INSTITUTO NACIONAL DE CIBERSEGURIDAD

GESTIÓN DE LA PRIVACIDAD, IDENTIDAD DIGITAL Y REPUTACIÓN ONLINE EN INTERNET

GOBIERNO DE ESPAÑA
MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

INSTITUTO NACIONAL DE CIBERSEGURIDAD

017

MÓDULO 8

Gestión de contraseñas

ÍNDICE

1. ¿Por qué son tan importantes las contraseñas?

En los años 60[1], las primeras contraseñas se limitaban al uso de una única computadora que compartían científicos del MIT, la primera fue creada por el profesor de informática del MIT Fernando Corbató. Estos científicos**,** accedían a contenido académico con diferentes niveles de privilegio. El resto del planeta vivía ajeno a esta circunstancia, ya que no existía el concepto de seguridad informática, tal y como lo entendemos hoy día.

A partir de los 60, el uso de contraseña fue incorporándose debido a la necesidad incipiente que tenían los sectores empresariales y académicos de proteger toda la información que disponían en sus sistemas informáticos.

En el año 1989 el científico británico *Sir Tim Berners-Lee* creó el primer sistema de gestión informática en línea conocido popularmente por `www´, fue entonces, cuando se produjo una auténtica revolución. Se empezaron a abrir las primeras direcciones de correo electrónico en plataformas novedosas que obligaban a disponer de una clave de acceso. En sus inicios, eran claves sencillas, y al no ser conscientes de la repercusión sobre nuestra privacidad, nos limitábamos a crearlas con una numeración correlativa o datos representativos, como nuestro nombre o apellidos.

Hoy en día guardamos bajo una contraseña una gran cantidad de información confidencial en diferentes servicios y aplicaciones. La captura y subasta de nuestros datos personales son el bien más codiciado por los ciberdelincuentes, junto con los delitos relacionados con la **usurpación de identidad** con fines relacionados con las estafas monetarias.

Para evitar esta situación, es de vital importancia el uso de contraseñas fuertes que actúen de barrera contra estos delitos cibernéticos.

El acceso a la banca *online*, correo electrónico, redes sociales y un sinfín de servicios más hacen que el uso de la contraseña sea vital para nuestros intereses. Contraseñas poco robustas y sencillas pueden llevar a su vulneración y, por tanto, a una exposición de nuestra privacidad. Nuestros hábitos han cambiado y, al igual que cerramos la puerta de casa al salir de ella, debemos cerrar bien el acceso a nuestros datos de carácter personal en los entornos digitales para evitar ser

[1]. Consultado en https://www.welivesecurity.com/la-es/2017/05/04/dia-de-la-contrasena-origen/

vulnerables, y este cierre no es otro que a través de la implantación y uso rutinario de contraseñas robustas.

Según un estudio realizado a finales de 2021 por la empresa WP Engine[2], las credenciales que utilizamos para proteger nuestros archivos son simples y fáciles de descifrar. El análisis muestral asciende a 10 millones de contraseñas arrojando los siguientes resultados:

The 50 Most Used Passwords				
1. 123456	**11.** 123123	**21.** Mustang	**31**. 777777	**41.** Harley
2. password	**12.** baseball	**22.** 666666	**32.** f*cky*u	**42.** zxcvbnm
3. 12345678	**13.** abc123	**23**. qwertyuiop	**33.** qazwsx	**43.** asdfgh
4. qwerty	**14.** football	**24.** 123321	**34.** jordan	**44**. buster
5. 123456789	**15.** monkey	**25.** 1234...890	**35.** Jennifer	**45**. Andrew
6. 12345	**16.** letmein	**26.** p*s*y	**36.** 123qwe	**46**. batman
7. 1234	**17.** shadow	**27.** Superman	**37**. 121212	**47**. soccer
8. 11111	**18.** master	**28.** 270	**38.** killer	**48**. tigger
9.1234567	**19.** 696969	**29.** 654321	**39**. trustno1	**49.** Charlie
10. dragon	**20**. michael	**30.** 1qaz2wsx	**40**. hunter	**50**. rober

Como se puede evidenciar, la cadena numérica 123456 es la que más se utiliza. Todas las contraseñas del listado están lejos de ser contraseñas seguras, no cumpliendo en la mayoría de los casos los requisitos básicos que veremos más adelante.

Las razones por las que se usan este tipo de contraseñas tan vulnerables suelen ser, entre otras, la facilidad de recordarlas, comodidad y por la falta de concienciación sobre seguridad informática a nivel general de la población.

