AGRADECIMIENTOS

Embarcarse en el proyecto de escribir un libro es un camino tan gratificante cuando se llega al final, como espinoso cuando se está recorriendo.

Infinidad de horas empleadas, mucho trabajo y esfuerzo puesto en cada línea, y multitud de problemas que, cada vez que tienen oportunidad, buscan el desaliento del escritor. Únicamente el apoyo y los ánimos de la gente a la que de verdad importas, hacen que todo merezca la pena, y permiten que la obra llegue a ver la luz.

Primera, y especialmente, gracias a Andrea. La primera en conocer el proyecto y en animarme a ello. Todo el tiempo invertido, tus consejos, tu aliento, y esa inquebrantable ilusión han sido los verdaderos artífices de que este sueño se convierta en realidad. Sin ti y sin tu sonrisa perpetua, nada habría sido posible.

Gracias a Irene y a Javier, por su lectura, sus correcciones, y sus opiniones. Habéis sido la gran prueba de fuego para conocer la verdadera utilidad del trabajo realizado.

Gracias a Feli, Corbe, Pablo, Julio, Michi, Rafa y David, por prestarse como conejillos de indias sin saber dónde se metían, sólo con la esperanza de poder ayudar a un amigo. Dad por hecho que lo conseguisteis.

Gracias a mi editor Julio Santoro, y a la editorial Ra-Ma, por ofrecerme esta oportunidad y apostar por la obra.

Y, finalmente, gracias a mi madre, simplemente por todo.

1

INTRODUCCIÓN

¿LO HARÍAS?

He salido a dar una vuelta con los amigos por el centro y al final se nos ha hecho de noche. Quería llegar a casa pronto, mañana tengo que madrugar, y al final es más tarde de lo que pensaba. No estoy lejos, así que voy a volver andando para ahorrarme el dinero del taxi, que nunca viene mal. Para llegar tengo dos caminos: puedo dar un rodeo e ir por las calles iluminadas o puedo cruzar el parque, que a estas horas está desierto y mal iluminado. He oído muchas historias sobre robos y violaciones que han sucedido en él a estas horas, pero me vendrá bien tardar poco en llegar para poder dormir un poco más, así que me voy a ir por el parque. No creo que a mí me vaya a pasar nada.

CASO 1.
A MÍ NUNCA ME VA A PASAR. SEGURIDAD DIGITAL

Cualquier persona que se preocupe por su propia seguridad no cruza ese parque. Damos el rodeo o incluso pagamos el taxi, nuestra vida está por encima de unos pocos minutos o unos míseros euros que podamos gastar. Tenemos muy claro que cualquiera puede ser objeto de un robo, una paliza, una violación o algo peor; conocemos a la perfección los peligros a los que nos enfrentamos en nuestra "vida real".

Estas medidas básicas de seguridad las hemos interiorizado y no nos cuesta nada llevarlas a cabo; en cambio, no estamos tan concienciados cuando se trata de

la seguridad en nuestra "vida digital", entendiéndose como tal aquella que influye sobre nuestros equipos informáticos y nuestro tiempo en Internet.

En los últimos años hemos sufrido una auténtica revolución digital. Hoy en día, prácticamente todo el mundo tiene en su casa un ordenador que está conectado a la red, e incluso millones de personas llevan encima un *smartphone* o una tableta conectados a Internet las 24 horas del día, lo cual debería convertir la seguridad digital en un asunto crítico para la casi totalidad de la población.

Pero, por desgracia, los usuarios no suelen estar tan concienciados de esta importancia como deberían. En muchas ocasiones he oído la típica frase de: *"Yo no necesito protegerme tanto. Si yo no tengo nada que le pueda interesar a nadie"*. Seguro que tú mismo o tú misma la has pronunciado en alguna ocasión. Tenemos la sensación de que a los delincuentes de la red únicamente les van a interesar los documentos confidenciales de gobiernos o grandes empresas, pero nada más lejos de la realidad: el ordenador de cualquier, y recalco **CUALQUIER** persona, puede ser objeto de algún ataque.

