La correcta gestión de las contraseñas como elemento esencial de **seguridad de la información**

Francisco Menéndez Piñera
CEO en SIGEA.
Consultor en Seguridad, Privacidad y Gobierno TI

> ***"Hay dos posibles puntos de fuga de información que pueden comprometer la seguridad: NOSOTROS y el SISTEMA DE INFORMACIÓN"***

Los responsables de seguridad de las organizaciones mantienen, desde el origen de los tiempos informáticos, una lucha constante con los usuarios (y, en ocasiones, también con los administradores de sistemas) a propósito del correcto uso de las contraseñas. En este artículo voy a intentar explicar cómo funciona el proceso de autenticación y el porqué de la importancia de la correcta gestión de las contraseñas.

Nos pasamos el día accediendo a diferentes sistemas informáticos, ya sea para temas profesionales o privados. Para que el sistema nos deje acceder debe tener la seguridad de que quien llama a la puerta es quien dice ser. Para ello existe el subsistema de autenticación, que utiliza uno o varios de los siguientes elementos para comprobar que realmente somos quienes decimos ser:

Algo que sabemos
(por ejemplo, una contraseña)
Algo que tenemos
(por ejemplo, una llave)
Algo que somos
(por ejemplo, nuestra huella dactilar)

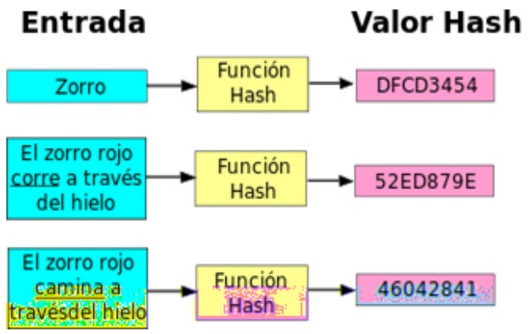
En la gran mayoría de los casos el sistema utilizado, por ser el más sencillo de gestionar, es el de autenticación por usuario y contraseña. El sistema nos pregunta primero nuestro usuario (¿quién eres?), y a continuación nos pedirá la contraseña de ese usuario.

Una vez que introducimos esta información, el sistema la compara con la que tiene almacenada en el subsistema de control de accesos, y decide si podemos o no acceder, y los permisos que tendremos en el sistema. La información que el sistema tiene almacenada es la que nosotros hemos introducido en el proceso de registro, o la que el administrador de sistemas ha generado al crear nuestra cuenta. En este último caso, lo primero que debemos hacer es cambiar la contraseña que nos han generado, para asegurarnos que solo la sabemos nosotros y el sistema, pero no los administradores de ese sistema, ya que las contraseñas se almacenan cifradas (o así debería ser).

De lo anterior, se deduce que hay dos entes que conocen nuestro usuario y contraseña, nosotros y el sistema de información. Por lo tanto, hay dos posibles puntos de fuga de información que pueden comprometer la seguridad.

Vamos a analizar primero cómo se intenta reforzar la seguridad por parte de los sistemas de información:

Como mencionaba anteriormente, las contraseñas se almacenan cifradas en bases de datos que gestiona el subsistema de control de accesos de los sistemas de información. Para ello, se suelen utilizar funciones HASH, funciones matemáticas que cifran la cadena de entrada en una cadena de salida de longitud fija y en formato hexadecimal. Este cifrado no es reversible; es decir, no es posible obtener la cadena de entrada a partir de la cadena de salida utilizando una función inversa. Cuando el usuario mete la contraseña durante el proceso de registro, se calcula su hash y es éste el que se almacena. Posteriormente, cuando un usuario quiere acceder, se calcula el hash de la contraseña introducida en ese momento y se compara con el hash almacenado. De esta forma, en el caso de que alguien consiga acceder a la base de datos de usuarios y contraseñas del sistema de información, lo que obtendrá será un conjunto de usuarios y los correspondientes valores hash de las contraseñas, que si son introducidos en el proceso de autenticación darán un error.



Parecería que, con este tipo de medidas, nuestras contraseñas están totalmente seguras por la parte de los sistemas de información. Pero no es así, en absoluto. Si “los malos” se hacen con una base de datos de contraseñas, tienen dos posibles maneras de atacarla:

Por diccionario: En un archivo se introducen miles de palabras y se calcula su hash. Posteriormente se busca ese hash entre los de la base de datos atacada y si se localiza ya tenemos la contraseña. Esta es la razón por la que se aconseja no utilizar palabras reales, que existan en el diccionario, como contraseña.

Por fuerza bruta: Se prueban todas las combinaciones posibles de caracteres alfanuméricos, calculando su hash y buscando éste en la base de datos atacada. Por este motivo, se aconseja el uso de contraseñas de una longitud mínima y complejas (que combinen números, letras minúsculas y mayúsculas, y caracteres especiales).

Veamos como influyen longitud y complejidad en dificultar ambos ataques, especialmente el de fuerza bruta:

El número de combinaciones posibles depende de dos factores: el número de caracteres utilizados (n) y el juego de caracteres posibles (c). La fórmula para saber el número total de combinaciones (T) es:

$$T = c^n$$

Si utilizamos contraseñas de cuatro caracteres y con un juego de caracteres solo numérico (como es el caso de los PIN de los teléfonos móviles), tendremos T=10^4 = 10.000 combinaciones posibles, del 0000 al 9999. Con la potencia actual de los ordenadores se tardaría unos pocos segundos en saber una contraseña de estas características por fuerza bruta.

Si en vez de utilizar solo caracteres numéricos, añadimos letras mayúsculas y minúsculas tendremos un juego de caracteres de 64 elementos (10 números, 27 mayúsculas y 27 minúsculas), con lo que ahora tendríamos T=64^4 = 16.777.216 combinaciones posibles. En este caso la fuerza bruta conseguiría su objetivo en aproximadamente un minuto.