[2]. Consultado en https://wpengine.com/resources/passwords-unmasked-infographic/

Estudios más recientes realizados por la empresa de ciberseguridad *Home Security Heroes*, publicó un informe basándose en la Inteligencia Artificial y usando la herramienta *PassGAN* para descifrar 15.600.000 contraseñas, arrojando los siguientes resultados; las contraseñas más comunes pueden ser descifradas en menos de un minuto, el 65% en menos de una hora, el 71% en menos de un día y el 81% en menos de un mes. En el siguiente enlace se puede ver más detalladamente estos datos: Datos herramienta PassGan.

¿Las contraseñas robustas nos garantizan la seguridad al 100%? En primer lugar, debemos tener claro que el concepto de seguridad total no existe y que, actualmente, con el uso de la IA, estamos mucho más expuestos a que los hackers accedan a nuestras contraseñas en menos de un minuto, tal y como hemos podido comprobar en la información anterior. Pero sí es cierto que podemos entender las contraseñas como una primera capa de seguridad que podemos hacer aún más robusta añadiendo una segunda capa o incluso tres capas a través del doble factor de autenticación y la autenticación multifactor respectivamente, que veremos en el apartado 3 de este mismo módulo.

2. Consejos y presentación

A continuación, vamos a exponer una serie de consejos y recomendaciones al respecto de cómo crear contraseñas seguras, los requisitos que deben cumplir y los sistemas que existen para gestionarlas y archivarlas.

Si eres de esas personas a las que les gusta ir un paso más allá en la gestión y configuración de contraseñas en las cuentas en línea, existen **servicios de gestores de contraseñas**. Estos permiten guardar de manera segura las principales contraseñas que se utilizan para acceder a los diferentes servicios de Internet. Con ello, te obligas a no tener una "clave para todo" sino diferentes credenciales para diferentes servicios. Con este sistema las tienes ordenadas y se activan en función del servicio en la red para las que se hayan creado mediante sistemas de autocompletado.

En la actualidad, hay muchas herramientas que tienen función de gestor de contraseñas. En general, suelen ser gratuitos con alguna opción de pago. Entre los más conocidos encontramos: LastPass y KeePass. No obstante, en el espacio web de ciudadanía (Oficina de Seguridad del Internauta, OSI) de INCIBE, en concreto en su sección de herramientas, encontrarás más opciones.

Además, tienes a tu alcance herramientas de tipo **generadores de contraseñas** (función que también suelen integrar los gestores de contraseñas), y que nos permiten crearlas desde el inicio de manera robusta. Existen múltiples servicios de generación de contraseñas efectivas. A modo de ejemplo, puedes probar:

- https://passwordsgenerator.net/es/

Este generador permite definir el número de caracteres, el uso de letras y números, mayúsculas, minúsculas y símbolos. Además, las contraseñas que compone son difíciles de descodificar, ya que no están sujetas a patrones personales.

Otra herramienta útil son los generadores de contraseñas basados en **accesos biométricos**, como puede ser mediante la huella dactilar, el acceso biométrico facial, el reconocimiento de la mano o incluso algunos más novedosos como el control del iris y la retina. En el siguiente artículo podréis obtener más datos sobre este hecho; la retina como identificación biométrica.

Por último, la **autenticación multifactorial**, MFA, precisa que la persona usuaria proporcione dos o más formas de autenticación para acceder a una cuenta o sistema.

En cambio, si no quieres utilizar estos recursos en línea y las quieres **generar por tu cuenta**, debes tener siempre presente las siguientes indicaciones y consejos:

- **No uses la misma contraseña** para diferentes fines: no mezcles las contraseñas del banco (por ejemplo) con las credenciales de tu dirección de correo electrónico.
- **Evita utilizar conceptos evidentes y cotidianos**, como tu nombre y apellidos, tus iniciales, el nombre de tu equipo deportivo preferido o el de tu mascota.
- **Tampoco utilices datos identificativos**, como tu fecha de nacimiento, dirección, DNI o número de la seguridad social.
- Procura darle una **longitud mayor de 8 caracteres**, introduciendo **letras, números, mayúsculas, minúsculas y símbolos**.
- **Evita utilizar contraseñas iguales** para diferentes servicios. Si un ciberdelincuente te roba una, podría acceder al resto de tus servicios online.
- **Cambia la contraseña periódicamente**. En caso de credenciales empresariales, estos cambios vendrán definidos por una política de seguridad de la información que indicará la periodicidad. Para uso personal se recomienda cambiarla, al menos, una vez al año o cuando existen sospechas de usurpación o brecha de seguridad.
- **Activa la verificación en dos pasos** siempre que sea posible para garantizar que eres tú el que estás accediendo a la plataforma o servicio. Además de tu

contraseña, pedirán verificación de algo que poseas (SMS en teléfono móvil) o algo que sea solo tuyo (huella dactilar).