Cuando hablamos de ciberdelincuentes no solo debemos pensar en el robo de secretos industriales o de estado; nos enfrentamos a una multitud de peligros que ni siquiera nos imaginamos (robo de datos personales, robo de datos bancarios, ciberacoso, espionaje o simplemente el uso remoto de tu máquina para cometer actividades delictivas), y en la mayoría de los casos, los usuarios se lo ponemos demasiado fácil a los "malos" para que puedan llevar a cabo sus planes.

Figura 1.1. Debemos concienciarnos de la importancia de nuestra seguridad digital

Todo aquel que use la red, ya sea para consultar el periódico, hacer transferencias bancarias o para actualizar sus redes sociales, debe tener un poco de celo con la información que maneja diariamente a través de Internet. La seguridad digital no solo compete a bichos raros que se encierran en sus habitaciones a trastear con sus ordenadores de última generación. La seguridad digital es un problema globalizado en la sociedad actual, o mejor dicho, debería serlo.

Ese es el fin que persigue esta obra. No va dirigida a usuarios avanzados en seguridad informática, sino que desde su inicio está planteada para que sea leída por el usuario de a pie, aquel que nunca ha pensado que a él le vaya a pasar nada por navegar por sus webs favoritas.

Tampoco pretendo crear expertos en ciberseguridad, ni mucho menos; con que aquel que al acabar de leer las páginas que tiene entre sus manos se dé cuenta de los peligros a los que se enfrenta (seguramente sin saberlo) en su día a día, y tenga unas herramientas básicas para defenderse de ellas, daré por bueno todo el trabajo y todas las horas invertidas en cada una de estas líneas.

Hemos de erradicar esa falsa sensación de seguridad que nos da estar delante de una pantalla encerrados en nuestra casa. Aunque pensemos que nada puede atacarnos, es muy probable que estemos mucho más expuestos a peligros de lo que lo estaríamos en la calle, por lo que cuando naveguemos por la red debemos ser tan precavidos, o más, de lo que lo somos normalmente en nuestra vida real.

Desgraciadamente, la seguridad informática plena no existe. Si alguien con los suficientes conocimientos va a por ti directamente, es muy probable que antes o después consiga su objetivo. Pero poniendo en práctica unas pocas medidas básicas de seguridad que voy a explicar a lo largo del libro, conseguiremos repeler el 99,9% de los ataques que podamos sufrir, ya que la mayoría de estos son ataques masivos lanzados a millones de usuarios a la vez y que buscan al rival más débil, a la gacela más lenta de la manada, para convertirla en su siguiente víctima. Si te proteges un poco, lo más normal es que busquen a alguien más incauto y se olviden de ti.

RECUERDA

Sé siempre igual de precavido en tu "vida digital" como lo serías en tu "vida real". Aunque pienses que tú no tienes nada que pueda interesar a los ciberdelincuentes, todo el mundo con un dispositivo conectado a Internet puede ser objetivo de criminales. Cambiando muy poco puedes protegerte ante la mayoría de ataques.

2

SEGURIDAD DIGITAL

2.1 SOFTWARE

¿LO HARÍAS?

¡Qué contento estoy! Acabo de comprar mi nueva casa. He tenido que ahorrar durante años, pero por fin la tengo. Ahora ya solo me queda disfrutarla. He estado meditándolo durante mucho tiempo y finalmente he decidido que no voy a ponerle la puerta ni las ventanas. En esta zona la temperatura es buena durante todo el año y nadie encontraría dentro algo que le interesase. ¡Con el tiempo que perdería teniendo que abrir y cerrar cada vez que quiero entrar! Mejor así, desde luego.

