado ha nacido otro con más éxito.

En su día Microsoft venció a Netscape cuando regaló el navegador web con su sistema operativo Windows. El Internet Explorer fue el vencedor, pero Netscape dejó su navegador a la fundación Mozilla, que desarrolló posteriormente el Firefox.

La parte más importante de un navegador web es el motor de navegación. Cuando pensemos en navegadores, debemos pensar en qué motor utiliza. Por ejemplo, Microsoft Internet Explorer emplea el motor Trident, y el Mozilla Firefox emplea el Gecko. Cuando AOL hace unos años compró Netscape, creó versiones del Netscape que podían usar indistintamente el Trident o el Gecko. Existen navegadores web como el Avant Browser o el Maxton que usan el motor del IE; pero existen otros, como el K-meleon o el Firefox que emplean Gecko. El caso de Opera es distinto, por ser un producto comercial desarrollado por una empresa privada y que nació mucho más tarde que el Internet Explorer o Netscape. Su motor es el Presto y no existe otro navegador que lo emplee.

Ha habido otros motores de navegación y mucho más navegadores, pero o no han tenido tanto éxito, están desfasados en cuanto a prestaciones y/o capacidades o se usan en ámbitos muy reducidos (como pasa con los navegadores específicos para Mac de Apple).

En principio, el más atacado es el Internet Explorer, que es el más extendido en el mundo, y donde los hackers saben que pueden hacer más daño por el simple hecho de ser muchos los usuarios que lo utilizan.

Como segunda opción a este navegador estarían el Firefox u Opera que son navegadores web mucho menos extendidos pero que proporcionan buenos resultados.

K-meleon es otro navegador que destaca por su agilidad y velocidad, basado en Gecko como Firefox.

Avant Browser y Maxton tienen el inconveniente de que aunque ofrecen más prestaciones que el Internet Explorer no dejan de ser vulnerables a muchos agujeros de seguridad de éste porque lo emplean para procesar las páginas web, es decir, usan como motor de navegación a Trident.

2.7.2. Internet Explorer 7.0

Internet Explorer, más conocido como IE, es el navegador web más utilizado en el mundo por el simple hecho de estar integrado con el sistema operativo Windows.

En octubre del 2006, suponía el 81% de toda la base de navegadores web instalada en el mundo. IE, ha perdido en los últimos años terreno frente a otras alternativas del mercado, ya que Microsoft no ha mejorado su producto en los últimos cinco años. Únicamente se ha dedicado a parchear el navegador conforme se han ido detectando nuevos bugs.

IE ha sido criticado por los continuos fallos de seguridad que han aparecido en los últimos años en su interior, algunos de ellos especialmente peligrosos. No hay que olvidar que un ataque al IE podía dar el control del sistema, máquina u ordenador a un hacker, debido a la integración existente entre el navegador web y el sistema operativo, que Microsoft siempre tuvo que defender en los tribunales.

Por otra parte, los desarrolladores web se vienen quejando desde hace mucho tiempo de la falta de soporte de IE para presentar las páginas web adecuadamente mediante CSS2, estándar que no es soportado actualmente, y en su totalidad, por ningún navegador web. Sin embargo, se acusa a IE de ser el que peor soporta este estándar y de no tener Microsoft ningún interés en soportarlo adecuadamente, siendo su browser el más extendido.

Tales problemas han llevado incluso a los desarrolladores web, a buscar soluciones alternativas que parcheen o rectifiquen el mal comportamiento de IE en determinados contextos o ámbitos. Un ejemplo podría ser éste, desde donde podemos acceder a una solución implementada por Dean Edwards.

Para acallar estas críticas en parte, y para no seguir perdiendo cuota de mercado frente a otras alternativas o productos que están saliendo últimamente, Microsoft acaba de lanzar el Internet Explorer 7.0.

Como puntos fuertes de este navegador tenemos:

1. Uso correcto de las pestañas, facilidad de navegación que nunca había estado disponible con IE y que ya incorporaban los demás productos de la competencia.
2. La aparición de thumbnails de las ventanas o pestañas abiertas, una novedad también disponible en Opera.
3. El fácil acceso a Favoritos y RSS Feeds, aunque las últimas versiones de Firefox y Opera también los han tenido en cuenta.
4. Su sistema anti-phishing, que compite directamente con el de Firefox 2.0.
5. El poco espacio usado en la parte superior de la pantalla.
6. El sistema de aviso de actualizaciones disponible.
7. La conservación del estado de la sesión (pestañas abiertas en el navegador).
8. En gran esfuerzo hecho en palabras de la propia Microsoft por mejorar al máximo la seguridad de este producto.

En contra podríamos decir:

1. No aporta nada nuevo que le haga destacar por encima de sus competidores más directos, excepto en el phishing, que por otra parte ya estaba disponible en Firefox.
2. Sigue sin soportar enteramente el CSS2, solo se han hecho mejoras. Se dejan estas tareas para más adelante, complicando la tarea de los desarrolladores.

2.7.3. Firefox 2.0

Se trata de un navegador web o browser creador a partir del código fuente liberado por Netscape en los años 90. En concreto Firefox, se apoya en Gecko el motor de Netscape para renderizar las páginas web.

El aumento en la utilización de este navegador por parte de la gente se produjo por ser la única alternativa libre y gratuita capaz de hacer frente al monopolio del IE. Anteriormente lo habían intentado el Mozilla y otros navegadores web no gratuitos como Opera. Pero en ningún caso consiguieron porcentajes de uso más allá de lo testimonial.

Firefox no ha progresado solamente por ser un buen y completo navegador. Le avalan otras razones, como el descuido de Microsoft en mejorar a IE, la falta de seguridad del mismo frente a numerosos bugs, el hecho de ser gratuito y el estar disponible tanto para Linux como para Windows, ya que sus mejores defensores han estado siempre en linux.

Profesionales del sector de la informática, empresas de seguridad, desarrolladores y empresas de consultoría han intentado en distintos informes demostrar que firefox es más seguro o que lo es menos que el IE de Microsoft.

En cualquier caso, las personas que creen o admiten que Firefox no es más seguro que IE, creen en la seguridad que supone usar un navegador que usa menos gente, ya que los hackers suelen cebarse más en el IE, por su importante base de usuarios instalada.

Firefox es uno de los navegadores con más posibilidades de ampliación y potenciación debido a la utilización de extensiones o complementos. No hay ningún navegador en el mercado que disponga de tantas extensiones para añadir funcionalidad al navegador como éste. De todas formas, no todas las extensiones son aconsejables, y de hecho hay artículos al respecto sobre la dudosa utilidad de algunas de ellas.

Dispone también de bloqueo de ventanas emergentes y permite garantizar la privacidad, configurando todos los datos que deben ser borrados al cerrar el navegador.

En cualquier caso, Firefox destaca por su capacidad de personalización mediante skins, su sistema anti-phishing, su gestor de descargas y su enorme número de extensiones.

En octubre del 2006, poseía casi el 13% del mercado mundial de navegadores, seguido muy de lejos por Safari (navegador de Apple para Mac), con casi el 4% del mercado mundial.

2.7.4. Opera 9.0.10

Opera es un producto comercial que hasta hace poco no era gratuito para uso personal. Se trata de algo más que un navegador, pues no solo incluye el browser, sino también un cliente de chat, un cliente de BitTorrent y programa de lectura/envío de emails.

Destaca por la posibilidad de reconocer las cookies que alberga nuestro navegador y conocer en detalle cada una de ellas, por sus facilidades para importar y exportar favoritos desde otros muchos navegadores, el módulo para gestionar notas, el sencillo instalador válido para todos los idiomas, la posibilidad de recordar sesiones, su capacidad para ver todos los links contenidos en una página y por su cuidado aspecto y fácil interfaz de usuario.

Es el único frente a IE y Firefox, capaz de almacenar grupos de pestañas o sesiones para continuar con ellas más tarde. Esta característica también está disponible en Maxthon, Avant Browser y K-meleon.

Desde el principio Opera puso mucho cuidado en respetar y seguir los estándares desarrollados para Internet y fue durante mucho tiempo pionera en este campo.

Opera tiene una base de clientes a nivel mundial, testimonial. Solo el 0,61% de los navegadores web usados para recorrer Internet pertenecen a este cuidado producto.

2.7.5. Maxthon 1.5.8 beta 120 y Avant Browser 11 beta 25.

Maxthon y Avant, son otros navegadores web del mercado de navegadores, muy poco extendidos. En realidad ambos productos son derivados del Internet Explorer, pues se apoyan en su motor web, Trident. Ambos son gratuitos.

Maxthon incluso puede utilizar parte de la funcionalidad del motor web Gecko para realizar las mismas tareas que lleva a término con el Trident. Aunque la funcionalidad del navegador se verá limitada.

Estos navegadores, debido a que se apoyan en un producto ya existente, completan la funcionalidad del IE, hasta llegar a resultados excelentes, en algunos casos impresionantes.

Naturalmente, el hecho de depender del motor Trident, perteneciente al Internet Explorer, supone que se pueden ver afectados por los mismos bugs que éste, riesgo que podemos ver o sentir compensado ante la avalancha de nuevas características que proporcionan.

Maxthon es el único de los navegadores que permite deshacer cierres múltiples de pestañas (Firefox puede hacerlo con una extensión), proteger pestañas con password que impide visualizarlas, dispone de un colector de texto, permite ocultarlo rápidamente (tecla viene el jefe) y como Opera permite ver toda la lista de links en una página web.

Como Opera dispone de un colector de texto para guardar links o anotaciones y permite utilizar gestores de descargas externos, permitiendo elegir uno de una amplia lista. Incluye también una lista de acceso rápido a utilidades del sistema o aplicaciones externas y tiene integrado el acceso a cuentas de correo de gmail.

Avant, por su parte, puede bloquear pestañas contra el cierre, aunque permite visualizarlas y no puede protegerlas por password como Maxthon. Además es el navegador que más opciones de refresco de páginas dispone.

Puede almacenar el rellenado de formularios completos, para posteriormente volver a rellenar el citado formulario completo de manera automática. Además permite proteger estos datos con contraseña. Esto le convierte en el más completo y seguro a la hora de almacenar información sobre formularios web.

Los dos navegadores además pueden bloquear pestañas para que no puedan cerrarse, permiten abrir grupos de pestañas que estábamos viendo la última vez que cerramos el browser, son los únicos que disponen de alias de páginas web (por ejemplo, si siempre visito la página web www.unmundodesensaciones.es , puedo escribir mundo y la página se abrirá igualmente), admiten gestos del ratón, bloquean publicidad, tienen capacidades de traducción, etcétera.

2.7.6. K-Meleon 1.0.2

El precursor de los navegadores web Mozilla y Firefox fue Netscape. K-Meleón es una versión adaptada de Mozilla y por tanto tiene parecido a Firefox.

Es bastante rápido a la hora de acceder a páginas web, aunque no tanto como Opera. Consume menos recursos que la mayoría de los navegadores. Al contrario que Firefox, dispone de gestos con el ratón, y puede almacenar grupos de pestañas para ser abiertas posteriormente.

Dispone de barra de búsqueda para múltiples buscadores simultáneos, y añade a su hermano mayor, Firefox, la capacidad de traducir páginas web.

No es tan vistoso como otros navegadores, pero es funcional, sencillo y dispone de algunas de las carencias que su “familia” arrastraba (Firefox 1.0).

2.7.7. Comparativa de navegadores

Navegadores Web	IE	Maxthon	Avant	Firefox	K-meleon	Opera
Versión actual	7.0	1.5.8. b120	11 b25	2.0	1.0.2	9.0.2
Motor de navegación/exploración web	Trident	Trident*	Trident	Gecko	Gecko	Presto

Facilidades de navegación	IE	Maxthon	Avant	Firefox	K-meleon	Opera
Navegación por pestañas	X	X	X	X	X	X
Permite abrir nuevas pestañas rápidamente	X	X	X	X	X	X
Cerrado rápido de pestañas	X	X	X	X	X	X
Permite abrir nuevas instancias del navegador	X	X	X	X	X	X
Deshacer cierre última pestaña		X	X	X	X	X*
Deshacer múltiples cierres de pestañas		X				
Almacenar grupos o sesiones de pestañas		X	X		X	X
Protección contra cierre de pestañas (bloqueo)		X	X			X
Protección con password a una pestaña		X				
Cargar múltiples páginas/pestañas al iniciar	X	X	X			
Recordar estado de la última sesión	X	X	X		X	X
Barras de Herramientas personalizables	X	X	X	X	X	X
Alias de URLs		X	X			
Mouse Gestures		X	X		X	X
Guardar páginas web como un solo archivo	X	X	X			X
Guardar Página HTML	X	X	X	X	X	X
Guardar Página completa	X	X	X	X	X	X
Refrescar página cada cierto tiempo personalizable		X	X			
Refrescar múltiples páginas cada cierto tiempo personalizable.			X			
Refrescar página actual	X	X	X	X	X	X
Refrescar todas las páginas/pestañas abiertas	X	X	X			
Permite ver la lista completa de links de la página		X				X
Barra de Búsqueda para múltiples buscadores	X*	X	X*		X	X
Barra de Búsqueda con algún buscador	X	X	X	X	X	X
Thumbnails de las ventanas abiertas	X					X

Facilidades de Texto	IE	Maxthon	Avant	Firefox	K-meleon	Opera
Colector de texto		X				X
Guarda Notas		X				X

Favoritos	IE	Maxthon	Avant	Firefox	K-meleon	Opera
Importar desde fichero html	X	X*				X
Exportar a fichero html	X	X*	X			X
Importa/Exporta Favoritos desde/a un backup propio		X				X
Importa Favoritos desde Opera			X	X		X
Importa Favoritos desde Firefox			X	X		X
Importa Favoritos desde Konqueror						X
Carga los Favoritos de otros browsers		X	X		X	

Seguridad	IE	Maxthon	Avant	Firefox	K-meleon	Opera
Bloqueo de ventanas emergentes	X	X	X	X	X	X
Bloqueo de publicidad		X	X			
Tecla viene el jefe		X				
Anti-phishing	X			X		
Permite desactivar elementos al cargar páginas web	X	XX	XX	X	XX	X
Admite https	X	X	X	X	X	X
Admite ftp	X	X	X	X	X	X
Lleva gestor de descargas propio	X	X	X	XX	X	XX
Admite gestores de descargas externos		X				

Facilidades visuales	IE	Maxthon	Avant	Firefox	K-meleon	Opera
Tamaño de fuente (pequeño, mediano, grande ....)	X	X	X			
Zoom (25%, 50%, 75%, 200%, ...)	X	X	X			X
Tamaño del texto (aumentar, disminuir tamaño fuente)	X			X	X	
Estilo (alto contraste, partes estructurales de la Pág.)						X

Privacidad	IE	Maxthon	Avant	Firefox	K-meleon	Opera
Permite eliminar información privada al cerrar		X	X	X	X	X
Auto-rellenado de formularios parcial	X	X*	X	X		X
Auto-rellenado completo de formularios		X*	X			X*
Protege auto rellenado de formularios con contraseña			X			
Almacenar online RSS, Favoritos y auto completar			X			
Gestión detallada de cookies						X

Otras	IE	Maxthon	Avant	Firefox	K-meleon	Opera
Soporte extra de funcionalidad por plug-ins	X	X	X	X	X	X
Acceso integrado a Gmail		X				
Mostrar / Ocultar en la Barra de Tareas		X	X			
Aviso de actualizaciones automáticamente	X	X	X	X		
Lector de Feeds	X	X	X	X	X	X
Utilidades Externas (Launch)		X				
Skins		X	X	X	X	X
Capacidad de Traducción		X	X		X	
Incorpora Cliente de Email						X
Incorpora Chat						X
Cliente de BitTorrent						X
El mismo instalador incorpora todos los idiomas						X
Idioma	Español	Inglés	Español	Español	Inglés	Español
Licencia	EULA	Freeware	Freeware	GPL	GPL	Free

Notas: Los Favoritos usados por Maxthon son los del IE.
Avant Browser tiene su propia lista de favoritos pero puede usar la de IE.
K-meleon usa los favoritos de Netscape, IE u Opera

2.7.8. Estadísticas de utilización de navegadores web

Empleo del Firefox en alguna de sus versiones (obtenido de aquí).

Datos de septiembre del 2006

Países de Europa	%	Países de Europa	%
Eslovenia	39%	Francia	19,6%
Finlandia	35,4%	Irlanda	19,1%
Eslovaquia	34,3%	Suiza	18%
Polonia	32,3%	Bélgica	16,9%
Rep. Checa	31,3%	Portugal	16,2%
Alemania	30,9%	Luxemburgo	16,1%
Croacia	30,1%	Noruega	14,6%
Hungría	28,7%	Lituania	14,2%
Estonia	24,9%	Italia	14,2%
Austria	23,5%	España	13,5%
Grecia	23,4%	Holanda	12,9%
Rumanía	22,8%	Reino Unido	12,4%
Letonia	22,4%	Dinamarca	12,4%
Bulgaria	21,3%	Ucrania	12,2%
Suecia	21,2%		

Utilización de Firefox por continentes (datos septiembre 2006).

Continente	%
América del Norte	13,5%
Sudamérica y Centroamérica	10,9%
Europa	21,9%
África	10,5%
Asia	10,6%
Oceanía	21,4%

2.8. Correo electrónico.

Hasta leer el correo se ha convertido en una tarea ardua cuando intentamos deshacernos del spam, de la publicidad, de los mensajes encadenados (hoax), de los correos con gruesos adjuntos en forma de presentaciones PowerPoint, de los mensajes en forma de una gran imagen en vez de texto, de la tendencia actual a que todos los mensajes sean HTML y no simple texto, permitiendo el engaño de los phishers y hackers mediante enlaces a adjuntos, links o direcciones de correo que no son lo que parecen, ni apuntan a donde creemos.

2.8.1. Clientes de correo

2.8.1.1. Introducción

Los clientes de email o lectores de correo, permiten acceder a los mensajes que un usuario propietario de una cuenta de correo, buzón o mail box recibe de otras personas o entidades. Al mismo tiempo puede enviar mensajes a otras personas o grupos de personas (a estas direcciones, se las llama listas de distribución).

Los mensajes de correo solemos almacenarlos en el disco duro sin cifrar y junto a ellos, almacenamos nuestros adjuntos. Los adjuntos son todos los archivos o documentos que anexamos al email. Pueden ser informes, documentos oficiales, fotos, presentaciones, contratos escaneados, etcétera. Naturalmente se almacenan dentro de cada email, y por tanto, en la misma carpeta donde los mensajes son almacenados.

Además, cuando abrimos los adjuntos, suele generarse una copia temporal del mismo en alguna ubicación del disco duro para que sea abierta y podamos ver su contenido. Esta copia no suele borrarse de manera automática.

El resultado de este comportamiento es que todo nuestro correo, conversaciones confidenciales, de trabajo o negociaciones quedan almacenadas en el disco duro sin protección alguna. Del mismo modo, es posible en algunos casos obtener la contraseña de cada cuenta de correo almacenada en el ordenador.

De todos los servicios disponibles en Internet, el más utilizado es el correo electrónico. Según el INE, de la gente que se conecta a Internet en España, el 76%

utiliza el correo electrónico, el 33% chatea y lee foros, y el 30,6% accede a bancos o servicios financieros.

Veamos los lectores de correo más extendidos.

2.8.1.2. Outlook Express

Es con diferencia el cliente de email más extendido. Tiene una agradable presencia y su manejo es sencillo. De hecho, apenas ha cambiado en la última década. Se integra perfectamente con el programa de mensajería instantánea Messenger de Microsoft y con NetMeeting.

En su contra, diremos que en los últimos cinco años, Microsoft no ha mejorado el producto ni lo ha modificado para dotarlo de mejoras necesarias, como sistemas anti-spam o la capacidad de detectar el phishing.

Outlook Express ha sido acusado de originar numerosos problemas de seguridad a los usuarios, fallos que han sido aprovechados por multitud de virus para propagarse y auto reenviarse a otros ordenadores o redes, extendiéndose con absoluta impunidad en intervalos muy cortos de tiempo.

También su sistema de filtrado mediante reglas de mensajes es considerado pobre, y su seguridad, baja. Es posible averiguar la contraseña almacenada de cada cuenta de correo con bastante facilidad.

Frente a eso, podemos decir, que no solo permite descargar correo de un número ilimitado de buzones o cuentas de correo, sino que actúa como lector de news, está disponible en Windows y Mac, dispone de corrector ortográfico y puede exportar la configuración completa de las cuentas de correo (datos de configuración y password) a un archivo que servirá para configurar posteriormente el Outlook Express de otra estación de trabajo.

Permite además que otros programas envíen emails a través suyo mediante la interfaz de programación MAPI, y puede ser configurado para avisar cuando la misma está siendo utilizada por alguna aplicación.

Dispone de opciones de seguridad para desactivar la carga de imágenes y contenido HTML, evitar la apertura de adjuntos, emplear firma digital o enviar el correo cifrado.

Por último decir, que soporta múltiples identidades.

2.8.1.3. Eudora

Eudora es un cliente de correo muy veterano y también bastante extendido. Tiene de muchas opciones y es muy completo. Dispone de un sistema anti-phishing y de filtros contra el spam. Existe además una versión gratuita del mismo (con algo de publicidad). Integra un sistema de búsqueda bastante rápido debido a que indexa los mensajes de correo almacenados. Está disponible para Windows, Linux y Mac.

Sin embargo, la empresa que lo desarrolla, Qualcomm, no va a continuar haciéndolo, pues se va a pasar a Thunderbird. Y futuras versiones de Eudora se basaran en Thunderbird.

Qualcomm ha llegado a un acuerdo con Mozilla, empresa que desarrolla Thunderbird, para que el código fuente de Eudora pase a ser OpenSource. La última versión disponible de Eudora es la 7.1 (en inglés) para Windows y la 6.2.4. para Mac.

2.8.1.4. Novell Evolution

Hasta ahora solo estaba disponible en Linux pero recientemente ha sido portado a Windows, aunque todavía carece de la suficiente estabilidad.

Es más que un lector de correo, se puede integrar con Exchange, dispone de lista de tareas para programar reuniones, agenda, calendario, etcétera.

La última versión para Windows, la 2.6.2. todavía carece de estabilidad. Se trata de una aplicación desarrollada para Linux, donde lleva mucho tiempo. Al haber sido recientemente portada a Windows, la aplicación todavía es lenta y algunas opciones a veces provocan el cuelgue del programa. Además, por estar pensada como un producto de empresa, equivalente del Outlook de Microsoft, ocupa bastante memoria cuando se pone en marcha y tarda en hacerlo (está compuesta por varios programas o procesos). En concreto, ocupa en memoria cerca de 55 Mbytes. Cuando gane en estabilidad para Windows, será el equivalente del Outlook de Microsoft, con bastantes más prestaciones que el OE.

2.8.1.5. Opera

Opera dispone de un producto bastante completo que consta de un navegador, un cliente de noticias, cliente de RSS, chat y lector de correo. Es un producto freeware, que funciona muy bien y es de fácil manejo. El producto de Opera se situaría a medio camino entre las empresas que han desarrollado solo un navegador o cliente de correo, y las que como Microsoft (Outlook) o Novell (Evolution) han desarrollado un producto más completo y potente para dar servicio a empresas.

2.8.1.6. Thunderbird

Este lector de correo está despegando con fuerza últimamente debido a que lo patrocina la misma empresa que desarrolló Firefox, es decir, Mozilla.

De momento es el único sustituto real a Microsoft Outlook Express y su futuro sucesor en Windows Vista, el Microsoft Windows Mail.

Es gratuito y dispone de versiones para Linux y para Windows.

Su última versión es la 1.5.0.8 y dispone de importantes funciones que rivalizan con las que Outlook Express no posee: lector de RSS, filtros de gestión del correo potentes, sistema de detección del spam con auto-aprendizaje, sistema anti-phishing, soporta extensiones (para añadirle más funcionalidad), temas o skins, etcétera.

A nivel de seguridad, como su rival, el OE, tiene firma digital, correo cifrado y acuse de recibos. Pero en temas de seguridad interna llega más allá, al cifrar todas las contraseñas de cuentas o buzones de correo mediante una password maestra. Intenta minimizar el espacio que utilizan los mensajes empleando la compactación automática, bloquea código Javascript, hace copias de seguridad de mensajes a medio escribir, y puede exportar la configuración de las cuentas mediante extensiones o programas adicionales (Mozilla Backup), también gratuitos.

Detecta nuevas actualizaciones por sí solo, y es capaz de aplicarlas.

2.8.1.7. Windows Mail

Es el sucesor de Microsoft Outlook Express y será incorporado en Windows Vista. No estará disponible para versiones anteriores de Windows a Vista.

Existen otros productos alternativos como i.Scribe o The Bat, aunque son productos comerciales con versiones limitadas freeware.

2.8.1.8. Resumen

Existe una gran variedad de clientes de correo, pero la mayoría de ellos son empleados por una muy pequeña minoría. Solo el Outlook Express, el Thunderbird y el Eudora son lectores de correo con una amplia base instalada de personas o empresas utilizándolos.

Otros productos como Evolution u Outlook pueden ser comparados, pero a otro nivel más cercano al propio de las empresas que necesitan gestionar agendas, direcciones de clientes, calendarios, tareas y reuniones de manera global y centralizada.

2.8.2. El spam

2.8.2.1. Introducción

Según la wikipedia el spam se define como:

Spam son mensajes no solicitados, habitualmente de tipo publicitario, enviados en cantidades masivas. Aunque se puede hacer por distintas vías, la más utilizada entre el público en general es la basada en el correo electrónico.

Se trata de enviar mensajes idénticos o casi idénticos a un gran número de direcciones. A diferencia de los correos electrónicos comerciales legítimos, el spam generalmente es enviado sin el permiso explícito de los receptores, y frecuentemente contiene varios trucos para sortear los filtros de spam. Las computadoras modernas generalmente vienen con cierta capacidad para enviar spam. El único ingrediente necesario es la lista de direcciones objetivo.

En España el spam está terminantemente prohibido por la Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSICE), publicada en el BOE del 12 de julio de 2002. Aparte, a los poseedores de bases de datos de correos electrónicos se les podría aplicar la Ley Orgánica de Protección de Datos (LOPD) por tratarse de datos de carácter personal. De hecho, las sentencias en España referidas al spam están relacionadas con esta ley.

La mayor parte de los mensajes (más del 40%) proceden de Estados Unidos (a pesar de que allí está prohibido), seguido por Corea del Sur (15%) y China (12%).

2.8.2.2. Por qué el spam es malo

Según el Instituto Nacional de Estadísticas el 57% de las personas que usan habitualmente Internet ha tenido o tiene problemas con el spam. El principal problema del spam, no es recibir mensajes publicitarios o fraudulentos diariamente que no han sido solicitados (donde se nos proponen negocios y asuntos aparentemente muy jugosos, pero con tintes de completa ilegalidad), sino que recibimos muchos correos, hasta el punto que puedes estar unos días fuera y cuando vuelves encuentras quinientos o seiscientos mensajes, que además han llenado tu cuenta, impidiéndote recibir correos que de verdad eran importantes.

Se calcula que la mayor parte del spam mundial lo emite un grupo de personas reducido que “compran” a hackers el acceso ilegal a ordenadores particulares o servidores, donde se instalan fraudulentamente programas que luego son utilizados para enviar el spam. Estos ordenadores son controlados remotamente y forman una botnet, o red que el hacker o spammer pueden usar para sus propios fines fraudulentamente y en contra de los intereses de su propietario (además del perjuicio legal que le puede suponer si es denunciado por el envío de spam).

Nota: En un estudio de Symantec Madrid aparece como la capital mundial con más pcs zombis (infectados y controlados remotamente) que son empleados entre otras cosas para el envío de spam. En España, el 84% del correo enviado es spam.

Recibir spam significa que las personas que envían spam tienen una base de datos o gran archivo con centenares de miles o millones de direcciones válidas de correo electrónico que han sido obtenidas por Internet, entre ellas, la nuestra.

Esas bases de datos se venden en foros o chats privados donde los spammers también adquieren todo lo necesario para llevar a cabo su tarea.

Las empresas que se dedican a la publicidad de manera legítima, siguiendo y respetando políticas de privacidad que supuestamente nosotros aceptamos al adquirir servicios de las entidades que a cambio de dinero han cedido nuestros datos a las empresas de publicidad, ven el spam como una amenaza. Si recibimos tanta publicidad, es probable que acabemos por no leer ningún correo basura, como también se llama al spam. El resultado final de esta actitud es que sus campañas publicitarias no serán efectivas, porque al final los usuarios, desecharemos toda la publicidad, ofertas, o correos que recibimos diariamente y que no provengan de personas conocidas o que no estén relacionados con nuestro trabajo.

2.8.2.3. La lucha contra el spam

Aunque existen leyes en España y Estados Unidos contra el spam, lo cierto es que no se respetan y los correos basura siguen llenando nuestros buzones de correo electrónico.

Por eso existen aplicaciones que se instalan en los servidores de correo, y que antes de enviar a sus destinatarios los emails que reciben, los analizan para conocer su origen y contenido y decidir entonces si deben llegar a su destino o son simplemente spam.

Estos servidores, además de métodos heurísticos para detectar el spam y expresiones regulares comprueban el origen de los mensajes y lo contrastan con grandes listas disponibles en Internet, donde aparecen aquellos ordenadores que se conoce con seguridad que envían spam. A estas listas de direcciones u orígenes conocidos como fuentes de spam, se las llama RBL (Relay Black List).

Otras listas serían las ORDB, de servidores maliciosos o mal configurados; y las de sistemas que son denunciados y reconocidos de forma contrastada como emisores de correo basura. Todas ellas permiten a los servidores de correo que sirven a los millones de usuarios de Internet reducir el problema del spam.

Para evitar el spam, nosotros también podemos aprovecharnos de las potentes herramientas anti-spam que están apareciendo. Por ejemplo, existen programas que filtran los correos que recibimos a diario en nuestras cuentas, incluso podemos encontrar paquetes especializados que constan de antivirus, firewall y programa anti-spam y que resultan fáciles de instalar en nuestros ordenadores.

O más fácil todavía, podemos adquirir un cliente de correo que incorpore su propio sistema anti-spam como Eudora o Thunderbird.

Del mismo modo, algunos de los servidores de correo de Internet, permiten personalizar filtros para evitar recibir spam de determinadas direcciones o con palabras concretas, lo que nos permite acotar un poco más el problema.

Precisamente porque cada vez hay más programas anti-spam, los spammers han empezado a enviar emails sin contenido, donde todo el texto va anidado dentro de una imagen, lo cual hace más difícil detectar que es spam.

2.8.2.4. Hoax o cadenas de mensajes

Seguro que ha recibido alguna vez un correo donde le advertían de alguna cosa mala o peligrosa pidiéndole que la difundiera por Internet para mayor seguridad de todo el mundo, o diciéndole que si no enviaba el correo a otras diez personas tendría muy mala suerte. Este tipo de correos, solemos enviarlos pulsando el botón de Reenviar. El resultado es que al propio correo vamos anexando todas las direcciones de las personas que lo han ido recibiendo o lo van a recibir. Así creamos listas enormemente largas de direcciones válidas de email. Estos correos que son recibidos por los spammers contienen muchas direcciones a las que luego enviaran basura.

Estas cadenas que se forman, donde un mensaje acaba siendo reenviado miles de veces, se llaman hoax y se basan en el desconocimiento de la gente o la superstición cuando hacen referencia a la suerte o la desgracia. No debemos reenviarlos. Podemos comprobar si un email recibido es un hoax en http://www.rompecadenas.com.ar/.

Existe otra variante de las cadenas de mensajes, donde se pide que se reenvíe un mensaje por solidaridad, o porque cuanta más gente lo reciba, determinada empresa ha prometido donar dinero para ayuda humanitaria o social.

La propagación de estos mensajes es piramidal y el número de personas involucradas es tal, que pronto se generan mensajes con centenares de direcciones de email. El mensaje, antes o después vuelve al emisor porque alguien se lo reenvía.

