GESTIÓN DE CONTRASEÑAS

Las contraseñas son el primer nivel de seguridad establecido históricamente en el mundo de la informática. En cuanto se introdujo el concepto de multiusuario en las primeras máquinas UNIX, se hizo necesario proteger el acceso de alguna forma. Un usuario que comparte un ordenador, no debía poder tener acceso a los mismos recursos que otro usuario, y mucho menos el mismo nivel de control que el administrador. Lo más sencillo en aquel momento era establecer una contraseña que fuese conocida exclusivamente por el usuario para garantizar que solo él tuviese acceso a los recursos que le pertenecían.

A partir de ahí, con la popularización de las redes, se hizo necesario proteger el acceso en remoto. Desde entonces, los métodos para autenticarse han evolucionado en complejidad y eficacia. Sin embargo, al margen de otros métodos como los *tokens* y la biometría, la contraseña siempre ha sido la fórmula por excelencia para proteger el acceso a diferentes recursos, tanto locales como online. Veremos diferentes tipos de ataques posibles contra las contraseñas y cómo elegirlas y gestionarlas adecuadamente.

I Recomendaciones generales

En 2010, la compañía Imperva ha realizado un estudio sobre los malos hábitos en el uso de contraseñas[1]. El estudio se basa en el análisis de 32 millones de contraseñas reales de usuarios que fueron sustraídas de un servicio web, publicadas en diciembre de 2009. Las conclusiones más interesantes extraídas del estudio son:

a. **Aproximadamente un 50% de contraseñas constaban de siete caracteres o menos.** Las contraseñas deben tener más de 8 caracteres. Para que las contraseñas sean de una longitud adecuada y además sencillas de recordar, se pueden utilizar frases completas que pertenezcan a canciones, poemas o similares, que el usuario sea capaz de evocar fácilmente y que, aunque complejas, le resulten familiares.

b. **El 40% sólo utilizaban letras en minúscula.** Una contraseña robusta debe utilizar el mayor número posible de juegos de caracteres y mezclarlos. Esto es, incluir letras mayúsculas, minúsculas, números y símbolos. Por ejemplo, se pueden usar los símbolos de interrogación, puntuación, etc., para crear una contraseña mucho más compleja.

Además de lo que indicaba el informe mencionado, se pueden añadir otros consejos sobre las contraseñas. Por ejemplo, no debería ser una palabra conocida, que pueda ser

[1] The Imperva Application Defense Center (ADC), 2010. *Consumer Password Worst Practices*. Disponible en: http://www.imperva.com/docs/WP_Consumer_Password_Worst_Practices.pdf

encontrada en un diccionario. Si se utiliza una sola palabra como contraseña, la palabra no debería existir, esto es, tendría que ser completamente aleatoria. Para conseguirlo, se pueden usar palabras existentes y añadir símbolos al principio, final o en medio. Esta recomendación no es necesaria si se utilizan frases completas, como ya se ha indicado.

Otro consejo útil es no utilizar la misma contraseña para diferentes servicios web o dispositivos, y evitar el uso de datos personales como fecha de nacimiento, número de teléfono, combinaciones sencillas como "12345", "abcde", etc. Diversos informes[2] indican que es práctica habitual utilizar una misma contraseña para diferentes portales o servicios. Esto supone un peligro ya que, ante un potencial problema de seguridad en alguno de ellos que expusiese la contraseña a un atacante, sería sencillo tener acceso a otros recursos de la víctima utilizando la misma clave. El uso de diferentes contraseñas implica la necesidad de gestionarlas de forma óptima, como veremos a continuación.

Es necesario encontrar un compromiso entre la facilidad de recuerdo y efectividad de la contraseña. Lo importante es su estructura, más que la posible complejidad. Combinar una estructura fácil de recordar y de longitud adecuada, con caracteres simbólicos y numéricos, puede ser lo más apropiado.

Siguiendo estos sencillos consejos, es posible evitar que la contraseña sea adivinada a través de los ataques que describimos a continuación.

