Gestión de contraseñas.
Laboratorio de Administración y Gestión de Redes y Sistemas
Grado en Ingeniería Telemática, 2022-2023
Escuela Técnica Superior de Ingeniería de Telecomunicación
Universidad Rey Juan Carlos

1. Gestión de contraseñas

1.1. Fatiga de contraseña

Uno de los principales problemas que tienen los usuarios con las nuevas tecnologías es el fenómeno denominado *fatiga de contraseña*. Para acceder a cada servicio, es necesario un nombre de usuario y una contraseña. Muchos usuarios tienen problemas para recordar estos datos, es fácil olvidarlos, perderlos. Incluso entre especialistas esto no es raro, aunque resulte muy poco profesional.

Cualquier navegador moderno permite almacenar las contraseñas necesarias para acceder a un sitio web, con lo que el asunto aparenta desaparecer en el día a día. Pero si el usuario no toma medidas adicionales, el problema aparece, agravado. Ejemplos:

- Las contraseñas están en el teléfono móvil, el móvil se pierde o se cambia por uno nuevo. Las contraseñas se pierden.
- Las contraseñas estén en el ordenador de casa. Si usamos un equipo diferente, ya no las tenemos.
- No todos los servicios están basados en el navegador. La cuenta para acceder al ordenador del trabajo, el pin de la tarjeta de crédito, el PUK del móvil, la tarjeta de coordenadas del banco...

En el artículo de Wikipedia *fatiga de contraseña* podemos encontrar información adicional.

1.2. Soluciones al problema

Hay varias formas de resolver el problema de fatiga de contraseña, unas mejores que otras

1. *Yo siempre uso la misma contraseña para todo*

Muy mala idea. Para empezar, es cada vez más complicado porque los diferentes servicios tienen distintas exigencias (longitud, caracteres aceptados, número de mayúsculas, de dígitos, de símbolos especiales, etc)

Lo peor es que es muy fácil ser víctima del siguiente ataque: *Bienvenido a televisiongratis.com. Registrate en nuestra web para ver el último capítulo de Juego de Tronos. Dinos tu dirección de correo. Elige tu contraseña*

Si el usuario usa la misma contraseña en su correo que en este web, en este momento el administrador de *televisiongratis.com* puede suplantarle, porque conoce su correo y su contraseña. Y una vez que ha entrado en el correo, puede entrar también en cualquier otro servicio, haciéndose pasar por usuario y pulsando en *he perdido mi contraseña, enviadme una nueva por correo*

2. *Yo lo apunto todo en mi agenda*. Puede ser aceptable, es mejor que la anterior. Aquí el problema es que perdamos la agenda, no la tengamos a mano o alguien nos la robe.

3. Apuntar las contraseñas en un documento de LibreOffice (o de Microsoft Word si confiamos en esta empresa y en el gobierno norteamericano). Esto también permite incluir tarjetas de claves escaneadas. Guardamos el documento cifrado (Figura 1)y hacemos varias copias. Eso sí, es imprescindible no olvidar la contraseña maestra con la que ciframos el documento.

4. Una herramienta de gestión de contraseñas. Por ejemplo, KeePassX

1.3. Contraseña maestra

Para las soluciones 3 y 4 del apartado anterior, es de vital importancia recordar una contraseña maestra, sin ella, habremos perdido el acceso a todas las demás. La ventaja fundamental es que se trata de una única contraseña. Una opción es apuntar un recordatorio de contraseña.

Ejemplo: partimos de una frase. *Rascayú, cuando mueras que harás tú.* Usamos la contraseña *R,cmqht?*. Y escribimos, en texto sin cifrar, el recordatorio de contraseña *canción de los años 40.*

1.4. gpg

Una solución sencilla pero muy robusta es gpg con cifrado simétrico. Guardamos nuestras contraseñas en un fichero de texto, lo ciframos con