2.8.2.5. Medidas contra el spam

Como comentábamos anteriormente, no es difícil hacerse con una lista de direcciones de correo electrónico a las que enviar spam. Cuando enviamos un correo electrónico a alguien, normalmente lo enviamos a un grupo de amigos, y en el campo “Para” o “To”, solemos poner toda la lista de direcciones. Cuando nuestros amigos lo reciben, si les gusta, pulsan el botón de reenviar y escriben la lista de amigos a los que desean enviar el correo. Y así sucesivamente, pero no tenemos en cuenta que cada vez que pulsamos reenviar, añadimos más y más direcciones de email válidas al correo.

Para los spammers hacerse con estos correos es una mina, porque fácilmente llegan a tener centenares de cuentas de email válidas. Sería más aconsejable por nuestra

parte cuando reenviamos un email, copiar el texto del mensaje que queremos enviar a un nuevo email para que no se información sobre las personas que lo recibieron anteriormente.

Del mismo modo, en vez de enviar un email poniendo a todos los destinatarios en el campo “To” o “Para”, podemos usar el campo “BCC” (Black Carbon Copy) o destinatarios ocultos, con lo que cada destinatario del mensaje solo se verá a él mismo como destinatario, y si reenvía el correo, no recibirán todos una lista de las personas a las que yo envié el email.

Cuando recibamos un correo que sea categorizado como spam, y el propio correo diga que podemos desuscribirnos pinchando en un determinado link, nunca debemos hacerlo, porque en ese caso, estamos diciendo al spammer que la cuenta sigue activa y que puede seguir enviándonos correo basura.

Del mismo modo, no debemos abrir estos correos, porque los spammers pueden comprobar entonces si la cuenta de correo que lo ha recibido, la nuestra, está activa. Una de las formas que tienen de hacerlo, es cuando al abrir el correo recibido, se carga una imagen, a veces de tamaño minúsculo e inapreciable desde sus servidores, con lo cual comprueban que la imagen ha sido descargada, y por tanto que el propietario de la cuenta ha leído el correo, lo que quiere decir que sigue activa.

Es aconsejable tener siempre varias cuentas de correo y separarlas para distintas tareas. Por ejemplo, para negocios o trabajo, la cuenta de la empresa; para suscripciones a productos, información, artículos de interés y demás, otra cuenta de email; y para pruebas o servicios no confiables, una cuenta que recibirá normalmente mucho spam y poco de interés.

No debemos olvidar que existen programas que realizan búsquedas por Internet para crear enormes listas de direcciones de email, como por ejemplo Advanced Email Extractor.

2.8.2.6. Envío de adjuntos realmente grandes (100 Mb o más)

Poco a poco, las líneas de comunicación que los operadores ponen a nuestra disposición (cable o ADSL) tienen mayor ancho de banda y permiten ratios sostenidos de transferencias mayores. Enviar programas, colecciones de fotos, o proyectos enteros por Internet, a amigos, compañeros de trabajo o familiares se ha convertido en una realidad. No hace falta decir que antes, enviábamos todo esto mediante emails fraccionados, y empleábamos herramientas que volvían a unir todos los trozos para recuperar el gran archivo original.

Nos encontramos con que la mayoría de los servidores de mail de Internet no permiten el envío de grandes archivos o adjuntos, ya que procesan mail, pero no se les considera servidores de archivos y no están orientados hacia la transferencia masiva de los mismos. Procesan millones de emails sí, pero de un tamaño máximo de varios megabytes y si intentamos enviar correos de mayor tamaño, los rechazan.

Para estos casos, existen servicios gratuitos (y otros de pago) que nos permiten enviar enlaces a colegas, desde donde podrán descargar los archivos de gran tamaño que les dejemos. Estarán disponibles por unos días, y podemos precisar que no puedan descargarlos sin el empleo de una determinada password.

Servicios de este tipo serían:

- http://www.mailbigfile.com/
- http://www.transferbigfiles.com/Default.aspx
- http://www.yousendit.com/

2.8.2.7. Proteger nuestra cuenta de email

Si publicamos nuestro email en una página web o documento electrónico no debemos poner nuestro email, por ejemplo pepitoperez@seguridad.es, sino algo como pepitoperez arroba seguridad.es. Así los robots que rastrean las páginas web buscando direcciones de email no la entenderían como tal.

Otro ejemplo, en vez de poner pepitoperez@seguridad.es, sería pepitoQUITALASMAYUSCULASperez@seguridad.es, o simplemente pepitoperezARROBAseguridadPUNTOes.

Aun así, hay que destacar que existen ya programas capaces de reconocer y filtrar estas técnicas para obtener las direcciones reales.

También puede trabajar con alias si es administrador de su dominio. Por ejemplo, supongamos que nuestra cuenta de correo es pepitoperez@seguridad.es. En ese caso, podemos crear la cuenta pperez@seguridad.es, que en realidad redirige todo el correo a pepitoperez@seguridad.es. Si con el tiempo empezamos a recibir spam en pperez, podemos borrarla y crear un nuevo alias, como podría ser pp@seguridad.es. Naturalmente la cuenta pepitoperez@seguridad.es, no la daremos nunca a nadie, y es la que verdaderamente recibe todo el correo desde los alias anteriores.

Existe también la posibilidad de que insertemos nuestra dirección de email en Internet en forma de imagen. Con ello evitaremos que los bots o robots que buscan direcciones válidas por la red, tomen la nuestra.

O codificar el texto que escribimos en los formularios y páginas web en formato Unicode, que los navegadores representaran correctamente, y los clientes de correo también, pero que los robots de los spammers no podrán interpretar fácilmente. Para hacerlo podemos acceder aquí (utiliza el Internet Explorer). También puedes probar aquí o en esta otra web.

En cualquier caso, la mejor medida de seguridad es evitar publicar nuestra cuenta de correo en foros, blogs, libros de visita, news, tablones de anuncios, documentos que se publiquen en Internet, etcétera. Y si recibimos mucho spam, tal vez debiéramos de plantearnos cambiar de dirección de email.

Cuando insertamos en una página web el código necesario para presentar nuestra dirección de email y que al pulsar sobre ella se abra un nuevo mensaje dirigido hacia nosotros, solemos escribir algo parecido a:

```
<a href="mailto:cuenta@dominio.com"<>nombre</a>

Por ejemplo:

<a href="mailto:ggarcia@hotmail.com"<>Gabriel García</a>

Si cambiamos ggarcia@hotmail.com por:

&#103;&#103;&#97;&#114;&#99;&#105;&#97;&#64;&#104;&#111;&#116;&#
109;&#97;&#105;&#108;&#46;&#99;&#111;&#109;

y Gabriel García por:

&#71;&#97;&#98;&#114;&#105;&#101;&#108;&#32;&#71;&#97;&#114;&#99
;&#237;&#97;

Quedando el código entonces así:

<a
href="mailto:&#103;&#103;&#97;&#114;&#99;&#105;&#97;&#64;&#104;&#111;&
#116;&#109;&#97;&#105;&#108;&#46;&#99;&#111;&#109;"<>&#71;&#97;&#98;&#
114;&#105;&#101;&#108;&#32;&#71;&#97;&#114;&#99;&#237;&#97;</a>

Evitamos que los programas conocidos como bots o arañas que
buscan direcciones válidas puedan encontrarlas con facilidad en
nuestras páginas web.
```

Según el siguiente artículo, unas 200 personas en el mundo generan el 80% del spam del planeta. Esta regla que se conoce con el nombre de Principio de Pareto y que se aplica a muchas áreas de nuestra vida, es cierta también aquí.

Además cuatro de los diez peores spammers del planeta son rusos, otro es ucraniano, dos son estadounidenses, otro vive en Hong Kong y el último de ellos, es chino.

El volumen del spam en octubre del 2006 fue de 61.000 millones de mensajes por día, el doble que el año anterior.

2.8.2.8. Dar nuestra dirección de email por Internet

Para evitar dar nuestra dirección de email por Internet rellenando formularios o cumplimentando solicitudes cuando no vamos a volver a pisar esas webs, o cuando solo necesitamos el contenido del primer email que nos envíen (con login y password que luego cambiaremos) y no deseamos volver a recibir publicidad de la citada empresa, tenemos varias opciones:

- Dar de alta una cuenta gratuita, lo cual suele ser engorroso porque tenemos que cumplimentar un formulario en Internet, aun cuando usemos datos falsos.
- Poner una dirección inventada como milogin@mailinator.com. La cuenta será creada automáticamente al entrar en la web de Mailinator y podremos

recibir correos sin necesidad de teclear una password para entrar en la cuenta. Cualquiera que conozca el login podrá entrar. La cuenta será borrada tras unas horas y nos servirá temporalmente para lo que haga falta. Solo podrás recibir texto, ni adjuntos ni imágenes. Como existen sitios que identifican a "@mailinator.com", como un dirección falsa, podemos cambiar el dominio, por: fastacura.com, fastchevy.com, fastchrysler.com, fastkawasaki.com, fastmazda.com, fastmitsubishi.com, fastnissan.com, fastsubaru.com, fastsuzuki.com, fasttoyota.com o fastyamaha.com.

2.8.2.9. Algo bueno sobre el spam

Los mensajes que enviamos por Internet pueden ser codificados mediante potentes herramientas de cifrado, o ahora, puede ser convertidos en inocentes mensajes de spam que podemos codificar/decodificar desde https://www.spammimic.com/ y que podemos proteger con password, si así lo deseamos.

Estos mensajes, que son aparentemente spam podrán enviarse por Internet y pasarán completamente desapercibidos. Podemos leer más sobre el tema, como funciona y qué seguridad proporciona en https://www.spammimic.com/feedback.shtml.

2.8.2.10. El spim

No solo el spam es una forma de publicidad que llena nuestros buzones de email. Recientemente los spammers han comenzado a utilizar los sistemas de mensajería instantánea, como MSN Messenger, o los propios de AOL y Yahoo para enviarnos publicidad. La palabra spim nace de la unión entre spam e Instant Messaging.

La única manera de evitarlo es especificar que solo admitimos mensajes de aquellas personas que están en nuestra lista de contactos, aunque eso puede suponer que no podamos conocer a otra gente nueva.

2.9. Compras por Internet.

Según las estadísticas del INE, el 8,41% de los españoles (36.832.201 personas) hizo al menos una compra por Internet en los tres últimos meses (datos del 2005). Eso quiere decir que aunque aun estamos muy lejos de los niveles de otros países europeos o de Estados Unidos, las ventas efectuadas por comerciantes a través de la web, no son nada despreciables.

Tendemos a pensar que cualquier web en la cual nos pidan el número de la tarjeta de crédito para hacer compras, es segura y que la misma empresa ya debe haber tomado las medidas necesarias para garantizar nuestra seguridad. Pero eso, no siempre es así.

Si la empresa está cifrando nuestras comunicaciones, en la barra de direcciones web debería aparecer https y no http. Del mismo modo, si la comunicación está cifrada,

deberíamos ver en la barra de estado el dibujo de un candado. Pero con las nuevas técnicas que usan hackers y phishers esto puede no ser bastante. (Ver sección phishing para más detalles.).

Además deberíamos revisar la política de privacidad que tiene la empresa en cuestión, para ver si se considera en el derecho a ceder nuestros datos a terceras empresas con el fin de que nos envíen publicidad o información sobre campañas publicitarias, ya sea a nuestra casa o dirección de email.

Del mismo modo, no deberíamos comprar a aquellas empresas que tienen como opción o te avisan de que lo hacen por defecto, el hecho de guardar el número de tu tarjeta de crédito en su base de datos.

Tampoco deberíamos responder a cuestionarios de carácter personal ni fiarnos de links o hipervínculos que nos llevaran a otros sitios web.

No deberíamos utilizar nuestra tarjeta de crédito o débito normal para realizar compras por Internet. En muchas webs no nos queda claro si la información que damos sobre nuestras tarjetas de crédito u otros datos personales son almacenados. Y en el fondo, y si lo pensamos bien, nada nos garantiza que la empresa en cuestión esté cumpliendo lo que dice que cumple.

Es buena idea tener una tarjeta específica para realizar compras, que se cobren en una cuenta bancaria aparte, y con un saldo limitado, nunca en la cuenta donde se ingresa el sueldo o la nómina o están los ahorros de toda la vida.

Es aconsejable que la tarjeta sea de crédito y NO de débito si compramos a tiendas ubicadas en Estados Unidos, ya que las compras con tarjetas de crédito están protegidas en Estados Unidos por la ley “Fair Credit Billing Act”. Tienes más información aquí.

Del mismo modo, debemos revisar las operaciones o movimiento de la cuenta que tenga asociada la tarjeta de crédito con regularidad.

Deberíamos cambiar el pin o número secreto de la tarjeta cada determinado número de compras y en cualquier caso deberíamos pedir una tarjeta nueva si tuviéramos dudas sobre el sitio web donde los hemos introducido (la tarjeta nueva lleva un número diferente y anula la anterior). Sobre todo si hemos objeto de algún fraude (pagar o dar los datos y nunca recibir la mercancía, ni que contesten a nuestros intentos de contactar con ellos). No debemos usar contraseñas como “1234” o “1111”, y en ningún caso deberíamos dar el pin a nadie.

Existen tarjetas especiales, creadas por entidades bancarias para operaciones por Internet, y son normalmente de uno o varios usos, después ya no tienen ninguna validez.

Otra alternativa es emplear los medios de pago tradicionales que a veces también están disponibles, como el pago contra reembolso u otros mecanismos de pago como Paypal, etc.

Aun así siempre podrán aplicarnos la técnica de Parsons para robar la identidad de la tarjeta de crédito en cajeros bancarios y realizar compras por Internet.

Se trata de una técnica muy empleada en Malasia, donde ha causado estragos. Se accede al cable de datos del cajero automático desde la parte trasera del mismo y se desconecta el cable, entonces le conectamos un reproductor MP3 en modo grabación de voz. Los datos recibidos se guardaron como tonos de música mp3 que luego podían revertirse para obtener el número de la tarjeta de crédito y la fecha de caducidad, aunque no el pin. De todas formas, muchas webs permiten comprar solo con el número y la fecha. Así logró hacer compras por más de 200.000 libras.

2.10. Phishing

2.10.1. Introducción

Según la definición de phishing que da la Wikipedia, podemos decir:

Phishing es un término utilizado en informática con el cual se denomina el uso de un tipo de ingeniería social, caracterizado por intentar adquirir información confidencial de forma fraudulenta, como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria. El estafador, mejor conocido como phisher se hace pasar por una persona o empresa de confianza en una aparente comunicación oficial electrónica, por lo común un correo electrónico o algún sistema de mensajería instantánea.

Sin embargo, puede producirse también por un simple mensaje a su móvil, una llamada telefónica o un mensaje emergente en el navegador web.

Otra definición dada para el phishing es la siguiente:

Se trata de mensajes de correo electrónico que intentan suplantar a entidades como bancos, tiendas online y otras empresas. Con el fin de requerir de los clientes que proporcionen información privada, o con el aparente fin de confirmar datos que serán capturados en páginas web falsas a las que llegaremos mediante enlaces en el propio email. Una vez los delincuentes tengan en su poder la información de los clientes de las entidades suplantadas procederán a utilizarlos en beneficio propio.

La palabra phishing tiene el significado en inglés de “pescar”.

En el caso del correo electrónico el phisher dispone antes del ataque, de una base de datos de direcciones de email válidas. Luego, se asegura de enviar un mensaje a miles o millones de personas con algún falso propósito. El objetivo suelen ser las cuentas bancarias o los datos de tarjetas de crédito de personas confiadas o inexpertas.

El phishing a fin de cuentas, solo es otra forma más de ingeniería social, pero de muy bajo coste y bastante rentable basada en la técnica del spam o inundación de las cuentas de email de los usuario de correo basura o publicitario.

Para engañar al usuario, utilizan páginas web y logotipos idénticos o similares a las entidades que se pretende suplantar. En ocasiones incluso las cargan del propio servidor oficial de la entidad, pero manipulan partes de la página o incorporan lo necesario para cambiar su funcionalidad o forma de operar.

Normalmente los atacantes simulan la web de la entidad legítima a la que suplantan. Y es por eso que el diseño de la web falsa es fundamental.

El usuario debe comprobar cuando conecte con la citada entidad por la web, que la comunicación está cifrada, es decir, que se trata de una página cifrada y que en la URL del navegador puede leerse https y no http. Del mismo modo, debe buscar el símbolo de un candado cerrado que indica que la comunicación es segura. Según el navegador usado, este símbolo puede ser el de una llave.

Si ejecutamos un doble clic sobre este candado o llave, podremos ver información del certificado de seguridad.

Existen webs de entidades donde aparentemente la página no está cifrada y se accede a ella por http y no por https. Normalmente lo que sucede es que la página está formada por varias partes llamadas frames o marcos, y aunque la página funcione con http, la parte de la misma donde introducimos el login y el password (los datos confidenciales), está protegida por https. En estos casos, la única manera de cerciorarse es observar el código fuente de la página web. Llegados a este punto, y como el usuario medio no suele saber esto (piensa que accede a estas páginas sin cifrado), si le colaran otra página similar sin medidas de seguridad, no notaría la diferencia.

Si los portales web de estas entidades, muestran de forma clara todos los elementos que estas páginas deben tener para ser consideradas seguras, es más fácil que el usuario detecte que esos elementos no están si los phishers intentan que se conecte a páginas falsas que imitan a las buenas.

En principio se estima que el phishing tiene un alto índice de éxito, ya que sobre el 5% de los emails consigue su objetivo y la víctima cae en el engaño.

El fraude comienza cuando el usuario recibe un mensaje de correo electrónico que dice pertenecer a alguna entidad, y por el que se solicita al cliente su clave de acceso alegando que se trata de una medida de seguridad, protección o que se está probando el sistema informático.

Naturalmente las personas que no tienen nada que ver con la entidad, no suelen darse por aludidas, pero como el email lo recibe tanta gente, siempre hay quien de verdad pertenece a la citada entidad. El email suele contener un link, enlace o hipervínculo a la página web oficial de esta entidad, sin embargo no suele apuntar al sitio que parece y nos llevará a cualquier otro lugar de Internet, donde los estafadores esperan que introduzcamos nuestros datos secretos.

No deberíamos olvidar que todas las entidades bancarias han anunciado ya que nunca solicitarían datos a sus clientes por email, por lo tanto no deberíamos confiar en esa clase de mensajes.

Del incremento del phishing durante el 2006, podemos leer aquí un artículo.

Como consejos a seguir, estarían:

- No responder a emails que vengan en idiomas distintos al nuestro.
- No responder a emails de organizaciones a las que no pertenecemos o en las cuales no tenemos ningún servicio contratado.
- Saber si nuestro banco envía algún tipo de email a sus clientes y que procedimientos sigue.
- No pulsar sobre ningún enlace contenido en estos correos. Si hemos de ir a alguna de esas páginas web, teclearemos manualmente la URL en el navegador.
- Fijarse si el mensaje va dirigido a nosotros en concreto, para ello mirar el campo "To" o ver si se trata de un email masivo. Aun así no debemos olvidar que este dato es falsificable.
- Verificar que el cuerpo del mensaje contiene datos que demuestran que va dirigido a nosotros, como nuestro nombre completo, nuestro DNI, teléfono, dirección, es decir, algo que nos identifique de manera unívoca.
- Verificar si contiene errores gramaticales, cosa bastante común en mensajes falsos escritos con poco cuidado.
- Tener actualizados los navegadores web y también el antivirus. Internet Explorer 7.0, Opera 9.1 y Firefox 2.0 incorporan herramientas anti-phising, aunque nunca podrán sustituir al sentido común del usuario.
- Si la página muestra errores no debemos confiar en ella tampoco.
- Buscar los símbolos https y del candado.
- Vigilar direcciones como http://www.mibanco.es:entrada.jsp?CodigoActivacionSeguridad=@trente.tw/index.html.

En el improbable caso de que piense que el mensaje es legítimo y ante la duda, contacte primero telefónicamente o físicamente con la entidad y verifique que el email es de ellos. Y naturalmente, para contactar con ellos, no utilice ninguno de los datos que llegaron con el email, como teléfonos, faxes, u otros datos de contacto.

Un video práctico de los consejos arriba mencionados, podemos verlo aquí, en la web de Microsoft.

Evitar un ataque de este tipo se lograr simplemente manteniendo una actitud de desconfianza hacia todo correo no solicitado o recibido de fuentes no fiables o que siéndolo, no suelen enviar o pedir este tipo de información por email. Es pues más sentido común que otra cosa.

Las comunicaciones con bancos o la compra por Internet, una vez nos aseguramos de la identidad de la empresa con la que estamos haciendo la transacción, es segura. El problema viene cuando por error o engaño nos conectamos a una web falsa, que siendo muy parecida a la anterior, simula ser buena y nos dejamos engañar.

Hasta hace poco, con las recomendaciones citadas arriba, era suficiente. Sin embargo, los hackers y phishers han encontrado un agujero de seguridad que permite sofisticar el ataque y engañar al usuario aunque la conexión parezca segura. Podemos

ver un vídeo en Hispasec sobre este tema. La vulnerabilidad afecta al Cross-Site Scripting (XSS). Para ver con más claridad el alcance del problema, podemos ver tres vídeos en Hispasec. Se trata de un caso real donde se muestra en el primer vídeo, la perspectiva de la víctima; en el segundo se aprecia la preparación por parte del phisher del ataque y en el tercero se habla del alcance del problema.

Esta nueva modalidad de fraude es más difícil de detectar y depende de cómo haya creado la entidad, empresa o banco su portal web para que sea vulnerable o no.

Los ataques XSS o CSS (Cross-site scripting) se basan en inyectar una URL o código malicioso dentro de una URL válida de acceso a un sitio web embebiéndola en el campo de datos. Así, se aprovecha el sitio web original y se manipula solo una parte del mismo, normalmente la parte donde el usuario introducirá sus datos (login y password o número de tarjeta de crédito) para que sean enviados al sitio web fraudulento y no al oficial de la entidad.

Estas técnicas dan resultado debido a la baja calidad en el desarrollo de los portales web. Como ejemplos tendríamos:

- Sustitución completa HTML:
  - http://mibanco.com/data?URL=http://www.hackers.com/engaño.htm
  - Cargaremos desde dentro del sitio mibanco.com, otro sitio completamente distinto, el de hackers.com, donde los hackers esperan para obtener sus datos.

- Introduciendo un script en la página web de la entidad:
  - http://mibanco.com/data?page=1&client=<código script del hacker>

- Haciendo que la página principal de la entidad cargue código malicioso externo:
  - http://mibanco.com/data?page=1&response=hackers.com%21ordenes.js & ...

Un problema añadido al phishing es que la mayor parte de los usuarios según un reciente estudio que puede descargarse aquí y del que se hace mención en un artículo de Barrapunto desconocen como funcionan y para qué sirven buena parte de los elementos del navegador.

El phishing ha sido el fraude online más empleado en el 2006.

2.10.2. El phishing como forma de vida [3] [4]

El phishing o robo fraudulento de datos bancarios con el fin de lucrarse económicamente es una actividad que aumenta cada día conforme disminuye el nivel de conocimientos técnicos necesarios.

Disponibles en Internet por unos pocos cientos de euros, los kits de phishing incorporan todo tipo de instrucciones y facilidades orientadas a engañar a las víctimas y obtener de ellas datos sensibles que puedan reportar beneficios. El phisher solo necesita decidir la entidad que decidirá suplantar y las técnicas y el canal que empleará para llevarlo a cabo. Es importante que la web imite lo mejor posible la imagen corporativa de la empresa que deciden suplantar.

Hay grupos que además dan soporte a estas personas a cambio de repartir los beneficios. Existen complejas redes criminales organizadas y descentralizadas que se reúnen en foros y chats. Allí se venden todos los servicios que los phishers necesitan. Están los hackers que ponen a disposición de los phishers las máquinas comprometidas que enviaran los miles de correos necesarios a los usuarios para que estos piquen. Son máquinas de empresas legítimas a las que se ha roto su sistema de seguridad y ahora están bajo el control de los hackers. Forman las llamadas botnets, redes donde cada ordenador es controlado mediante un programa o bot que a su vez recibe órdenes desde algún canal de chat.

Las víctimas serán redirigidas en los emails a un dominio web propiedad del phisher y que ha sido comprado previamente, normalmente mediante una tarjeta de crédito robada, para que no figuren sus datos reales.

Se necesita aún la lista de emails a los que enviar el mensaje fraudulento. En Internet los spammers venden bases de datos completas con direcciones válidas a precios irrisorios (apenas unos euros por cada millón de direcciones).

Los phishers venden luego la información obtenida a estafadores conocidos como carders o cashers que utilizaran los datos para desvalijar a los propietarios. Hablamos ya de pines, números de tarjetas de crédito y códigos cvv2 (número de seguridad al reverso de la tarjeta formado por tres cifras). Estos estafadores transferirán el saldo a personas contratadas por anuncios como "gane dinero desde casa en su tiempo libre", que se encargarán de enviar este dinero fuera del país a cambio de un porcentaje y que cuando se rastreen los movimientos de las personas a las que se ha vaciado la cuenta bancaria, serán detenidas por la policía. A las personas que reclutan a estos pobres desgraciados conocidos como mulas, se les llama scammers.

Otro sistema consiste en crear duplicados de las tarjetas de créditos y realizar compras en establecimientos o extraer dinero en cajeros.

Después de obtener la información, el phisher borra el rastro de las operaciones. La experiencia hace que cada vez los ataques sean mejor ejecutados, sean más convincentes, duren menos tiempo y sean más rentables.

2.10.3. El pharming, una variante del phising.

La definición que da la Wikipedia es:

Pharming es la explotación de una vulnerabilidad en el software de los servidores DNS (Domain Name System), o en el de los equipos de los propios usuarios, que permite a un atacante redireccionar un nombre de dominio (domain name) a otra máquina distinta. De esta forma un usuario que introduzca un determinado nombre de dominio, que haya sido redireccionado, en su explorador de Internet, accederá a la página web que el atacante haya especificado para ese nombre de dominio.

Los ataques mediante pharming pueden realizarse de dos formas: directamente a los servidores DNS, con lo que todos los usuarios se verían afectados. O bien atacando a ordenadores concretos, mediante la modificación del fichero "hosts" presente en cualquier equipo que funcione bajo Microsoft Windows.

La técnica de pharming se utiliza normalmente para realizar ataques phishing, redireccionando el nombre de dominio de una entidad de confianza a una página web, en apariencia idéntica, pero que en realidad ha sido creada por el atacante para obtener los datos privados del usuario, generalmente datos bancarios.

Como herramientas para detectar el phishing tenemos:

- http://toolbar.netcraft.com/
- http://www.earthlink.net/software/free/
- http://www.trustwatch.com/
- http://www.google.com/tools/firefox/index.html
- http://www.spoofstick.com/

Si desea obtener más información en español sobre el apasionante mundo del phishing, puede leer las siguientes noticias:

- Artículo en PC Actual de marzo del 2006.
- PC World – Julio 2006 – La economía sumergida del phishing.
- El Cross-Site Scripting (XSS).
- Estudio sobre navegación segura aplicado a usuarios.
- Algunas técnicas sencillas de phishing.

Y en inglés:

- www.antiphishing.org
- www.ngssoftware.com/papers/NISR-WP-Phishing.pdf
- www.fraudwatchinternational.com/internetfraud/phishing/report.pdf
- http://www.cloudmark.com/releases/docs/wp_economy_of_phishing_10500406.pdf
- www.honeynet.org/papers/phishing

2.11. Malware y Spyware.

2.11.1. Spyware

Si miramos en la wikipedia, veremos que el término spyware se define como:

Los programas espía o spyware son aplicaciones que recopilan información sobre una persona u organización sin su conocimiento. La función más común que tienen estos programas es la de recopilar información sobre el usuario y distribuirlo a empresas publicitarias u otras organizaciones interesadas, pero también se han empleado en círculos legales para recopilar información contra sospechosos de delitos, como en el caso de la piratería de software. Además pueden servir para enviar a los usuarios a sitios de Internet que tienen la imagen corporativa de otros, con el objetivo de obtener información importante.

Pueden tener acceso por ejemplo a: el correo electrónico y el password; dirección IP y DNS; teléfono, país; páginas que se visitan, que tiempos se está en ellas y con que frecuencia se regresa; que software está instalado en el equipo y cual se descarga; que compras se hacen por Internet; tarjeta de crédito y cuentas de banco.

Los programas espía pueden ser instalados en un ordenador mediante un virus, un troyano (informática) que se distribuye por correo electrónico, o bien puede estar oculto en la instalación de un programa aparentemente inocuo.

Los programas de recolección de datos instalados con el conocimiento del usuario no son realmente programas espías si el usuario comprende plenamente qué datos están siendo recopilados y a quién se distribuyen.

Normalmente nos damos cuenta de que tenemos algún producto spyware en el ordenador, porque notamos alguno o varios de los siguientes síntomas:

- El equipo se ralentiza en las tareas diarias rutinarias.
- La conexión a Internet siempre va muy lenta.
- Se nos cambia la página de inicio del navegador web y no hay manera de restablecerla.
- Nos asaltan mensajes de publicidad o avisos de warning advirtiéndonos de infecciones en el pc que realmente no tenemos para que así compremos determinados productos que prometen mantener nuestro pc a salvo.
- Nos aparecen de vez en cuando ventanas emergentes con temas porno.
- En los navegadores web tenemos barras de herramientas que no queremos y no podemos quitarlas ni desinstalarlas.
- Cada vez tenemos menos control sobre el ordenador y éste está más cargado de spyware, con lo que se acentúa la lentitud, las pantallas emergentes, los anuncios, etcétera.

Debemos tener en cuenta que existen además programas o aplicaciones que dicen ser productos anti-spyware. Muchos de ellos son de dudosa calidad y/o efectividad. Y en el peor de los casos, algunos de ellos son spyware camuflado, con lo que instalarlos solamente empeorará las cosas.

Podemos distinguir entre los programas que detectan y eliminan spyware por una parte, y aquellos que solamente inspeccionan el registro de Windows para ver qué programas se ejecutan al iniciar el ordenador. Estos últimos nos servirán para evitar que determinadas aplicaciones que pueden ser virus o spyware se puedan poner en marcha al encenderse el pc, pero no para desinstalar o borrar estos productos.

En el caso de que sean del primer tipo, no siempre detectaran todo el spyware que haya en el pc, por eso es buena idea escanear el pc con varios de ellos. Algunos de los productos disponibles en el mercado de forma gratuita son:

- Spybot - Search & Destroy
- Ad-ware. Puedes saber más del producto aquí.
- SpywareBlaster. Para saber más pincha aquí.

Existen incluso detectores de spyware que no necesitan ser instalados, sino que escanean tu pc online, es decir, conectándose a Internet y aceptando la instalación de un componente ActiveX (por lo que estas páginas deben visitarse usando el Internet Explorer):

- Trend Micro

Podemos antes de instalar cualquier producto que se auto-defina como anti-spyware, comprobar si otras personas que lo han probado ratifican su utilidad, no sirve para nada y se trata de un programa de spyware encubierto. En esta web, podrás verlo, o también en esta otra.

Respecto al segundo grupo, es decir, los programas que verifican qué aplicaciones arrancan o se inician al encender el ordenador, tenemos:

- Startup Inspector
- Starter
- Startup-Mechanic

Con ellos podremos desactivar o anular el inicio de aquellos programas no se necesarios, o que puedan considerarse “no aconsejables” en nuestro sistema.

2.11.2. Malware

La palabra malware proviene de una agrupación de las palabras (malicious software). Se define como tal a cualquier programa que intenta acceder a información privada del usuario en el PC, dañar el propio ordenador, o afectar de alguna manera a su funcionamiento o a los datos que contiene con algún objetivo.

Como técnicas para hacer todo esto, se emplean virus, gusanos, troyanos, programas de spyware, la apertura de puertas traseras en los sistemas, exploits de vulnerabilidades conocidas, rootkits, etcétera.

En definitiva, el spyware estaría incluido en una categoría más amplia denominada malware, como también lo estarían los virus.