II Ataques comunes

La contraseña, como forma de entrada hacia diferentes recursos, siempre ha sido un objetivo deseado por los atacantes. Por tanto los métodos para conseguirla han existido desde que existen las contraseñas en sí mismas. Los ataques más comunes son:

a. **Ataques de diccionario.** Existen listas de cientos de miles de palabras en archivos de texto en todos los idiomas, accesibles de forma pública. Son utilizadas por programas automáticos para realizar ataques por diccionario. Estos ataques consisten en comprobar cada una de esas palabras contra algún recurso protegido, y esperar que alguna resulte la contraseña válida. Existen programas capaces de probar decenas de miles de contraseñas por segundo, aprovechando la potencia de los ordenadores actuales. Además, también están disponibles de forma gratuita en la red programas específicos contra servicios o recursos concretos. Por ejemplo contra servidores de correo, cuentas FTP, etc. El atacante habitualmente escoge un nombre de usuario (víctima) y prueba de forma constante todas las palabras del diccionario para intentar

[2] Disponible en: http://www.telegraph.co.uk/technology/news/6125081/Security-risk-as-people-use-same-password-on-all-websites.html, http://www.readwriteweb.com/archives/majority_use_same_password.php

encontrar la contraseña. Si el sistema protegido no limita este ataque, bloqueando el acceso después de un cierto número de intentos, el atacante tiene vía libre para realizar tantas comprobaciones como desee. Se pueden encontrar diccionarios temáticos con listas enormes de palabras relativas a un tema concreto (nombres de mujer, de hombre, profesiones, etc.) según pueda encajar mejor en el perfil de la víctima.

b. **Ataques de fuerza bruta.** Básicamente, se basan en la misma técnica que los ataques por diccionario. La diferencia es que este método va un paso más allá, y se comprueban todas las posibles combinaciones existentes en un conjunto de caracteres, y no solo palabras de un diccionario. Esto quiere decir que si, por ejemplo, el objetivo es adivinar una contraseña de 6 caracteres o menos, el atacante comenzará probando la contraseña "a", y sucesivamente añadiendo caracteres: "aa", "aaa", "aaaa", aaaaa", "aaaaaa", luego "aaaaab" etc, hasta acabar con "zzzzzz". En este ejemplo, si solo se utilizan letras minúsculas, la combinatoria da un potencial de 481.890.304 posibles intentos. Con la potencia de los sistemas actuales, probar todas estas posibilidades puede ser cuestión de horas o minutos. En la jerga, esto se llama *crackear* las contraseñas.

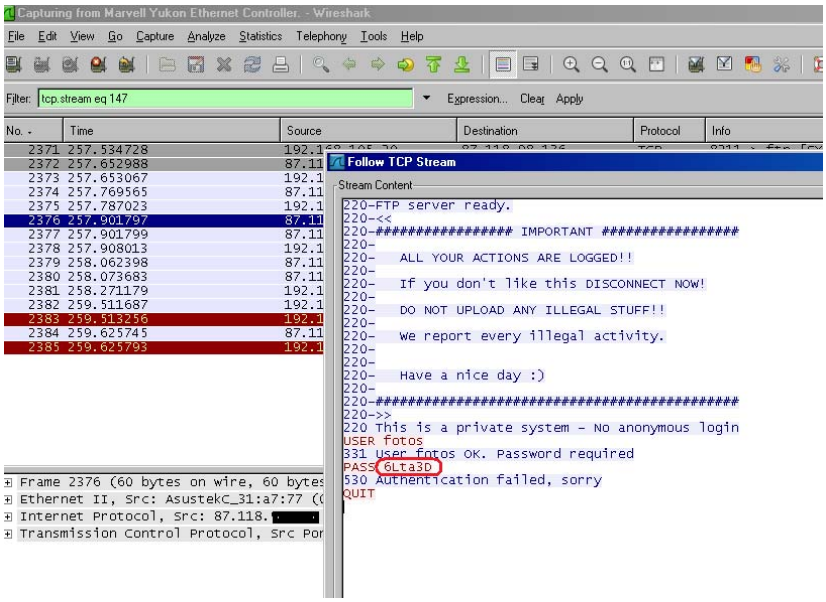
Existen servicios web en los que un usuario podría enviar un archivo protegido por contraseña, por ejemplo, y previo pago de una cantidad, sería hipotéticamente devuelto sin cifrar. Estos servicios suelen basarse en la fuerza bruta de decenas de máquinas para poder probar todas las combinaciones posibles.

Ilustración 1: Página que ofrece sus servicios de *crackeo* de contraseñas

Fuente: INTECO

c. **Ataques en la Red.** Las contraseñas pueden viajar por la Red en texto claro, esto quiere decir que no están cifradas de ninguna forma y cualquier atacante con acceso al tráfico que se transmite desde nuestro ordenador podría ver la contraseña (y usarla). Para que esto ocurra, se pueden dar dos escenarios. Podría ocurrir que el ordenador estuviese infectado por un troyano, o bien que algún atacante se encontrase en la red interna (conectado al mismo router que la víctima), buscando este tipo de información. En redes inalámbricas, el hecho de que un atacante se encuentre en la misma red resulta más sencillo de lo que parece, puesto que no debe acceder físicamente al router para conseguirlo. Para evitar que los datos viajen en texto claro por la Red, es necesario asegurarse que se utiliza cifrado (por ejemplo, en la web, el SSL) para acceder a los diferentes recursos web.