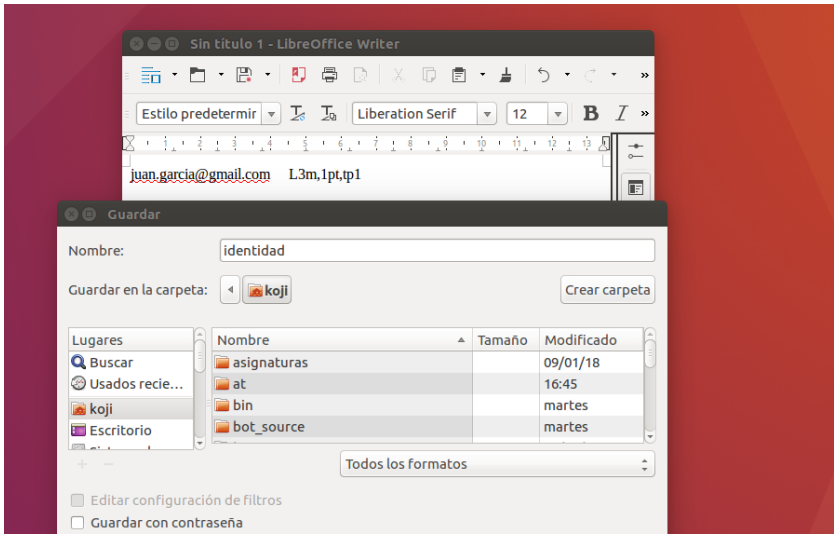

Figura 1: Guardar fichero con contraseña en LibreOffice.

`gpg -c fichero.txt`. Esto nos genera un fichero `fichero.txt.gpg` que podemos descifrar con `gpg -d fichero.txt.gpg`. Es muy conveniente añadir el recordatorio de contraseña en un fichero de texto adicional, en claro.

Una limitación de este enfoque es que para usar el fichero, es necesario que se vea en pantalla.

1.5. KeePassX

KeePassX es una aplicación que permite guardar y gestionar nuestras contraseñas de manera razonablemente segura. Es bastante popular y se desarrollada activamente desde 2005 como software libre y gratuito. Por todo ello es razonable suponer que no tiene problemas serios o puertas traseras, habrían sido detectados. Está disponible para Microsoft Windows, Linux y MacOS. Todas el contenido que añadamos se cifra con algoritmos estándar de buena calidad, AES o Twofish con claves de 256 bits.

Para guardar contraseñas de poco valor, por ejemplo de páginas web que no sean especialmente importantes y que no usemos mucho, posiblemente podemos confiar en la opción de autoguardado del navegador. Pero para otros usos de mayor importancia, como nuestro correo principal, bancos, trabajo, contraseñas del teléfono movil, etc, el uso de una aplicación como KeePassX es muy conveniente.

KeePassX tiene otra característica útil: la contraseñas se pueden usar aunque estamos rodeados de personas que puedan ver nuestra pantalla, puesto que permite copiar y pegar contraseñas sin mostrarlas. Si guardamos nues-

tras contraseñas en un documento de un procesador de textos, no tenemos esta ventaja.

1.5.1. Contraseña maestra y archivo llave

Además de una contraseña maestra, KeePassX permite usar los denominados *archivos llave*. Es un concepto similar al de una llave mecánica tradicional, algo que una persona necesita para acceder al sistema, que puede ser copiado con relativa facilidad. Así, para poder acceder a las contraseñas, hace falta tener ese archivo llave, típicamente guardado en un pendrive, en un cd, etc

Podemos configurar KeePassX para que sea necesario o bien la contraseña maestra, o bien el archivo llave, o bien ambas cosas.

1.5.2. Organización de KeePassX

En KeePassX, el concepto de mayor orden jerárquico es el de *base de datos*. Es un fichero donde guardaremos nuestras contraseñas, todo el contenido de este fichero estará cifrado con una única clave maestra. Un usuario individual normalmente tendrá una única base de datos, mientras que en entornos donde haya contraseñas compartidas entre varios usuarios, será normal emplear varias bases de datos, posiblemente una para individuo y otra diferente para cada grupo.

Dentro de cada base de datos, se definen *grupos* (de contraseñas). Una organización típica sería tener por ejemplo un grupo para el ocio, otro para el trabajo o estudios, prácticas, etc

Dentro de cada grupo, añadimos *entradas*. Una entrada es una contraseña, junto con otra información relacionada. En el apartado *añadir entrada* podemos añadir la siguiente información:

- Título

  Nombre que asignamos a la entrada.

- Nombre de usuario

- URL

  Universal Resource Locator. Una dirección web, la del sitio donde se usa la contraseña.

- Expira

  Por motivos de seguridad, es conveniente cambiar de vez en cuando las contraseñas. Para ello, podemos indicar aquí una fecha de caducidad

de la contraseña. Cuando llegue ese momento, quedará marcada como caducada para recordar al usuario que debería cambiarla, aunque no se borra de la base de datos.

- Notas

  Es un espacio reservado para las anotaciones que nos parezcan convenientes.

En el apartado *avanzado* podemos añadir:

- Atributos adicionales

  Similares a las notas, pero pueden ordenarse por categorías.

- Adjuntos

  Permiten incluir cualquier fichero en la entrada. Un código QR, una tarjeta de claves, etc.

1.5.3. Uso de KeePassX

Una vez que nos hayamos familiarizado con los conceptos básicos de esta aplicación, su uso es muy sencillo.