2.12. Espionaje interno.

Son cada vez más las empresas que se sienten perjudicadas por el uso que sus empleados hacen de la intranet o red de la empresa. La mayoría de los empleados chatean, compran, leen el correo, miran las noticias, o buscan nuevos empleos en Internet, pero durante su jornada laboral y no en su tiempo de ocio.

En cierta ocasión, estuve hablando con el dueño de una empresa que se dedicaba a cablear redes, normalmente industriales en polígonos empresariales y me comentó que les habían llamado para cambiar toda una red, porque "no tiraba". Tras varios días de verificar las infraestructuras y comprobar que todo era correcto, descubrieron que un empleado se bajaba videos y películas de Internet saturando la red de la empresa.

En otra ocasión una importante universidad española fue advertida seriamente por Red Iris, la red de investigación nacional de España, porque su máximo caudal de tráfico se había alcanzado un domingo por la tarde, cuando no había nadie en la universidad.

Los empresarios no desean que los empleados pierdan tiempo en su trabajo y como la infraestructura de red es de ellos, pueden poner los medios que crean oportunos para ver cómo se emplea la red. En principio, si la red va a ser monitorizada, y los servicios comprobados, la empresa tiene obligación de advertirlo al empleado. A partir de ese momento puede espiar o "esnifar" lo que se envía y/o recibe por la red.

Se supone que el único correo que se debe enviar por la red de la empresa es que el afecta a cuestiones del negocio, con lo que capturando o espiando estos mensajes, solo se accede a información no confidencial. Se parte del supuesto legal, de que comprar por Internet o solucionar cuestiones de carácter personal, se hace fuera del horario laboral.

Al espiar las comunicaciones o infraestructura de red, la empresa puede:

- Ver que webs se visitan más.
- Ver qué empleados usan más la red.
- Averiguar a qué servicios se accede.

Y por tanto descubrir actividades consideradas ilícitas como:

- Saber si los empleados buscan empleo o envían currículums a otras empresas.
- Insultan o denigran a jefes o compañeros en sus emails.
- Si están planeando algo, hablando con sindicatos, preparando una huelga o expresando su descontento.
- Conocer quienes son los más descontentos / contentos con las políticas de la empresa.

Lo que permite a las empresas:

- Presionar a los empleados que les interesa echar.
- Conocer sus pretensiones o intenciones con antelación.
- Los problemas / expectativas personales de cada uno.
- Y actuar en consecuencia.

Aunque en principio está prohibido espiar de esta manera sin previo aviso, existen empresas que lo hacen. Por eso siempre debemos ser muy cuidadosos con lo que decimos o hacemos a través de la intranet de la empresa.

2.13. Identificadores

2.13.1. Por Hardware.

En enero de 1999, Intel, el mayor fabricante de microprocesadores para computadores del mundo, dijo que su nuevo procesador, el Pentium III llevaría un número de identificación único, el PSN o Pentium Serial Number, que ayudaría al despegue del comercio electrónico y que podría usarse como identificador en transacciones comerciales de todo tipo.

La existencia de ese identificador y el hecho de que pudiera ser consultado y utilizado no gustó a organizaciones que defienden nuestro derecho a la privacidad. El identificador haría que una vez asociado el número en cuestión a una persona, supiéramos donde había navegado, qué había comprado, etcétera. El anonimato en Internet habría desaparecido.

Aunque finalmente Intel desactivó esta opción en los Pentium III, su imagen quedó dañada y fue acusada de ceder a las presiones de alguna agencia gubernamental de los Estados Unidos, por lo que decidió no añadir esta característica en su siguiente gama de procesadores (Willamette). Las supuestas ventajas en cuanto a seguridad no fueron suficientes frente a los grupos de presión que exigieron a Intel la retirada del PSN. Para los procesadores Pentium III en el mercado, Intel ofreció una utilidad que deshabilitaba el citado identificador.

En abril del 2000, Intel anunció oficialmente que sus nuevos procesadores, no llevarían la citada característica.

El interés demostrado por determinadas empresas para identificar a los usuarios en Internet, pone a veces en entredicho el anonimato en la red de redes. Internet es un lugar donde la gente puede moverse, expresar sus deseos, sus necesidades, conversar o relacionarse de forma anónima. Pero para poder ofrecernos lo que “necesitamos”, otros necesitan identificarnos como sujetos únicos, con gustos, preferencias y poder adquisitivo concretos.

Para conectarnos a Internet, los ordenadores utilizan un protocolo conocido como TCP/IP versión 4. El crecimiento exponencial en el número de dispositivos conectados a Internet, ha hecho necesario desarrollar un nuevo protocolo donde el

identificador utilizado para conectar a Internet sea más largo y por tanto pueda dar cabida a más dispositivos, ya que en algún momento no podremos seguir numerándolos porque se nos acabaran los números (algo parecido a lo que sucede en las matrículas de los coches).

Sin embargo, y aunque IP v.4 permitía ser configurado para proteger la privacidad de los usuarios, en IP v.6, la asignación del identificador basado en el número único que se almacena en la tarjeta de red, anulará nuestra privacidad, pues aunque cambiemos de proveedor de Internet, como nuestro pc, siempre llevará la misma tarjeta de red, parte del identificador usado en IP v.6 siempre será el mismo, y por tanto será posible reconocernos en Internet.

2.13.2. Por Software.

En marzo de 1999, el New York Times avisó que los archivos generados por Word, Excel o Powerpoint en Office 97, contenían un identificador único generado a partir del identificador de la tarjeta de red. Microsoft tuvo que publicar el modo de borrar estos identificadores de sus archivos y retiró definitivamente el citado identificador en Office 2000 y productos posteriores.

Existe un informe que trata estos temas en Internet y puede ser encontrado en http://www.paris-conference-2001.org/eng/contribution/dinant_contrib.pdf y también en http://notebook.ifas.ufl.edu/privacy/.

2.14. Programas que vulneran nuestra privacidad (Word).

Todos recordamos aquellas versiones de Word que funcionaban sobre Windows 3.11, antes que naciera Windows 95 con su interfaz gráfica y todas las versiones que vinieron después.

En aquella época, ya se adivinaba que Word era un programa muy grande, más complejo que otros de la competencia como el WordPerfect, y que no era muy fino en su funcionamiento. Podías abrir el Word y cerrarlo poco después, y veías que te quedaba un poco menos de memoria libre que antes de que lo abrieras. ¿Por qué? – pensabas. Si he cerrado el Word, ¿por qué no me ha devuelto toda la memoria que ha empleado para ponerse en marcha? Si repetías la operación de abrir y cerrarlo varias veces más, al final, no te quedaba memoria para hacer nada. Llegaba un momento en que sin tener ningún programa abierto, no tenías memoria. Aquello era una mala gestión de recursos por parte del Office de Microsoft. Muchas versiones se han sucedido después: Office 95, Office 97, Office 2000, Office XP, Office 2003 y Office 2007.

Todo el mundo se pregunta porqué a veces un documento de Word ocupa tanto espacio cuando está vacío. Un documento de texto, apenas ocupa nada si está vacío.

Mucha gente ha comprobado que después de crear y modificar un documento durante varios días, si seleccionabas todo el texto del documento en el Word, creabas un documento nuevo, y pegabas todo el texto del original, al grabar el nuevo documento ocupaba bastante menos que el original, y eso a pesar de contener lo mismo.

La respuesta a este hecho curioso, es que el Word almacena no solo el estado del documento actual, sino los cambios que se van haciendo. Puede parecer una tontería, pero atenta contra nuestros derechos.

Supongamos que yo empiezo a escribir un documento de Word a mi jefe, donde le amenazo por ser tan borde, tan mala persona y tener tan poca ética como tiene. Es un documento que voy a enviarle por email, donde le cuento las cosas que se de la empresa y como pienso utilizarlas para tirar de la cuerda si sigue pisándome. Dos días después de haberme enfadado tanto por congelarme el salario por segundo año consecutivo mientras él se compraba un coche nuevo, me lo pienso y modifico el documento, lo suavizo, le pido que sea más agradable, quito las advertencias de denuncia y las pruebas que tengo sobre ello, y finalmente le envío el email.

En principio mi jefe no puede ver todo ese texto que quité o cambié, pero sigue ahí, y con las herramientas adecuadas podría ser recuperado y utilizado contra mi. El texto no ha desaparecido del documento, sigue en él, aunque no aparece.

El problema es que esas herramientas existen. Y es por eso que en estos casos, se recomienda abrir un nuevo documento y pegar el texto definitivo, para que no se guarden en este segundo documento los cambios que he comentado.

Este comportamiento no es exclusivo de Word, lo padecen también Excel y PowerPoint.

Aun recordamos la polémica desatada por los informes de Blair y sus ministros en Gran Bretaña por las supuestas armas de destrucción masiva de Irak, donde se distribuyeron documentos de Word, con datos ocultos, que mostraban los cambios que se habían ido haciendo a los documentos, algunos de los cuales, no sentaron bien al llegar a los medios de comunicación.

Hay documentos de Word en Internet, que según Simón Byers, tienen incluso más de 500 palabras ocultas. El verdadero problema de esto, es que se pueden ver las intenciones originales del documento antes de que se hicieran más sutiles, o incluso textos “recordatorio” que expresan hechos o sentimientos en términos de cómo los pensamos en realidad.

Así pues debemos con cuidado con lo que publicamos.

2.15. La ley de Protección de Datos.

La Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal, más conocida como la LOPD, obliga a las empresas que posean ficheros con datos de carácter personal a tomar las medidas necesarias para garantizar su seguridad.

Es sustituta de la Ley Orgánica de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal (LORTAD) de 1992, que solamente se aplicaba al tratamiento automático de datos.

El 26 de junio de 1999 entra en vigor el reglamento de seguridad (R.D. 994/99) que desarrolla la ley y obliga a las empresas de activar todos los mecanismos necesarios para proteger sus datos.

La nueva ley es aplicable a todos los datos de carácter personal que sean almacenados en soporte físicos con posibilidad de tratamientos posteriores, y sin importar si provenían del sector público o privado.

Intenta proteger derechos fundamentales como son la intimidad y el honor de las personas. Y los datos obtenidos sobre ellas, solamente podrán emplearse para las finalidades con que se pidieron, incluyendo también fines históricos, estadísticos o científicos.

La ley no se aplica a los datos de carácter exclusivamente personal o domésticos.

Además es importante que estén actualizados y respondan a la situación real. Si quedan incompletos, inexactos o dejan de responder a la situación real, han de ser borrados o corregidos.

Siempre que hayan cumplido la finalidad para la que fueron recogidos deberán ser
destruidos, y en caso de no ser posible, serán bloqueados. Además debe garantizarse que la identidad de las personas incluidas en los ficheros o bases de datos no podrá ser recuperada posteriormente, cuando se haya cumplido la finalidad para la que fueron recabados.

No se pueden recoger datos mediante engaños, falsedad o medios fraudulentos. Se debe avisar a las personas a quienes se requieran los datos que van a ser incluidas en un fichero, debe avisárseles también de para qué se usará la información y quien tendrá acceso a ella.

Del mismo modo, se debe advertir de si es o no obligatorio suministrar los datos para un determinado servicio, de la posibilidad de ejercer el derecho a cancelarlos y/o rectificarlos, de las consecuencias que se derivan de la obtención o no de los datos, y de la identidad o responsable o representante del mismo encargado del tratamiento de los datos, quien tiene como obligación evitar su perdida, acceso no autorizado o alteración de los mismos.

Toda persona puede ejercitar su derecho a que los datos que una citada entidad posee de ella sean borrados o al menos bloqueados.

La Ley de Protección de Datos Española es la más dura a nivel europeo, con sanciones que van desde los 600 euros hasta los 600.000 aproximadamente. Y establece también el tipo de protección que debe dársele a la información en función de su categoría.

Podemos leer más sobre el tema en la Agencia de Protección de Datos, en https://www.agpd.es. Del mismo modo, podemos leer más sobre la seguridad de los datos en la LORTAD.

2.16. He de decirte algo pero no quiero que sepas quien soy.

Todos nos hemos preguntado a veces sobre la posibilidad de avisar a alguien sobre algún tema espinoso sin enfrentarnos al riesgo de ser malinterpretados o que se nos presionara para obtener más información que la que deseamos dar sin colocarnos contra la pared.

En Internet parece que todo es anónimo, pero lo cierto es que los servidores a los que accedemos registran quienes somos, con quien contactamos, qué estamos enviando y a quien.

Pues bien, todavía podemos enviar un mensaje a alguien ocultando nuestra identidad y sin dejar nada que pueda identificarnos como responsables del envío.

Se trata de un mensaje a lo James Bond, que se autodestruirá en un número determinado de segundos, tras un número concreto de lecturas o al cabo de algunos días.

Y podemos hacerlo desde esta web:

http://www.willselfdestruct.com/secure/submit

2.17. Navegación anónima.

Como comentábamos anteriormente, cuando navegamos por Internet, muchos de los servicios a los que accedemos registran nuestra IP como método estándar de identificación, eso quiere decir que si siempre usamos el mismo ordenador para acceder a determinados servicios y ese equipo siempre tiene la misma IP, nos tienen completamente identificados.

Si deseamos acceder a Internet como usuarios anónimos, siempre podemos emplear un proxy para mejorar la velocidad de acceso a portales y servicios, y de paso, si el proxy en cuestión lo permite, hacerlo de manera anónima.

Supongamos que deseamos acceder a un portal web, en ese caso, podemos escribir la dirección en el navegador, y en vez de acceder directamente al portal, nuestro navegador pasará la solicitud de la página web al proxy propiedad de algún proveedor de servicios (ISP), que es quien reclamara la página en cuestión, siendo él quien se identificara por nosotros para luego enviarnos la página o datos que hemos solicitado.

Naturalmente al no ser nosotros quien la accedemos directamente, la ip de acceso que quedará registrada no es la nuestra sino la del proveedor.

El proveedor está obligado a registrar quien accede a sus servicios, pero a no ser que infrinjamos la ley o la justicia lo requiera, nuestros accesos jamás serán públicos ni podrán ser empleados para conocer nuestros gustos o intereses, con lo que nuestra privacidad queda protegida.

Acceder a través de estas empresas a Internet tiene un coste, es decir, es necesario normalmente para garantizar la calidad, pagar una pequeña cantidad mensual o anual.

Es importante distinguir lo que sería un servicio proxy de un servicio proxy anónimo. Los proxies se emplean en Internet para mejorar el acceso a Internet y la velocidad con la que se accede a los servicios. Pero en nuestro caso, más que mejorar las prestaciones, lo que deseamos el garantizar el anonimato.

Existen muchos proxies públicos, aunque la mayoría no son anónimos, podemos ver listas de ellos en http://www.publicproxyservers.com/index.html. Existen incluso otros pequeños programas que podemos instalar en nuestro pc y que nos advierten de la disponibilidad de proxies públicos.

Ejemplos de proxies de pago pueden ser:

- http://www.proxyplus.cz/
- http://www.proxomitron.info/

Y uno de los más completos y conocidos por los usuarios (de pago) sería éste:

- http://www.anonymizer.com/

Bibliografía

[1]. Según las estadísticas del Instituto Nacional de Estadísticas (INE), de las personas que disponen acceso a Internet, el 78% lo usa desde casa, el 30% accede a la Red desde casa de amigos o familiares, el 51% lo hace desde el trabajo, el 17% desde un centro de estudios, el 13% desde un centro público y otro 13% desde cibercafés o similar.
Eso significa que la propia casa y el trabajo son los dos lugares favoritos para conectarse a Internet.

[2]. Según el INE, en España, la mitad de los hogares tiene PC, ya sea en la forma de un ordenador de sobremesa, un portátil o una PDA. De los hogares que disponen de ordenador, el 52% tiene solamente uno, lo que quiere decir que la familia lo comparte,

con lo que, un riesgo o error de seguridad asumido por un miembro de la familia también afecta al resto.

[3]. Casos de empresas que han perdido datos de sus clientes o portátiles con información confidencial se producen continuamente.
En junio del 2006 se perdió un portátil de la consultora Erns & Young con los números de las tarjetas de crédito de 240.000 clientes de la web hotels.com.

[3]. Un artículo muy completo e interesante sobre phishing.
[4]. Otro artículo sobre phishing.

Webs que venden piezas para asegurar ordenadores:

- http://www.anchorpad.com/
- http://www.computersecurity.com
- http://www.kensington.com/
- http://www.pcguardian.com

Un artículo muy completo sobre la seguridad en portátiles:
Laptop Security. Locking Down the laptop by Paul Korzeniowsky

Capítulo 3. Técnicas básicas de protección del PC

3.1. Introducción

Cuando la gente pregunta qué puede hacer para proteger su ordenador, piensa en términos distintos a los que uno utiliza cuando quiere proteger su casa. Ponemos una puerta blindada, una alarma, rejas en las ventanas y pensamos que ya es muy difícil que consigan acceder a nuestra casa. Sabemos que es posible, pero bastante más difícil.

En informática puedes tener el antivirus al día, pero puede aparecer hoy un virus nuevo, y mañana se te infecta el ordenador sin que puedas hacer nada. En ocasiones, incluso te deja de funcionar el equipo y desconocemos la causa. ¿Falló el antivirus?, ¿fue el firewall lo que no resistió el embate de los hackers?, ni siquiera lo sabemos.

Explicar a alguien que proteger tu equipo con mimo y gastar tu dinero en su seguridad, puede un día concreto no servir para nada, no es asumible en general por el público. Lo cierto es que garantizar la seguridad de un ordenador al 100% no es posible, y encima, protegerlo adquiere a veces grados de complejidad que resultan asombrosos para el usuario medio.

Aun así, hay muchas cosas que pueden hacerse para proteger un ordenador por encima de la media, y aunque parezca increíble, puede servirnos para no padecer en cinco años un solo incidente informático. Sin embargo, eso no garantiza que no nos pase nada, solo que tengamos una frecuencia de incidencias bastante menor a la de aquellas personas que se protegen poco o nada.

No piense en su ordenador como un electrodoméstico más, ni en su agenda electrónica o PDA como solo una agenda. Si contiene información vital para usted como contraseñas, pins, teléfonos, piense en ellos como aparatos sensibles. Deje de pensar en ellos como simples máquinas que pueden robarle y revender más tarde. Se trata de información. ¿Pasea usted su diario personal cuando sale de casa y lo deja en cualquier parte?

Haga copias de seguridad de sus datos a menudo (luego veremos como) y lleve siempre una copia consigo, pero disponga de otras en distintos lugares (oficina, chalet, etcétera). Destruya las copias de seguridad viejas.

No use lo mismo que todo el mundo porque los hackers dedican siempre más tiempo a atacar lo que usa más gente, es cuestión de simple estadística. No use Windows, si no le importa emplear alguna distribución de Linux o pasarse a Mac OS de Apple ¿Por qué? Porque Windows lo usa la mayoría.

¿Emplea Outlook Express? Cambie a Eudora, Thunderbird, Evolution o cualquier otro producto con una cuota de mercado muy inferior.

Nadie se toma la molestia de buscar agujeros de seguridad en aplicaciones poco utilizadas y que afectarían a pocos usuarios. Esto solo se hace con ataques dirigidos contra empresas por temas de espionaje industrial.

Por lo mismo, emplee otros navegadores web que no sean el Internet Explorer y recuerde que dispone de alternativas gratuitas al Office como el OpenOffice y que existen muchas alternativas al Word, la última viene de la mano de Google en http://docs.google.com.

Si ya no usa una determinada aplicación, quítela de su ordenador. Así evitará que cualquier fallo de seguridad en la misma, pueda ser empleado para violar la seguridad de su pc.

Asegúrese de actualizar regularmente Windows, Office, y cualquier producto que emplee y para el que hayan salido nuevos parches de seguridad.

No deje su pc en manos de sus hijos, familiares o amigos si lo usa para tareas sensibles. No permita que cualquiera le instale software a su ordenador. Controle que se instala en el ordenador y qué páginas web son visitadas.

3.2. Las contraseñas.

3.2.1. Introducción

Es bien conocido por parte de todos, que las personas tenemos dificultad para recordar contraseñas largas y complejas. Por eso solemos seleccionar las mismas para varias cosas. Suelen ser cortas, sencillas, y no las cambiamos en mucho tiempo.

No todos somos como ese japonés que ha batido su propio record al recordar los cien mil primeros decimales del número pi y que ha necesitado 16 horas para recitarlos.

En cierta ocasión un experto de seguridad informática que se dedica a asesorar empresas dijo que podía violar la seguridad de alguna de las empresas más importantes del mundo (Fortune 500) en un mes.

Le preguntaron cómo lo haría, y dijo que era sencillo. Bastaba con ofertar a la gente de esas empresas algún servicio por Internet que fuera atractivo, jugoso, y gratuito. Naturalmente para conectarse al servicio, habría que identificarse con un login y una password o clave secreta que el usuario elegiría.

Según las estadísticas, la mayoría de ellos utilizaría la misma password que usaba en los ordenadores de la empresa. Además esa password podría saberse a qué ordenadores pertenecía o daba acceso, porque la mayoría de la gente se conecta desde el trabajo a Internet. El corolario a esto es claro, no reutilice contraseñas.

Por si fuera poco, en las empresas o sitios donde hay alguien encargado de que las contraseñas se cambien a menudo, o tengan cierta dificultad, acaba descubriéndose

que los usuarios se las apuntan en la cartera, el bolso, bajo el teclado del ordenador o en un post-it pegado al monitor.

3.2.2. Normas para crear contraseñas.

- Las contraseñas deben ser largas. Hoy en día, nadie recomienda contraseñas de menos de 15 caracteres.
- Formadas por toda clase de símbolos: Deben contener números, letras en mayúsculas y minúsculas y signos de puntuación o caracteres espaciales como son: | @ # ~ $ % & / ( ) = ¿ ? ^ * { } \ º ª - , etc.
- No deben usarse para más de una tarea o acceso a un servicio.
- Tareas distintas deben requerir contraseñas distintas.
- Deben cambiarse al menos anualmente y en caso de que se requiera mucha seguridad, mensualmente.
- No deben ser palabras contenidas en el diccionario común.
- Ni ser parte del nombre o apellidos, fechas importantes, datos como el DNI, dirección donde vivimos, número de la seguridad social, de la tarjeta de crédito, números de teléfono o secuencias de teclado.

En "Datos de seguridad de contraseñas", podemos vemos ver la dificultad de romper contraseñas de longitud baja o media por los hackers (inferiores a los nueve caracteres).

Si queremos generar contraseñas difíciles de averiguar, podemos recurrir a la página web: http://passwd.thebugs.ws/index.php, donde podremos elegir el tipo de caracteres empleados, la longitud de las contraseñas e incluso si deben poderse pronunciar para que sean más fáciles de recordar.

Y nunca debemos olvidar que la mayoría de los problemas de seguridad se producen por la mala calidad de las contraseñas elegidas.

En http://www.securitystats.com/tools/password.php, podremos verificar si nuestra contraseña es lo bastante buena, aunque no debemos introducir la verdadera, sino una parecida. Debemos entender la seguridad como una actitud no como una obligación.

3.2.3. Las frases de paso.

Como recordar contraseñas largas y difíciles de escribir y memorizar como puedan ser: "f%$m_.+w"q=.&N{*" es una tarea demasiado ardua para la mayoría de la gente, nacieron las frases de paso.

Una frase de paso es una contraseña compuesta por varias palabras y que hace referencia a un tema que nos resulta fácil de recordar, por ejemplo:

- Tanto va el cántaro a la fuente que al final se rompe.
- Tanto monta monta tanto Isabel como Fernando.

- El príncipe de las mareas.
- Superman returns.
- Los cuatro fantásticos.

Si respetamos las mayúsculas del inicio de frase y de los nombres propios, ya tenemos algo un poco más difícil de adivinar.

Cojamos la frase “Tanto va el cántaro…”.

Eliminamos las vocales:

Tntvlcntrlfntqlfnlsrmp.

Añadamos después de “Tanto” un & y al final algo como “3x4=12”. Ahora tenemos: Tnt&vlcntrlfntqlfnlsrmp3x4=12.

Esta contraseña es más difícil de averiguar. Si la tecleamos unas pocas veces seguidas, veremos que la escribimos bastante aprisa y que ya no es tan difícil de recordar. Estamos usando normas nemotécnicas para recordar la contraseña, o lo que es lo mismo estamos buscando un símil que nos facilite recordar la clave secreta.

Pongamos otro ejemplo:

Queremos una contraseña larga y difícil de seguir cuando escribimos en el teclado. Está comprobado que hay gente capacitada para seguir los movimientos de una mano sobre el teclado. Así que es bueno que tecleemos las contraseñas a dos manos.

En cualquier caso, siempre hay teclas, en cada mitad del teclado, que una mano accede a ellas más fácilmente y rápidamente. Es por eso que después de presionar una q no deberíamos ir a buscar una n, y menos si escribimos la contraseña con una mano.

La idea es que la mano, cuando comience a teclear en una zona, use varias teclas cercanas entre ellas antes de pasar a otra zona. Esto se aplica sobretodo a gente que no sabe mecanografía.

Es recomendable también que tengamos que presionar determinadas teclas varias veces para que se pierda en la memoria del que mira el orden y la posición de las teclas que hemos presionado con exactitud. Si presionamos una sola vez cada tecla resulta fácil recordar si la hemos presionado o no por parte de alguien que se fije; si la presionamos muchas veces, y cambiando el orden con otras, resulta mucho más difícil averiguarlo.

Y desde luego las teclas elegidas tienen que permitirnos escribir con velocidad. Todos sabemos que es difícil, por la configuración del teclado qwerty.

Podríamos elegir: quequesoeseseeso, es decir que-queso-es-ese-eso.

Al teclearla veremos que se pierde la noción de cuantas veces tecleamos la e y la ese. Alguien que lo vea, recordará el orden de las teclas, pero no cuantas veces hemos pasado por ellas. Naturalmente faltaría añadir algo más a la contraseña.

En cualquier caso, la frase de paso no debería ser algo muy conocido como un refrán, el nombre de un escritor, o el título de una película. No, si no hacemos algún cambio. Una contraseña, donde conociendo la primera parte, otras personas puedan averiguar la segunda parte, no es una buena idea. Ahora, si la primera parte permite obtener la segunda, pero hemos hecho un par de cambios que dificultan considerablemente que sea averiguada, entonces podemos darla por válida.

Sin embargo, para las personas realmente con poca capacidad de memoria, existe la posibilidad de que solo recuerden una única contraseña y usen programas que memorizan y cifran tantas contraseñas como queramos. Con recordar una, el programa nos da la lista de todas las demás. Ejemplos de este tipo de herramientas serían Password Safe o KeePass, ambos gratuitos.

Por último existe la llamada tarjeta de identificación que es una tarjeta, de tamaño similar al DNI o a una tarjeta de crédito, que al pasarla por un lector incorporado en los teclados de los ordenadores nos permite identificarnos sin necesidad de clave alguna.

3.3. Windows, Office y updates.

Para evitar accesos indebidos al sistema operativo de nuestro ordenador y que cualquier persona pueda aprovechar un agujero de seguridad nuevo que ha aparecido recientemente, debemos asegurarnos de tener el ordenador tan actualizado como sea posible.

De vez en cuando, Microsoft que es la empresa que ha creado Windows 3.11, Windows 98, Windows 98SE, Windows NT, Windows Millenium, Windows 2000, Windows XP y Windows Vista, descubre un nuevo agujero de seguridad, que bien aprovechado por los hackers puede darles acceso completo a nuestro PC.

Esta es la causa de que continuamente debamos estar actualizando nuestro ordenador con parches de seguridad que en ocasiones han generado también nuevos riesgos.

Sin embargo las cosas no son tan fáciles como parecen. Existen momentos en los cuales nos podemos ver en el peor de los aprietos y no podremos hacer nada por evitar que nuestros ordenadores sean saboteados o infectados.

En ocasiones, Microsoft ha reconocido una vulnerabilidad en alguno de sus programas (Windows, Office, Internet Explorer, etcétera) y los hackers han desarrollado rápidamente una herramienta para romper la seguridad de estos ordenadores, mientras que Microsoft ha tardado tiempo en crear un parche para solucionar el problema (o nunca lo ha hecho).

Esto ha sucedido frente a agujeros de seguridad muy complejos de taponar, o que requerían importantes cambios en el sistema operativo para subsanarlo. ¿Y qué hacemos mientras? ¿Dejamos de usar el PC y lo apagamos? ¿Y si nunca sacan un

parche? En estos casos, nos vemos obligados a seguir empleando el sistema operativo y rezar porque no nos pase nada mientras seguimos trabajando a diario. Es por eso que las copias de seguridad del sistema y de los datos son aquí tan importantes.

Supongamos que se descubre una vulnerabilidad en un producto de Microsoft, y desarrollan el parche. Si tenemos normalmente el ordenador desconectado de Internet, para bajarnos el parche hemos de conectarnos a Internet. Pero, y si mientras lo hacemos, nos ataca el citado virus o hacker, y consigue acceder a nuestro pc, aprovechando la citada vulnerabilidad, ¿qué haremos entonces? Esta opción que parece sacada de una mente enferma, es lo que sucedió con los virus conocidos como Blaster y Sasser que infectaron decenas de miles de máquinas, y que, por suerte, el único daño que causaban, era apagarlas.

Puede incluso darse el caso de que usted se marche de vacaciones y cuando vuelva hayan salido cinco o diez parches nuevos. Si conecto el pc a Internet para actualizarlo, corro el riesgo de que resulte infectado antes de que el servidor me proporcione los citados parches. Puedo obtener los parches desde otro ordenador para luego instalarlos manualmente en mi pc, pero es lento, farragoso y se necesitan algunos conocimientos técnicos para hacerlo, claro.

La situación se decanta hacia nuestro lado cuando es un virus el que aprovecha una vulnerabilidad de Windows para acceder al ordenador, porque entonces tenemos la posibilidad de que la empresa que fabrica el antivirus que usamos en nuestro pc también saque un parche para protegerlo hasta que Microsoft solucione el fallo.

Con el Office sucede lo mismo, existen riesgos cada vez que alguien descubre un fallo de seguridad que afecta a alguno de los programas que van dentro de este paquete ofimático. Hace poco se encontró un agujero de seguridad que afectaba a todas las versiones del Office desde Office 97 pasando por Office 2000, Office XP y Office 2003, era una vulnerabilidad relacionada con las imágenes JPEG.

¿Qué habría pasado si alguien hubiera descubierto hace tiempo esta vulnerabilidad y no hubiera dicho nada? ¿A cuantos ordenadores podría haber accedido para robar información sin que nos enteráramos nunca de cómo había sucedido?

Según los últimos estudios, lo peor está por llegar. Hasta ahora, los hackers, crackers o piratas informáticos como también se les llama, atacaban Windows, porque era el sistema operativo más usado en el mundo. Pero hoy han descubierto formas más rápidas de detectar agujeros de seguridad en el paquete ofimático Office.

Utilizan “fuzzers”, es decir, herramientas capaces de rastrear el código de Office y de generar miles de llamadas al sistema con la intención de averiguar cuales son capaces de bloquearlo. Por eso se están sucediendo fallos de seguridad en Word, PowerPoint y Excel cada vez con más frecuencia.

El objetivo es centrarse menos en el sistema operativo que parece más protegido por Microsoft, que ha hecho grandes esfuerzos por convertir a Windows 2000 y Windows XP en el sistema más seguro del mercado, y dedicarse más a otros productos también con una gran base instalada de usuarios como Office, los navegadores web, el visor Flash Player o los reproductores multimedia.

Desde hace no mucho tiempo, se sabe que existe un mercado negro de vulnerabilidades a la venta. Un grupo de hackers descubre un fallo en algún producto o sistema, (normalmente el sistema más rentable es Windows por los más de 800 millones de pcs en el mundo con él instalado) y en vez de decirlo, vende la información.

Necesitamos usar los ordenadores, pero también debemos saber que sufren de fallos de seguridad que los hace vulnerables y que pueden ser objeto de sabotaje. Esta posibilidad no solo existe, sino que cada vez tiene una probabilidad más alta, debido a que:

- Todos usamos los mismos productos en nuestros ordenadores.
- La informática se desarrolla cada vez más aprisa, y priva la tecnología sobre la estabilidad y la madurez de los productos.
- Existen intereses que garantizan que esos problemas nunca sean del todo erradicados.
- Priva la sofisticación, la estética, y las ventas más que la fiabilidad, robustez o seguridad. No se aplica la filosofía de seguridad por diseño.