Ilustración 2: Atacante visualizando una contraseña FTP que circula por la red local en texto claro



Fuente: INTECO

d. **Ingeniería social.** Esta es una de las técnicas más efectivas y, a la vez, con más variantes que puede usar un atacante para obtener una contraseña. Consiste en el uso de técnicas de engaño o persuasión para conseguir que la propia víctima proporcione la información deseada sin que se sienta amenazada. Puede consistir en una llamada telefónica o un email a la víctima haciéndose pasar por el servicio técnico y pidiendo la contraseña, por ejemplo. También suele ser común investigar a la persona en sus hábitos, gustos personales, etc., con el fin de obtener un perfil más preciso. Con esos datos, un atacante podría realizar más

tarde un ataque por diccionario mucho más certero. Por tanto, la ingeniería social puede utilizarse como complemento para mejorar otros ataques.

Normalmente muchas webs que ofrecen contenidos protegidos por contraseña (por ejemplo, los sistemas de correo) disponen de un sistema de recuperación basado en una pregunta secreta, que suele consistir en un dato personal que pocas personas conocen. Si esa información es divulgada (o alguna pista que permita deducir las respuestas a estas preguntas) otros servicios usados por el usuario pueden verse comprometidos. El atacante solo tiene que simular que es la víctima que ha perdido la contraseña, y proporcionar la respuesta correcta como garantía de que es el legítimo dueño quien reclama el cambio de password. Si los datos que introdujo la víctima son correctos (por ejemplo, "nombre del colegio en el que estudiaste", o "segundo apellido de tu madre") el atacante podría tener acceso a la web protegida por contraseña sin necesidad de conocerla.

Ilustración 3: Pregunta secreta necesaria para poder restablecer una contraseña del correo de Yahoo

Fuente: Yahoo.es

e. ***Shoulder sniffing*.** Esta técnica consiste en espiar al usuario que utiliza su contraseña para ver cómo la teclea, o bien visualizarla en la pantalla si el sistema no utiliza la ocultación con los típicos asteriscos. Para que tenga éxito, el atacante debe situarse físicamente cerca de la víctima. Esta situación es común en sitios públicos de acceso a la Red, como cibercafés.

III Programas de gestión de contraseñas

Los programas de gestión de contraseñas ayudan a manejarlas de forma segura, sin necesidad de que se recuerden todas las que se necesitan. Además, permiten su almacenamiento (y a veces, su creación) utilizando un cifrado fuerte de manera muy cómoda.

Normalmente se basan en el cifrado fuerte de un archivo, que almacenará y ordenará todas las contraseñas. Para acceder al archivo cifrado, el usuario tendrá que recordar una única password, que suele ser llamada maestra o palabra de paso. Ésta permitirá el descifrado del archivo y, por tanto, acceso al resto de contraseñas almacenadas. Es de vital importancia, por tanto, que esta palabra de paso sea muy robusta para que el resto no se vean en peligro. También es sumamente importante que no sea apuntada ni divulgada en forma alguna.

Veamos algunos de los programas gratuitos más eficaces en este aspecto.

PasswordSafe

Es uno de los más populares, gratuito y de código abierto. Esto último garantiza que el programa no contiene ninguna puerta trasera que permita a sus creadores obtener los datos de cualquier usuario. El hecho de que las contraseñas son tratadas con criptografía pública garantiza su seguridad (al menos, con los métodos conocidos hasta hoy). Tiene una versión que funciona en cualquier sistema operativo y es muy sencillo de manejar.

El programa crea un archivo con la extensión *psafe3*. En él se encontrarán todas las contraseñas cifradas que introduzcamos. Puede ser trasladado de forma segura en una llave USB o en cualquier otro soporte puesto que, a menos que alguien conozca la contraseña maestra, los datos no estarán accesibles.