CASO 2.
¡PREPARAD LAS DEFENSAS! SOFTWARE DE PROTECCIÓN

Nadie en su sano juicio deja su casa totalmente abierta a cualquiera, con todas sus pertenencias al alcance de la primera mano malintencionada que decida entrar en ella. Esto es algo que todos tenemos muy claro en nuestra vida real, pero que muchas veces obviamos en nuestra vida digital.

Protegemos nuestros hogares con un sistema de "capas de cebolla" que va aumentando en función del valor de lo que guardemos dentro y del nivel de seguridad que queramos obtener. Instalamos una puerta, añadimos una cerradura, la blindamos, ponemos un perro y un cartel que advierte al posible intruso sobre la fiereza del mismo, instalamos cámaras de seguridad, contratamos un vigilante, colocamos sensores de movimiento.

Todo nos parece poco para mantenernos a salvo, pero en el ordenador no instalamos un antivirus que, al final, lo único que hace es ralentizarnos el trabajo y nunca nos ha entrado ningún "bichito". Al igual que en nuestra vida real sabemos de qué y cómo debemos protegernos, es necesario que nos concienciemos de que la vida digital precisa de las mismas precauciones.

Figura 2.1. Los virus informáticos nos pueden crear muchos problemas

El mercado nos ofrece multitud de herramientas que nos van a ayudar a conseguir este objetivo y será nuestra responsabilidad saber cuáles elegir e instalar. Existen grandes compañías dedicadas al desarrollo de soluciones de seguridad informática en cuyas manos podemos ponernos con total seguridad, e incluso aplicaciones gratuitas que nos darán una protección bastante aceptable sin tener que hacer ningún desembolso.

Lo que sí es primordial tener en cuenta es no instalar nunca ningún *software* de seguridad pirateado en nuestros ordenadores, puesto que en la gran mayoría de los casos son programas que ya vienen con el "regalito" dentro, y que nos van a instalar algún tipo de *malware* (código malicioso) que evidentemente nunca va a detectar nuestro sistema de protección, ya que él mismo es el encargado de transmitirlo.

Para poder presumir de una protección lo más amplia posible deberíamos disponer en nuestro equipo de:

- **Antivirus**: programas que buscan prevenir, detectar y eliminar distintos tipos de *malware* que puedan llegar al sistema. Si no nos importa pagar, por menos de 50 euros al año podemos obtener antivirus de gran calidad desarrollados por McAffe, Panda, Norton, Kaspersky, Avira o AVG. En cuanto a herramientas gratuitas, son muy valoradas las de Avira, Avast o Panda.

- ***Antispyware***: su finalidad es combatir los llamados programas espía, que se dedican a recopilar información de nuestro equipo y enviársela al atacante. También pueden realizar otras tareas que no son propiamente espías, como la muestra continua de *pop-up*, redirigir solicitudes de páginas o cambios en la configuración del sistema. Malwarebytes Anti-Malware o SUPERAntiSpyware, como *software* de pago, y Super Antispyware, Windows Defender o Spybot Search and Destroy, como *software* libre, están considerados algunos de los mejores *antispyware* del mercado.
- ***Firewall***: *software* que controla las conexiones que salen y entran en mi equipo, evitando que alguien no autorizado entre en el sistema. ZoneAlarm y ComodoFirewall son los reyes indiscutibles en el mercado de los *firewalls*, tanto en sus versiones de pago como las gratuitas.
- ***Antiadware***: se emplean para evitar la acción de los programas de publicidad computacional que generalmente basan su funcionamiento en la aparición de *pop-up*, cambio de páginas de inicio y los motores de búsquedas de los navegadores o la instalación en los mismos de barras de herramientas o de búsqueda. AdwCleaner y AT-Destroyer son dos buenas herramientas dedicadas a este fin, aunque la mayoría de las mencionadas en el apartado del *antispyware* también cumplen la misma función.
- ***Antispam***: Herramientas utilizadas para prevenir el correo basura. SPAMfighter o Spamihilator se pueden encontrar de forma gratuita por Internet, aunque la mayoría de gestores de correo actuales ya incorporan sus propios sistemas internos de *antispam*.