Para actualizar nuestro ordenador debemos usar los siguientes enlaces web:

- http://windowsupdate.microsoft.com/
- http://officeupdate.microsoft.com

Nota: Recientemente (finales abril 2007) Microsoft ha cambiado la web de actualización a http://update.microsoft.com, y permite actualizar desde aquí, todo el software de Microsoft.

Microsoft Baseline Security Analizer

Esta herramienta de Microsoft que se puede descargar gratuitamente en su web inspecciona nuestro pc de arriba abajo en busca de parches críticos que deberían haber sido aplicados y no están en el sistema, servicios que no son necesarios pero están en marcha, o configuraciones inapropiadas del sistema que deben ser corregidas para mejorar la seguridad. Además es capaz de detectar spyware o malware. En concreto debería emplearse junto a SpyBot por ser complementarios.

Es muy efectivo eliminando spyware que se anexa al Internet Explorer y que a veces no hay forma de eliminar. Con este programa cualquier nueva barra o plugin detectado como spyware será erradicado.

3.4. Más actualizaciones

¿Usa usted habitualmente programas descargados de Internet? Sí claro, todos los hacemos. Ahí fuera existen magníficas aplicaciones para retoque fotográfico, escuchar música, descargar videos, juegos, y mucho más. Pero si desea probar software tenga cuidado, no sea que esté instalando troyanos.

Un troyano es un programa que aparentemente hace una cosa y en realidad hace otra, como enviar todos sus datos personales desde el pc a un ordenador central en Internet, mientras usted retoca las fotos o escucha música.

Asegúrese antes de instalar nada que el programa en cuestión está disponible en una web fiable de descarga de software (suelen indicar si escanean los archivos y si están limpios de virus) o que lo descarga de la web del propio fabricante del software, no de cualquier lugar extraño, o de terceros.

Revise los archivos descargados con un antivirus, y si instala sus programas favoritos, asegúrese de actualizarlos tan pronto existe una nueva versión. Así evitara al menos los fallos de seguridad conocidos. No piense usted que los parches son una idea solo de Microsoft, cada vez más software necesita de updates para evitar bugs. Para más información entre en esta página de PCWorld.

Y si se trata de un programa que no utiliza quítelo de su ordenador, ocupa espacio, y puede ser una fuente de riesgos innecesarios.

3.5. Antivirus

Mucha gente no dispone de antivirus porque se debe pagar un promedio de treinta a treinta y cinco euros semestralmente para mantenerlos al día. Si consideramos el valor del tiempo que podemos necesitar para dejar todo lo que teníamos en su sitio cuando un determinado virus entró en el ordenador y borró nuestros datos o dañó el sistema operativo, es una cifra pequeña económicamente hablando.

Además, actualmente existen varios antivirus gratuitos que probaremos más adelante en el curso y que nada tienen que envidiar respecto a los comerciales.

Sin embargo, tener un antivirus implica que se actualice continuamente y eso supone que tenemos conexión a Internet. Si no es así, deberemos cada cierto tiempo (una semana, un mes) conectarnos a Internet (desde un cibercafé por ejemplo) para bajarnos manualmente la actualización del antivirus y luego ponerla en casa. Existen antivirus que facilitan bastante esta tarea y otros que la complican bastante, ya que los antivirus comerciales de hoy en día están principalmente pensados para actualizarse conectándose ellos mismo directamente a Internet desde casa.

Instalar más de un antivirus en el PC no mejora las cosas. Es cierto que hay antivirus que se actualizan más aprisa que otros; y también los hay más robustos frente a

ataques de virus que intenten quitarlos del PC. Sin embargo la mayoría de los productos disponibles hoy en el mercado son bastante sólidos. Instalar más de un antivirus en el PC, está totalmente desaconsejado porque pueden detectarse mutuamente como virus. ¿Y eso por qué puede pasar? Cada antivirus tiene la "foto" o las características que identifican a cada virus. Si los dos antivirus tienen esa lista de huellas que permite identificar a los virus, puede ser que cada uno identifique al otro, como uno o más virus diferentes.

Así que lejos de hacer bien su tarea, se pueden dedicar a atacarse mutuamente. No es por tanto aconsejable tener más de uno de ellos instalado simultáneamente.

Muchos usuarios se quejan de que su ordenador se ralentiza mucho al instalar un antivirus, y eso es porque no está lo bien configurado que debería. Por ejemplo, supongamos que tenemos un archivo zip de 2500 Mbytes que vamos a almacenar en un DVD y que contiene todo lo que para nosotros es valioso en el ordenador. Se trata pues de un caso sencillo de copia de seguridad. Al marcar el archivo para enviarlo al DVD, y si tenemos activada la protección en tiempo real del antivirus, es decir, que todo aquello que intentemos ver, tocar, o manipular, antes de dejarnos abrirlo, sea escaneado, podemos encontrarnos con que el ordenador se queda muerto durante varios minutos por el enorme tamaño del archivo.

Lo que ha sucedido es que el antivirus está configurado para escanear los archivos zip comprimidos. Como el archivo es tan grande, tarda mucho tiempo.

Lo mismo sucede cuando metemos un disquete en la disquetera, accedemos con el explorer a la misma, y el ordenador se queda un minuto o minuto y medio sin responder. El antivirus está configurado para escanear el disquete tan pronto intentamos acceder a él y hasta que no termina nada podemos hacer.

Otro caso, cada vez menos extendido, es el de las personas a las que la grabación de cds les ha fallado por intentar usar la grabadora con el antivirus activo. Esto pasaba antiguamente con ordenadores menos potentes que los actuales y donde el escaneo de los archivos que se pretendían pasar a un cd, ralentizaba tanto el envío de datos a la grabadora, que se abortaba la copia.

El propio personal informático que trabaja a veces con programas propios de hackers para probar la seguridad de la red, o comprobar la efectividad de los mismos, sufre incidentes con el antivirus, el cual borra sistemáticamente estas herramientas en tiempo real. Usarlas implica por tanto, desactivar el antivirus.

En ocasiones podemos trabajar con el PC y ver como repentinamente caen las prestaciones del mismo. Probablemente se ha iniciado alguna actividad programada de verificación del disco duro (el antivirus revisa todo el disco duro para ver que no ha entrado ningún virus durante un descuido del usuario, o cuando el antivirus no estaba activo).

No solo sufrimos los inconvenientes debidos a la intromisión de estos programas en nuestras tareas con el pc, sino que a veces, no son capaces de defenderlo. Este es el caso cuando el virus que ha atacado nuestro ordenador es reciente y la compañía que

produce las actualizaciones aun no ha preparado una vacuna que el antivirus pueda emplear contra el nuevo virus.

En definitiva, que si queremos convivir con el antivirus y no acabar haciendo como hace mucha gente, que lo desactiva, porque afecta al rendimiento del pc, debemos leernos el manual y tenerlo bien configurado lo cual puede darnos muchos quebraderos al principio.

Existen antivirus gratuitos que funcionan bastante bien como son:

- F-Prot for DOS*: http://www.f-prot.com/download/download_fpdos.html
- Ad-Aware SE Personal: http://www.lavasoftusa.com/
- Antivir Personal Edition Classic 7: http://www.free-av.com/
- avast! Home Edition: http://www.avast.com/eng/avast_4_home.html
- AVG Free: http://free.grisoft.com/doc/1/lng/us/tpl/v5
- ClamWin: http://www.clamwin.com/
- Bit Defender: http://www.bitdefender.com/site/Main/view/Download-Free-Products.html?menu_id=21
- Comodo Antivirus: http://www.antivirus.comodo.com/
- PC Tools Antivirus FreeEdtion: http://www.pctools.com/free-antivirus/

Nota: Cuando decimos que son free, libres, o gratis, en la mayoría de los casos lo son para uso no comercial y personal. A veces solo pueden instalarse en un único pc. Es recomendable leerse las condiciones de uso del producto antes de descargarlo. Algunos son completamente gratuitos y sin restricciones.

Existen también otras opciones para casos de emergencia donde necesitamos verificar que nuestro pc no está infectado o que un determinado archivo está limpio de virus. La segunda opción se da cuando tenemos un ordenador limpio y deseamos introducirle algún programa o ejecutable cuya procedencia no nos garantiza que no esté infectado.

La mayoría de las webs que nos permiten realizar una búsqueda online de virus y troyanos en el pc, lo hacen instalando en memoria software mediante controles ActiveX, por lo que es necesario emplear el Internet Explorer:

- Escaneo de troyanos de Windows Security
- McAfee FreeScan
- Panda ActiveScan
- Symantec Scan
- Trend Micro HouseCall

Otra alternativa son los antivirus gratuitos que no eliminan los virus, pero nos advertirán si estamos infectados por alguno:

- http://www.vintage-solutions.com/English/Antivirus/Super/index.html

También existen antivirus comerciales que dan un mayor soporte como son:

- Panda Antivirus
- Trend Micro
- McAfee Antivirus
- F-Prot
- NOD32
- Zone Alarm Antivirus
- Invircible (sin patrones de virus)
- SOLO Antivirus
- Protector Plus
- Quick Heal Antivirus
- Kaspersky antivirus
- Norman
- Norton Antivirus
- Principal Antivirus
- Sophos

Además, algunas de estas empresas proporcionan una enciclopedia de todos los virus conocidos, sus nombres y sus efectos:

- http://www.f-prot.com/virusinfo/index.html/
- http://www.avira.com/en/threats/
- http://www.avast.com/i_kat_66.php
- http://grisoft.com/doc/62/us/crp/0
- http://www.pandasoftware.com/spain/virus_info/?track=36140
- http://es.trendmicro-europe.com/enterprise/vinfo/encyclopedia.php
- http://www.enciclopediavirus.com
- http://www.f-secure.com/security_center/

Muchos de los antivirus comerciales disponen de versiones de evaluación completamente funcionales durante 15 o 30 días.

Si somos muy paranoicos y deseamos un nivel máximo de seguridad en la detección de antivirus, podemos tener instalado varios, aunque solamente uno debería funcionar en tiempo real. Podemos entonces instalar el Scanner Integrator de Handy Bits que puede escanear el disco duro para localizar virus, empleando todos los antivirus detectados como instalados en el pc.

Es muy importante saber, que distintos antivirus pueden dar nombres distintos al mismo virus o identificaran con otro subnombre a una variante del mismo, por lo que si detectamos un virus concreto en nuestro ordenador o archivos, es buena idea utilizar la enciclopedia propia de la empresa desarrolladora del antivirus.

Lo fundamental es que esté bien configurado, que escanee lo que nos interesa, que lo haga cuando no nos molesta, que se actualice a menudo, que sea cómodo de usar y fácil de configurar y si tenemos dudas, siempre podremos recurrir al servicio técnico.

El antivirus junto al firewall son la primera barrera de defensa que tiene un ordenador. Si está conectado a Internet, la primera barrera externa es el firewall; y la

primera interna, es el antivirus. En caso contrario, lo esencial es el antivirus cuando no hay conexión a Internet.

Hoy en día los antivirus también se han convertido en paquetes completos y aunque se venden por separado, no es raro que le acompañe el firewall, el programa correspondiente anti-spam, algún producto para copias de seguridad, e incluso la capacidad de detectar spyware o malware.

Según el INE, el 88% de la población con ordenador en España y que se conectan a Internet (base poblacional de 16.800.715 personas) dice tener antivirus, aunque solo dos tercios lo actualizan al menos cada tres meses. El 42% dice tener cortafuegos para proteger su conexión a Internet.

En cualquier caso, los antivirus no son ni serán nunca la solución a todos sus problemas, ya que también presentan vulnerabilidades o fallos de seguridad. Si desea saber más lea este reciente artículo.

Nota: Microsoft incorporará a Windows Vista un nuevo servicio denominado Windows Live OneCare, disponible inicialmente en Estados Unidos que ofrecerá protección antivirus adaptada a las necesidades de empresas y usuarios, apoyándose para ello en soluciones desarrolladas por socios y terceros, y compitiendo así con empresas dedicadas a la seguridad y protección de los pcs.

3.6. Firewalls

Un firewall es una aplicación que detecta los intentos por parte de los programas instalados en nuestro ordenador de conectar con máquinas de Internet, lo que le permite evitar que nuestros datos sean enviados por spyware o malware a hackers, spammers y otros cyberdelincuentes. A este férreo control que nuestro firewall ejerce sobre todo el tráfico de salida, mejor conocido como tráfico saliente se le une una estricta barrera de paso que limita el acceso que cualquier programa externo (que viene desde Internet) obtiene para llegar a nuestro pc. Es decir evita la mayor parte del tráfico entrante.

En definitiva, un firewall aísla nuestro pc, evitando que las aplicaciones que lleva instaladas, algunas de las cuales pueden ser maliciosas envíen información hacia afuera y del mismo modo evita conexiones o intentos ilegales de acceso desde fuera.

Aparentemente la idea es magnífica, pero no queremos prohibir todo el tráfico de entrada, ni tampoco todo el de salida. Si prohibimos todo el tráfico de entrada, no podremos ver las páginas web que queremos visitar, ni recibir emails, ni descargar música, videos, etcétera. Del mismo modo, si no permitimos tráfico de salida, no podremos enviar emails, ni permitiremos que determinadas aplicaciones envíen información a amigos o compañeros.

Es pues necesario configurarlo poco a poco para que no sea tan hermético y permita lo suficiente para que podamos llevar a cabo nuestras actividades diarias, pero no cualquier otra indebida o fraudulenta. Durante este proceso de aprendizaje mutuo (nuestro y del firewall), ambos aprenderemos como funcionar mejor, y aunque al

principio puede ser complicado o difícil entender algunos aspectos, cada vez es más necesario. Del mismo modo, prácticas tan habituales como usar programas P2P, como emule o Kazza, y compartir archivos en la red de casa, pueden verse afectados por no configurar el firewall adecuadamente.

Tanto Windows como Linux llevan uno. Los antivirus suelen ir acompañados de un firewall, pero como solo se recomienda tener uno activo a la vez, tendremos que elegir cual cumple mejor nuestras expectativas. En cualquier caso, con la era de los firewall, los ordenadores, a cambio de protegerse, han complicado la vida a los usuarios, pues son muchas las veces que las comunicaciones con el exterior no funcionan y el usuario medio desconoce la causa, llegando a veces a la más absoluta desesperación.

Ejemplos de firewalls gratuitos* no integrados en suites de seguridad o paquetes antivirus serían:

- ZoneAlarm.
- Sunbelt –Kerio Firewall.
- Omniquad Firewall.
- Comodo Firewall.
- Premidius Firewall.
- R-Firewall.
- SensiveGuard Firewall.

Nota: Por gratuitos se entiende normalmente, que lo son para uso no comercial y de instalación en el hogar. De todas formas, siempre es conveniente antes de descargar el producto, leerse las condiciones de uso que constan en la licencia.

3.7. Anti-spyware

El spyware o malware no sabemos muchas veces como ha llegado a nuestro pc. ¿Fue al instalar determinado software? ¿O fue cuando hice clic por error en aquella página web? ¿Entró debido a una vulnerabilidad o fallo de seguridad del navegador?

Poco importa. En ocasiones por mucho interés que pongamos no sabemos como ha llegado hasta nuestro pc, pero lo cierto es que puede ralentizarlo, enviar información privada sobre nosotros o aun peor, actuar de manera malintencionada robándonos datos o haciéndonos aparecer culpables de ataques contra otros servicios en Internet.

De una forma o de otra, nosotros no deseábamos que se pegara a nuestro pc de esa manera y ahora queremos borrarlo. Hablamos de pequeños programas que muchas veces no encontramos la forma de desinstalarlos por más que lo intentemos. Algunos son capaces incluso de reinstalarse si intentamos borrarlos de forma abrupta. Utilizan técnicas cercanas a los virus para que no podamos quitarlos del sistema, o peor aun, sustituyen componentes del navegador o los modifican para que no podamos deshacernos de su presencia.

A tal punto ha llegado el asunto que se ha hecho necesario la utilización de programas expertos en detectarlos y erradicarlos. Se han convertido en pequeños virus,

no necesariamente malignos o dañinos en sí mismos, pero siempre molestos y violando nuestra privacidad. Es por esto que muchos antivirus incorporan ahora un detector de spyware propio, como ha pasado con el firewall.

Es por tanto aconsejable que el pc pase un chequeo de vez en cuando para detectar estos programas y eliminarlos. Programas que realizan este tipo de tareas y son gratuitos serían:

- SpyBot
- Microsoft BaseLine Security Analizer
- Ad-aware

El nuevo sistema operativo de Microsoft, Windows Vista, dispone de una herramienta, Windows Defender, encargada de la eliminación del spyware, aunque según ciertos estudios, no parece muy eficaz. Otros artículos hablan incluso de que Microsoft estaría interesada en comprar alguna de las empresas productoras de adware, amenazas que en teoría combate su Windows Defender.

En cualquier caso, y al contrario que con los antivirus, que solo debemos instalar uno; con las herramientas anti-spyware y aunque tengamos alguno residente, nunca está de más disponer de otros adicionales para verificar el disco duro. No todos los programas anti-spyware detectaran todas las amenazas. Algunas incluso solo serán detectadas por un buen antivirus. Y también aquí existen quejas sobre la calidad de algunos de esos productos spyware, como es el caso de Ad-Aware.

Si queremos más información podemos visitar esta página o esta otra.

Si queremos evitar que al acceder a páginas web el navegador descargue enlaces de publicidad, páginas reconocidas como peligrosas, descargue spyware o falsos cuadros de diálogo que acabaran por instalarnos en el pc molestos banners, podemos lograr que todos esos enlaces que no son principales al contenido o la información que estamos buscando no sean descargados. Para ello basta con hacerle creer al navegador que los servidores de donde debe descargárselos son nuestro propio ordenador, que como naturalmente no dispone de ellos, dará como resultado que no sean encontrados.

La forma de hacerlo se basa en el funcionamiento de los DNS y la manipulación del archivos HOSTS de nuestro ordenador. Podemos descargar algunos de estos archivos y leer más sobre como funciona en:

- http://www.mvps.org/winhelp2002/hosts.htm
- http://www.everythingisnt.com/hosts.html
- http://pgl.yoyo.org/adservers/

3.8. Filtros contra el spam

Si utiliza habitualmente el Outlook Express, y todavía no dispone de Windows Vista con la nueva versión de Windows Mail, sabrá usted que las reglas de filtrado de spam del Outlook Express son muy básicas y pobres y con una capacidad de autoaprendizaje nula (Esa es la razón por la que mucha gente se ha pasado a Thunderbird).

Outlook Express fue creado por Microsoft hace ya bastantes años y se echan en falta habilidades como la capacidad de enfrentarse al phishing o el filtrado automático del spam (correo basura) mediante autoaprendizaje y una mayor potencia en las reglas personalizables de filtrado.

Teniendo en cuenta que sobre un 80% de los correos recibidos diariamente son spam y que cuando nos vamos de vacaciones hemos de vaciar nuestras cuentas varias veces para que no resulte llena ante la barbaridad de spam recibido, creo que podemos decir que el spam es un problema serio, que puede incluso conducir a una denegación de servicio cuando personas interesadas en contactar con nosotros no pueden hacerlo porque nuestras cuentas de correo están llenas o simplemente porque borramos sus mensajes confundiéndolos con spam.

La consecuencia final es tiempo y dinero perdido, menor rendimiento, posibilidad de no recibir correo importante o peor aún, el riesgo de caer en el phishing o abrir correos infectados por virus. Algunos spammers (o personas que envían el spam) comprueban si abrimos sus correos para volver a bombardearnos con más emails basura, al verificar que nuestra cuenta de email está activa, es decir, es utilizada.

Por muy cuidadosos que seamos frente al spam, antes o después, un compañero, amigo o conocido introduce nuestra dirección de email en una lista de distribución haciendo fácil que los spammers la detecten y nuestra cuenta sea bombardeada con spam.

En About.com, podemos ver una lista de programas que combaten con eficacia el spam (http://email.about.com/cs/winspamreviews/tp/anti-spam.htm) y también, de otra lista (http://email.about.com/cs/winspamreviews/tp/free_spam.htm) con los mejores programas anti-spam gratuitos del mercado.

Los más interesantes por sencillez o facilidad de uso (para mí) son:

- Spamihilator
- Mailwasher

3.9. Puntos de Recuperación/Restauración

Los puntos de restauración de Windows, son copias de seguridad que el sistema operativo realiza cuando detecta cualquier modificación que puede afectar a la estabilidad del sistema. Se trata de la opción "Undo"(deshacer) del procesador de textos aplicada al sistema operativo. Esta opción le permitirá deshacer las últimas modificaciones que dejaron a su pc en un estado inservible o incapaz de arrancar.

Los puntos de restauración podemos crearlos manualmente, y también podemos desactivarlos si no deseamos emplearlos. Windows también los utiliza y genera de manera automática cuando se producen determinados sucesos en el sistema como son:

- Al instalar una nueva aplicación si la misma es compatible con la API de restauración del sistema.
- Al instalar un nuevo parche o actualización de Microsoft.
- Al restaurar el sistema, se crea un punto previo de restauración que permitirá deshacer más tarde la restauración.
- Antes de restaurar una copia de seguridad o un driver que no esté firmado.
- Al deshabilitar la creación de puntos de restauración y volverlos a activar.
- Cada cierto tiempo.

Podemos crear distintos puntos de seguridad, que quedaran almacenados en el disco duro y nos permitirán dejar el sistema operativo en su estado original en determinada fecha (siempre y cuando exista un punto de restauración realizado ese día).

Al restaurar el sistema mediante un punto de restauración siempre es posible deshacer la restauración. Los puntos de restauración se aplican al sistema operativo y no a los datos o documentos que podamos haber borrado o perdido. De hecho, almacenan información sobre el registro, ficheros protegidos por el sistema, configuración de IIS, perfiles locales, la base de datos COM+, etcétera.

Y es aconsejable borrar los más antiguos cada cierto tiempo, pues ocupan espacio innecesariamente en el disco duro. Si queremos saber un poco más sobre como se comportan podemos visitar esta página.

3.10. Defragmentar el disco duro.

El hecho de emplear el disco duro para almacenar información en él, hace que cada vez esté más desordenado, conforme vamos borrando y añadiendo nuevos archivos. Piense usted en una estantería de su casa donde tira un libro que ya no necesita y deja un hueco, luego tira otro y deja otro hueco. Si más adelante compra dos nuevos libros rellenará ambos huecos con ellos. Pero, ¿qué pasa si solo compra usted uno muy grueso? Necesitará tener ambos huecos juntos para introducir el nuevo libro, con lo cual, probablemente desplace los libros para dejar los dos huecos juntos. Eso lo hacemos porque se trata de un objeto físico indivisible, pero lo que almacenamos en el disco duro es información virtual, es decir, nosotros vemos el documento como un archivo unificado, pero el ordenador lo puede haber partido en dos para llenar los dos huecos que había libres. Solo él sabe que el documento está repartido por el disco duro

en trozos. Cuando nosotros lo requerimos busca cada trozo, los une y nos presenta el documento entero.

Esto, que aparentemente no tiene importancia, y que es más una cuestión del sistema operativo que nuestra, supone recuperar cada parte del documento de una ubicación distinta antes de que podamos visualizarlo. Naturalmente el citado concepto se aplica también a juegos, imágenes, fotos, videos, música y programas. Buscar cada trozo para luego unirlos ralentiza al ordenador. Y con el tiempo puede convertirse en algo insostenible sobretodo cuando el disco duro se va llenando, los archivos son muy grandes y hay ya muchos trozos.

El problema es más grave cuando empleamos el sistema de archivos FAT32 que el de NTFS. Normalmente se emplea NTFS en los sistemas basados en Windows 2000, XP y Vista, donde los discos superan los 32 GB.

Otros sistemas operativos emplean formas distintas de almacenar los archivos, como sería el caso de Linux donde la estructura de archivos empleada es ext3 o Extensión 3.

Defragmentar el disco duro, es una tarea que suele hacerse partición a partición. Si solo tenemos unidad C en nuestro ordenador, lo aplicaremos a la unidad C. Si tenemos el disco duro dividido en unidad C y D, deberemos aplicar esta tarea a C y D por separado. Aunque D, por ser la partición de datos será la que más se fragmente. Si el ordenador dispone de una unidad lectora / grabadora de cds o dvds, aquí no se podrán reestructurar los datos ni aplicar una defragmentación. Primero, porque muchos cds y dvds no son regrabables; y segundo, porque antes de almacenar datos en estos medios, ya se han defragmentado y cada archivo se ha guardado entero consecutivo al anterior.

Defragmentar es un proceso que consiste básicamente en buscar todos los trozos de un archivo, hacerle hueco y ponerlos juntos. Esta tarea que se realiza archivo por archivo, debe hacerse cada cierto tiempo y es necesario que al menos nunca llenemos sobre un 10 o 20% del disco duro, porque en caso contrario, el sistema operativo no dispondrá de espacio temporal para almacenar lo que va moviendo.

El defragmentado solo puede hacerse si previamente el sistema de archivos no encuentra errores en el sistema de archivos, es decir, si la tabla índice que le dice al sistema operativo en qué parte del disco se almacena un archivo y qué longitud tiene, no está dañada.

Al proceso de revisar la estructura de archivos y ver que es correcta se la llama verificar o vulgarmente, “chequear” el disco. De nuevo aquí se aplica el concepto de hacerlo partición a partición.

3.11. Llevar el equipo al Servicio Técnico (S.A.T.)

Supongamos que usted no sabe nada de informática. Pero percibe que el ordenador no va como antes, no ha hecho nada por revisarlo en los últimos meses a pesar de que el pc produce de vez en cuando mensajes de error en pantalla que usted no entiende. No sabe / no quiere / no tiene tiempo / o no desea aprender a hacer copias de seguridad.

Ni siquiera conserva la caja donde vino el pc cuando lo compró y desde luego no recuerda donde están los drivers del ordenador ni el manual ni demás cosas que venían con el equipo.

Sin embargo, el pc todavía funciona aunque a veces se cuelga y tiene que resetearlo. Ya no se apaga cuando le da usted la orden desde el sistema operativo y tiene que apagarlo usando el botón que hay para ello.

El otro día el ordenador se reseteó y usted sabe que si se estropea, ya tiene dos años y la garantía no lo cubre más. En definitiva, que el pc necesita que lo revisen.

Suele usted llevar el coche para que le hagan la revisión Pre-ITV o lo lleva a revisar antes de irse de vacaciones. Le verifican entonces los niveles de aceite, las ruedas, las luces, los frenos, y demás.

¿Y por qué no lleva su pc al servicio técnico para que lo revisen? Ellos pueden hacerle la copia de seguridad que usted no sabe hacer. Ellos pueden reinstalar el pc si es necesario. Pueden decirle si el pc funcionaría mejor con algo más de memoria, mejor refrigeración, más espacio, decirle si está infectado con virus o limpiarlo. ¿Cuanto puede costarle? Tiene usted coche y paga un precio elevado por su seguro anualmente, también paga la ADSL, ¿acaso su ordenador no merece una revisión anual?

Recuerde que un ordenador necesita un mantenimiento y ante usted pueden hacerle tareas tan variadas como:

- Limpiarle el polvo por dentro para que no frene/estropee los ventiladores.
- Mejorar su refrigeración con pasta térmica, o poniendo un disipador más grande.
- Comprobar el sistema de archivos.
- Escanear el disco duro en busca de virus, spyware o malware.
- Defragmentar los discos para mejorar el rendimiento.
- Crearle una copia de seguridad
- Reorganizar sus videos y fotos.
- Ampliar la capacidad cambiando algún componente.

Un ordenador no debe “utilizarse mientras funcione” hasta que deja de funcionar. Debemos darle el mantenimiento que merece o dejará de servirnos. Si usted no sabe o no quiere hacerlo busque un Servicio Técnico que lo haga.

Notas

[Tarjetas de crédito]. Utilice tarjetas de crédito para las compras en Internet. En los Estados Unidos, la ley limita su responsabilidad si alguien captura su número de tarjeta de crédito y lo utiliza ilegalmente. Sin embargo, la ley no protege de la misma manera a las tarjetas de débito. Aunque le parezca que su tarjeta de débito funciona como una de crédito, utilice una tarjeta de crédito. Verifique con la compañía de tarjeta de crédito, el banco o la empresa en línea para obtener más información sobre su protección.

[qwerty] . El teclado qwerty fue creado cuando se pretendía dificultar la velocidad a la que las personas tecleaban en las máquinas de escribir antiguas, donde dos teclas presionadas en un intervalo de tiempo demasiado corto podían quedar enganchadas la una con la otra. Actualmente se emplea por estar su uso muy extendido, pero lo cierto es que no es la mejor (más rápida) ni más cómoda distribución del teclado para escribir.

Capítulo 4. Técnicas para minimizar los riesgos

4.1. Introducción

En el capítulo anterior, comentábamos lo que debía hacer para reducir el número de padecimientos propios y los de su ordenador. Y aunque él no pueda darle las gracias, usted se ahorrará quebraderos de cabeza si los sigue.

Pero ¿qué sucede si usted los sigue al pie de la letra y aun así sigue siendo atacado y entran en su ordenador? Ya hablamos del riesgo de que alguien descubra una vulnerabilidad en su pc para la que el fabricante/desarrollador de software aun no tenga solución.

Frente a esto, solo podemos procurar el empleo de software en nuestros ordenadores que no esté en el punto de mira de los hackers. Ya dijimos que los hackers, virus y programas maliciosos (spyware y malware) centran su mirada en los productos más difundidos, porque pueden extender su control más aprisa, y en mayor número que en los otros casos, lo cual los hace también más rentables.

Por eso es recomendable dejar de usar lo que la mayoría utiliza. Forme usted parte de la minoría, y desde luego, nunca se limite a una solución.

¿Es cliente habitual de Internet Explorer? Pásese a Firefox 2.0.1. ¿Esta semana ha surgido un nuevo agujero de seguridad en Firefox 2.0.1? No importa, no lo use, utilice de momento el navegador web Opera y espere a que resuelvan el fallo en Firefox.

Usted podría responderme que no puede dedicar tiempo a enterarse de si Firefox tiene un nuevo fallo de seguridad que ha aparecido esta semana. Y le digo sinceramente que tiene razón. Pero en igualdad de condiciones y aunque siga empleando el Firefox con fallo incluido, sigue teniendo menos posibilidades de ser infectado que si usa Internet Explorer, simplemente es una cuestión de estadísticas.

Lo mismo puede aplicarse a los top ten del mercado de software en otras ramas. No hace falta ser muy listo para suponer que entre los programas más utilizados en el mercado mundial de los computadores están:

- Internet Explorer
- Word
- Excel
- Windows
- Outlook Express

Y para todos ellos existen equivalentes, menos conocidos, menos empleados y por tanto menos atacados. Simplemente empleamos éstos porque en muchos casos venían con Windows sin necesidad de instalar nada.

4.2. El uso de un navegador alternativo

Si maneja usted perfectamente Internet Explorer, y sigue usted en la versión 6 o anteriores, no le costará nada pasarse a Firefox u Opera. En cualquier caso, son muchas las ventajas de usar navegadores que integran plug-ins. IE 7 los tiene, pero su número, como en el caso de Opera, no puede rivalizar ni de lejos con los de Firefox.

Firefox tiene miles de plug-ins o complementos para facilitarle el acceso a Internet, apartar el exceso de publicidad que le atosiga, y reducir el ancho de banda consumido, muchas veces en anuncios, ventanas emergentes y demás links que no le aportan nada.

Usar un navegador alternativo, no significa que haya uno mejor que otro. Todos tienen ventajas y desventajas. Y todavía existen muchos sitios web en Internet, incluso webs oficiales (Administraciones Públicas) que no funcionaran correctamente si usted emplea otro navegador que no sea el Internet Explorer. En ese caso, no tendrá más remedio que emplearlo si la información le interesa. Pero serán casos puntuales.