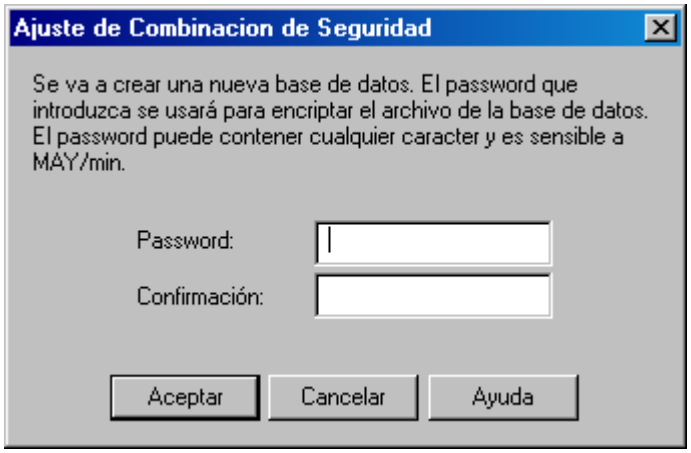
Lo primero es crear una nueva base de datos que contendrá las contraseñas. El programa permite la creación de tantas bases de datos (archivos *psafe3*) como se deseen. Cuando se ejecuta por primera vez, pide lo que será la contraseña maestra. Es importante que el usuario elija una contraseña de una gran longitud, que combine símbolos, números, mayúsculas, minúsculas, etc, y que esta no sea apuntada jamás en ningún sitio.

Ilustración 4: Ventana inicial de instalación de PasswordSafe

Fuente: INTECO

Si el usuario pierde esta contraseña, perdería el acceso a la base de datos.

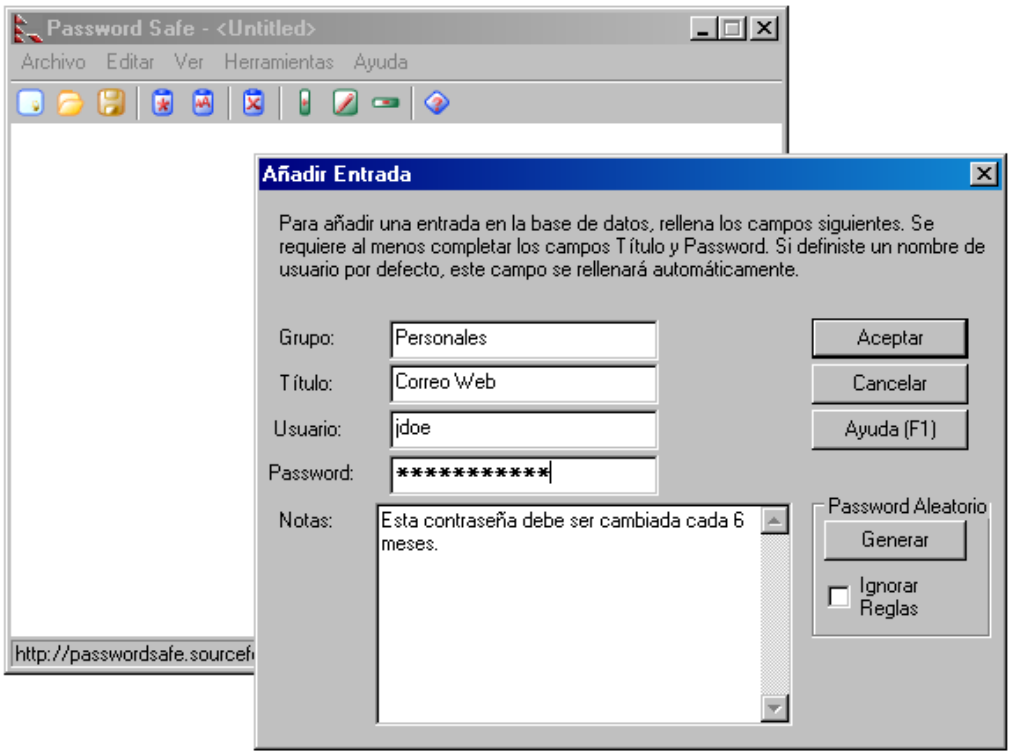
Ilustración 5: Diálogo de creación de la contraseña maestra de PasswordSafe



Fuente: INTECO

Una vez creada la base de datos, es posible introducir tantas entradas como el usuario desee. El programa mostrará en un formato de árbol las contraseñas agrupadas y accesibles.