- **Evita guardar contraseñas en la nube**, especialmente si el servicio no cifra la información. Un *hackeo* o un ataque masivo a servidores en la nube pueden poner en peligro tus contraseñas.
- **Nunca facilites tus contraseñas** a nadie por correo electrónico, ni en formato papel ni verbalmente. Recuerda que la contraseña es personal e intransferible y nuestro concepto de seguridad no tiene por qué ser el de otro.
- **Considera usar alguna frase en tu contraseña.** No te limites a usar una sola palabra combínalas en una frase "Niñafelizjuegamuñeca24".
- **Emplea reglas mnemotécnicas.** Las reglas mnemotécnicas pueden ser unas grandes aliadas a la hora de generar contraseñas y, lo más importante, recordarlas. Algunos ejemplos pueden ser añadir asteriscos al principio y al final de la contraseña, convertir las letras de una palabra en concreto en números, etc.

De manera adicional, se deben aplicar las siguientes recomendaciones:

No envíes información privada o de relevancia a través de conexiones HTTP, ya que los mensajes en este tipo de conexiones pueden ser objeto de ataques de tipo *sniffing* (ciberataque a paquetes de datos que circulan por redes) muy fácilmente al no viajar cifrada la información por la Red. **Deberías usar conexiones que cifran tu información, como HTTPS.**

No permitas que tus navegadores web (Firefox, Chrome, Safari u Opera) **guarden tus contraseñas**, especialmente si compartes el dispositivo con otros usuarios. Podrían acceder a todas tus cuentas de usuario.

No accedas al banco o a cuentas importantes desde ordenadores que no sean de tu uso habitual, pueden copiar tu credencial con facilidad si hubiera instalado algún programa malicioso en él.

No te conectes a redes wifi públicas. No es seguro acceder a tus espacios privados, ya que la red podría estar configurada de manera insegura y otra persona conectada a ella intentar captar la información que intercambias por Internet, incluidas las contraseñas.

Siempre que vayas a **introducir tu usuario y contraseña** para un servicio bancario, hazlo **desde las webs corporativas oficiales de las entidades bancarias.** Nunca lo hagas desde enlaces provenientes de otras webs, *banners* publicitarios, SMS, etc.

Mantén actualizados los sistemas operativos (Windows, macOS, iOS o Linux) **y navegadores** (Chrome, Firefox, Opera, etc.) con los últimos parches de seguridad.

Sigue protocolos de mesas limpias en tu actividad personal y profesional. Evita dejar anotaciones sobre credenciales en pósits, libretas, carpetas abiertas del escritorio del PC, etc. Bloquea el ordenador y el teléfono siempre que dejes de usarlo o vayas a estar ausente.

Con todas estas recomendaciones, podrás hacer una gestión segura de tus contraseñas. ¡Ponlas en práctica!

3. Doble factor de autentificación

De manera cotidiana y tradicional el acceso a nuestro entorno digital se ha llevado a cabo mediante usuario y contraseña, mecanismo insuficiente para aquellos servicios en línea, cuyos riesgos pueden entrañar daños graves sobre nuestra reputación, salud, economía, etc.

Muchas brechas de seguridad a lo largo de los últimos tiempos han expuesto millones de credenciales de distintos servicios *online*, poniendo en riesgo la confidencialidad, integridad y disponibilidad de los datos de las personas afectadas. Además, la llegada de la pandemia a nuestras vidas ha obligado a la realización de pagos electrónicos a los que no estábamos acostumbrados con anterioridad. Estos pagos electrónicos deben disponer de mecanismos robustos de seguridad que reduzcan las vulnerabilidades propias del proceso electrónico y eviten el robo y uso posterior por parte de los ciberdelincuentes.

En nuestro ordenamiento jurídico, los servicios de pago electrónico están regulados por el Real Decreto-ley 19/2018, de 23 de noviembre, que se traspone de la directiva europea conocida como PSD2 y que tiene por objeto la aplicación de **estrictos requisitos de seguridad para garantizar los pagos electrónicos** y la protección de datos[3]. Para cubrir ambos aspectos se requieren sistemas de **doble factor de autenticación, conocidos como 2FA**.