Muchos de los más peligrosos agujeros de seguridad de IE son propios de tecnologías creadas por Microsoft, como ActiveX, y no existen en Opera o Firefox. En ocasiones, un exceso de funcionalidad, que a lo mejor no necesitamos, puede colocarnos en situaciones de riesgo que programas ajenos a nuestro pc pueden aprovechar para entrar en él, robarnos información o inutilizar el sistema operativo.

Utilizar productos independientes o de competidores les obliga a todos ellos a innovar constantemente, lo que es bueno para nosotros, los usuarios.

Si es usted usuario del Internet Explorer 7 pronto verá como su vida se convierte en un infierno. Intentará acceder a páginas donde ha entrada toda la vida y no podrá si no certifica esos sitios webs como seguros o de confianza. Si intenta descargar archivos de sitios que el navegador no los reconoce como “de confianza” tendrá problemas. Pruebe a entrar en el sitio de Office Update con su IE 7 configurado por defecto, y verá usted como no lo consigue. Ya no existe una opción de “Seguridad Baja”, solo dispone de “Seguridad Alta” o “Personalizable”. Busque entre todas las opciones de seguridad de IE 7, e intente averiguar qué debe cambiar para que le permitan entrar en la citada página. Verá que no es nada fácil y Microsoft debió comprobarlo, porque a los pocos días del lanzamiento del IE 7, modificó su página de update para Office, y de nuevo, los usuarios vimos la luz al final del túnel.

Microsoft cree que la política de “Prohibir Todo por defecto” es la más adecuada, lo malo es que se ha llegado a tal punto de paranoia, que un usuario desesperado acabará desactivándola completamente para evitar volverse loco.

Conocer productos alternativos no solo significa mayor protección, sino la posibilidad de cambiar de producto si las condiciones, el precio, las prestaciones y/o limitaciones del que usa actualmente han dejarlo de interesarle.

Nota: Es conocido que el talón de aquiles de Firefox es la ejecución de código Javascript, que bajo determinadas condiciones puede producir agujeros en el sistema,

pero puede evitarlo desactivándolo permanentemente, o haciéndolo de forma más coherente mediante plugins como NoScript.

4.3. El uso de un lector de correo alternativo

Outlook Express es conocido por sus múltiples agujeros de seguridad en el pasado. Las vulnerabilidades más graves provenían de los archivos adjuntos que el usuario ejecutaba a veces pensando en que nada malo había de suceder. Posteriores vulnerabilidades hicieron que los virus pudieran ejecutarse desde scripts anexos al mensaje y donde ni siquiera era necesario visualizarlo para que el virus infectara el sistema.

Los virus aprovecharon las capacidades extra añadidas por Microsoft y que ningún otro lector de correo electrónico del mercado tenía para realizar acciones como leer la agenda de correo, auto reenviarse y propagarse así a través de amigos y conocidos.

Pronto miles de variantes aprovecharon otros pequeños agujeros de seguridad para multiplicar su capacidad de infección y los mecanismos de propagación.

Este fue un caso claro, donde las prestaciones alcanzadas mediante mejoras no compensaron los riesgos añadidos.

Además Microsoft hizo poco o muy poco por mejorar las prestaciones de su lector de correo frente a nuevas amenazas como el spam.

Actualmente existen muchos sustitutos al Outlook y al Outlook Express en el mercado, tanto gratuitos como comerciales.

4.4. El uso de un sistema operativo alternativo.

Desde los tiempos de Windows 3.1, Microsoft domina el mercado de los pcs y compatibles. Actualmente se ha extendido a móviles (Windows Mobile), PDAs, sistemas de entretenimiento de salón y otros dispositivos. A Windows 3.0, le siguieron Windows 3.1, Windows 3.11, Windows NT 3.5, Windows NT (4.0), Windows 98, Windows Millenium, Windows 2000, Windows XP y Windows 2003.

El sistema operativo Windows XP tiene sus días contados y la fecha marcada como final en su mantenimiento es el 19 de abril del 2009. Su sucesor, es Windows Vista, disponible en el mercado desde enero del 2007.

La mayoría de los usuarios utiliza un sistema operativo propietario de Microsoft, ya que normalmente al comprar un ordenador, también compramos una licencia de software, lo que nos permite adquirir el pc e instalarle un sistema operativo de manera legal.

Sin embargo, en los últimos tiempos han surgido con fuerza otras alternativas a Windows, principalmente Linux en todas sus variantes o clones, algunas de estas versiones, pensadas especialmente para los usuarios con menos conocimientos.

Del mismo modo que en Windows hablamos de versiones, en Linux hablamos de distribuciones. Todas las distribuciones disponen de unos elementos básicos comunes, lo único que las diferencia es la amplitud de herramientas que contienen y a qué sector va orientada la misma (utilidad y facilidad de uso).

En http://es.wikipedia.org/wiki/Categor%C3%ADa:Distribuciones_Linux, podemos ver una lista de la mayor parte de ellas. También en http://es.wikipedia.org/wiki/Distribuci%C3%B3n_Linux podemos ver una lista de distribuciones comerciales y no comerciales (gratuitas), número de paquetes (software: utilidades y aplicaciones) que integra, etcétera.

Una queja muy común de los nuevos usuarios de Linux o que quieren migrar a Linux, es que no saben cuales son los programas que deben emplear para hacer lo mismo que hacían en Windows. Eso pueden encontrarlo aquí.

Otra queja es que les gustaría darse primero un tiempo para probar Linux antes de quitar Windows de su ordenador definitivamente. Existen versiones de linux que se pueden poner en marcha desde un CD o DVD, así conservamos Windows en el disco duro y Linux en el CD. Linux no modificará el disco duro y conservaremos lo que teníamos hasta que estemos decididos.

Pero hay tantas versiones de Linux (distribuciones) que decidirnos se hace difícil. Es entonces cuando debemos visitar primero webs como DistroWatch para decidirnos por una y ver lo que opinan otras personas sobre la facilidad de uso que proporcionan y la orientación de la misma. Si queremos asegurarnos que sea una distribución conocida, con buen soporte porque tiene una comunidad de usuarios muy extendida, podemos pulsar en el enlace “Distribuciones Principales”, o si queremos ver qué aspecto tienen visitaremos la web de OsDir.

Todavía existen personas que piensan que Linux no dispone de entorno gráfico, o que no es tan potente como el de Windows. Podemos verificar que eso no es cierto en los enlaces anteriores.

4.5. El procesador de textos alternativo.

El Word no es el único procesador de textos. Y Office no es la única suite ofimática, existen por un precio mucho menor (a veces son gratuitos) otras opciones que pueden ofrecernos lo mismo o algo equivalente. No se trata de obtener microprogramas capaces de hacer de todo, sino de ver que usamos en realidad del Office de Microsoft para poder buscar productos alternativos. Normalmente solemos emplear un subconjunto pequeño de toda la funcionalidad que el paquete ofimático ofrece.

Si pensamos en paquetes ofimáticos gratuitos, tenemos el OpenOffice y el EasyOffice. Sun Microsystems, principal contribuyente al proyecto OpenOffice, ofrece

una versión comercial, denominada Sun StarOffice 8, pero incorporando nuevas características como thesaurus, imágenes prediseñadas (cliparts) y soporte técnico. Cada licencia oscila entre los 32 y los 80 euros. Se incluye un procesador de textos, una hoja de cálculo, un programa de dibujo, otro de presentaciones, y otro para gestionar bases de datos. El OpenOffice también se distribuye en una versión portable para llevar en lápiz USB que puede descargarse aquí.

De pago, aunque muy económico tenemos también la Office 602, un producto que integra procesador de textos y hoja de cálculo compatibles con los de Microsoft. Incluye distintos precios en función del número de licencias, pero para empresas grandes dispone también del cobro de una cantidad fija independiente del número de usuarios.

Y de precio más elevado, aunque inferior a la Office de Microsoft tenemos la office de Corel, la denominada Corel Wordperfect MX3 (sobre 370 € por licencia) y la de IBM, Lotus SmartSuite (sobre 340 € por licencia).

Otra suite de aparición reciente es la de Gobe, la cual consta de procesador de textos, hoja de cálculo, presentaciones y editor de imágenes. Por ahora está disponible solamente en Windows por 50 dólaresa y existe una versión trial para probarla durante treinta días.

Podemos comparar los precios de algunos de ellos y los programas incluidos aquí. Y podemos leer más sobre estos productos en la página de CNET Reviews.

En linux, existen también KOffice y Gnome Office, ambas son suites gratuitas.

O podemos incluso emplear offices que no requieren que los instalemos, ni ocupan espacio en nuestro disco duro. Es el caso de offices gratuitas disponibles vía web en Internet como Ajax13 o Google Docs (aunque la privacidad aquí no está al 100% garantizada).

4.6. La organización de los datos en el disco duro.

No deberíamos comprar un pc, instalarle el sistema operativo y comenzar a escribir documentos, almacenar películas, vídeos, música, fotos, etcétera. Deberíamos pensar en conceptos como:

1. Qué vamos a almacenar, tipo de contenido.
2. Que espacio puede llegar a ocupar.
3. Cual va a ser la distribución de los datos en el disco.
4. Quienes van a poder acceder a ellos.

Deberíamos dividir al menos el disco duro en dos mitades, una para el sistema operativo y las aplicaciones que pensemos instalar y otra para los datos, archivos, documentos, etcétera. Al hecho de dividir el disco duro en dos partes, se le conoce como particionar el disco. Si decidimos separar el sistema de los datos, nos harán falta al menos dos particiones.

Supongamos que instalamos varios programas en el ordenador y el día que decidimos desinstalarlos algo falla, los archivos que no llegaron a quitarse del disco seguirán ahí para el resto de la vida del ordenador. Podemos borrar el directorio donde instalamos el programa, pero no sabemos los drivers o librerías que añadió al sistema operativo ni los cambios que hizo en el registro de Windows. También puede darse el caso de que un virus dañe el sistema operativo, o que deseemos probar una aplicación nueva pero nos de miedo que afecte negativamente a otras que poseemos, ¿qué hacer?

Si tenemos una copia o "foto" del estado del sistema operativo previa a lo que pretendemos hacer, siempre podremos volver a ese estado anterior. Bastará con restaurar el sistema operativo, y no tendremos que pensar en si se pierden los datos porque los tenemos en otra partición.

Del mismo modo, recuperar los datos no afectará al sistema operativo. Y si los tenemos bien organizados podemos fácilmente realizar búsquedas, copiarlos a otro dispositivo extraíble y llevárnoslos a otro ordenador.

También podemos aplicar sistemas de copia de seguridad diferentes, más específicos y más eficientes al sistema y los datos al considerarlos lo que son, tipos de datos distintos. Cualquier empresa de reparación de pcs, puede reinstalarle el sistema operativo, pero nadie puede recuperar sus documentos si los ha perdido, o al menos no garantizarlo. Incluso borrados, existen bastantes más posibilidades de recuperar los datos si los tenía en otra partición distinta a la del sistema operativo.

Existen herramientas pensadas para ayudarnos a averiguar donde los almacenamos, lo que ocupan, etcétera, con el fin de que podamos organizarlos. Del mismo modo, existen utilidades capaces de reparticionar el disco para crear nuevas particiones donde no las había reduciendo el tamaño de otras, por lo que ni siquiera es necesario borrar el disco, ni tiene porqué resultar una experiencia dramática.

Del mismo modo que separamos datos y sistema, es necesario comprobar la coherencia del sistema de archivos que los almacena cada cierto tiempo. A esto se le conoce como comprobar la coherencia de la estructura del sistema de archivos.

4.7. Las Copias de seguridad.

En la actualidad, los discos duros de los ordenadores son capaces de almacenar (ordenadores normales de trabajo o del hogar) de 200 a 300 Gbytes de datos. Mucha gente llena el disco duro de películas, vídeos, música, enciclopedias, fotos, etcétera.

Este tipo de información no es la que se entiende para hacer una copia de seguridad o backup cada cierto tiempo. Si quisiéramos hacer de una sola vez una copia de seguridad de todo esto mensualmente, tendríamos que usar un medio de almacenamiento profesional, que sería bastante caro, y dedicaríamos un día íntegro para que el ordenador hiciera una copia de seguridad completa, que pudiéramos sacar de casa y almacenar en algún lugar seguro.

Pero eso era antes. En estos tiempos, podemos montar un disco duro extraíble al mismo pc, y hacer una copia completa de todo lo que contiene el que está dentro del ordenador. Incluso podemos hacer una semanal y tener cuatro discos duros para almacenar cuatro copias de seguridad en el mes.

Aunque esto es posible, normalmente las películas queremos verlas y borrarlas; o si nos gustan, las acabamos pasando a un CD o DVD para guardarlas. Lo mismo sucede con la música, las colecciones de fotos y todas aquellas cosas que una vez vistas o creadas nos interesan y las salvaguardamos de manera individual.

Siguen en el disco por lo cómodo que es acceder a esta información rápidamente, pero ya no es necesario preservar copias, porque en su momento ya las hicimos. Normalmente, los datos críticos, aquellos que afectan a nuestro trabajo, hobbies, o intereses reales, caben o pueden caber perfectamente en un máximo de dos dvds.

No olvidemos que la información, cuando realizamos una copia de seguridad, reduce su tamaño a la mitad. Es decir, que en un DVD, por ejemplo no caben 4,5 Gigabytes, sino que perfectamente entran 9 o 10 Gb si se incluyen documentos o trabajos que por ser de texto básicamente, al comprimirse, reducen hasta en 10 a 1 el espacio original que ocupaban.

Cuando hablamos de copias de seguridad no solo hablamos de proteger nuestros datos, sino en definir los pasos que tenemos que dar para recuperar después de un desastre, es decir, la capacidad para volver a dejar el sistema en su estado anterior al problema que destruyó los datos en el menor tiempo posible y con la fiabilidad adecuada.

La única amenaza para que las copias de seguridad no estén disponibles cuando sean necesarias, somos nosotros mismos, ya que hacer una copia de seguridad suele considerarse como perder tiempo, tiempo que a veces consideramos que es mejor emplear en otras cosas. Al final, las copias de seguridad se distancian en el tiempo, y llega un día en que cuando las necesitamos de verdad, la última copia de seguridad disponible dista mucho de reunir toda la información que hemos perdido.

Realizar copias de seguridad entraña riesgos y también ventajas. Por ejemplo es importante tener copias de seguridad, pero ¿qué pasa si nos las roban? Esto ya deja ver dos cuestiones con claridad. La primera es que las copias de seguridad deberían estar cifradas. Eso quiere decir que si los datos del ordenador se pierden y mientras estemos recuperándolos de la última copia de seguridad, no podremos acceder a ellos mientras el proceso no esté finalizado. La segunda cuestión a tener en cuenta, es que todas las copias de seguridad no deben almacenarse en el mismo sitio, ni en la misma casa.

Si tenemos cien cds o dvds de copias de seguridad de los últimos cinco años y solo queremos la información de los dos últimos, podemos tirarlos, pero primero será necesario destruirlos, rayándolos, perforándolos, quemándolos y estropeándolos a base de “freírlos” durante cinco minutos en un microondas.

Hacer una copia de seguridad o establecer una política de copias de seguridad, es decir, cuando se harán las copias, de qué cosas, con qué frecuencia, etcétera, supone una

tarea previa bastante ardua si nunca lo hemos hecho antes: Es necesario unificar, reunir, compactar todos nuestros documentos y archivos valiosos en unas pocas ubicaciones desde las que haremos la copia de seguridad.

Las verdaderas copias de seguridad deberían ir identificadas de forma que solo nosotros pudiéramos saber lo que contienen. Lo correcto es identificar una copia de seguridad como sigue: “Datos del PC de casa a fecha 21/03/2005 DVD 1/3”. Sin embargo, si alguien captura el DVD o todos mis dvds sabrá cual es la última copia de seguridad, de cuantos dvds consta, etcétera. Si lo etiqueto así: Datos 121.35, no será tan fácilmente identificable.

De vez en cuando es necesario intentar recuperar correctamente la última copia de seguridad para verificar que sabemos hacerlo, que podemos hacerlo en un tiempo razonable y que el proceso funciona sin fallos inesperados.

Aunque parece trivial, no debemos utilizar medios que no sepamos que son fiables. Por ejemplo, si tenemos un disco duro que no usamos porque renquea, no lo usaremos para la copia de seguridad. Tampoco emplearemos cintas gastadas una o mil veces, cds vírgenes baratos o sin marca, y ningún otro medio de baja fiabilidad.

Existen personas que gustan de hace copias de seguridad completas cada cierto tiempo, lo cual les garantiza que cada copia de seguridad contiene todos los datos que emplean a diario. Otras personas realizan una de estas copias mensualmente y luego utilizan copias diferenciales o incrementales.

Existen distintos tipos de copias de seguridad:

- La completa, donde se hace una copia de todos los archivos que deseamos respaldar, proteger o conservar.
- La diaria, donde se guardan los archivos que han sido modificados en el día de hoy. El bit de archivo no se resetea.
- Incremental, formada por los ficheros que han cambiado desde la última copia completa o la incremental anterior. Se salvaguardan los archivos con el bit de archivo activo que luego es reseteado. Naturalmente si el archivo vuelve a cambiar el bit se activará de nuevo.
- Diferencial, contiene los archivos que se han modificado desde la última copia completa. Sin embargo cuando se salvaguardan los archivos con el bit de archivo activado, éste no es reseteado, con lo que se salvaguardan todos los archivos modificados o que se van modificando.
- Copia, donde se salvaguardan los archivos indicados pero el bit de archivo no es modificado. Así no se afecta al estado de las copias incrementales o diferenciales.

Las copias de seguridad se hacen normalmente en medios de almacenamiento que son reutilizados, y en que cualquier caso, cuando llegan al final de su vida útil son retirados después de ser borrados o destruidos.

El problema de almacenar las copias de seguridad y de garantizar el buen estado de las mismas en ocasiones se traslada a una empresa externa. A este proceso se le llama outsourcing.

Existen empresas en Internet que admiten que utilizando Internet y programas especialmente desarrollados por ellas y a un coste de apenas unos pocos euros o dólares mensuales, almacenemos nuestras copias de seguridad en un servidor que ponen a nuestra disposición. Con esto, garantizamos la integridad de las copias de seguridad, al almacenarlas en un lugar externo al propio donde están los datos originales. Programas como estos serían el Mozy Remote Backup o el Carbonite.

Evidentemente también podemos gestionar nosotros nuestras copias de seguridad, empleando el propio NTBackup que viene con Windows o programas como el Cobian Backup.
Nota: Según un estudio del 2004 de la empresa Recovery Labs el 47% de la gente que entrevistaron ha perdido datos de valor del ordenador en algún momento de su vida. Además el 57% reconoció que las medidas que tomaba de protección para proteger sus datos eran insuficientes.

Una alternativa a las copias de seguridad, y que mejora considerablemente el concepto de disponibilidad de los datos, son las copias de sincronización.

El concepto no es otro que tener los mismos datos ubicados en dos sitios distintos al mismo tiempo y cuando realizamos cambios en uno de ellos, asegurarnos que de manera automática, se reflejen en el otro.

Este concepto es muy empleado por gente que trabaja en varios lugares y necesita gran disponibilidad local de los mismos, normalmente debido a su tamaño, su número o debido a que no tiene la posibilidad de interconectar los pcs en los que trabaja normalmente en una red, por temas de seguridad o por ser ámbitos distintos.

En caso de que la conexión no sea un problema, otra opción es centralizar los datos en una ubicación a la que se puede acceder remotamente mediante contraseñas o certificados digitales, asegurando la comunicación entre el pc donde estoy y el que guarda los datos con un canal seguro o cifrado.

Es decir, yo necesito aquí y ahora un determinado documento. Me conecto a un servidor que está en Internet normalmente. Lo traigo desde allí, hago mis cambios, lo imprimo, etcétera y luego lo vuelvo a enviar al citado servidor. Entonces lo borro del pc donde lo he modificado. Cuando llego a mi casa si necesito volver a abrirlo, lo vuelvo a descargar desde este servidor y repito el proceso. Me basta por tanto con realizar copias de seguridad de mis datos de forma centralizada, es decir, sobre el servidor de donde los descargo. Puede incluso que lo realice la empresa que mantiene el servidor en Internet.

4.8. Versiones originales y/o legales de programas.

- Utilizar programas sin tener licencia para hacerlo, es ilegal.
- Emplear cracks o parches para reventar aplicaciones de empresas que desarrollan software, es ilegal.
- No respetar la licencia del producto, es ilegal.
- Copiar nuestro software con licencia a otras personas o empresas, o instalar software como si fuera multilicencia sin serlo, es ilegal.

Pero esa no es la cuestión que nos preocupa aquí. Hablamos de seguridad y de privacidad. Si empleamos productos descargados de Internet con parches que los hacen funcionar aunque no tengamos licencia, podemos estar descargando software en malas condiciones.

¿Quien nos asegura que las intenciones de las personas que lo modificaron no eran otras que las de compartir ese software con nosotros? Y si al instalarlo introducimos en nuestro pc virus, troyanos o cualquier tipo de malware, entonces, ¿qué haremos?

Luego está el hecho de que muchos programas, o peor aun, sistemas operativos si detectan que son piratas dejan de actualizarse. Es el caso de Windows XP. Ya existen versiones piratas de Windows Vista, pero probablemente pronto Microsoft se asegurará de que dejen de funcionar correctamente o actualizarse.

Si no deseamos pagar el software, la mejor alternativa es buscar equivalentes libres en vez de arriesgar nuestros documentos, emails, datos, etcétera, cosa que a la larga nos saldrá de seguro, más cara.

Capítulo 5. Políticas de Seguridad

Definir una política de seguridad es pensar lo que hará cuando se encuentre ante determinadas situaciones que supongan o puedan suponer riesgos para su ordenador y la información que contiene.

Del mismo modo que le dice a sus hijos que no hablen con extraños o decide no bajarse del coche en determinados momentos, debe pensar que hará cuando se encuentre ante situaciones como estas:

- ¿ Debería proteger mis datos en el ordenador para que nadie más pueda verlos?
- ¿ Es seguro que mi hijo emplee el pc que tengo en la empresa con la base de datos y demás información que necesito para hacer mi trabajo y se dedique a navegar por Internet o instalar juegos con sus amigos?
- Si pierdo mañana todo lo que tengo en el pc, ¿cómo me afectaría eso?
- ¿Tengo datos personales de clientes o empleados en mi o mis ordenadores?
- ¿Cuánto tiempo pasa entre copia y copia de seguridad? ¿Puedo permitirme perder tantos días de faena? ¿Qué coste económico tiene para mí? ¿Cómo afecta eso a mi empleo, clientes, etcétera?
- ¿Dónde están mis copias de seguridad? ¿Están protegidas?
- ¿Puedo permitirme quedarme sin ordenador unos días mientras el SAT (Servicio de Asistencia Técnica) lo repara, reinstala o recupera?

Preguntarse esta clase de cosas, le dará inmediatamente la importancia adecuada a su ordenador, a la información que almacena y a su disponibilidad. Es decir, conocerá usted cual es el coste y se planteará si necesita emplear tiempo y dinero prodigándole más atenciones o puede morirse de asco en un rincón.

Protéjase siempre esperando lo peor, me refiero a la pérdida completa del equipo y de todo lo que contiene. No suponga que solo va a tener incidentes de pequeño calado, aunque así pueda acabar sucediendo.

El primer punto de su política de seguridad debería ser la desconfianza:

- No instale, no copie, no pruebe, no juegue, con todo aquello que no tenga muy claro que no le dará problemas.

Y si es de los que piensa que siempre existen riesgos aunque sean pequeños, tome las medidas oportunas.

¿Esto puede hacerme algún mal? ¿Me compensa el bien que me hace?

O si lo prefiere:

Si lo hago, accedo, abro o utilizo, ¿qué es lo peor que puede pasar? ¿Y lo mejor?

Con estas sencillas pautas, podemos empezar a vislumbrar el camino para preservar nuestra seguridad, nuestra tranquilidad, y correr los menores riesgos posibles. Muchas veces las respuestas vienen dadas por el sentido común:

- ¿Abro un adjunto de email cuyo contenido es un archivo ejecutable? No. Un rato de diversión puede convertirse en una desdicha si se trata de un virus o herramienta de hacking.
- ¿Abro los correos de gente que no conozco? No.
- Actúe con su PC o portátil como si se lo fueran a robar mañana y supiera incluso la hora. Borre lo innecesario, preserve lo importante, cifre lo que sea de valor, no lleve más que lo indispensable, no lo deje en cualquier lugar y vigílelo de cerca.
- Cuente con que su casa puede arder mañana, y también su oficina. Puede que el novio de su hija sea un pirómano.
- No cuente con que el ordenador funcione dentro de cinco minutos. Solo es una máquina y a usted, no le debe nada.
- Use el PC del trabajo para trabajar. Quiere divertirse en su tiempo de ocio, pues compre otro PC para el ocio, no mezcle sus actividades.
- No use o trabaje con lo que usa o utiliza todo el mundo. Cualquiera que desee hacer daño, siempre busca hacerlo a la mayor cantidad de gente posible, porque es más rentable. Forme parte de las minorías.
- ¿No le dijeron de pequeño que no hablara con extraños? Pues no proporcione ahora todos sus datos a la primera web que se los pida. Compre en sitios web importantes, conocidos, avalados si puede ser por su banco o empresas de prestigio que no puedan exponerse a verlo disminuir. No busque comprar el CD de música en el sitio más barato.
- Piense que se puede falsear el membrete de un email. Puede NO venir de la persona que dice venir. Cuando desee abrir un hipervínculo asegúrese de donde apunta, aprenda a descubrir como verlo. Haga lo mismo con el envío de emails, verifique que el nombre de la persona a la que contesta o envía un email se corresponde con la que usted conoce.
- No se suscriba a servicios de recepción de email por Internet, use cuentas de correo dedicadas a ese efecto.
- Aprenda la dinámica de reinstalar su ordenador una vez al año. Tenga otro de emergencia, completamente operativo y con lo estrictamente necesario.
- No haga transferencias desde su banco habitual por Internet si no puede limitar las cuentas desde las que puede hacerse y la cuantía diaria.
- Vigile su PC semanalmente para eliminar el spyware o malware. No abra el correo spam, no crea que puede ganar dinero fácilmente. No visite páginas con contenido sexual si estima que necesita que su ordenador siga funcionando mañana.
- Si desea probar software nuevo, no use su ordenador habitual. Si desea navegar y puede permitírselo, navegue en un PC que no sea el de trabajo.
- Sea paranoico, piense antes mal que bien y si no sabe si puede causarle problemas, no lo haga. Pregúntelo primero a personal especializado.
- No deje su ordenador, no deje que lo toque quien no sepa tener el mismo cuidado que usted pone. ¿Lo necesita imperiosamente? Pues cuídelo.

Antes tales medidas uno puede preguntarse si merece la pena.

¡Claro que no!

Pero los humanos no somos siempre razonables y le daré un ejemplo de ello.

Todos tenemos coche (casi todos). La media de velocidad en las grandes ciudades europeas es de 10 Km/h gracias a los atascos. Pagamos barbaridades por un coche en el momento de la compra, por el seguro a todo riesgo a prueba de indeseables envidiosos que lo rayaran, le pincharan las ruedas, etc; por el impuesto de circulación, el de matriculación, la plaza de garaje, la gasolina, las revisiones y reparaciones, la ITV, los neumáticos y en algunas ciudades europeas se paga un impuesto adicional por circular por el centro. Se ha comprobado que es más barato ir todo el tiempo en taxis, pero no siempre están disponibles y es más cómodo emplear el coche que el transporte público. Y claro está, tenemos coche.

Si usted tuviera un bolso grande y lo usara todos los días cuando sale a comprar, pasear, trabajar, etcétera, ¿se le ocurriría hacer lo siguiente?:

- Llevar en él todo el dinero que tiene en el banco.
  - Sin embargo en el ordenador portátil solemos llevar todos nuestros documentos, declaraciones de renta, emails de los últimos años…..
- Llevar todas las tarjetas de crédito, cartillas del banco, y claves secretas apuntadas en un papel.
  - Pero en los navegadores web almacenamos las claves secretas para acceder a nuestro banco por Internet, y hacer transferencias, compras, etcétera.
- Llegar al trabajo con el bolso lleno de cartas enviadas a los compañeros de trabajo diciéndoles lo borde y asqueroso que es nuestro jefe.
  - Pero empleamos el pc de la empresa para enviarnos correos entre compañeros criticando a los jefes y que luego, incluso borrándolos, a veces permanecen en el disco duro del ordenador.
- Llevar una colección de varios centenares de fotos de mujeres u hombres desnudos o en escenas eróticas.
  - En el pc, mucha gente almacena miles de ellas, con lo que en caso de pérdida o de curiosos, nuestros gustos sexuales o desviaciones quedan al descubierto.

Usted no emplea la agenda personal de citas para guardar sus pensamientos íntimos del día, para eso emplea un diario que deja en casa, en algún lugar solo conocido por usted y privado. Dispone por tanto de dos “libretas”, empleadas en contextos distintos y para cosas diferentes, y también se les aplica una seguridad “diferente”.

Será usted quien decida cuantos ordenadores necesita, qué almacenar en cada uno de ellos, qué debe considerarse confidencial y qué no, y por qué. Con esto, hemos llegado a la conclusión que toda la información no tiene la misma importancia ni debe protegerse de la misma manera.

Por último existen programas que pueden ayudarle a proteger sus datos, ya que pueden obligarle a introducir una clave para acceder a ellos cuando enciende el pc, o en

caso de que pase demasiado tiempo sin que usted acceda a ellos, pueden ser borrados remotamente cuando el pc se conecta a Internet y haya sido robado, por ejemplo.

En cualquier caso, cifrar la información se está convirtiendo en algo imprescindible en los computadores actuales, y la potencia de los mismos, hace que el esfuerzo adicional de hacerlo les reste unas mínimas prestaciones.

Nuestro problema es que todavía no pensamos en el ordenador como una herramienta más, sino como algo mágico y maravilloso que es capaz de hacer muchas cosas. Cuando se apaga la televisión de repente, siempre miramos si el cable de la luz hace buen contacto. En el pc, tan pronto se apaga pensamos en el servicio técnico, muchos ni siquiera hacemos las comprobaciones básicas que haríamos con otro electrodoméstico.

Un ejemplo de cómo puede irse al traste la seguridad de nuestros ordenadores cuando otros los usan o están en la red de la empresa, sería éste.

Para evitarlo son necesarias las políticas de seguridad, donde usted decide qué debe y qué no debe hacerse en general. Luego debe traducir la forma de comportarse en normas concretas que deberán aplicarse mediante procedimientos.

Pongamos un ejemplo.

Si nuestra política es no permitir que nadie instale software en nuestro pc sin permiso expreso; la norma sería que el software debe ser original y no descargado de Internet. La forma de instalarlo sería el procedimiento. Por ejemplo, antes de instalarlo, escanear el cd o el medio en que viene el software con un antivirus para ver que está “limpio” y comprobar en la web del fabricante o webs especializadas que no tiene bugs o fallos de seguridad críticos conocidos, o en caso de tenerlos, bajarse las actualizaciones de la web oficial para instalarlas.

En definitiva, la política sería la forma de actuar a grandes rasgos; las normas serían la manera de dar cumplimiento a la política especificando que está permitido y que no de manera más concreta. Y los procedimientos serían los pasos para llevar a cabo la tarea, dentro de las normas permitidas y aplicando la política definida.

Si en una empresa pequeña o en casa no es necesario siempre reflejarlas por escrito, en empresas medianas o grandes, la seguridad y la necesidad de que sean conocidas por todos son sumamente importantes. La pérdida de información o de servicios por vulneración de seguridad puede arruinar o desprestigiarlas, ocasionando pérdidas millonarias. Podemos ver aquí lo que sería la aplicación en una empresa.

En el peor caso, una política de seguridad no define solo lo que debe o no debe hacerse, sino quien o quienes son responsables de que determinadas acciones no se produzcan, se desatienda la seguridad, o se ocasione una pérdida de datos.