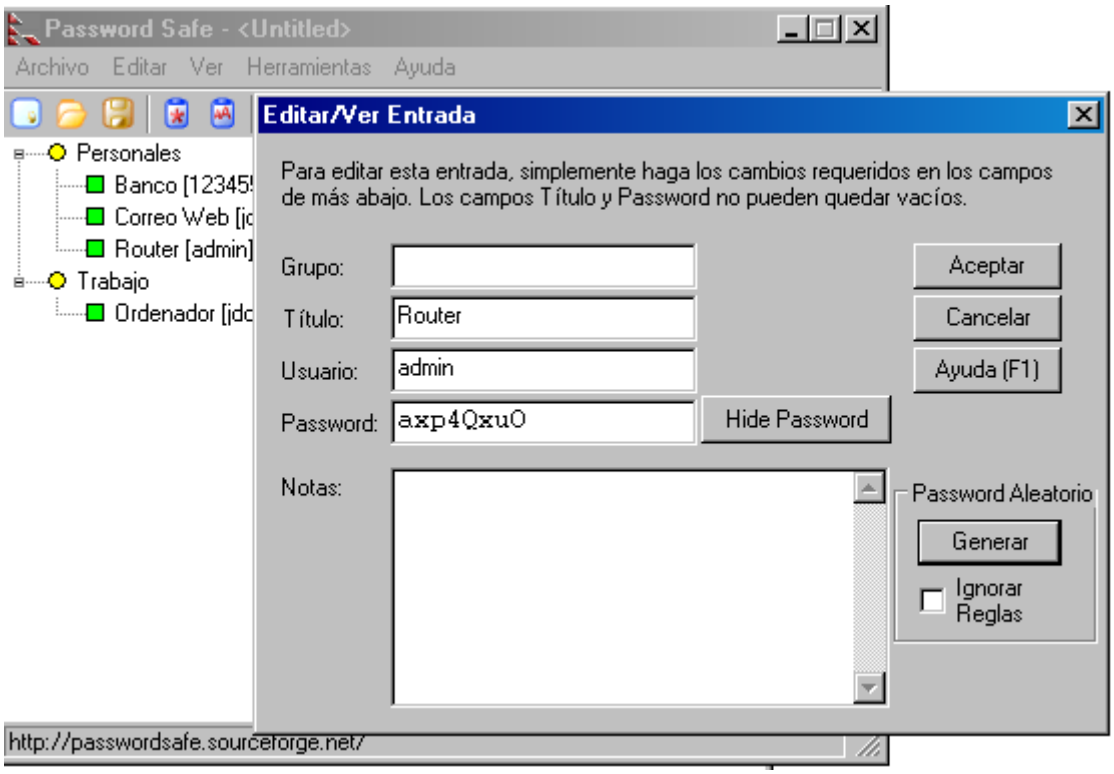
Ilustración 6: Creando una contraseña dentro de la base de datos de PasswordSafe



Fuente: INTECO

Para acceder a ellas, solo será necesario abrir el programa y realizar un doble clic sobre la contraseña deseada. Esta pasará al portapapeles del sistema y así podrá ser pegada en cualquier página que la necesite. De esta forma, el usuario ni siquiera debe conocer la clave para utilizarla. Si se desea, también puede ser visualizada e introducida a mano en el teclado.

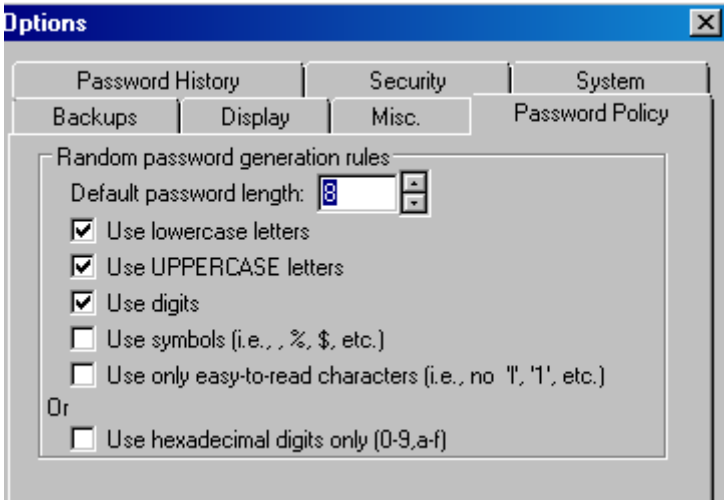
Ilustración 7: En PasswordSafe, las contraseñas pueden ser visualizadas



Fuente: INTECO

PasswordSafe permite la generación de contraseñas aleatorias según unas reglas que el propio usuario puede definir: longitud, combinación de mayúsculas y minúsculas, caracteres usados, etc.

Ilustración 8: Directiva de generación de claves en PasswordSafe



Fuente: INTECO

El programa permanece residente en la bandeja de entrada de Windows. Para volver a activarlo y que muestre de nuevo el árbol, será necesario hacer doble click sobre su icono. Si ha pasado un tiempo mayor a una cantidad de minutos configurable en los que ha permanecido inactivo, el programa se bloqueará y será necesario introducir de nuevo la contraseña maestra para volver a tener acceso al árbol. Esto impide que alguien con acceso físico al sistema pueda abrir el programa tras un tiempo de inactividad.

Está disponible en español en una versión anterior (con menos funcionalidades) a la actual en inglés.