No siempre es necesario instalar una herramienta distinta para cada una de estas protecciones, ya que en la actualidad las compañías de seguridad tienden a ofrecer paquetes que incluyen varias de ellas juntas como solución combinada.

Figura 2.2. Principales empresas de seguridad informática del mercado

Sean cuales sean las aplicaciones que finalmente instalemos es fundamental que nos encarguemos de mantenerlas continuamente actualizadas para que puedan hacer frente a las nuevas amenazas que se vayan descubriendo.

RECUERDA

Nunca olvides proteger tu equipo con software de confianza y mantenerlo actualizado. Esta es la primera barrera que nos protege de las amenazas externas y puede evitarnos muchos problemas.

CASO 3.
SIEMPRE A LA ÚLTIMA. ACTUALIZACIÓN DEL SOFTWARE

¿LO HARÍAS?

Según dicen en el telediario, esta última semana ha habido muchos casos de hogares desvalijados por una banda organizada. No rompían las ventanas ni entraban por la fuerza, por lo visto habían encontrado un fallo en las cerraduras, casualmente iguales que la que tengo instalada yo en mi puerta, y podían entrar sin ningún problema. La empresa que me colocó la puerta me dijo que si alguna vez pasaba esto les llamase, que me cambiaban la cerradura por una nueva con mayor seguridad, pero ponerme ahora a buscar el teléfono, quedar con ellos para un día determinado y tener que esperarlos, que seguro que llegan tarde… Mejor voy a dejarlo tal y como está, así me ahorro las molestias y seguro que con toda la gente que tiene este modelo de cerradura a mí no me toca.

Si a cualquiera de nosotros nos dicen que la cerradura de nuestra casa puede ser abierta por delincuentes, no dudamos ni un segundo en correr a la ferretería a comprar una nueva para evitar ser robados. Sin embargo, cuando el aviso nos llega desde nuestro ordenador no le prestamos la misma atención y, en muchas ocasiones, omitimos los mensajes que nos piden que actualicemos nuestro *software*.

Estas actualizaciones, que tantas molestias nos causan, no nos llegan por capricho de los desarrolladores. Los motivos por los que las lanzan a sus usuarios pueden ser varios (nuevas funcionalidades, mayor compatibilidad, etc.), pero uno de los más importantes es la corrección de fallos de seguridad detectados que son

corregidos mediante estos "parches" (códigos que integran nuevas funciones o solucionan problemas existentes en programas ya instalados).

Toda empresa dedicada al desarrollo de herramientas *software* que se precie, debe disponer de un departamento de seguridad lo suficientemente importante como para poder analizar sus productos en busca de *bugs* (agujeros de seguridad por donde un atacante puede acceder a nuestro sistema), corregirlos tan rápido como sea posible y hacérselos llegar a sus clientes, para que no sean víctimas de ataques malintencionados.

Para cualquier usuario que desee sentirse seguro es imprescindible mantener actualizado todo su *software*, desde el sistema operativo o el antivirus, hasta los paquetes de ofimática o los lectores de ficheros PDF, a través de los cuales se producen muchos más ataques de los que podemos pensar al trabajar con archivos de texto aparentemente inofensivos. Nunca, bajo ningún concepto, debemos trabajar con versiones para las cuales el desarrollador haya dejado de dar soporte, ya que éstas no se actualizan y quedan totalmente expuestas a los fallos de seguridad que se encuentren desde ese momento, sin que nadie haga nada por solucionarlos.

La mayoría de los sistemas operativos y las aplicaciones actuales tienen implementada una opción que nos permite hacer las actualizaciones de los mismos de forma automática, de modo que el usuario puede olvidarse de esta tarea. Aun así, siempre es recomendable que tengamos un cierto control sobre el estado de actualización de nuestro *software*.