Es decir, podría usted ser responsable de pérdidas de información millonarias si se demostrase que desobedecer una política de seguridad ha provocado riesgos para la empresa en la que trabaja, ocasionando daños o algún tipo de perjuicio.

El simple hecho de desobedecer las políticas de seguridad ya puede suponer el despido por tratarse de una norma interna de la empresa que debe ser obedecida. No hablemos si el incidente por incumplimiento ha provocado daños o estragos internos.

Si estas políticas están por escrito y se le dieron al entrar en la empresa o se le advirtieron, nunca podrá decir que no las ha cumplido por ignorancia o desconocimiento. Asegúrese de conocerlas y de estar al tanto de los cambios que se producen en ellas. Son más comunes en las empresas grandes, en las centradas en tecnología, información, en las que proporcionan servicios de outsourcing y en las empresas públicas.

Capítulo 6. Recuperación rápida del sistema

6.1. Introducción

En este capitulo veremos como proteger, empleando el menor tiempo posible, nuestro sistema operativo y nuestros datos. El objetivo es hacer una copia o backup del sistema, es decir, proteger el sistema operativo por una parte y los datos por otra, para evitar su pérdida.

Razones que pueden provocar su pérdida son una avería del disco duro del ordenador, un virus, un borrado accidental, un archivo modificado por error y guardado posteriormente (sobre escritura), una contraseña perdida que obliga a recuperar el archivo original que estaba sin cifrar, etcétera.

Para salvaguardar la información de nuestro ordenador en poco tiempo, y que la tarea en sí, no sea tediosa y lenta, tenemos que aprender a organizarla de manera eficiente, es decir, la tarea de backup ha de ser cómoda, lo más automática posible y con un coste razonable de tiempo y dinero. Cuanto más fácil sea llevarla a cabo, menos pereza nos producirá, y más a menudo la completaremos.

La mejor manera de no olvidarnos de ningún documento cuando hacemos la copia de seguridad o de no engrosar inútilmente la copia del sistema operativo es tener claramente separados datos e información, de aplicaciones y sistema operativo; además de conocer la ubicación y el tamaño de cada parte.

En el caso de Windows 2000 y XP, estas son algunas ubicaciones donde se almacenan normalmente los datos de los usuarios:

- **Datos de las aplicaciones:**
  - C:\Documents and Settings\Usuario\Datos de programa.
  - C:\Documents and Settings\Usuario\Configuración local\Datos de programa.

- **Caché Web:**
  - C:\Documents and Settings\Usuario\Configuración local\Archivos temporales de Internet.

- **Cookies:**
  - C:\Documents and Settings\Usuario\Cookies.

- **El Escritorio:**
  - C:\Documents and Settings\Usuario\Escritorio.

- **Favoritos:**
  - C:\Documents and Settings\Usuario\Favoritos.

- **Historial de navegación web:**
  - C:\Documents and Settings\Usuario\Configuración local\Historial.

- **Configuración Local:**
  - C:\Documents and Settings\Usuario\Configuración local.

- **Música:**
  - C:\Documents and Settings\Usuario\Mis documentos\Mi música.

- **Fotos:**
  - C:\Documents and Settings\Usuario\Mis documentos\Mis imágenes.

- **Videos:**
  - C:\Documents and Settings\Usuario\Mis documentos\Mis vídeos.

- **Mis Documentos:**
  - C:\Documents and Settings\Usuario\Mis documentos.

La lista de ubicaciones es interminable, y crece con cada aplicación que instalamos. Sin embargo, todas las ubicaciones son rutas o subdirectorios que terminan en la carpeta “Documents and Settings\Usuario”, la cual va creciendo hasta alcanzar un tamaño inaceptable, donde muchos de los archivos ni siquiera sirven para nada aunque alguna vez tuvieron su utilidad.

No deberíamos guardar nuestros documentos en esta ubicación, conocida como “perfil de usuario”. Es el primer sitio donde un hacker o un virus intentaría buscar información de interés, y además es una ubicación controlada por el sistema operativo donde se almacenan datos temporales de él mismo, de la configuración de seguridad del usuario y de otras aplicaciones. Pronto no sabremos que podemos borrar y que no, por eso es mejor disponer de una ubicación controlada completamente por nosotros y donde las carpetas, sus nombres, y su utilidad dependan de nuestras decisiones únicamente.

Centralizar todos los documentos o información valiosa para nosotros en un directorio o unidad facilitará tareas como verificar la integridad del sistema de archivos, comprobar si alguno de ellos está infectado por virus, proteger con los permisos adecuados los documentos si el ordenador es compartido, conocer su tamaño, realizar búsquedas, sustituciones en archivos, organizarlos en grupos, y como no, realizar las copias de seguridad.

Cuantas más copias de seguridad tengamos almacenadas, dispondremos de una mayor fiabilidad a la hora de recuperar nuestros archivos. Por ejemplo, imaginemos que buscamos cierto documento que necesitamos y no lo encontramos en el disco duro. Se ha borrado, y no sabemos ni cuando ni como, lo que nos obligará a buscarlo primero en la copia de seguridad de esta semana, luego de la semana anterior y así sucesivamente. Si solo mantenemos un par de copias de seguridad puede ser que la copia más antigua no conserve el archivo en cuestión. Esto es lo que suele pasar cuando almacenamos las copias en unos pocos medios regrabables y los vamos sobrescribiendo. Esto puede hacerse, pero debemos de disponer de los suficientes soportes ópticos para almacenar el

número adecuado de copias que requiera nuestro trabajo y poder retrotraernos a versiones más antiguas de un documento o programa.

Nunca debemos, si solo tenemos una copia de seguridad en medios regrabables, que reescribirla, porque mientras grabamos la nueva copia de seguridad en los cds o dvds donde estaba la anterior, y mientras el proceso no queda completado de manera satisfactoria, no tenemos ninguna copia de seguridad.

Cuanto más a menudo hagamos las copias de seguridad, menos cambios perderemos cuanto nos veamos obligados a recuperar la información de una de ellas.

No basta con hacer las copias, de vez en cuando, es necesario probarlas para ver que están correctamente creadas, son funcionales y que sabemos restaurarlas adecuadamente. Eso nos permitirá mejorar el proceso, decidir si necesitamos una grabadora de cds o dvds más rápida, un mejor disco duro, u optimizar el proceso mediante alguna herramienta.

Lo primero que debemos hacer es establecer cuando se harán las copias de seguridad y qué datos se copiaran. Existen empresas que nada más disponen de copias totales, y otras que llevan a cabo una copia total al mes, y todas las demás son diferenciales o incrementales.

También es importante disponer de unas instrucciones escritas de los pasos que debemos seguir para restaurar una copia de seguridad en caso de pérdida de información. Esto es fundamental, ya que realizar los backups es una tarea que haremos a menudo, pero restaurarlos, es algo que únicamente se hace si se pierde información, con lo que la frecuencia es mucho menor.

Esquemas conocidos de copias de seguridad son los siguientes:

- Padre-Hijo: donde cuatro cintas se emplean para las copias de lunes a jueves (hijos) y otras dos se hacen el viernes de cada semana. Con las seis cintas, podemos cubrir hasta 6 días.

- Abuelo-Padre-Hijo: se emplean 4 cintas para los días de lunes a jueves (hijos); otras 3 cintas se emplean para almacenar cada viernes del mes excepto el último; y otras seis para almacenar el último viernes de cada mes. Con este esquema tenemos 13 cintas para proteger 6 meses de información. Si aumentamos las cintas de los meses de 6 a 12, con un total de 19 cintas cubriríamos un año.

- Existen sistemas complejos como el de las Torres de Hanoi, que con 10 cintas, y siendo 2 elevado a n menos 1 la fórmula , podemos cubrir 1023 días, aunque el desgaste de las cintas con numeración más baja es excesivo y obligaría a reemplazarlas pronto.

Nota: Estos esquemas fueron pensados para cintas reutilizables, ahora debemos pensar en cds/dvds regrabables que son mucho más económicos o en soportes ópticos de un solo uso (no reutilizables).

En el mejor contexto posible y si la cantidad de datos no es demasiado grande, interesa emplear copias totales. En caso contrario, trabajaremos con las diferenciales, lo cual, si nos vemos en un apuro, nos obligará a restaurar la total y la última diferencial. Pero en ocasiones la diferencial es aun demasiado grande, por lo que se opera incluso con incrementales. Todo depende del volumen de datos a gestionar, y de la cantidad que de ellos son modificados diariamente.

6.2. Medidas para optimizar el proceso de recuperación.

6.2.1. Instalación del sistema operativo.

Un ordenador nuevo suele venir con un sistema operativo preinstalado, que normalmente se almacena en la unidad C, que es la única partición existente y que ocupa todo el disco duro.

Si el pc viene con el sistema operativo preinstalado, es lo que se conoce como producto OEM (Original Equipment Manufacturers). El fabricante nos entrega el ordenador con el sistema operativo funcionando y si con el tiempo el ordenador deja de funcionar, deberemos emplear un disco de recuperación que dejará el sistema operativo como el día en que compramos el pc y que viene con el mismo.

Esta solución oculta un problema. Dejar el pc tal cual lo compramos incluye perder todas las aplicaciones y datos que hemos instalado desde entonces o creado por nosotros mismos, por lo que antes de recuperar el sistema a su estado inicial, más vale tener una copia de seguridad de todo. Así al menos podremos restaurar nuestros datos.

Los fabricantes y las tiendas que venden sus equipos permiten también comprar el sistema operativo en CD o DVD, de modo que si un día nos falla, nosotros podamos reinstalarlo sin perder los datos o aplicaciones que teníamos en el disco duro. Aunque en el caso de las aplicaciones podría ser necesario reinstalarlas.

En cualquier caso, siempre podemos optar por hacer copias completas del sistema o distinguir los datos, del sistema operativo y las aplicaciones. Estas “fotos” del estado del equipo nos ahorran el esfuerzo de reinstalar el sistema operativo, de aplicar el cd de restauración del fabricante que no nos deja el ordenador como lo necesitaríamos o de tener que llevarlo al Servicio Técnico; pues en pocos minutos podremos dejar el ordenador en funcionamiento.

Los discos duros actuales alcanzan ya capacidades de 500 Gbytes, y se hace difícil encontrar discos con menos de 160 o 200 Gbytes. Sin embargo, y a pesar del espectacular crecimiento de la capacidad de almacenamiento, los sistemas operativos siguen ocupando poco espacio respecto al tamaño de los discos. Windows XP ronda los 2 o 3 Gbytes; y Vista en su versión más completa, la Ultimate, no requiere más de 15 Gb. Luego vendrán las aplicaciones, juegos y los parches y actualizaciones del sistema operativo.

Sea cual sea nuestra situación, si disponemos de un disco de 160 Gb, bien podemos crear una partición (unidad C) para el sistema operativo de unos 30 Gb o 40 Gb y dejar el resto de espacio libre para los datos.

6.2.2. Creación de una partición para datos.

El espacio restante del disco duro podemos emplearlo para crear una segunda partición, la unidad D, donde almacenaremos nuestros documentos, email, videos, fotos, etcétera. Separar dentro del mismo disco el espacio del sistema operativo y de los datos, supone que podemos fácilmente recuperar lo uno o lo otro, y hacer copias de solo una parte. Almacenar los datos y el sistema operativo juntos, puede hacer que con el tiempo no sepamos con exactitud la ubicación de todos nuestros documentos, emails, favoritos, etcétera y nos olvidemos de salvaguardarlos o los borremos por error. Separarlos nos permite saber lo que ocupan, y nos permitirá protegerlos más fácilmente como veremos más adelante.

Si un virus afectó ayer a nuestro sistema operativo, bastará con recuperarlo desde la última copia de seguridad, sin borrar los últimos documentos que utilicé ayer por la tarde y que se almacenan en la unidad D. Recuperar así una parte, no implica dañar la otra.

Si deseara instalarme un nuevo sistema operativo como Linux Fedora Core o Suse Linux, solo me haría falta eliminar el contenido de la unidad C, pero D, con todos mis documentos, proyectos, etcétera no sería alterada.

6.3. Imágenes del sistema operativo.

No se puede hacer una copia de seguridad del sistema operativo mientras este está iniciado. Por ejemplo, desde Windows XP, no podemos hacer una copia completa del sistema operativo, ya que muchos de los archivos que habría que copiar están siendo usados por Windows y no permite su acceso.

Además está el detalle de que al estar en uso, están siendo modificados continuamente, con lo que a lo mejor lo salvamos en la copia de seguridad, y justo entonces el sistema operativo vuelve a modificarlo. A lo mejor este archivo ha de estar sincronizado con otro y copiamos el archivo A cuando acaba de ser modificado, y el B antes de que lo sea. El resultado es que ambos archivos no están sincronizados y el operativo podría detectarlos a ambos como corruptos.

Por todo esto, es necesario arrancar el ordenador con otro pequeño sistema operativo desde el que hacer la copia de seguridad. Este pequeño sistema, que suele ser modular, lo introduciremos en el ordenador mediante un cd, un dvd, un disquete o incluso un lápiz usb. Lo más normal es emplear un disquete o un CD y se les conoce como disco de arranque. Mucha gente emplea los discos de arranque derivados de los que generaba Windows 98, y otros emplean disquetes basados en otro sistema operativo que no es el MSDOS, pero sí compatible con él, como el Caldera DOS, el FreeDOS, etcétera. Terminada esta primera fase, se ejecuta el programa encargado de realizar una

copia de seguridad de la partición donde está el sistema operativo. Esta aplicación genera una imagen o "foto" del estado del mismo. La imagen según su tamaño estará formada por varios archivos grandes, que almacenaremos en cds o dvds y suelen ocupar el equivalente a la mitad del espacio ocupado en la unidad C (gracias a la compresión) y todavía menos cuando se trata de una copia de seguridad de la unidad de datos, la D (aunque aquí se suelen emplear métodos distintos y no la copia de toda una partición).

6.3.1. El disco de arranque.

El disco de arranque más sencillo puede generarse desde Windows 98. Si no disponemos de ningún sistema antiguo desde el que generarlo, podemos buscar disquetes de arranque por Internet:

- http://www.bootdisk.com/bootdisk.htm.
  - Y elegir el disco de Windows 98SE OEM.
- http://freepctech.com/pc/002/files010.shtml.
  - Y elegir Windows 98 & Windows 98SE.
- http://www.ultimatebootcd.com/,
  - Desde donde podremos arrancar el ordenador con un CD, dispone de muchas utilidades.
- http://www.answersthatwork.com/Downright_pages/Boot_Disks_and_Boot_CDs.htm
  - Bootdisk Windows 98 SE con CDROM

Naturalmente deberíamos escanear los disquetes con un antivirus, y probarlos primero en un ordenador cuyo contenido pudiéramos arriesgar. No olvidemos que es un disquete creado por un desconocido.

6.3.2. Crear la imagen.

Una vez pongamos el ordenador en marcha con estos disquetes y se complete su inicialización, se quedará a la espera de que le demos órdenes. Una manera adecuada sería emplear herramientas que hay en el mercado, como Ghost, Drive Image, Partimage, TrueImage o PartitionSaving, que realizan copias completas de una partición (para salvaguardar el sistema operativo y las demás aplicaciones instaladas).

Algunos de ellos permiten grabar directamente la copia a CD o DVD, otros la copiaran a otro disco duro, otra partición o dispositivo y luego será necesaria copiarla a cds o dvds manualmente.

El Hiren's BootCD 8.9 contiene buena parte de las herramientas anteriormente citadas. Y permite arrancar el ordenador sin crear un disquete, ya que el CD actúa como tal.

Es aconsejable emplear herramientas que permitan cifrar o proteger con password las imágenes, eso es debido a que, aunque separemos el sistema operativo de los datos, Windows XP y Vista almacenan mucha información sobre el propio usuario en C:\Documents and Settings y c:\Users. La mayoría de esta información es basura,

pero no toda, por lo que de vez en cuando deberíamos eliminar toda aquella que atente contra nuestra seguridad o privacidad, y asegurarnos que la imagen o conjunto de archivos que almacenan todo el contenido de la unidad C, es ilegible para aquellos que no tengan la password.

Nota: Algunas de las herramientas del Hiren's CD son:

- Partition Magic 8.0.5
- Gdisk 1.1.1
- Otros sustitutos del Fdisk de MSDOS.
- Norton Ghost 11
- Partition Saving 3.30
- True Image 8.
- F-Prot Antivirus
- McAfee Antivirus
- Y mucho más

6.3.3. Soporte o medio para la copia.

Normalmente las copias de seguridad emplean como soporte físico los cds o dvds como hemos comentado anteriormente. Para el sistema operativo y dado su tamaño, suelen emplearse dvds. Si se emplean cds es necesario estar atento durante el proceso de copia de seguridad, ya que será necesario insertar varios de ellos conforme la aplicación los reclame.

El empleo de cds regrabables o dvds regrabables no suele aconsejarse, sobretodo de dvds, porque existen unidades lectoras que luego no son capaces de leerlos adecuadamente. Además los dvds son más sensibles a las ralladuras, los cambios de humedad y temperatura, etcétera.

Actualmente y cada vez más, se están empleando discos duros portátiles USB para realizar las copias de seguridad. Sin embargo llevar una copia de los datos de nuestro pc en ellos, es solo eso, una copia. Como no disponemos de copias anteriores, no podemos recuperar documentos erróneamente modificados o que nos gustaría ver como estaban la semana pasada. Esto sucede porque no disponemos de versiones anteriores del documento. Esto, más que una copia de seguridad, es una copia sincronizada de lo que hay en el ordenador y existen programas especializados para realizar copias por sincronización entre dos o más pcs, o dentro del mismo, entre distintas ubicaciones que deban tener contenidos similares (como SyncBackup o FileSync).

Si decidimos almacenar las copias de seguridad en cds o dvds podemos usar herramientas de comprobación de la grabación para ver que todo el contenido sea accesible, o emplear la opción de verificar del propio programa de grabación.

Existen herramientas que verifican el estado de un disco óptico (CD/DVD) en caso de que sea muy importante poder garantizar el estado de las copias de seguridad

más antiguas, asegurando que siguen funcionando correctamente y que se conservan en buen estado).

6.3.4. Etiquetado y almacenamiento.

Las copias de seguridad deben ser etiquetadas para que sean fácilmente identificables. Debe indicarse si se trata del sistema operativo (sistema operativo y aplicaciones), datos (archivos en general) o ambos. Es necesario indicar la fecha en que se hizo, tamaño de la copia, número de cds, dvds u otros soportes físicos que la forman (deben ir numerados por orden); tipo, ya sea total, incremental o diferencial; y programa empleado para hacerla, además de la versión del mismo.

Deben almacenarse en un lugar seguro, y no deberían estar todas juntas ni al lado del pc del que se supone que son copia. Tampoco tienen que estar sometidas a un exceso de frío o calor ni en lugares con demasiada luz.

6.3.5. Recuperación de la imagen.

Restaurar o recuperar una imagen, no es más que emplear el mismo programa que usamos para realizar la copia de seguridad, pero de manera inversa. En vez de leer del disco duro y grabar en un soporte óptico, lee de un soporte óptico y escribe en el disco duro. Es un proceso más rápido que el anterior, ya que el proceso de descompresión apenas requiere esfuerzo frente al de compresión que fue necesario al crear la copia de seguridad.

6.4. Salvaguardar los emails y la agenda de direcciones.

Para facilitarnos la tarea de hacer una copia de seguridad de nuestra agenda de contactos, de nuestros emails y de la configuración de las cuentas de correo existen varias aplicaciones.

En el caso de Outlook Express, el producto de mensajería de Microsoft, y el más empleado en todo el mundo, se hace complicado localizar la ubicación de nuestros correos electrónicos, pues se almacenan en un directorio bastante difícil de encontrar por parte del usuario.

Cambiar la ubicación del correo o del almacén de correo tal y como lo nombra Microsoft tampoco es sencillo.

Por ello, podemos emplear herramientas como Identity RegRead que nos permiten localizar el directorio donde se guarda el almacén de correo; y que también localiza la libreta de direcciones o Windows Address Book (wab).

Existe incluso un programa capaz de averiguar las contraseñas de nuestras cuentas de correo electrónico en caso de que las tengamos almacenadas en la configuración y las hayamos olvidado. O siempre podremos exportar la configuración

de la cuenta (incluida la clave) para importarla en otro ordenador, y poder seguir accediendo al correo.

Si se trata del Mozilla Thunderbird, podemos emplear el Mozilla Backup para generar una copia de todo nuestro email, nuestra agenda de contactos, la configuración de nuestro correo, etcétera a un archivo zip, que podemos cifrar mediante password.

Por tanto, hacer copias de seguridad de nuestros emails no requiere demasiado esfuerzo. En el caso del Outlook Express, podemos realizar una copia del directorio donde está el almacén de correo o exportarlo desde el propio programa; la configuración de las cuentas puede exportarse también, y la libreta de direcciones puede copiarse o exportarse incluso a un archivo CSV. Con el Thunderbird, se da el caso de que existe un programa que realiza todas estas tareas, generando un solo archivo con todo lo necesario.

Estos archivos resultantes podemos además cifrarlos antes de grabarlos en algún medio extraíble o soporte como veremos luego.

6.5. Copias de seguridad de los datos.

6.5.1. Formas de almacenamiento

Dentro de nuestros datos, conviene separar aquellos archivos grandes o muy grandes, como películas o música que no deberían formar parte de nuestras copias habituales de seguridad.

Las películas, si ya las hemos visto y no nos interesa guardarlas, no tiene sentido que acaben en una copia de seguridad. Si deseamos preservarlas porque nos gustan, lo normal es acabar almacenándolas en CD o DVD y lo mismo se aplica a la música.

Si tenemos algún directorio con software, probablemente no variará con la misma rapidez que nuestros documentos, agendas, presentaciones o informes.

Aquí por tanto, podemos apreciar que estamos clasificando la información en grupos, separando aquello que debe ser tratado de forma especial por su tamaño o por la ínfima variación que sufre su contenido con el tiempo frente al resto.

Lo que queda tras eliminar este primer subconjunto, es lo que nos interesa ahora. Esos miles o centenares de pequeños archivos que suponen la gran mayoría de información y que varían constantemente.

Al restar la música o las películas, solamente nos queda otro tipo de información que necesita un tratamiento especial: las fotos o imágenes. Este tipo de archivos suele ocupar bastante espacio, no solemos borrarlos, aunque si que van creciendo en número y ocupan cada vez más espacio; pero sobretodo, al igual que la música y las películas no se pueden apenas comprimir al hacer una copia de seguridad para reducir el espacio que ocupan.

Para el resto de los documentos, podemos crear un paquete o archivo comprimido con todos ellos. Existen muchas herramientas para hacerlo. Existen el 7zip, Winrar, IZArc, Winzip, Filzip, y otros muchos compresores más.

Gracias a ellos, los documentos pueden reducirse a una ínfima parte de su tamaño original. Guardar los datos de esta manera permite almacenarlos en poco espacio. El nombre del archivo comprimido nos dirá lo que contiene y la fecha en que se hizo la copia. Otra cuestión es si podemos poner una password o clave secreta a ese archivo comprimido para que no pueda ser abierto por nadie excepto por el propietario. La clave servirá para descifrar el archivo, protegido con algún algoritmo de cifrado, como pueda ser AES de 128 o 256 bits (caso de Winzip).

Esta suele ser la manera más sencilla de operar, pero no la más segura. Algunos de estos compresores necesitan la password para descifrar de los archivos, pero no para ver la lista de los mismos, y como los nombres de los ficheros suelen ser auto explicativos, cualquiera puede saber lo que contiene la copia de seguridad, aunque no pueda abrir los archivos.

Además existen programas que por fuerza bruta intentan averiguar la contraseña de estos archivos cifrados, por lo que se recomienda que sea lo más compleja y larga posible. Ejemplos de programas para obtener la password de archivos cifrados, lo tenemos aquí y aquí.

Existen herramientas capaces de comprimir y cifrar los archivos individualmente de manera transparente al usuario. Un doble clic sobre el archivo cifrado daría paso a un cuadro de diálogo donde se nos pediría la password y luego el archivo se descomprimiría en una ubicación temporal desde donde se abriría inmediatamente mediante la aplicación oportuna. Al cerrar el archivo en cuestión, éste sería borrado de su ubicación provisional, no sin antes haberlo cifrado y comprimido para sustituir al original.

Este sistema es el empleado por EFS o sistema de archivos encriptado de Microsoft, pero va ligado a Windows. Fuera de ese sistema operativo los archivos no podrían descifrarse. Además en el proceso de cifrado, se crea una copia del archivo original, y luego éste se borra, pudiendo ser recuperado del disco duro por no haberse ejecutado un proceso de wiping sobre el mismo.

Otro ejemplo de esta manera de funcionar es AxCrypt, que sí que sobrescribe el archivo original, y comprime y cifra el nuevo. Incluso gestiona los archivos temporales cuando el archivo cifrado es abierto, y se asegura de borrarlos del disco duro cuando terminamos de acceder a ellos o modificarlos.

También existen herramientas de copia de seguridad como Cobian Backup.

Por último, podemos crear unidades de disco virtuales donde almacenar nuestros archivos y salvaguardar nuestros documentos. Dentro de ellas podremos borrar, copiar o modificar archivos sin preocuparnos por nada. Se acceden mediante password y nadie puede leer su contenido sin poseer la password. Ejemplos de estos productos son Bestcrypt, TrueCrypt y FreeOTFE.

6.5.2. Medios de almacenamiento.

Ya tenemos la copia de seguridad, pero ¿dónde la almacenamos para que esté a salvo de malas manos, malos tratos, incendios, pérdidas, etcétera?

Algunas de las mayores organizaciones, empresas o bancos del mundo han sufrido el robo de información en sus carnes. Muchas protegían adecuadamente sus ordenadores, servidores, sistemas de información, pero los ladrones robaron sus copias de seguridad. Por eso es importante cifrarlas, como hemos visto anteriormente.

También es necesario que cuando nos hagan falta estén disponibles. El término adecuado es disponibilidad. Las copias de seguridad deberían estar físicamente en otra ubicación que no fuera nuestra casa o nuestra empresa pero relativamente cerca de ella.

Existen empresas que a través de la ADSL y tras instalarnos un programa que nos ayuda en el proceso, nos permite programar cuando deben hacerse las copias de seguridad en nuestros ordenadores y luego las envía a la empresa destinataria. Allí se envían cifradas y podemos recurrir a ellas si nos vemos en apuros. Se supone que los datos enviados y que van cifrados con algún algoritmo de cifrado seguro son tratados correctamente por este programa, que es el encargado de garantizar su seguridad y nuestra confidencialidad.

La pregunta entonces es, ¿pero es la empresa de confianza? ¿Puedo fiarme?

No hace falta fiarse. Si primero comprimimos nuestros backups o copias de seguridad en el propio ordenador, y los ciframos, cuando sean enviados a la empresa que los almacena y protege, nadie allí podrá acceder a su contenido y solamente nosotros podremos accederlos cuando nos haga falta.

Nosotros cifraremos primero nuestras copias de seguridad, y el programa que nos instalamos para enviar nuestros datos a los servidores volverá a cifrarlos de nuevo, pero en cualquier caso, y sea así o no, Irán cifrados primeramente por nosotros.

Ejemplos de servicios de este tipo son Mozy Remote Backup y Carbonite.

Otro modo de almacenamiento si tenemos una cuenta de correo de GMail o de Yahoo es emplear este espacio como disco duro virtual cosa permitida por ambas empresas o utilidades de terceros (Gmail 1,2; Yahoo).

Existen más empresas que permiten compartir archivos en Internet, incluso que regalan cantidades enormes de espacio en disco:

- http://www.mydatabus.com/
- http://www.webdrive.dk/setlang.php?lang=english
- http://www.flashspace.co.uk/
- http://briefcase.yahoo.com/

Eso sí, siempre que empleemos almacenamiento externo, deberíamos cifrar los documentos o dejarlos en los servidores en formato cifrado. Es posible que estas empresas protejan nuestros datos, ¿pero quien lo garantiza?

6.6. Réplicas

En ocasiones disponemos de varios ordenadores: el del trabajo, el de casa, el del lugar de vacaciones y nuestro portátil. Y con todos ellos accedemos a la misma información.

Al principio íbamos copiando los documentos que nos hacían falta de un ordenador a otro. Luego cuando aparecieron los lápices usb y los discos duros portátiles, dejábamos nuestros datos en ellos, y bastaba con conectar el dispositivo que llevaba todos nuestros documentos al ordenador que estuviéramos empleando en ese momento.

Primeramente un lápiz usb era suficiente, pero pronto no bastaron 4 Gb sino que necesitábamos más capacidad, y pasamos a un disco duro compacto de 100 Gb, que se conectaba al pc de turno mediante un puerto usb o firewire. Pero había que cargar con él y nos daba miedo que lo perdiéramos o nos lo robaran.

Hubo gente que se le ocurrió la brillante idea de poner en marcha en su casa o empleando los servicios de algún proveedor de Internet, un servidor ftp con todos sus datos. Ahora estaban accesibles desde cualquier lugar del mundo mediante una sencilla password. Aunque no tuvieron en cuenta que con password o sin ella, los datos de un servidor ftp viajan sin cifrar. Pronto estos servidores ftp se cambiaron por servidores FTP seguros que empleaban por bajo protocolos como SSL 3.0, TLS 1.0 o SSH. Ahora para conectarse hacía falta una contraseña y todos los datos viajaban cifrados por la red.

Bastaba con conectar el ordenador de turno a este servidor FTP seguro y descargarse todo lo necesario. Luego trabajábamos sin conexión a la red, en nuestro pc local, hacíamos los cambios oportunos, y volvíamos a sincronizar los datos más modernos de nuestro pc con los del servidor FTP seguro. Y dejábamos el problema de realizar las copias de seguridad del sitio FTP seguro al proveedor de Internet.

Otros no deseaban pagar al proveedor de Internet por darles este servicio, y decidieron emplear programas de sincronización para mantener los mismos datos en el pc de casa y en el del trabajo. Por las noches los dos ordenadores se intercambiaban información cifrada previamente por el usuario, o sin cifrar si no tenía nada de confidencial. De nuevo uno de estos dos ordenadores se sincronizaba con el disco duro portátil que a su vez era empleado con el tercer ordenador, el portátil.

La sincronización protege de la pérdida, pero no mantiene versiones de documentos y no recupera documentos antiguos que hayan podido borrarse de todas las réplicas. Además requiere un buen ancho de banda, saber cual es el estado de los documentos en cada equipo y nunca perder la perspectiva de cómo (quien es el origen y el destino) y cuando se realiza la sincronización.

6.7. Cuando solo importan los datos

Supongamos que para nosotros únicamente es importante el ordenador en cuanto que nos presta determinados servicios, pero no necesitamos estar instalando o actualizando software a menudo. Además nuestros datos son externos al pc, los llevamos en algún medio extraíble o simplemente están en otra partición.

En definitiva que no hacemos copias de seguridad del sistema operativo a menudo, porque no cambiamos continuamente lo que hay instalado, ni nos importa demasiado los cambios que podamos hacer en el escritorio. En ese caso podemos emplear soluciones rápidas para mantener el equipo en perfecto estado.

Lo usaremos para trabajar, haremos las pruebas que queramos, pero al reiniciar el ordenador estará como al principio. Esto puede hacerse así.

Documentación adicional

Copias de Seguridad. Wikipedia.
Copias de Seguridad. Esquemas.

Copias de Seguridad Remotas. Carbonite.
Copias de Seguridad Remotas. Mozy.
Copias de Seguridad Local. Cobian Backup.
Copias de Seguridad de Email. MozBackup.

Capítulo 7. Técnicas para proteger la información

7.1. El proceso de inicio del ordenador.

7.1.1. La BIOS.

Cuando enciende el ordenador, inmediata arranca el sistema operativo. Esta suele ser la configuración por defecto de la mayoría de ordenadores, pero puede usted configurarlo para que nada más sea encendido, exija una password para arrancar el sistema operativo.

Esta opción puede seleccionarse desde dentro de la BIOS, o programa de configuración del hardware de su ordenador. Naturalmente tendrá que poner una password o clave a la bios para que no entre cualquiera y desactive la clave de arranque.