Puede ser descargado desde: http://passwordsafe.sourceforge.net

KeePass

Se trata de un programa gratuito y de código abierto. Puede usarse en todo tipo de plataformas, desde PC hasta teléfonos inteligentes. Es más completo que PasswordSafe, con funcionalidades y facilidades añadidas.

Por ejemplo, permite el uso de ficheros para proteger la base de datos. Esto significa que el usuario no solo está protegido con una contraseña maestra, sino que tiene la posibilidad de proteger el acceso con cualquier archivo (ya sea un mp3, un texto, etc.) al que se llama *key file*. Un hipotético atacante no solo necesitaría conocer la contraseña, sino disponer del archivo concreto para poder acceder a la base de datos.

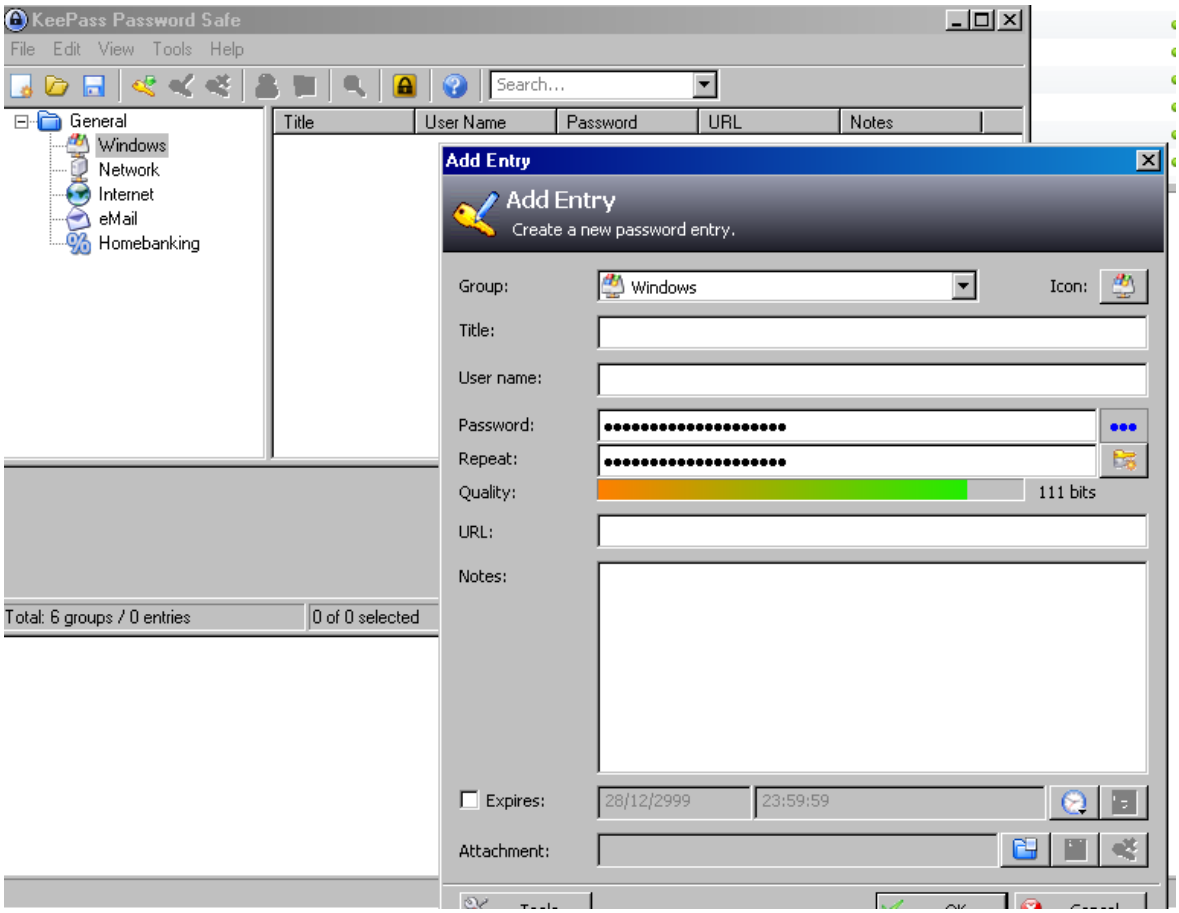
Ilustración 9: Diálogo de creación de contraseña maestra en KeePass

Fuente: INTECO

El funcionamiento básico es muy parecido al del programa PasswordSafe mencionado anteriormente. Crea un archivo cifrado con la contraseña maestra, con un key file o con

ambos, que almacenará el resto de contraseñas. En una estructura ordenada de árbol, se almacenarán todas las contraseñas.