En cualquier caso, aunque ya seamos conscientes de la importancia que tienen las actualizaciones, no podemos bajar la guardia y aceptar cualquier cosa que nos proponga actualizar nuestro sistema. Los ciberdelincuentes también han tenido esto en cuenta y han encontrado aquí otra vía de infección de nuestros ordenadores, disfrazando como parches su propio malware para que nosotros mismo lo instalemos. Para estar seguros de que esto no nos va a suceder solo debemos instalar las actualizaciones que nos llegan a través de los canales oficiales del desarrollador y no fiarnos de lo que podamos encontrar en cualquier página de Internet, por muy bonito que sea lo que nos ofrecen.

RECUERDA

Mantén todo el software de tu equipo siempre actualizado. De esta manera estarás tapando los agujeros de seguridad que se vayan descubriendo y se lo pondrás más difícil a los intrusos que se quieran colar en tu sistema.

CASO 4.
EL CERRAJERO DESCONOCIDO. DESCARGAS EN LA RED

¿LO HARÍAS?

Acabo de volver a casa y me he dado cuenta de que no tengo las llaves. No sé si las habré perdido o me las he dejado dentro cuando me fui, pero no hay nadie en casa ni tengo otro juego fuera, así que no me va a quedar más remedio que llamar a un cerrajero de guardia, con la consiguiente factura que me va a cobrar. Pero tengo suerte: sé que hay gente que se ofrece a venir hasta mi casa para abrirme la puerta y cambiarme la cerradura sin cobrarme absolutamente nada. Me fiaré de ellos y me ahorraré ese dinero que me viene muy bien.

Si alguien se ofrece a hacernos ese trabajo desinteresadamente, lo primero que pensamos es que tiene algún objetivo oculto. Nadie trabaja gratis, y menos cuando por esa misma labor mucha gente cobra una cantidad importante de dinero. Tal vez, de primeras, me venga bien no pagar la cantidad que me pediría un cerrajero de guardia, pero es muy probable que a los pocos días llegue a mi casa y me la encuentre desvalijada. Lo que en un principio nos ha hecho ahorrarnos unos euros, a la larga nos ha salido mucho más caro.

De forma contraria a lo que nos pasa en la vida real, donde entendemos que cualquier trabajo tiene un precio para quien lo realiza, la proliferación en Internet de páginas de descarga ilegales nos ha creado la errónea idea de que en la red todo se puede encontrar de forma gratuita. Pero esta falsa creencia nos puede poner en grave peligro.

Los cibercriminales saben que muchos usuarios buscan desesperadamente hacerse con diferente material sin necesidad de pagar nada por él, y aquí han vuelto a encontrar una nueva fórmula de ataque, llenando las páginas y aplicaciones de descargas (ya sean de *software*, libros, juegos o material multimedia) de *malware* con el que infectar a todo aquel que descargue ese contenido.

Te descargas la última versión de tu *software* preferido de retoque de fotografías, pero antes que pagar por él en la página del desarrollador, entras en una red P2P para descargarlo gratis. Lo instalas y ejecutas el *crack* o el *keygen* que viene en la carpeta para que quite la restricción del periodo de prueba y listo, ya tienes el programa a tu merced. Tú te has fiado de quien ha subido ese *crack*, pero no sabes qué es lo que realmente has ejecutado en tu equipo; y de repente tu escritorio se ha llenado de iconos que no sabes de dónde han salido, tu navegador tiene unas barras de herramientas que no habías visto nunca, no hacen más que salir ventanas

de publicidad según trabajas y, cuando quieres hacer una búsqueda en Internet, tu buscador habitual ha sido sustituido por un tal ASK del que nunca habías oído hablar.

Está claro, ya te han infectado. No sabes cómo ha pasado, puesto que no has hecho nada raro últimamente con el ordenador, pero la verdad es que tú mismo has sido el responsable de la infección.