Esta clave puede ser eliminada o borrada, pero para ello es necesario abrir el ordenador y utilizar un switch que está instalado en la placa base del computador (donde están pinchados todos los componentes).

Sin embargo, algunos fabricantes de BIOS han creado passwords por defecto para cada modelo de bios, y algunas de esas passwords por defecto pueden encontrarse por Internet. Así que no piense que este sistema de protección es la panacea. Solo la combinación de varios sistemas de protección le proporcionarán la suficiente seguridad.

Además existen herramientas para crackear, es decir, obtener estas passwords. Algunos de los mecanismos empleados se incluyen en el Hiren's CD.

7.1.2. Cargador multisistema.

Si instala más de un sistema operativo en el ordenador, por ejemplo Windows 98 y Windows XP, el programa de instalación de Windows XP introducirá en su ordenador un cargador, es decir, cuando arranque el ordenador, se le permitirá elegir entre iniciar Windows 98 o hacerlo en Windows XP.

Existen otros cargadores que permiten arrancar entre distintos sistemas operativos aunque todos no sean de Microsoft, suelen llamarse bootloaders en inglés o gestores de arranque porque permiten seleccionar el sistema operativo que se iniciará.

Los más conocidos son el grub y lilo, que funcionan con cualquier distribución de linux, es decir, le permiten poner en marcha alguna versión del sistema operativo linux u otros operativos, como puedan ser las diferentes versiones de Windows (Vista, XP, Server 2003, etcétera).

Normalmente estos gestores muestran un menú para seleccionar el sistema operativo y permiten poner contraseña para que no se pueda iniciar el mismo si no se conoce. Esto añade un elemento de seguridad adicional.

Si el ordenador en cuestión está configurado en la BIOS para poder arrancar desde disquete, y no tiene configurada una password en bios para iniciarse, podemos borrar o sobreescribir la configuración de lilo y grub para que no pidan password al iniciar.

Por ello es aconsejable que no permitamos en la bios el arranque desde cd o disquete. Cuando haga falta ya cambiaremos este parámetro (por ejemplo, para hacer las copias de seguridad).

7.1.3. Syskey.

Si emplea Windows 2000, XP o Vista, dispone de la utilidad Syskey. Al arrancar Windows, y antes de que aparezca el escritorio o se le pregunte el login y password con el que desea iniciar sesión, se le pedirá una contraseña. Esta contraseña se emplea para cifrar y descifrar todos los pares login y password que Windows tiene por cada usuario.

7.1.4. El sistema de autenticación.

Tras arrancar Windows o Linux, normalmente deberá iniciar sesión con un determinado usuario y password. Este sistema le protege de un acceso no autorizado a su escritorio, su email, y demás archivos y documentos.

Existen herramientas que permiten descifrar los passwords de Windows por fuerza bruta. En cualquier caso y para obtener la información inicial que permite hacer esto, es necesario ser administrador del sistema, por lo que no debe otorgar a nadie ese rol.

7.2. Protección del email

La mayoría de los usuarios emplea Outlook Express para leer el correo y buena parte de ellos, no saben donde se almacena su correo dentro del disco duro, ni las contraseñas, ni la agenda de contactos.

No es culpa nuestra no saberlo. De hecho es bastante difícil localizar los ficheros que almacenan todo nuestro email. Sin embargo existen programas sencillos y potentes que pueden localizar ambas cosas, como el Outlook Express Identity Identifier. Y disponemos de scripts para reubicar la agenda en localizaciones más sencillas como alguno de éstos. Y desde luego disponemos de herramientas como ésta, para hacer una copia de seguridad completa de todo nuestro correo, agenda, configuración de cuentas de email, etcétera sin mayores complicaciones.

Idealmente el directorio donde almacenamos todo nuestro correo debería estar en una unidad cifrada como luego veremos, pero al menos de momento, con estas herramientas podríamos asegurarnos una copia de seguridad para caso de emergencia.

Tampoco deberíamos almacenar en el Outlook Express nuestras contraseñas de correo, ya que son fácilmente descubribles. Si tenemos alguna duda, siempre queda la posibilidad de ejecutar esta herramienta para comprobarlo.

Si no usamos el Outlook Express sino su alternativa más conocida, el Mozilla Thunderbird, ya sabéis que las passwords de las cuentas de correo puede almacenarse, pero cifrada mediante otra contraseña que solo nosotros conocemos.

El correo sigue siendo accesible, pero al menos tenemos una mayor capacidad para proteger las contraseñas. Existe una utilidad llamada MozBackup que permite llevar a cabo una copia de seguridad de cuentas, configuración, passwords de correo, los emails, etcétera. (Es mejor emplearlo en inglés, la traducción al castellano es pésima).

7.3. Protección / cifrado de archivos

7.3.1. Cifrado mediante EFS.

EFS es el sistema de cifrado de archivos incorporado por Microsoft en Windows 2000 y XP. Este sistema de protección permite cifrar los archivos o carpetas deseados para que otros usuarios que no sean el legítimo no puedan acceder a datos confidenciales.

Como restricciones para emplearlo tenemos las siguientes:

- Solamente es aplicable a sistemas de archivos que empleen NTFS, y no FAT32 o FAT.
- La versión de Windows XP conocida como Windows XP Home Edition no dispone de la tecnología EFS de cifrado.
- EFS no puede aplicarse a archivos comprimidos.
- Los archivos que están en la carpeta donde está instalado Windows, y aquellos otros que estén marcados como archivos de sistema no pueden ser cifrados (por razones evidentes).
- Si aplicamos la técnica de cifrado a una carpeta, podremos decidir si se aplicará a los archivos que se creen directamente dentro, o también a las subcarpetas y archivos que puedan contener éstas.

Para cifrar los contenidos del disco duro (archivos y carpetas) es necesario disponer de un certificado. Si lo perdemos, o si reinstalamos el sistema operativo sin salvaguardarlo, aunque tengamos copia de los datos será imposible recuperarlos (abrirlos o leer su contenido). Para evitar este tipo de problemas, el certificado con el que hemos cifrado las carpetas o documentos puede y debe ser exportado (a un disquete, por ejemplo) y protegido. Al exportarlo, el propio Windows nos pedirá una clave de

cifrado si exportamos la parte privada del certificado (en caso de exportar solamente la parte pública no es necesario).

Un certificado consta de dos partes: la parte privada, que es la clave que empleamos para descifrar nuestros documentos; y la parte pública, que es la empleada para cifrarlos.

Si alguien poseyera nuestra parte pública podría cifrar documentos, pero solo nosotros con la parte privada podríamos descifrarlos.

Como no es aceptable que la pérdida del certificado por parte de un usuario deje inaccesibles para siempre todos sus documentos cifrados, aparece la figura de los agentes de recuperación, es decir, personas capaces de recuperar los datos de aquellos usuarios que hayan perdido su certificado y no puedan acceder a sus datos. En una empresa, donde existe un dominio, esto se hace mediante el administrador del dominio, que es la única persona autorizada por defecto a recuperar los archivos cifrados. Puede autorizarse a otras personas, como también es posible desautorizar al administrador. En cualquier caso, es importante que exista al menos un agente de recuperación.

En un entorno doméstico, no existe la figura del agente de recuperación por defecto, pero puede crearse uno manualmente.

Para cifrar una carpeta o archivo, abriremos el menú contextual estando sobre él, y elegiremos propiedades. En la pestaña general, pulsaremos en el botón de Opciones avanzadas y marcaremos la casilla de “Cifrar contenido”. Nos preguntará, en caso de que se trate de una carpeta, si deseamos cifrar solo el contenido del primer nivel o todos los archivos y subcarpetas que pueda contener.

El resultado será un archivo o carpeta verde, indicando que está cifrado; frente al típico color azul que muestran las carpetas y archivos comprimidos.

La primera vez que cifremos un archivo o carpeta, se generará un certificado en caso de que no lo tuviéramos. El certificado se puede exportar, y si incluye la parte pública y la privada, será necesario protegerlo con una contraseña que pedirá el propio sistema operativo.

Es posible añadir los certificados de más usuarios a un archivo (no así a una carpeta) para que puedan acceder también al mismo.

Un artículo muy completo sobre EFS en castellano puede ser leído aquí.

Decir que la seguridad de EFS se basa en el algoritmos de encriptación DES de 128 bits (40 bits fuera de EEUU). Este algoritmo no es muy seguro, y es posible desencriptar los archivos mediante las herramientas adecuadas.

En este artículo, podemos ver otros fallos de seguridad conocidos en la manera de operar con EFS y como superarlos.

Nota: Windows 2000 y XP emplean DES para cifrar los archivos. Pero a partir de Windows XP SP1 y Windows 2003, se emplea AES de 256 bits por defecto. Si cifras

archivos o carpetas en Windows 2003 o XP con SP1 o posterior, Windows 2000 o XP no podrán descifrarlos. Puedes leer más sobre el tema aquí.

7.3.2. Compresores de archivos.

La forma más sencilla de hacer una copia de seguridad es reunir todos los archivos y carpetas en un solo archivo comprimido y si es posible, cifrado.

Con ello se consigue optimizar el espacio que ocupa la copia de seguridad, aunque se dificulta el acceso a los archivos individuales.

Ejemplos de programas conocidos capaces de hacer esto son:

- Winzip
- Winrar
- Filzip
- 7zip
- IZArc

Existen muchos más compresores, como podemos ver en:

- http://www.donationcoder.com/Reviews/Archive/ArchiveTools/index.html.

Aunque muchos de ellos permiten crear archivos zip protegidos con el algoritmo de cifrado pkzip 2.0, cada vez son más los que trabajan con AES por ser más seguro. Algunos de los compresores tienen formatos de compresión propios, pero normalmente incompatibles entre sí. Solamente el formato zip es reconocido por todos ellos.

Los más rápidos son Winzip y Winrar, aunque no siempre son los que mejor comprimen. Ambos son soluciones de pago (entre 30 y 45 euros aprox. según versión y producto).

Si deseamos emplear soluciones gratuitas, podemos probar Filzip, 7zip o IZArc. El sistema de cifrado de los archivos zip (2.0) ha quedado superado por AES, en sus versiones de 128, 192 y 256 bits.

Es aconsejable que el compresor utilizado permita crear ejecutables auto extraíbles, es decir, que los archivos comprimidos puedan descomprimirse y descifrarse solos, sin necesidad del programa compresor que lo creó. Esto nos permitirá descomprimirlos en cualquier ordenador sin necesidad de instalar nada.

Programa	Versión	Zip 2.0	AES-128	AES-192	AES-256	SFX
Winzip	11.1	X	X		X	X
Winrar	3.70	X	X		X	X
Filzip	3.06		X			X
7zip	4.45				X	X
IZArc	3.7	X	X	X	X	X

7.3.3. LockNote

El programa Steganos Locknote, nos permite escribir documentos en forma de archivos ejecutables con la extensión ".exe". La idea es que el archivo ejecutable incluye un editor de textos parecido al notepad de windows además del propio documento. Con Locknote podemos cifrar el documento incluido dentro del archivo ejecutable con el algoritmo AES de 256 bits.

De esta forma tenemos archivos de texto cifrados que podemos desplazar de un ordenador a otro, con capacidad de autoedición (modificación del archivo y de la password de cifrado del mismo) sin necesidad de instalar nada adicional en el ordenador donde estemos.

Para evitar que el archivo pueda resultar demasiado grande, el ejecutable original de Locknote, antes de incluirle dentro documentos (cifrados o no) es menor de 300 Kb. La versión actual de Locknote es la 1.0.3. Se trata de un producto gratuito y descargable desde aquí. Para más información podemos visitar la web http://locknote.steganos.com.

7.3.4. AxCrypt

Es una herramienta para cifrar/descifrar archivos o carpetas con el algoritmo AES de 128 bits. Si me sitúo sobre un archivo y pulso el botón derecho del ratón me dará la opción de cifrarlo; si ya estaba cifrado, me permitirá descifrarlo. Si se trata de una carpeta, me permitirá cifrar todos los archivos y subcarpetas que tiene dentro recursivamente o en caso contrario, descifrarlos. También funciona si selecciono un grupo de archivos sueltos de una carpeta e intento cifrarlos.

La primera vez que quiera cifrar cualquier objeto me pedirá una password. Si le pido que la recuerde, no volverá a pedírmela cuando cifre otro posteriormente. Si la indico como clave por defecto, cualquier archivo que intente cifrar o descifrar intentará aplicarle la password anterior.

Puedo cifrar un archivo mediante una password y también mediante una clave generada y contenida en un archivo, o mediante ambas.

Supongamos que cifro un documento con la extensión txt. AxCrypt añadirá a la extensión txt una posterior, la de axx (axcrypt). Cuando haga doble click sobre el archivo, AxCrypt lo descifrará (pidiendo la password si es necesario) y dejará el archivo txt en una ubicación temporal. Luego buscará qué programa está asociado a la extensión txt y lo llamará para que abra el documento (normalmente el notepad). Cuando terminemos de manipular el documento y cerremos el notepad, AxCrypt cifrara el archivo y sobreescribirá con él al original. Luego sobreescribirá el archivo sin cifrar de la carpeta temporal para que no pueda ser recuperado.

En caso de que durante el proceso Axcrypt se colgara, la próxima vez que lo empleemos para cifrar o descifrar archivos, borrará todos los temporales que hayan sido creados por él mediante un proceso de sobreescritura.

La última versión es 1.6.3. Y podemos descargarla aquí.

7.3.5. BestCrypt

Es la primera aplicación que veremos para crear unidades virtuales cifradas en el disco duro y donde almacenaremos nuestros documentos.

Es un producto comercial de pago, aunque no muy caro (sobre 60 euros). Su principal ventaja es que dispone de versión para linux y Windows, con lo que puede funcionar en una gran variedad de sistemas: Fedora Core, Redhat Enterprise, Madrake Linux, Windows 98, Windows ME, Windows 2000, XP, etcétera; lo que nos permitirá crear una unidad cifrada y accederla desde distintos sistemas operativos.

Una vez tenemos claro el volumen de datos que vamos a almacenar en la unidad virtual, crearemos la misma mediante la opción de “Crear Container” que es como la mayoría de estos programas conoce y nombra a las unidades virtuales cifradas.

Decidiremos la ubicación de la nueva unidad, el algoritmo de cifrado, la password de protección del container y el tamaño. También especificaremos la letra de unidad que se le asignará. Si por ejemplo tenemos el sistema operativo en la unidad C y el DVD en la unidad D, podemos asignarle una letra desde la E a la Z.

Bestcrypt tiene opciones para desmontar automáticamente la unidad tras cierto tiempo de inactividad, al cerrar sesión o mediante combinaciones o atajos rápidos de teclado. Además protege la unidad virtual contra el borrado completo de la misma de forma accidental. Todo esto son medidas de seguridad muy útiles que no todos los programas que veremos tienen.

También recuerda las últimas unidades cifradas abiertas y permite preguntar por un password por unidad al iniciar sesión, montándolas así automáticamente. El icono de la bandeja de entrada nos permite acceder al panel principal de opciones, montar o desmontar las unidades cifradas habituales, desmontarlas todas rápidamente, etcétera.

Al intentar desmontar las unidades, Bestcrypt comprobará si están siendo usadas, en cuyo caso, nos preguntará si deseamos continuar con el cierre a pesar de que pueden perderse datos. El desmontaje automático por timeout no se ejecutará si detecta que algún programa está accediendo a la unidad.

Es posible añadir nuevas contraseñas al container, de modo que podamos emplear otra para acceder a él. Si deseamos desestimar la antigua, la única manera de hacerlo es crear un container nuevo, con una nueva clave, y copiar todo el contenido del viejo container al nuevo, borrando el contenedor viejo.

También es posible montar un contenedor como de solo lectura para que la información que contiene no pueda ser cambiada o borrada.

Además permite la creación de contenedores virtuales ocultos dentro de otros contenedores virtuales logrando así un nivel más alto de seguridad y dispone de una herramienta para cifrar el archivo de paginación de windows.

Suponiendo que creemos muchos contenedores por temáticas, empresas, clientes o servicios, Bestcrypt permite organizarlos en grupos para facilitar su gestión.

Le acompaña una utilidad, BCWipe, para borrar archivos del disco o sobreescribir áreas aparentemente libres del disco duro. Se utiliza para sobreescribir espacios donde antes hubo información y se pretende que todo sea sobrescrito para que nunca pueda recuperarse, o al menos para dificultarse el proceso.

También permite especificar si a un contenedor podrán acceder todos los usuarios o solamente el actual en caso de que el mismo se almacene en el disco duro por ejemplo, y no en un disco extraíble.

Podemos obtenerlo aquí para probarlo o comprarlo.

Nota: La versión probada de Bestcrypt es la 7.20, la 8.0 está en fase beta, aunque promete mejoras en cuanto al acceso a contenedores, algoritmos de cifrado, compatibilidad con Windows Vista, puntos de montaje, etcétera.

7.3.6. TrueCrypt

Disponible en http://www.truecrypt.org/, es un producto bajo licencia open source. Tiene funcionalidad similar a la de BestCrypt, pero es gratuito.

Cifra unidades virtuales, o dispositivos completos, aunque se recomienda emplear unidades virtuales. Permite el uso de volúmenes ocultos y dispone de varios algoritmos de cifrado.

Es capaz de desmontar las unidades virtuales tras cierto tiempo, al entrar el equipo en ahorro de energía o activarse el protector de pantalla.

Permite emplear keyfiles, además de passwords como contraseña de acceso al contenedor. Incluso permite emplear varios archivos como keyfile, sin importar si son archivos mp3, wav, de texto o binarios. Todo ello robustece la seguridad frente a keyloggers instalados sobre el sistema.

Dispone de atajos de teclado personalizables para distintas acciones y recientemente ha aparecido una versión para linux.

Dispone de un modo portable para poder emplearlo sobre un dispositivo extraíble como un lápiz USB sin necesidad de instalarlo, podemos ver como prepararlo aquí, y aquí.

Su desarrollo estuvo parado algún tiempo (o al menos no aparecían versiones nuevas). Sin embargo con las últimas mejoras, no tiene nada que envidiar a Bestcrypt. La última es la 4.3 y soporta incluso Windows Vista.

7.3.7. FreeOTFE

En poco menos de un año, ha aparecido otra alternativa a TrueCrypt que ha evolucionado muy aprisa. Destaca por su gran versatilidad, potencia y posibilidades, aunque no es tan sencillo de manejar como los otros dos programas anteriores.

FreeOTFE dispone de más algoritmos de cifrado que los productos anteriores, de un modo portable, es compatible con unidades cifradas virtuales creadas bajo Linux con cryptoloop y dm-crypt, dispone de volúmenes ocultos, puede cifrar particiones o container, dispone de atajos de teclado y permite añadirle módulos de desarrollo propios.

La última versión es la 2.0 y se encuentra en http://www.freeotfe.org y dispone de una interfaz gráfica adicional conocida como Secure Tray Util.

Dispone de versión para ordenador y PDA. El código fuente está disponible y es gratuita, para uso público.

7.3.8. PGPDisk

Otra herramienta gratuita y similar a TrueCrypt era PGPDisk, disponible en http://www.pgpi.org/products/pgpdisk/, sin embargo, el programa en cuestión ha dejado de ser gratuito y las versione posteriores son de pago.

7.3.9. Envío de archivos por email

En ocasiones, desearemos enviar archivos o documentos importantes y privados a alguien por Internet, esto puede hacerse juntándolos en un archivo zip comprimido y con password. Sin embargo, mucha gente no confía en el formato zip porque piensa que al ser muy empleado, puede ser objetivo de hackers o crackers.

Existen otras alternativas. Una, sería crear una unidad virtual con Truecrypt para enviarla como archivo adjunto, o formar un zip comprimido que luego podría ser cifrado con herramientas como AxCrypt o File Vault. Ambos permiten que el fichero, una vez recibido, se autodesencripte y se descomprima en un directorio con todo su contenido original, es decir, que el receptor no necesita tener estos programas instalados, solo conocer la password. Sin embargo, enviar estos archivos como auto-desencriptables, implica que son ejecutables, y muchos servidores de correo en Internet o en intranets, borran los archivos .exe en cuanto los detectan como adjuntos, ya que a veces son causa de infecciones víricas.

Aun así merece la pena emplear estos programas para cifrar archivos o zips y enviarlos de forma segura por email.

7.4. Dónde almacenar las passwords.

Muchas veces necesitamos recordar infinidad de passwords, pero no sabemos donde almacenarlas. A todos nos gustaría recordar una sola password y disponer de un lugar donde poder almacenar las demás, que estarían disponibles a partir de la password original.

Si además pudiéramos clasificar estas passwords por tareas, actividades o agruparlas de algún modo sería perfecto. Estaría bien que pudieras acceder a la clave oportuna, copiarla en el portapapeles, pegarla en el cuadro de autenticación correspondiente y borrarla posteriormente del portapapeles; todo claro está, sin que se viera por pantalla para que otras personas no pudieran anotarla o recordarla.

La base de datos con contraseñas tendría que estar cifrada para que no pudiera ser accedida sin necesidad de emplear el programa que las guarda.

Pues existen un par de programas que hacen todo esto y un poco más, y son:

- Password Safe
- Keepass

Capítulo 8. Dominios y redes corporativas

8.1. Introducción

Ante el avance imparable de las tecnologías de la información, el crecimiento de las empresas y las organizaciones, y la rotación del personal laboral, se hace necesario controlar más que nunca cómo utilizan los empleados su tiempo durante la jornada laboral, qué usos dan a los recursos informáticos y quienes son los usuarios habituales de estos sistemas.

Estas empresas suelen centralizar el control y seguridad de la información que poseen, la salida a Internet, los backups, los servicios de impresión, las actualizaciones de antivirus y sistemas operativos, el correo electrónico, etcétera.

Es por esto que la funcionalidad se organiza en torno a servicios, y cada servicio se compone de recursos que a su vez se administran por personal (informático o no) cualificado.

Por ejemplo, el correo electrónico, puede almacenarse o no en un servidor, o puede estar en cada ordenador, almacenado en su disco duro local, pero para el envío y recepción del correo, independientemente de donde se almacene, será necesario un servidor, que probablemente registrará quien envió qué y cuando lo hizo.

Para almacenar los datos de la empresa, se emplearan servidores corporativos de archivos o bases de datos que estarán almacenadas en algún sitio, cuyos logs o sistemas de registro dirán con precisión qué archivos se abrieron, desde qué ordenador se hizo y cuando sucedió, o quien borró qué archivos.

Las copias de seguridad también estarán centralizadas en uno o varios servidores con hardware redundante y dispositivos masivos de almacenamiento.

Si los ordenadores tienen conexión a Internet, seguramente pasarán a través de un proxy o firewall corporativo que registrará todas las comunicaciones, el origen, el destino, el protocolo empleado y el tipo de información enviada, además del tamaño.

Si la empresa es lo suficientemente grande, existirá un servidor corporativo de antivirus donde se registrará qué pcs se infectaron recientemente, cuales son los que suelen infectarse más, cuales fueron los virus causantes reconocidos y qué ordenadores presentan la última versión del antivirus y cuales no se han actualizado aún.

En definitiva, organizar las necesidades de la empresa como servicios y asignar unos recursos concretos para ello, permite que controlando el servidor que gestiona ese servicio, podamos auditar todo lo que sucede en torno a él.

A este proceso en el cual se acumula información de cómo se está empleando cada servicio en cada momento, se le llama auditoría. Existen empresas que no la

activan porque consume o puede consumir demasiados recursos, porque desconocen que pueden hacerlo, o simplemente porque no disponen del tiempo o personal para analizarla y detectar cualquier anomalía producida. Otras empresas la acumulan y solo la estudian en caso de que se produzca algún incidente.

Con la auditoría podemos conocer todos los detalles de cómo, cuando y quien. Eso supone que en las empresas, la privacidad de nuestros actos puede ser nula y que por tanto debemos ir con cuidado a la hora de utilizar estos servicios para nuestro provecho particular, porque esa información puede ser capturada por las personas que controlan el sistema informático y ser causa de despido, dar lugar a transacciones fraudulentas con nuestros datos bancarios o de crédito, o provocar que cuestiones que se comentaron de manera privada sean conocidas por todos dentro de la empresa.

8.2. El control del administrador del dominio.

En la mayor parte de los sistemas operativos, los usuarios no disponen de privilegios para hacer cualquier cosa sobre el sistema. Eso quiere decir que existe la figura de un superusuario conocido como administrador o root capaz de acceder a nuestro ordenador con total impunidad que es quien instala programas, lo configura, etcétera. Como los datos que se almacenan en nuestro trabajo se supone que son propiedad de la empresa, y el administrador o personal que administra todos los ordenadores de la red se supone que goza de la confianza de la empresa, puede fisgonear en nuestro disco duro sin necesidad de acercarse físicamente a nuestro ordenador y sin que seamos conscientes de ello.

Más aun, normalmente puede incluso suplantarnos, modificar registros, pues tiene el control total del sistema o sistemas a su cargo. Esto significa que no disponemos de privacidad real en este entorno.

8.3. Las GPOs o directivas.

Incluso en el caso en que gestionemos nuestro ordenador como consideremos oportuno y tengamos privilegios de administrador en el mismo, estos pueden ser cancelados. Nuestra password de acceso al sistema siempre puede averiguarse con más o menos esfuerzo, o en el peor caso, puede ser cambiada. Y si hemos cifrado nuestros datos con credenciales o certificados propios de la empresa o derivados de ellos, el administrador podrá descifrarlos. Este es el caso por defecto del sistema de seguridad EFS o cifrado del sistema de archivos que Windows incorpora, donde el administrador por defecto es el único capaz de descifrar los datos de todos los ordenadores de la empresa.

Además configuraciones específicas que apliquemos al ordenador para que estas cosas no sucedan siempre podrán ser sobrescritas por el administrador, dados los privilegios de que disponen en la red. Normalmente lo harán mediante directivas, permisos especiales o scripts que les permitirán acceder a todo aquello que había sido denegado o prohibido.

8.4. Los recursos compartidos.

Los recursos compartidos en nuestro pc suelen ser fuente de problemas. Compartimos una carpeta para que alguien acceda, y a la semana siguiente, cuando otra persona necesita un determinado documento lo introducimos en la misma carpeta, y le damos también a ella permisos de acceso. Nos olvidamos que ahora todo lo que contiene está a disposición de dos personas. Poco a poco se convierte en un recurso "para todo" donde dejamos información para personas distintas las cuales no deberían tener acceso a la totalidad.

Le ponemos una contraseña sencilla para que todos accedan y al final cualquiera puede entrar. Pongamos un ejemplo típico y veremos lo que pasa.

La persona A comparte un recurso y le pone de contraseña "nuez". La persona B accede a este recurso compartido y coge y deja otros documentos. Al cabo de un tiempo se une la persona C al grupo, y todos siguen usando el recurso compartido de A. Un día A no va a trabajar o su ordenador se avería y la carpeta compartida de A no está disponible. Entonces llega B y crea su propia carpeta compartida. C pregunta por la contraseña. B para hacerlo fácil le envía un email diciendo que es la de "siempre", es decir, "nuez". Al cabo de un tiempo, A se va de la empresa y D hereda su ordenador. A le dice que la password del recurso o carpeta compartida es "nuez". Para entonces B y C emplean el recurso que creó B. Un día A prueba a acceder a la carpeta compartida de B y emplea la única contraseña que conoce, "nuez". Naturalmente la información entre B y C no era para D, en quien aún no confían como en A, pero D tiene acceso a información que no le corresponde, porque de hecho D no tiene ahora las mismas funciones que A.

Los recursos compartidos deben emplearse para tareas concretas y no reutilizarse. Tampoco deben reutilizarse las contraseñas, ni enviarse por correo o ser apuntadas en papel. Es importante que sean largas. Existen programas capaces de averiguarlas por fuerza bruta y empleo de diccionarios.

Incluso existen aplicaciones capaces de rastrear la red para emitir una lista de ordenadores que comparten recursos y los nombres de los mismos.

8.5. Programas de control residentes.

Existen aplicaciones que nos permiten ver en un momento dado lo que está haciendo determinado usuario en su pantalla, lo que está escribiendo, los procesos que tiene abiertos, las direcciones web que está visitando, e incluso realizar capturas de pantalla periódicas, que es lo mismo que estar delante de su monitor. Incluso se puede capturar y almacenar todo lo que teclea en su ordenador, o cuando inicia o cierra sesión para saber a qué hora llega al trabajo o termina.

8.6. POP e IMAP.

El correo electrónico o email puede almacenarse en nuestro ordenador, es decir, de forma local o en un servidor central. En el primer caso significa que el correo utiliza el protocolo pop; en el segundo, estaremos empleando IMAP.

El hecho de que nuestro correo se almacene en un servidor imap implica que los administradores de esos servidores pueden acceder a él. Existen sentencias judiciales que dictan que el email interno de la empresa no se considera privado porque se supone que no se emplea para uso personal, solamente laboral, o que al menos debería ser así.

En el caso de que empleemos correo basado en el protocolo pop, queda almacenado en nuestro propio pc. De nuevo los administradores o personal informático de la empresa pueden tener acceso a todo el correo sin mayores complicaciones.

En definitiva, y aunque no suele hacerse, e independientemente del programa de correo empleado, nuestro correo siempre puede ser escudriñado por el personal informático o por el gerente de la empresa. Todo ello, hace que debamos ser cautos en la manera en que lo empleamos, lo que enviamos o lo que decimos. Y deberíamos no enviar a través de él, correos de carácter personal o que puedan ponernos en alguna clase de apuro en caso de conocerse el contenido del mismo.

8.7. Las sesiones abiertas.

Del mismo modo, deberíamos bloquear la sesión en nuestro ordenador si nos ausentamos del puesto de trabajo. Y deberíamos tener el protector de pantalla activo, para que tras cinco minutos de inactividad, el ordenador quede bloqueado.

No debemos olvidar, que con el ordenador encendido, y la sesión iniciada con nuestro login y password, somos responsables de lo que se haga con el ordenador, ya que aparentemente somos nosotros los que estamos sentados frente a él.

8.8. El origen falso de los emails.

Es posible falsificar el origen de un email, de tal modo que parezca venir de la persona que viene incluida en el campo remitente. Sin embargo, lo que no es posible falsificar, es la IP del ordenador desde el cual fue enviado, pues es una información que no envía el ordenador que transmite el correo, sino que incluye el propio servidor que recibe el correo para volverlo a enviar a su destinatario.

Mirando el código fuente del correo es posible verificar si procede o no de quien dice venir. Aun así, y ante cualquier duda sobre la procedencia de un email, siempre es buena idea acercarse físicamente a la persona que se supone que lo ha enviado para cerciorarnos, no sea que alguien nos esté tendiendo una trampa o actuando de mala fe.

8.9. Servicios y tráfico.

Del mismo modo que es posible que los administradores escudriñen dentro del disco de los ordenadores, es posible también que comprueben que puertos tienen abiertos y cuanto tráfico se envía o recibe desde ellos.

Existen herramientas que permiten ver los servicios que oferta nuestro ordenador a los demás ordenadores de la red. Por ejemplo, una de ellas es nmap. Si la citada herramienta rastrea nuestro pc y encuentra disponible el puerto 80, normalmente es porque nuestro pc tiene instalado un servidor web y es posible acceder a él desde el navegador.

Si tenemos abierto el puerto 22, es porque admitimos conexiones remotas por ssh, el equivalente seguro de telnet. Si está abierto el puerto 123, es porque nuestro pc tiene instalado un servidor de news.

En definitiva que cada puerto se corresponde a un servicio que el ordenador presta o puede prestar a la comunidad. Existen puertos dedicados a autentificar usuarios, a compartir archivos, a imprimir, etcétera.

Normalmente no solemos cambiar el puerto por defecto para prestar esos servicios, lo que hace que sea fácil conocer que servicios tenemos activos.

Naturalmente servicios como el eMule o Kazza también tienen puertos concretos que emplean para la transferencia de archivos.

Si la empresa tiene todos sus ordenadores conectados a la red, normalmente mediante switches, pueden saber cuantos datos diarios, semanales, mensuales, etcétera envía nuestro ordenador.