Cabe resaltar el hecho de que los términos identificación y autenticación no son lo mismo, aunque pueden pertenecer al mismo proceso realizado. La **identificación**

[3] Real Decreto-ley 19/2018, de 23 de noviembre, de servicios de pago y otras medidas urgentes en materia financiera.

en un sistema informático que consiste en la capacidad de identificar de forma exclusiva a un usuario dentro de un grupo, comparando los datos del individuo a identificar con los datos de cada uno de los del grupo (comparación 1 a muchos). La **autenticación** es el acto de probar que es cierta la identidad reclamada por ese individuo. En este caso, se comparan los datos del individuo con aquellos asociados a la identidad que se reclama (comparación 1 a 1).

Este proceso de autenticación toma especial relevancia en los últimos años como consecuencia de que **solo la identificación no era suficiente como capa de seguridad para evitar accesos no autorizados a un sistema.**

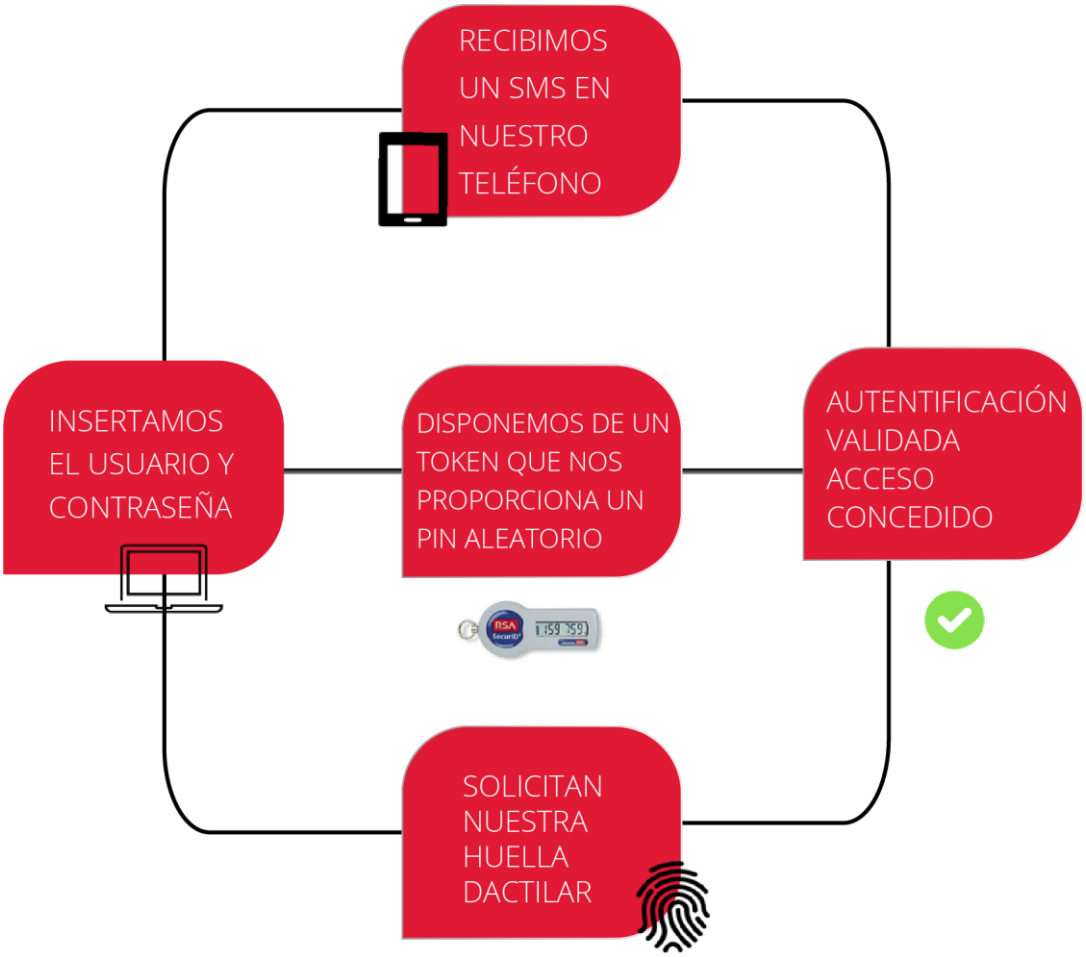
- **El 2FA proporciona entre otras:**

- Una capa adicional de seguridad que dificulta la posibilidad de acceso a nuestros servicios en línea por parte de terceros.
- Previene el robo de identidad.
- Cumple con las regulaciones establecidas en ciertas industrias, ya que en algunos casos se vuelve un requisito regulador para el cumplimiento de las leyes de seguridad y protección de datos.
- Concienciación sobre seguridad.