Figura 2.3. Noticia de la Vanguardia digital sobre descargas piratas

Evidentemente no todas las descargas en Internet son peligrosas. Hay *software* libre, cuyo desarrollador lo cede gratuitamente a todo aquel que lo quiera utilizar, o *freeware*, que permite el uso del programa bajo unas determinadas condiciones. Pero en muchas ocasiones saber descargar de forma segura en Internet es una labor bastante complicada que requiere años de experiencia para poder hacerlo de forma correcta.

Aún con esto, nos podemos encontrar con la necesidad de realizar alguna descarga desde la red, situación ante la cual debemos seguir una serie de consejos para no correr riesgos innecesarios:

- Nunca realices descargas ilegales de ningún tipo de contenido.
- Si quieres utilizar algún programa de pago, busca alternativas de *software* libre antes que versiones "crackeadas". Te ofrecerán las mismas posibilidades sin riesgo de infección, y sin estar cometiendo un delito, por supuesto.
- Mantén tu antivirus actualizado.
- Descarga únicamente de los sitios web oficiales o de sitios de confianza. Pon atención, hay sitios que parecen los oficiales, pero que en realidad son meras copias de estos para estafarte.

- Fíjate en que la extensión del archivo que descargas concuerda con lo que tú estás buscando. Si descargas un archivo de texto no puede tener una extensión .exe.
- Ten especial cuidado con el contenido de archivos comprimidos (.rar o .zip). Es muy fácil esconder en ellos *malware* entre el resto de ficheros.
- Comprueba que el tamaño del archivo que vas a bajar es acorde con el tipo de fichero que supuestamente es. Si ves un texto de 1 GB o un archivo de vídeo de 500 KB, desconfía.
- Si descargas desde páginas web de enlaces o redes P2P, consulta los comentarios de otros usuarios sobre el enlace (nos pueden dar información de si el enlace es de fiar o no), quién ha subido el archivo (puedes buscar referencias en Internet) o las Fuentes de descarga, o lo que es lo mismo, la cantidad de gente que tiene ese material (normalmente es más fiable cuanta más gente lo tiene. Si descargas un malware nadie quiere dejarlo en su equipo).

RECUERDA

Sé precavido en las descargas que haces por internet. Acudir a las descargas ilegales para ahorrarte unos euros puede hacerte perder muchos más después y darte quebraderos de cabeza. Busca software libre que pueda cubrir tus necesidades sin poner en riesgo tu seguridad.

CASO 5.
LA LLAVE QUE TODO LO ABRE. CONTRASEÑAS SEGURAS

¿LO HARÍAS?

Estoy harto de tener que cargar en el bolsillo cada día con un montón de llaves distintas, me abulta demasiado. Además, he leído hace poco que han inventado unas nuevas llaves maestras que son totalmente planas, no tienen muescas, abren cualquier cosa y de las que tú mismo puedes hacerte tus propias copias por si las pierdes. No voy a perder ni un segundo más y voy a instalar una cerradura de este tipo en mi casa, en el coche, en el trabajo. Así solo me hará falta tener una llave y, al ser tan fácil de reproducir, si la pierdo me hago otra y listo.

Las cerraduras y las llaves se inventaron por algo. Nadie quiere que cualquiera pueda entrar en su casa cuando le apetezca y hacer lo que le venga en gana, así que en nuestras propiedades más valiosas instalamos puertas con cerraduras que únicamente pueden ser abiertas con la llave que solo nosotros tenemos.

Aunque me pesen un poco más en el bolsillo, prefiero llevar un juego de llaves para cada cosa. Si pierdo las llaves de mi coche, no quiero que puedan entrar en mi casa. Incluso nos sentimos más seguros cuanto más compleja es la forma de la llave, así será mucho más difícil reproducirla.