1. Creamos una nueva base de datos, le asignamos contraseña y/o archivo llave. (Figura 2)

   Este fichero deberíamos copiarlo en varios lugares, su pérdida puede causarnos problemas muy severos. Por ejemplo una copia en un pendrive en casa y otra en un servicio de almecenamiento en la nube. Aunque alguien acceda al fichero, no podrá consultarlo sin la contraseña. Tampoco nosotros.

2. Después de ponerle la contraseña, guardamos la base de datos y entonces nos preguntará el nombre. Esto puede ser poco intuitivo: tal vez esperes que primero pregunte el nombre y luego la contraseña, pero no, es al reveś, primero la contraseña y luego el nombre

3. Añádimos uno o más grupos (Figura 3). Esto puede hacerse desde dos sitios

   - Menú *grupos*, *añadir grupos*.
   - Haciendo clic con el botón secundario en el panel izquierdo, aparece un menú contextual con la opción *añadir nuevo grupo*.

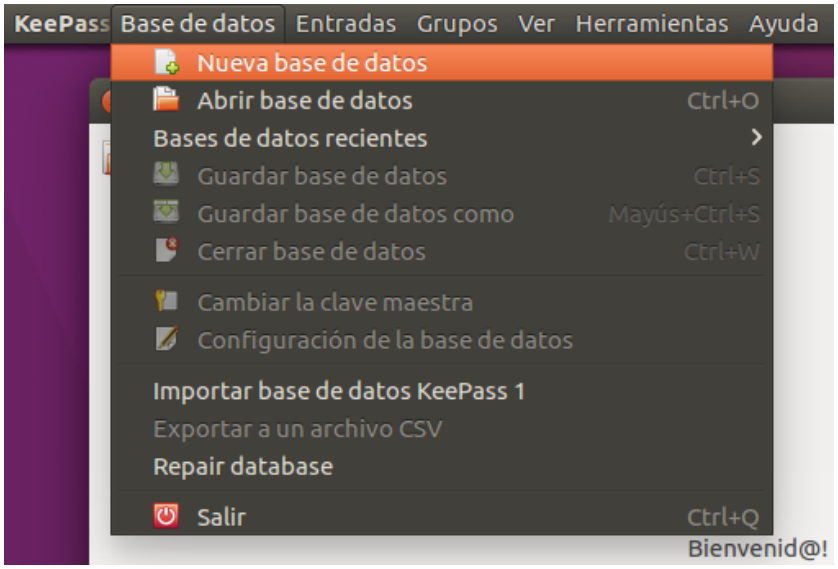

Figura 2: Crear una nueva base de datos.

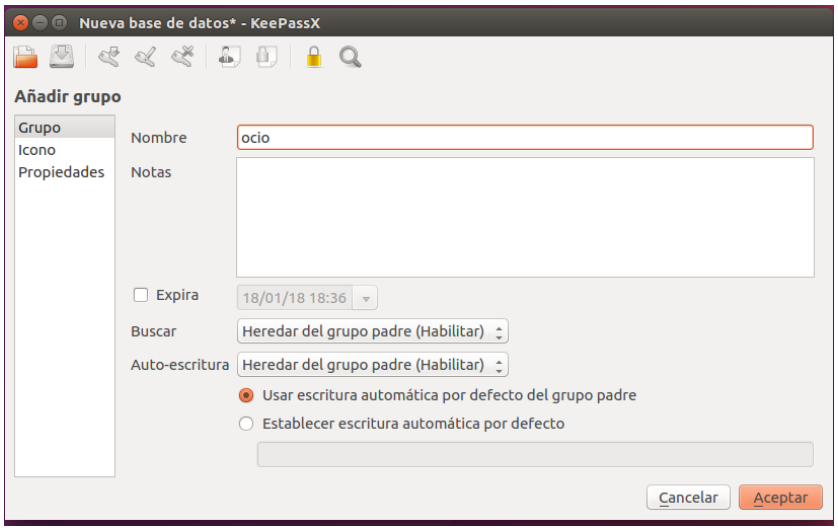

Figura 3: Añadir un grupo.