Si a eso le añadimos los alrededor de 40 caracteres especiales que existen (@#$%_-*+[] ...), obtendremos T=104^4 = 116.985.856 combinaciones posibles, utilizando tan solo cuatro caracteres. En este caso la fuerza bruta conseguiría su objetivo en aproximadamente tres minutos.

Sin embargo, aumentando la longitud de la contraseña a 8 caracteres, y utilizando todo el juego de caracteres, obtendríamos T=104^8 = 13.685.690.504.052.700 combinaciones posibles, y un ataque por fuerza bruta necesitaría alrededor de 464 años para tener éxito.

Una vez conocido lo anterior, veamos qu**é podemos poner de nuestra parte** los usuarios para aumentar la seguridad de nuestra información.

Lo primero, las contraseñas son secretas. Ya sé que es obvio, pero no lo parece viendo los usos y costumbres de los usuarios. Nuestras **contraseñas solo las debemos saber nosotros** y no se dan a nadie, ni al administrador de sistemas ni al dueño de la empresa para la que trabajamos. Un caso habitual es que nos pidan la contraseña del correo del trabajo para que se pueda acceder a él mientras estamos de vacaciones. Nadie tiene que saber la contraseña de nuestro correo profesional, hay varias formas de solucionar ese problema; como, por ejemplo, la redirección de correos.

Debemos utilizar **contraseñas robustas,** con una longitud mínima de ocho caracteres y utilizando el mayor juego de caracteres posible (en algunos sistemas no admiten caracteres especiales, y en otros solo caracteres numéricos).

Las contraseñas que usemos **no deben ser palabras de uso común** que se pueden encontrar el diccionario español, inglés, etc.

Una buena opción es **utilizar frases** que, aunque utilizan palabras de uso común, son muy robustas por la longitud. Además, podemos realizar algunas sustituciones de caracteres. Las obvias (5 = S; 0 = O; 3 = E) son sencillas y conocidas, pero también ayudan a aumentar la complejidad. Por ejemplo, una contraseña que sea “Mi perro se llama Oscar” se transformaría en “Mi p3rr0 53 llama 05car”

Nuestras contraseñas deben ser **impersonales.** Es decir, nada que tenga que ver con nuestros datos personales: fecha de cumpleaños, nombre del perro (ya sé que lo he utilizado en el ejemplo anterior), números de teléfono, DNI, etc.

Debemos utilizar **contraseñas diferentes** para cada caso. Si utilizamos la misma contraseña para todas las redes sociales, y alguien descubre nuestro usuario y contraseña para una de ellas, lo primero que va a hacer es probar en el resto de redes sociales con el mismo usuario y contraseña. Una contraseña que tiene que

> ***“Nuestras contraseñas deben ser impersonales y diferentes para cada caso”***

ser espacialmente robusta (larga y compleja) es la de la cuenta de correo que utilizamos como cuenta principal, que es donde recibimos las confirmaciones de nuestros registros en los diferentes servicios, donde nos avisan si ha habido algún incidente con nuestras cuentas en las redes sociales, y que, habitualmente es el mismo correo que utilizamos como usuario en multitud de sitios. Esa cuenta de correo principal tiene que tener una contraseña robusta y diferente a las utilizadas en cualquier otro sitio.

Es especialmente importante no utilizar las mismas contraseñas **para temas personales y para temas profesionales.**

Mucho cuidado en **sitios públicos**, especialmente en las cafeterías. Una de las formas más habituales de robo de contraseñas sigue siendo la que se conoce como "shoulder surfing" (mirar por encima del hombro). Sobre todo con los móviles, cuyo PIN solo es de 4 dígitos; primero intentan averiguar el PIN observándote cuando lo introduces y, solo entonces, hacen todo lo posible por robártelo.

Las contraseñas **se deben cambiar** con una frecuencia que dependerá de su importancia. Las más importantes se deben cambiar con mayor frecuencia. Las de temas profesionales y la de nuestra cuenta principal de correo deberían cambiarse, al menos, cada seis meses; o inmediatamente cuando tengamos la sospecha de que alguien la pueda conocer.

Donde sea posible, y especialmente para las contraseñas más importantes, conviene utilizar el **doble factor de autentificación**. Al principio del artículo vimos que hay tres tipos de elementos para autentificarnos. Hasta ahora solo hemos hablado de "algo que sabemos", la contraseña.

En muchos sitios ya podemos añadir un segundo factor de autentificación que el servicio nos solicitará además de la contraseña. Este segundo factor ("algo que tenemos") puede ser un código que nos envíen al móvil, nuestro DNI electrónico, etc.

A estas alturas os estaréis preguntando cómo gestionar vuestras contraseñas con todos estos requisitos y con la cantidad de ellas que utilizamos a diario. Por supuesto, las contraseñas **no deben estar anotadas** en ninguna libreta, ni en esas famosas etiquetas amarillas que parecen diseñadas para ello. Lo adecuado es utilizar un **gestor de contraseñas** (existen varios gratuitos y de pago). Se trata de una aplicación que nos permite almacenar nuestras contraseñas de forma cifrada, y gestionarlas cómodamente. Eso sí, la contraseña utilizada para acceder a nuestro gestor tiene que ser especialmente robusta y, a la vez, fácil de recordar.

Como auditor de seguridad de sistemas de información, me encuentro habitualmente con muchos errores en la gestión de las contraseñas, tanto por parte de los usuarios como por parte de las organizaciones. Espero haber ayudado, con este artículo, a aclarar algunos conceptos y a la concienciación de la importancia de una correcta gestión de las contraseñas.