Si trasladamos este concepto a nuestra vida digital, nuestras propiedades más valiosas son las cuentas que utilizamos, en las que tenemos toda nuestra información, sus cerraduras son las credenciales de acceso y nuestra llave para abrirlas es la contraseña que utilicemos en cada caso. Para nuestra casa queremos una puerta blindada con una llave difícil de copiar, eso está claro, pero cuando se trata de la contraseña de nuestro correo electrónico parece que no tenemos tan clara esta preferencia.

La autenticación mediante nombre de usuario y *password* es, sin duda, la más extendida en la red. Cualquiera que use un ordenador conectado a Internet de forma habitual maneja muchas de estas credenciales al cabo del día, y por comodidad o por miedo al olvido, tendemos a usar los mismos datos para todo tipo de sesiones: correo electrónico, redes sociales, cuentas bancarias, páginas de compra *online*…

Este es el primer gran error que cometemos. Si un ciberdelincuente consigue romper nuestra contraseña del correo electrónico, automáticamente le hemos facilitado el trabajo para que pueda acceder a cualquier otra cuenta en la que nos autentiquemos con esos datos.

Hemos dado el primer paso hacia nuestra seguridad digital en cuanto a contraseñas se refiere. ¿Qué más podemos hacer? Después de conseguir que si nos roban un *password*, sea solo uno el que se lleven, nuestro segundo paso debe ser intentar que no nos roben ese tampoco, para lo cual nos vamos a asegurar de que nuestra contraseña sea lo suficientemente robusta como para que no nos la puedan romper fácilmente.

Para poder considerar una clave como robusta debe cumplir las siguientes características:

- Debe tener una longitud mínima de ocho caracteres. Cuanto mayor sea, más difícil será de romper.
- Estará formada por letras mayúsculas, minúsculas, números y caracteres especiales o signos.

- No será una palabra con sentido propio, ni una combinación de ellas. Existen programas que, mediante diccionarios, van probando las palabras de los lenguajes como posibles contraseñas hasta que encuentran la que es en realidad.
- No contendrá información personal (fechas, nombres). Poner la fecha del cumpleaños o el aniversario es un método muy extendido pero poco seguro, más teniendo en cuenta la cantidad de información personal que exponemos en las redes sociales al alcance de cualquiera.
- Serán distintas para cada página o aplicación.
- Las cambiaremos de forma periódica. Cada año puede ser bueno renovar todas nuestras claves.

Figura 2.4. Debemos ser conscientes de la importancia de la seguridad de nuestras contraseñas

Bien, ya sabemos cómo tienen que ser nuestras contraseñas, pero está claro que inventarnos y (sobre todo) recordar estos "chorros" de caracteres sin sentido no nos va a resultar una tarea trivial. Tranquilo, para todo hay solución.

Existen infinidad de páginas web donde podemos encontrar generadores de claves aleatorias según las características que nosotros le marquemos. Por ejemplo, en *http://www.clavesegura.org* se nos ofrece una potente herramienta donde podremos elegir la longitud (de 4 a 20 caracteres) y el tipo de caracteres que queramos incluir.

Esto nos va a ofrecer una gran seguridad en cuanto a la fortaleza de nuestras contraseñas, pero al no ser nuestras se nos pueden olvidar muy fácilmente. Tenemos también la opción de desarrollar las nuestras propias siguiendo los pasos que se explican en el "Anexo II - Crear contraseñas seguras", donde explico un método muy sencillo para obtener claves robustas y fáciles de recordar.

¿Y cómo hago yo ahora para recordar todo esto? Mi 04041994 me lo aprendía sin problema, pero no voy a ser capaz de aprender mi nueva J7*huo45_CXt6W, y como ésta, tengo otras diez o veinte. Ya está, las voy apuntando todas en un papel o en un documento de Word y cuando las necesite solo las tengo que consultar ahí. Error.

No estamos haciendo todo esto para ahora dejar las contraseñas al alcance de cualquiera que vea nuestro papel o que abra nuestro archivo. Para esta tarea recurrimos a los gestores de contraseñas.