Debemos tener en cuenta que, aunque la finalidad que se persigue es la misma, los conceptos técnicos de doble factor de autenticación (2FA) y verificación/autenticación en dos pasos no son realmente lo mismo. La pequeña diferencia radica en que, en el primer caso, se utiliza algo que tienes, que es solo tuyo, como, por ejemplo, la huella dactilar o el tono de voz; mientras que, en el segundo caso, se verifica algo que sabes, como, por ejemplo, una contraseña o un código recibido por SMS a tu teléfono.

En cualquier caso, en general, la autenticación abarcará alguno de estos tres parámetros fundamentales: el conocimiento de algo que solo sabemos nosotros (SMS o PIN), una propiedad nuestra (móvil, llave, memoria USB o *token*) o parámetros biométricos (huella, retina o voz).

Veamos algunos ejemplos de 2FA en la siguiente imagen:



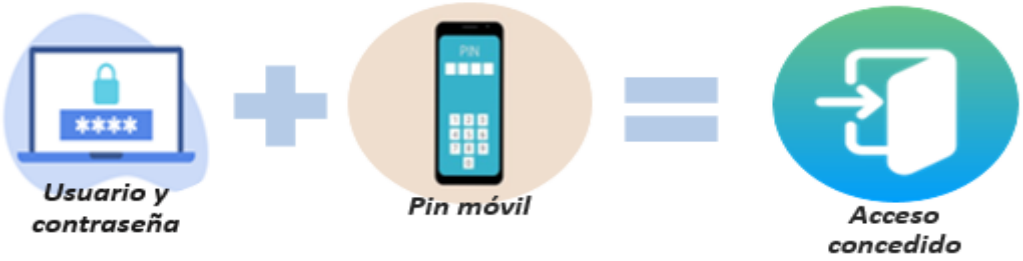
¿En qué casos es útil habilitar el doble factor de autenticación? El 2FA no es exigido por todos los servicios. Lo recomendable es habilitarlo en aquellos casos o procesos electrónicos en los que entrañen riesgos para nuestra privacidad y que pudieran llevar asociados también delitos económicos. Debería estar siempre habilitado en los casos de verificación de una operación bancaria; accesos como administrador de sistemas en una empresa; gestiones de tiendas *online*; acceso a imágenes y datos de menores, historia clínica, perfiles de redes sociales, etc.

¿Activar el 2FA garantiza la seguridad total? La seguridad total como concepto no existe, pero dentro de los sistemas de acceso a entornos digitales, buscar refuerzos como la doble autenticación nos acercan a esa situación ideal.

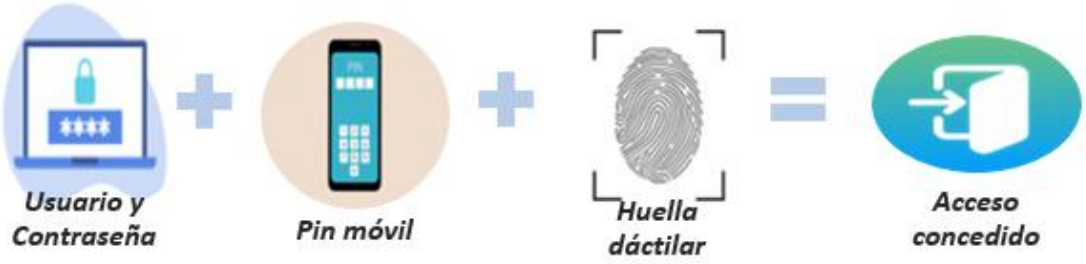
¿Es lo mismo doble factor de autenticación 2FA que autenticación multifactor MFA?

Existe una ínfima diferencia entre estos dos términos, y es que el 2FA usa dos métodos diferentes de identificación, y la MFA, utiliza sistemas de autenticación que precisa dos o más métodos de verificación para dar acceso a la persona usuaria.

En las siguientes imágenes se pueden ver dos ejemplos:



Ejemplo 2FA



Ejemplo MFA

Podría decirse que el 2FA es un subconjunto del MFA.

Por último, y para concluir con este módulo, nos planteamos la siguiente pregunta acerca de los tipos de autenticación descritos: **¿cuáles son más seguros y cuáles los más vulnerables?** Si nos ceñimos al concepto de riesgo asociado a una posible captación de una credencial, el sistema de 2FA que utiliza y envía un SMS con un PIN a nuestro teléfono móvil es mucho más elevado que verificar un segundo paso con nuestra huella dactilar. Un *hacker* puede introducir un *malware* en nuestro teléfono móvil para capturar el SMS correspondiente al 2FA, pero difícilmente podrá robar nuestra huella. Algo que es solo nuestro (voz, huella o retina) aporta mayores garantías que algo que poseemos, que puede caer en otras manos.