4. Seleccionamos un grupo y añadimos entradas. (Figuras 4 y 5) También podemos hacerlo desde dos sitios

   - Menú *entradas*, *añadir nueva entrada*
   - Icono *añadir nueva entrada*, (una flecha verde apuntando hacia una llave)

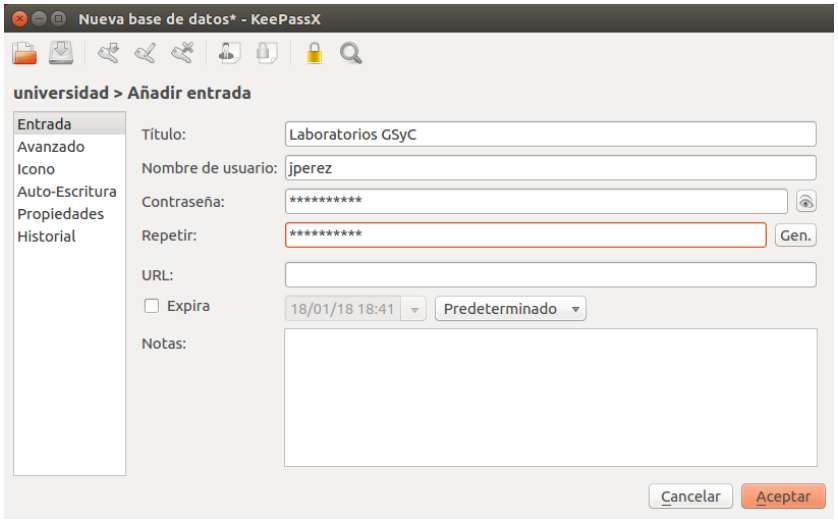

Figura 4: Añadir una entrada. Campos básicos.

   Por omisión las contraseñas nunca se muestran en pantalla. Para verlas, pulsamos en el icono que representa un ojo. También está disponible el botón *gen*, que generará una contraseña aleatoria de calidad. (Figura 4)

5. Una vez creadas las entradas, para usarlas basta hacer clic sobre la que necesitemos. Recordando que podemos copiar y pegar, sin que la contraseña se llegue a ver en pantalla [1]. (Figura 6)

[1] Esta opción no siempre funciona en Ubuntu 16.04, puede solucionarse instalando el paquete xsel:i386

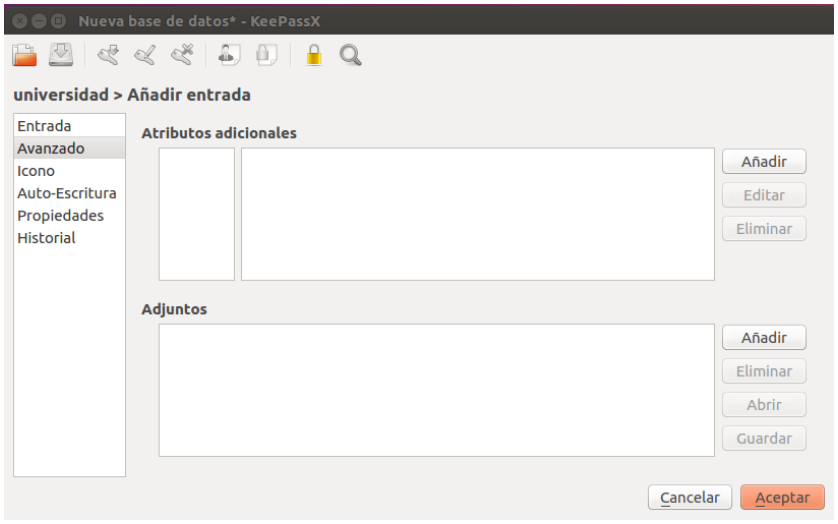

Figura 5: Añadir una entrada. Campos avanzados.

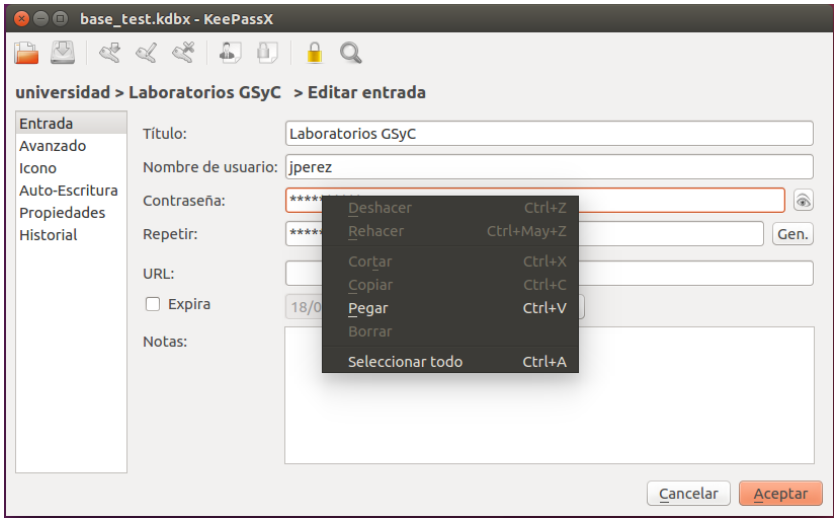

Figura 6: Consultar una entrada.