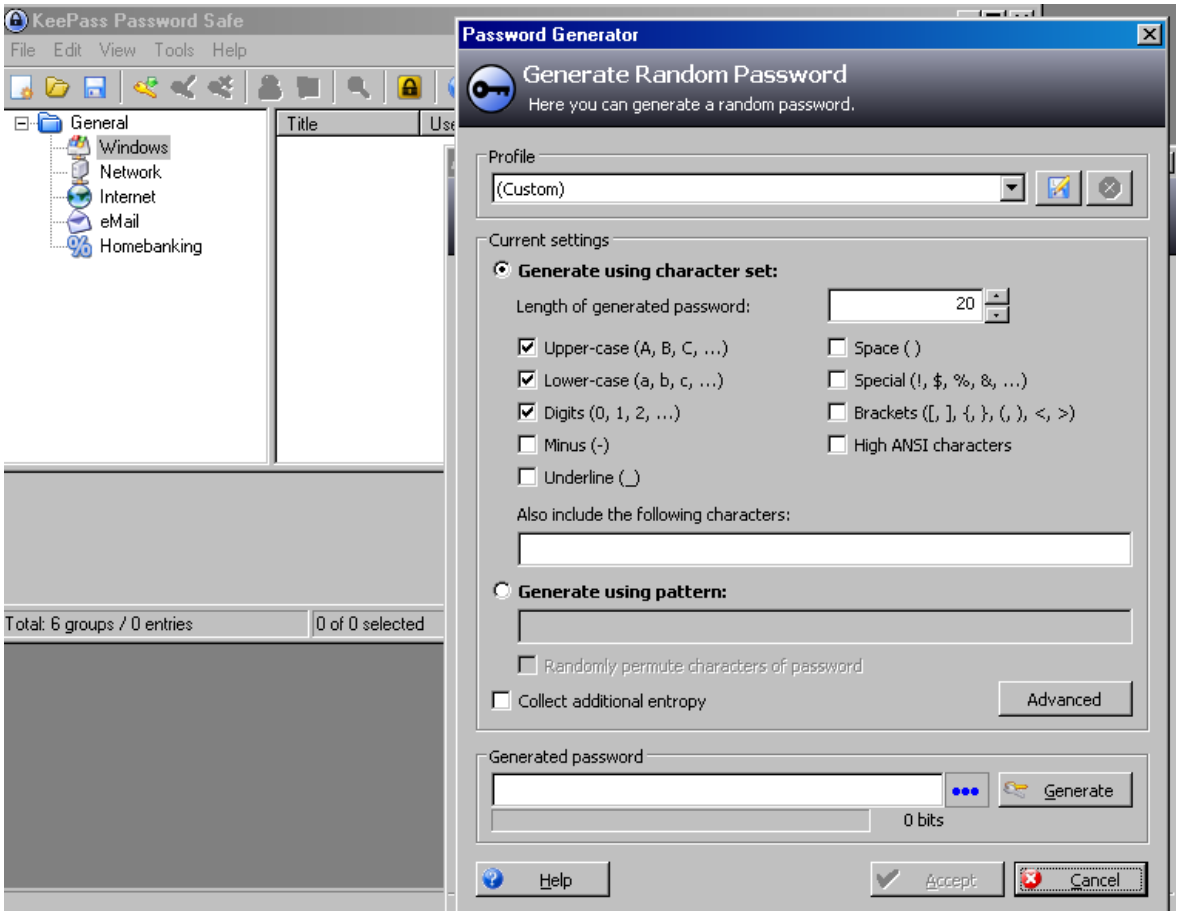
Ilustración 10: Creando una contraseña dentro de KeePass



Fuente: INTECO

KeePass también permite generar contraseñas fuertes. Así, el usuario no elige la contraseña sino que el propio programa el que lo hace respetando todas las recomendaciones anteriormente mencionadas o las directrices que el usuario desee. Por ejemplo, se puede definir una longitud mínima y un conjunto de caracteres determinado que puede incluir o excluir ciertos símbolos, caracteres, etc.

Ilustración 11: Ventana de generación de contraseñas en KeePass



Fuente: INTECO

A diferencia del resto de programas, acepta *plug-in*[3] para aumentar su funcionalidad. Está disponible para diferentes plataformas y en distintos idiomas.

Puede ser descargado desde: http://keepass.sourceforge.net/

Lastpass

Lastpass es un programa reciente que extiende la funcionalidad básica de otras utilidades en su categoría. No es de código abierto, pero sí cuenta con una versión gratuita.