Un gestor de contraseñas no es más que una aplicación que incorpora una base de datos donde vamos almacenando todas nuestras credenciales, y que para acceder a ella requiere de un nuevo *password*. LastPass o 1Password son ejemplos de este tipo de *software*, que con un interfaz y un manejo muy sencillo nos brindan este plus de seguridad que buscamos.

Mi consejo es instalar uno de estos programas, que son multiplataforma, y que podremos tener en nuestro ordenador y nuestro teléfono móvil, y para acceder a él crear una contraseña fuerte que seamos capaces de recordar fácilmente, como explico en el Anexo II. De esta forma podemos tener una clave distinta para cada sitio, robusta y que no olvidemos nunca.

Pero nada de esto será efectivo si aun habiendo tomado todas estas medidas le desvelamos nuestro password a alguien. Nosotros podemos estar preocupados por nuestra seguridad, pero no sabemos el uso que va a hacer de ella cualquier otra persona, así que el mayor requisito de seguridad que tenemos que seguir es no compartir nunca nuestras claves con nadie. Las contraseñas son una información personal y secreta, y así deben continuar siéndolo.

RECUERDA

Procura que tus contraseñas sean robustas y cámbialas de forma periódica. Nunca compartas con nadie tus contraseñas, no le des a cualquiera la llave de la puerta de tu intimidad digital.

CASO 6.
LA LLAVE EN LA CERRADURA. NO RECORDAR CONTRASEÑAS AUTOMÁTICAMENTE

¿LO HARÍAS?

Me he estado fijando últimamente en la cantidad de tiempo que pierdo todos los días al llegar a casa solo para abrir la puerta. Tengo que ponerme a buscar las llaves en la mochila, que casi siempre están al fondo del todo, sacarlas, meterlas en la cerradura y girar hasta que puedo entrar. Pero creo que he encontrado la solución; voy a dejar las llaves puestas todos los días, así cuando llegue ya no tengo que buscarlas y gano un poco de tiempo y comodidad.

Si en la puerta de mi casa pongo cerraduras es para mantenerme a salvo de intrusiones no deseadas. No tiene ningún sentido dejar las llaves puestas para que el primero que pase por delante las vea y, únicamente girando el bombín, entre en mi vivienda y pueda hacer dentro de ella lo que quiera; incluso podría cambiar la cerradura por una nueva impidiéndome entrar a mí en ella.

Como ya hemos visto en el caso anterior, la contraseña que nosotros empleamos en nuestras cuentas hace las veces de llave para acceder a su contenido. Si alguien sabe nuestro nombre de usuario y nuestro *password*, ya tiene la dirección y las llaves para entrar.

En nuestro día a día utilizamos una gran cantidad de páginas web y aplicaciones que se sirven de este sistema de autentificación para su uso, y en muchas de ellas, nos ofrecen la posibilidad de recordar en el equipo tanto el nombre de usuario como la contraseña, con vistas a nuestra comodidad al no tener que introducir los datos cada vez que deseemos entrar en ellas. Pero lo que en un principio nos puede parecer una ayuda, se puede convertir en una grave amenaza hacia nuestra seguridad digital.

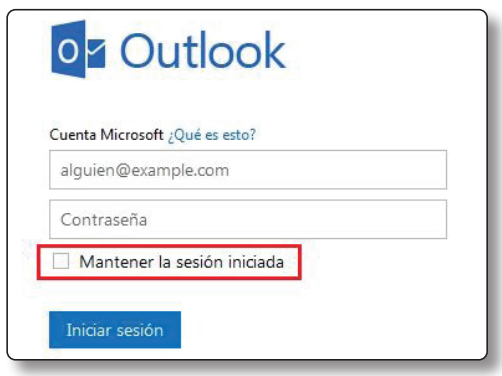

Figura 2.5. No debemos almacenar nuestros datos de inicio de sesión en webs y aplicaciones