Si los demás envían 100 Mb al mes, y nuestro pc cuadruplica esa cifra, es probable que investiguen si estamos descargando música, compartiendo archivos, películas o tenemos servicios internos no permitidos como servidores ftp o web propios.

Todo ello de nuevo apunta a que no debemos saltarnos las políticas internas en cuanto a qué servicios están permitidos en nuestra oficina y cuales no deberíamos instalar o utilizar.

Evidentemente puede resultar sospechoso que nuestro pc tenga un gran tráfico por la noche, cuando en teoría estamos durmiendo en nuestra casa. Aunque todo este tipo de comportamientos anómalos no suelen ser revisados hasta que alguien se queja del mal funcionamiento de Internet, de la red interna de la empresa, etcétera; es decir, hasta que nuestros excesos afectan a la operativa diaria de la empresa.

Capítulo 9. Recuperación de datos

9.1. Introducción

Son muchas las veces a lo largo de nuestra vida que tiramos algo que después hubiéramos necesitado. En informática, borramos archivos o los modificamos para darnos cuenta posteriormente de que eran más necesarios de lo que pensábamos.

En el mejor de los casos tenemos una copia de seguridad a mano para recuperarlo, pero a veces está desfasada o no sabemos donde está, o peor aún, descubrimos para nuestra sorpresa que no podemos leer el CD donde se encuentra, o que en esa copia tampoco está el archivo perdido. Es entonces cuando comprobamos que lo perdimos “hace tiempo”, pero no conservamos tantas copias de seguridad anteriores como para encontrarlo.

Los virus, los fallos del hardware, las prisas, los cuelgues en las aplicaciones en las que confiamos o el uso compartido de los datos nos vuelven muy vulnerables. Ni siquiera una gran disciplina en nuestro trabajo, ni un constante goteo de copias de seguridad nos puede proteger de perder el trabajo hecho en el día de hoy.

Desconocemos las posibilidades que pueden ofrecernos algunas aplicaciones para realizar copias de seguridad temporales de nuestros archivos, las herramientas para verificar el estado de nuestros discos duros, las herramientas de sincronización programada o las copias de seguridad automatizadas. Un dia de mucha faena nos hace obviar todas las medidas de seguridad. Pasa el tiempo, no sufrimos pérdidas de datos y vamos relajándonos poco a poco, … y es entonces cuando se produce otro incidente.

Las preguntas son varias: ¿qué podemos hacer para recuperar ese archivo que acabamos de eliminar del disco duro? ¿Existe algún modo de recuperar nuestros datos después de meses de esforzado trabajo? La peor situación se produce cuando hace meses que no hacemos copias de seguridad. Todavía existe gente que no las ha hecho nunca.

Si estamos desesperados siempre podemos recurrir a servicios profesionales, como los de Recovery Labs. Y si desde luego, si nunca hemos empleado herramientas de recuperación, no es buen momento empezar a hacerlo justo en el instante en que nos hacen más falta. Las prisas, los nervios y la falta de conocimiento en el manejo de las herramientas, son malos enemigos.

9.2. No emplear la partición donde estaban los datos originales.

Desde luego emplear herramientas de recuperación, es algo que no deberíamos hacer con el sistema operativo arrancado, porque Windows escribe en el disco continuamente, principalmente en el archivo de paginación o swapping, lo que quiere decir que si necesita ampliar la memoria virtual y escribir en disco, puede emplear el hueco dejado por el archivo o archivos que hemos borrado erróneamente, lo cual lo hará irrecuperable.

Del mismo modo, los archivos que podamos recuperar deberemos guardarlos en otro medio distinto a aquel donde están los archivos perdidos. En caso contrario, podemos acabar sobrescribiendo lo que aun nos queda por recuperar por los archivos recién recuperados o por el propio archivo de paginación de Windows (por esto es importante que el archivo de paginación de Windows tenga el tamaño adecuado).

9.3. Herramientas de recuperación de archivos borrados.

9.3.1. PC Inspector File Recovery.

Disponible en http://www.pcinspector.de/file_recovery/es/welcome.htm. Es freeware y permite recuperar archivos incluso cuando se han perdido las referencias a ellos en la estructura de del sistema de archivos y la tabla de localización de los mismos está dañada. Opera en sistemas de archivos FAT (12/16/32 bits) y NTFS.

Permite recuperar archivos recorriendo la estructura lógica del sistema de archivos o realizando búsquedas por el disco duro físico, indicando para ello el sector de comienzo y de fin.

Admite criterios de búsqueda, como archivos con determinada extensión y que contienen determinado texto en su interior.

El programa dispone de varios idiomas, entre ellos el español.

Su equivalente para recuperar fotos y elementos multimedia de memorias Flash, Memory Stick, SmartMedia, SD, XD y otros medios es PC Inspector Smart Recovery.

9.3.2. E-rol

Sistema de recuperación de archivos gratuito puesto por Recovery Labs en Internet, accesible desde la dirección http://www.e-rol.com/, y que permite recuperar archivos o datos del disco duro mientras estamos conectados a Internet de forma totalmente gratuita.

Solamente funciona sobre NTFS y es necesario visitar la página empleando Internet Explorer, pues se instala en el sistema a través de un componente ActiveX.

Podemos ver más información sobre este software de Recovery Labs en el artículo de vnunet.

Nos permite ver todo el sistema de archivos completo o solo los archivos borrados. La ventaja de este sistema es que no es necesario instalar ninguna aplicación en el ordenador (aunque el componente ActiveX en el disco duro ocupa espacio y supone un pequeño riesgo de que sobrescriba alguno de los archivos que deseamos recuperar).

Admite búsqueda dentro de archivos por contenido como PC Inspector. Y es capaz de determinar que porcentaje del archivo está intacto y qué porcentaje está dañado o perdido. Así podemos decidir si merece la pena recuperarlo o no.

9.3.3. Soft Perfect File Recovery

Destaca por su extrema sencillez, permite recuperar archivos por unidades lógicas o particiones y no rastreando por el disco duro físico. Solamente permite recuperar archivos en perfecto estado, de los demás no da indicaciones. Lo mejor, además de ser gratuito es su sencillez, su tamaño, que no necesita instalación y que recupera archivos tanto en NTFS como FAT.

Podemos leer más sobre él en http://www.softperfect.com/products/filerecovery/ y podemos descargarlo junto con otras muchas herramientas desde la página de descargas de Soft Perfect.

9.3.4. Undelete Plus

Como el anterior, permite recuperar archivos fácilmente, es gratuito también y puede utilizarse la versión que se instala y dispone de documentación y la versión que se compone de un solo archivo, no se instala y no lleva la documentación, aunque el programa es bastante auto-explicativo. Disponible en http://www.undelete-plus.com/, Ocupa 1 Mb aprox. Recupera información desde particiones lógicas y no permite hacerlo desde el disco duro físico.

Podemos descargar el programa de instalación (que ocupa 1 Mb aprox.) desde http://www.downloadcenter24.com/system-utilities/undelete-plus.html o disponer directamente del ejecutable sin ayuda (que ocupa 0,5 Mb) desde http://www.undelete-plus.com/files/undelete_plus.exe.

9.3.5. Roadkils Undelete

El más pequeño de los programas para recuperar archivos. Apenas 60 Kbytes, en inglés, para FAT y NTFS. No ordena archivos y es necesario recorrer toda la lista para recuperar o buscar uno en concreto porque no tiene filtros ni posibilidad de ordenar por tamaño, extensión, etcétera.

Descargable desde http://www.roadkil.net/undelete.html como freeware.

9.3.6. Avira UnErase Personal.

Necesita instalación. Ocupa solo medio megabyte y permite recuperar archivos solo por unidades lógicas. Son apenas 4 archivos que todos juntos ocupan medio megabyte. No permite recuperar por discos físicos, solo por unidades lógicas y tampoco es muy cómodo para hacer búsquedas.

Se puede descargar aquí.

9.3.7. FreeUndelete.

Poco más de 1 Mb, búsqueda por unidades lógicas, permite filtros, opera con FAT y NTFS como sistema de archivos.

Puedes descargarlo aquí.

9.3.8. Otros que no aportan novedades sobre los anteriores.

- ADRC Data Recovery Software Tools.

9.3.9. Listas de herramientas de recuperación de archivos.

Podremos buscar siempre herramientas de recuperación de archivos freeware en varias webs que mantienen listados al respecto:

- http://www.thefreecountry.com/utilities/datarecovery.shtml
- http://lifehacker.com/software/lifehacker-top-10/lh-top-10--free-computer-system-recovery-tools-251903.php.
- http://www.freebyte.com/filediskutils/#datarecovery

9.4. Recuperación de archivos dañados.

Para recuperar archivos con formatos concretos, que han quedados parcialmente dañados o corruptos existen menos aplicaciones que para recuperar archivos borrados. De todas formas si el archivo es lo suficientemente importante y ha quedado corrompido, lo más aconsejable es recurrir a servicios profesionales como los de Easy Recovery o los de Recoveronix.

9.5. Recuperación de archivos comprimidos (dañados o password perdida).

9.5.1. Winzip

Winzip es un compresor/descompresor de archivos y carpetas muy empleado para empaquetar directorios y sistemas de archivos que luego pueden almacenarse cómodamente en cds (copias de seguridad) o enviarse por email. Además permite proteger los archivos zip creados mediante contraseña y cifrarlos por distintos algoritmos.

Sin embargo, si perdemos la contraseña, nuestra única manera de recuperar el contenido del zip es emplear programas que por fuerza bruta (a base de probar miles de contraseñas por segundo) intentan averiguarla. Según la potencia del ordenador y la longitud de la clave, el proceso puede durar minutos o días. Si el algoritmo de cifrado es AES, la posibilidad de encontrar la password si es larga, o lo que es lo mismo, el número de passwords probadas por segundo decae muy drásticamente. En caso de emplear AES, la fuerza bruta puede no ser la mejor opción.

Ejemplos de herramientas para recuperar una password perdida serían:

- Zip Password Finder de Aston Soft
- Visual Zip Password Recovery de Zip Cure Co.
- Zip Password.
- Advanced Zip Password Recovery
- Advanced Archive Password Recovery
- Turbo Zip Cracker
- Atomic ZIP Password Recovery
- Otro más aquí.
- Lost Password

Herramientas para reparar archivos zip serían:

- Zip Repair
- Zip Recovery ToolBox
- Advanced Zip Repair
- Actual Zip Repair
- Zip Repair Tool
- Kernel for Zip
- Object Fix Zip
- Zip Recovery
- Recovery Toolbox for Zip

9.5.2. Winrar

Recuperación de passwords perdidas:

- Lost Password
- Rar Password Cracker
- Advanced Archive Password Recovery
- RAR Password Recovery
- Turbo Zip Cracker
- Atomic Rar Password Recovery

Recuperación de archivos dañados:

- Advanced Rar Repair
- Actual RAR Repair
- Rar Recovery Toolbox
- Rar Repair Tool
- Recovery Toolbox for RAR

9.5.3. Otros links de interés

Para archivos protegidos:

- Vagos.es
- Intelore
- Lost Password
- Accent Office Password Recovery
- Atomic Password Recovery

Para archivos dañados:

- Nucleus Technologies
- Easeus

9.6. Recuperación de cds dañados.

A pesar de que la mayoría de la gente cree que los cds y dvds pueden durar muchas décadas, lo cierto es que estos soportes ópticos dependen y mucho de las condiciones en las que son almacenados (temperatura y humedad), del desgaste de los mismos (rozaduras, rayas, suciedad), de la compatibilidad de nuestra grabadora con el sustrato del medio óptico (todos los cds y dvds no están hechos con los mismos materiales y por tanto no tienen las mismas propiedades), de la velocidad a la que lo hayamos grabado en el soporte, etcétera.

Lo cierto es que en las peores condiciones, y sin contar desperfectos físicos como roces, suciedad o ralladuras, en tan solo dos o tres años el soporte óptico puede empezar a sufrir errores de lectura, que acabaran por dejarlo en un estado inservible.

Por eso existen herramientas de recuperación de información, que intentan leer archivos, carpetas y la estructura del propio sistema de archivos desde soportes ópticos deteriorados.

Con la enorme cantidad de formatos existentes de CD y DVD, hoy en día no basta con las habilidades típicas de recuperación de archivos, sino que algunas de estas aplicaciones soportan todo tipo de formatos de video.

Herramientas para este tipo de tareas serían:

- IsoBuster, compatible con cds, dvds y Blue-Ray. Una herramienta muy potente a un precio muy económico (30 dólares).
- CDRoller, para cds y dvds. De precio similar al anterior y con muchas prestaciones.
- BadCopy Pro
- DiskInternals CD&DVD Recovery
- MultiData Rescue
- CD/DVD Diagnostic
- CD/DVD Data Recovery
- CD/DVD Data Recovery Software de Nucleus Technologies.
- Dead Disk Doctor
- inDisc Recovery
- CD Check (cds y dvds).
- Si el problema son las rayas o manchas en la superficie del medio óptico podemos recurrir a una herramienta que pulirá los discos de nuevo para que la superficie quede impoluta. Aquí hay otra.

Artículos interesantes sobre recuperación de datos en soportes ópticos:

- http://www.percontra.net/2corruptcddvdrecovery.htm

9.7. Empresas de recuperación en general.

- Ontrack
- Disk Data Recovery
- Recover Data

Capítulo 10. Destrucción de los datos en el PC

10.1. Introducción

En ocasiones deseamos tirar un PC viejo y sustituirlo por otro, o queremos cambiar el disco duro para poner uno con más capacidad. Cuando pensamos en hacer esto, normalmente traspasamos al ordenador nuevo los datos del viejo y dejamos el viejo en un rincón, por si el nuevo fallara. Conforme pasa el tiempo, y si nada negativo nos sucede, el PC antiguo va recogiendo polvo, hasta que dos años más tarde pensamos que molesta y decidimos tirarlo. Para entonces ni siquiera recordamos para qué lo usábamos antes de tener el nuevo, y pensamos que los datos que contiene ya están desfasados. Es entonces cuando lo tiramos a la basura sin más, o como mucho, formateamos el disco duro con un formato rápido considerando que es suficiente.

Aunque esta forma de actuar no suele dar mayores problemas a la mayoría de la gente, no estamos haciendo lo que deberíamos. Existen estudios que demuestran que con algo de esfuerzo y conocimientos técnicos, es posible recuperar con equipos relativamente poco sofisticados, los datos del disco duro que en principio parecen irrecuperables.

Lo peor del caso, es que no hace falta llegar tan lejos. Cualquiera con un par de herramientas de las disponibles en Internet de manera gratuita, puede recuperar archivos del disco duro que aparezcan como borrados pero que no hayan sido sobrescritos.

Como avance a esto último, todavía sería posible recuperar información a partir de restos de archivos y de hecho se han desarrollado aplicaciones forenses, como se las conoce, para escudriñar en el disco duro de máquinas que han sido atacadas por hackers y donde la información que pudiera haberse utilizado para averiguar el origen del ataque había sido borrada.

Tenemos pues dos niveles en cuanto al tipo de herramientas, las de recuperación de información borrada; y aquellas que usan técnicas más avanzadas y lentas para procesos de recuperación profesionales y más completos.

No es extraño que existan maneras de recuperar información incluso cuando el disco duro, o cualquier componente del mismo han resultado averiados. Existen empresas que se dedican precisamente a recuperar información valiosa donde se puede asumir el elevado coste de hacerlo.

En definitiva, antes de deshacernos de un disco, deberíamos asegurarnos que la información es irrecuperable. Pensemos que dañar los chips que rodean al disco no logra este propósito porque alguien con el suficiente interés y conocimiento puede conseguir que recuperen la información de los platos del interior del disco, que están sanos. Es necesario triturarlo con detalle o bien recurrir a herramientas que practiquen

técnicas de borrado intensivo sobre el disco, hasta que las probabilidades de recuperar algo en él caigan casi a cero.

Clarifiquemos antes que nada, que estos borrados no dañan el disco duro, y que de hecho, podemos borrar o destruir la información con estas herramientas, y cualquier persona a la que le regalemos o vendamos nuestro viejo ordenador, va a poder utilizar el disco sin problemas.

Herramientas que permiten este tipo de procesos serían Eraser, DBAN(Darik´s Boot and Nuke), Secure Delete o Autoclave (*). Luego podemos intentar recuperar la información para ver si realmente ha sido fulminada con herramientas como TestDisk, The Coroner's Toolkit, PC Inspector File Recovery, Restoration 2.5.14 o PC Inspector Smart Recovery (para tarjetas de memoria).

(*) El autor de Autoclave ha dejado de mantenerlo y aconseja emplear DBAN, al que considera un producto muy completo.

Evidentemente el peligro de que nuestros datos puedan ser recuperados, proviene del hecho de la necesidad de recuperar datos de gran valor que empresas o particulares han perdido en alguna ocasión y para lo que no estaban preparados adecuadamente.

Cuando pensemos en deshacernos de algún dispositivo de almacenamiento, como un lápiz USB, la memoria de una cámara de fotos (xD, Compact Flash, SmartMedia, SD), microdrives, y cualquier otro dispositivo, siempre deberemos aplicar estás técnicas, que no son exclusivas de discos duros.

En caso de que los datos almacenados hagan referencia a nuestros pacientes, clientes, datos personales o fiscales de otras personas, la Ley Orgánica de Protección de Datos nos exige que sean destruidos correctamente. No hace falta irse muy lejos para encontrar aplicaciones caseras a estas normas.

Si un amigo no se aclara con la declaración de la renta, y se la hacemos en nuestro ordenador, y al poco, nos deshacemos del pc, debemos garantizar que sus datos (los nuestros son decisión nuestra) no acabaran en manos de otras personas. Y debemos tomar medidas para asegurarnos de esto.

Es pues un tema legal más trascendente de lo que parece a simple vista. De hecho existe un estándar, el ISO 17799 dedicado a este tema y en concreto el punto 10.7.2 habla precisamente de la destrucción de los medios donde se almacena la información.

Formatear un disco duro por procedimientos estándar, incluso si no marcamos la casilla de borrado rápido, no garantiza que la información no pueda recuperarse. Un borrado sin sobre escritura no puede garantizar esto. No solo la sobre escritura es necesaria, sino que más pasadas normalmente producen un mayor grado de irrecuperabilidad. Existen estándares del Departamento de Defensa de los EEUU sobre estos temas, también de la OTAN y otros basados en estudios, como el de Peter Gutman.

Durante el curso veremos en acción el Darik´s Boot and Nuke y a Eraser. DBAN dispone de distintos métodos de borrado como el estándar canadiense RCMP TSSIT OPS-II, el del Departamento de Defensa de los EEUU, DoD 5220-22.M, y el considerado más seguro, el método Gutman.

10.2. Protección en Windows de datos borrados.

Cuando una aplicación en Windows 2000 o XP se inicia en el sistema operativo y reclama memoria, el sistema operativo se la proporciona. Sin embargo, la aplicación podrá usarla, pero no leer lo que había en ella antes de que le fuera entregada para su uso. Esto es porque Windows 2000 y XP cumplen la normativa de seguridad C2.

Este mismo procedimiento que se aplica a la memoria RAM o memoria temporal, se aplica también al espacio en disco. Cuando una aplicación intenta escribir en disco, lo hace a través de Windows y no tiene acceso directo al disco duro. Así, si los bloques de información en el disco duro son por ejemplo de 4096 bytes, y el programa en cuestión escribe 4000, no tiene acceso a leer los otros 96 bytes, que contendrán información previa a que Windows asignara ese bloque. El propio Windows no permite acceder a esos datos viejos que están grabados en restos de bloques que fueron sobrescritos. Pero si arrancamos el ordenador sin usar el sistema operativo y empleamos herramientas especiales, es posible ver esas áreas y recuperar restos de información que pueden ser muy útiles.

La única forma de evitar esta actividad, es sobrescribir los finales de bloques no utilizados por las aplicaciones, del mismo modo que el resto de bloques que actualmente no se usan, pero que se usaron alguna vez y contienen información borrada.

10.3. Wiping.

Wiping es el proceso de sobrescribir un fichero o determinados bloques del disco, en ocasiones, múltiples veces, para asegurar su borrado total.

Para hacer esto, que ya no es un borrado completo, se utilizan herramientas que sobrescriben ficheros o todo el espacio vacío de un disco duro. Sin embargo, si se intenta hacer con el sistema operativo encendido, y sobretodo cuando intentamos sobrescribir bloques del disco parcialmente ocupados por el sistema operativo, éste se puede desestabilizar, lo que hace aconsejable hacerlo cuando no está activo.

Borrar un bloque que está parcialmente ocupado es sencillo. Supongamos el caso anterior, donde el bloque contiene 4096 caracteres, pero los datos solo ocupan 4000. El programa de borrado o wiping leerá el bloque de 4000 caracteres, borrará los 4096 caracteres y volverá a escribir los 4000. Sin embargo si los bloques que borramos están ocupados parcialmente por el sistema operativo, el sistema puede detectar esta actividad como sospechosa y puede intentar bloquear este mecanismo. De nuevo, es aconsejable hacerlo sin que el sistema operativo esté activo.

10.4. Otros sistemas de archivos

Existen sistemas de archivos que disponen de journaling, es decir de elementos redundantes para recuperar información del disco duro si éste sufre daños lógicos en las tablas donde se almacena la lista de bloques del disco duro que forman cada archivo.

Esto, dificulta el proceso de wiping. Además en estos sistemas de archivos, el propio sistema operativo puede realizar tareas de optimización que dificultan el seguimiento o ubicación de archivos e información de recuperación de los mismos.

La forma más cómoda de garantizar que podremos borrar todos los datos de un disco tanto en áreas libres, como ocupadas por archivos que ya no queremos conservar, es dedicar una parte del mismo a crear una unidad virtual cifrada o una partición de datos cifrada, que posteriormente, cuando deje de usarse puede ser eliminada como si se tratara de un gran fichero. Naturalmente, al borrarla de manera tradicional podría ser recuperada si antes de destruirla no hacemos un proceso de wiping. Pero aunque pudiera recuperarse, y al estar toda la información cifrada, de nada serviría recuperarla.

Es por eso que en nuestras máquinas deberíamos tener unas unidades dedicadas en exclusiva a los datos, que deberían estar cifradas y separadas de la partición o disco donde están las aplicaciones, el sistema operativo o los ficheros de swap.

Si queremos que el proceso de wiping sea completamente satisfactorio cuando borramos áreas libres o parcialmente libres de un disco duro, debemos usar sistemas de archivos que no dispongan de redundancia en la protección de los datos o de journaling, ya que podrían quedar restos de los mismos.

Por ejemplo, emplear FAT32 en Windows para los datos; o ext2 en Linux / Unix. La mejor alternativa es almacenar siempre los datos en una unidad cifrada que si luego no la necesitamos, podemos destruirla. Y emplear el proceso de wiping sobre la unidad, partición o disco donde se almacena el sistema operativo y las aplicaciones, con intención de eliminar posibles rastros de información confidencial que puedan generar esas aplicaciones o el fichero de swap del propio sistema operativo.

En definitiva, y simplificando la cuestión: De vez en cuando deberíamos programar nuestro pc para que todo el espacio del disco duro que está vacío sea sobrescrito, con la intención de que cualquier cosa que hubiera en él no pueda ser recuperada por si fuera información confidencial. Es posible que no podamos garantizar al 100% que hemos borrado todo aquello que pueda ser considerado confidencial, por eso, es buena idea, utilizar alguna herramienta cada cierto tiempo, que permita arrancar el ordenador sin emplear el sistema operativo del disco duro para hacer la misma tarea de manera más eficaz y con más garantías.

Sin embargo, hacer esto, solamente palia el problema de que muchas aplicaciones generan archivos temporales por el disco duro y el hecho de que almacenamos los datos o documentos importantes sin ninguna seguridad y en cualquier lugar del disco. Eso se puede evitar si utilizamos técnicas de cifrado, generando

unidades encriptadas virtuales que contendrán todos nuestros documentos, lo cual garantiza que ni recuperándolos, puedan ser leídos o entendidos.

Utilizar el sistema de archivos cifrado de Windows (EFS) no garantiza la seguridad de nuestros documentos. Cuando ciframos un archivo mediante EFS, se crea una copia nueva del mismo cifrada, pero el original solamente es borrado, y no sobrescrito, con lo que podría ser recuperado del disco si no es sobrescrita toda el área que ocupaba mediante alguna utilidad.

10.5. Programas de borrado de archivos

10.5.1. Sdelete.

Es una herramienta de SysInternals, disponible antes aquí, que ahora puede descargarse de la web de Microsoft aquí (Microsoft ha comprado SysInternals).

Este comando en línea permite borrar el espacio libre de un disco, o borrar archivos y directorios. Es posible seleccionar el número de pasadas de sobre escritura que deben hacerse en el disco. Trabaja desde Windows.

Es capaz de borrar toda la información, aunque no garantiza que pueda borrar el nombre de los archivos almacenados en el área libre del disco duro. Es decir, garantiza que si determinados archivos, o un área aparentemente vacía del disco, pero donde antes existían documentos, son sobrescritas por Sdelete, no podrá recuperarse la información, pero puede que sí pueda recuperarse el nombre de los archivos originales que estaban allí.

Es eficaz para borrar archivos y directorios, aunque utiliza un sistema indirecto para borrar el espacio en disco, como hacen los demás que operan con Windows encendido que no garantiza al 100% su efectividad, aunque desde SysInternals dicen que es así.

10.5.2. Eraser

Desarrollado y disponible en la web http://www.tolvanen.com/eraser/ hasta la versión 5.3, actualmente es un proyecto GPL mantenido por Garret Trant en la web http://www.heidi.ie/eraser/ y cuya última versión es la 5.8.

Funciona en todas las versiones de Windows. Le acompaña otra utilidad, el EraserD, que permite borrar el archivo de paginación arrancando para ello el ordenador con un disquete. Esto no puede hacerse desde Windows porque éste lo bloquea para su uso exclusivo y ningún programa puede acceder a él mientras Windows está arrancado.

Otra alternativa es dejar a Windows sin archivo de paginación, reiniciar el equipo y borrar el espacio vacío que hay en el disco y que antes era ocupado por el archivo de paginación. Esta opción es más tediosa, porque supone en primer lugar que

disponemos de suficiente memoria para que Windows funcione sin el archivo de paginación, y porque requiere desactivar la memoria virtual, reiniciar el pc, borrar el espacio libre del disco duro, volver a activar la memoria virtual y volver a reiniciar el pc entonces.

10.5.3. File Shredder de Tecnum Systems

File Shredder de Handy Bits es un programa que permite sobreescribir archivos y carpetas para su completa destrucción. Es posible indicar el número de pasadas, así como una combinación de teclas para abrir directamente el programa.

Dispone de una papelera virtual donde podemos dejar caer cualquier documento y carpeta y será completamente destruida (sobrescrita), sin necesidad de realizar la operación a base de emplear menús contextuales sobre cada objeto.

Está disponible en http://www.handybits.com/shredder.htm y es free para uso personal, que no empresarial.

10.6. Borrado del disco duro

10.6.1. DBAN (Darik's Boot and Nuke)

Una herramienta bastante eficaz y que soporta varios estándares para el borrado de discos duros es DBAN, esta herramienta genera un disquete de ordenador mediante el cual podemos arrancar el pc, para después seleccionar el disco duro que deseamos sobreescribir, el método empleado, el número de pasadas, y si queremos hacerlo realmente o probar la simulación. Además nos hará un cálculo aproximado del tiempo que necesita para llevar a cabo el proceso y que suele ser de bastantes horas para discos grandes.

Capítulo 11. Educar a los usuarios

La idea de enseñar a los usuarios a protegerse de los males que entraña la informática, Internet, los hackers y los programas maliciosos, parece a simple vista correcta. La educación siempre es buena.

Pero si esto funcionase, a estas alturas, los usuarios sabrían manejarse y defenderse ante todas estas amenazas, y sin embargo no es así. No pueden defenderse porque simplemente, y por mucho que sepan, siempre están expuestos. Incluso preocupándose de todo lo que hemos visto en este curso siempre puede surgir una nueva amenaza como un virus o un bug reciente del sistema operativo que sea aprovechado maliciosamente para acceder a su ordenador.

Y no hablemos de los usuarios noveles que se compran por primera vez un ordenador y no saben lo que es la informática ni han oído nada de todo lo que hemos visto aquí.

No es cuestión de cuantificar amenazas, o de conocer todos los peligros, porque son muchos, muy variados y constantemente surgen otros nuevos. Si actuamos utilizando la seguridad como meta en cada cosa qué hacemos; si buscamos la sencillez y no la sofisticación;si preferimos lo probado a lo nuevo, si somos desconfiados por defecto, si dudamos de las tecnologías hasta conocerlas a fondo y no somos los primeros en adoptarlas, es probable que siempre las sintamos como una ventaja y no nos produzcan grandes quebraderos de cabeza.

No podemos ser inmunes, pero podemos aspirar a proteger nuestros datos, a recuperarnos de los golpes y a saber a qué estamos expuestos, es decir, a conocer, al fin y al cabo, la verdad. Se trata de que no nos engañen cada vez que nos prometen un producto nuevo, maravilloso, milagroso que protegerá completamente a nuestros ordenadores, que nos dejará dormir tranquilos.

Cuando la mayoría de los ordenadores no tenían conexión a Internet, este problema era muy reducido. Bastaba con escanear con el antivirus todos los programas o datos que íbamos a introducir en el pc primero. Con eso, y un poco de organización dentro del ordenador, además de algunas tareas de mantenimiento para mantener el equipo en un estado óptimo, era suficiente.

De hecho todavía existen personas que emplean un ordenador para conectarse a Internet y otro completamente separado para lo demás

Ha sido necesaria la aparición de Internet y la interconexión de los ordenadores en redes de todo tipo masivamente, lo que ha dado al traste con las arquitecturas actuales de sistemas operativos y la forma de programar las aplicaciones.

El verdadero kit de la cuestión no reside en los usuarios, sino en los que diseñan los programas, los sistemas operativos y añaden la seguridad como algo que viene posterior a la moda, la tecnología, la innovación o la belleza y el estilo. La seguridad no es un añadido, o no debería serlo. Los sistemas antes que agradables, vistosos o

multifuncionales deberían ser seguros por diseño. No es casualidad que los sistemas más seguros solo hagan una tarea en la que están especializados y no cumplan los criterios de estética más avanzados. ¿Alguien piensa que la estética sea un criterio fundamental en el recuento de los miles de carros de compra que se procesan a diario en los supermercados de los grandes centros comerciales?

Mientras no prive la seguridad por diseño, solo ponemos un parche en el sistema, nos defendemos de los síntomas, quejándonos de los correos que abren (los usuarios), de que no tienen el antivirus actualizado, de que no saben lo que es el phising o de que no actualizan Windows o abren todos los archivos adjuntos de sus emails. Son demasiadas tecnologías, demasiadas cosas. No pueden trabajar pensando que cada pieza del puzzle puede ser una trampa para estafarlos. La informática debería ser segura por diseño, pero claro, entonces no sería tan rentable.

Sin embargo pronto los usuarios exigirán mayor calidad conforme el mercado madure y si aumenta el número de opciones escogerán el producto que les proporcione el menor quebradero de cabeza.

Se nos dice que son fallos debido a la pronta evolución de la tecnología, cuando en el fondo es solo una cuestión de marketing y de calidad. En informática soportamos lo que no aguantaríamos en otros campos, y eso se debe a que es una tecnología todavía inmadura.

La única obligación exigible al usuario es que emplee su sentido común a la hora de emplear su ordenador, no que sepa de informática.

Nota: Un artículo muy interesante sobre este tema, y que consta de tres partes puede ser leído en:

- http://laflecha.net/canales/seguridad/articulos/6ideas
- http://laflecha.net/canales/seguridad/articulos/6ideas2/
- http://laflecha.net/canales/seguridad/articulos/6ideas3

Para los usuarios no entendidos en informática, el tercer link es posiblemente el que puede resultarles más revelador y cercano.

Espero que este libro haya ayudado a entender y comprender conceptos, herramientas y en definitiva a facilitar la vida de muchos usuarios.