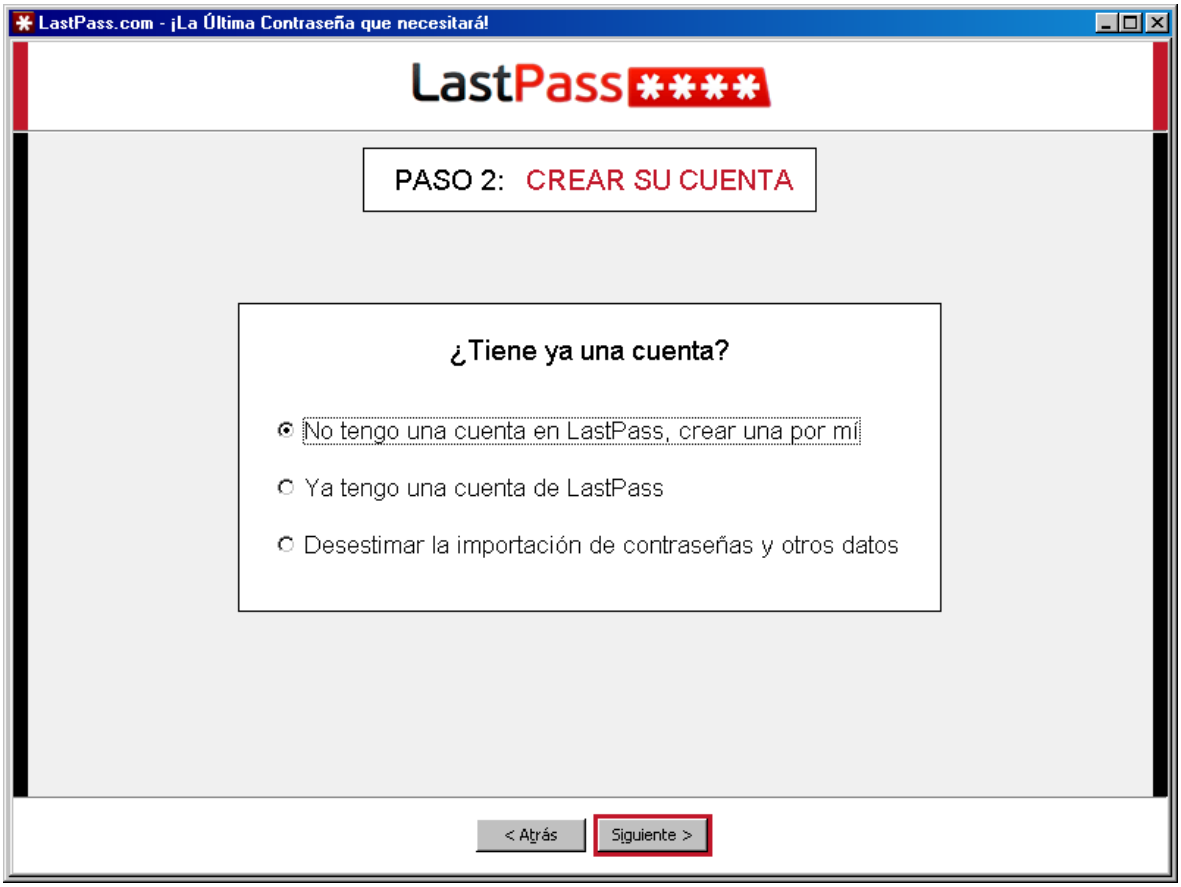
La diferencia fundamental con el resto de programas analizados aquí es que Lastpass permite almacenar las contraseñas en sus servidores, de forma que estarán disponibles para el usuario desde cualquier lugar, de forma segura, después de haber introducido una contraseña maestra. Para ello, es imprescindible crear una cuenta en los servidores del fabricante, como primer paso.

[3] *Plug-in*: programa complementario.

Esto añade la funcionalidad de copia de seguridad de las contraseñas, puesto que al mantenerse almacenadas en servidores de terceros, si el usuario pierde su base de datos en local, siempre podrá recuperarla desde los servidores de los creadores del programa.

Otra gran diferencia es que LastPass permite rellenar automáticamente los formularios de las páginas que el usuario desee, de forma que no tendrá que recordar ninguna contraseña y, además, ni siquiera teclearla. Para ello utiliza complementos que se instalan en el navegador.

Ilustración 12: Creación de cuenta en los servidores de LastPass



Fuente: INTECO

Permite además la generación de contraseñas de forma automática según las directrices que el usuario le indique.

Ilustración 13: Creación de contraseñas seguras en LastPass

Fuente: www.lastpass.com

Está disponible en diferentes idiomas. Funciona bajo diferentes plataformas, navegadores, dispositivos móviles y sistemas operativos.

Puede ser descargado desde: http://lastpass.com