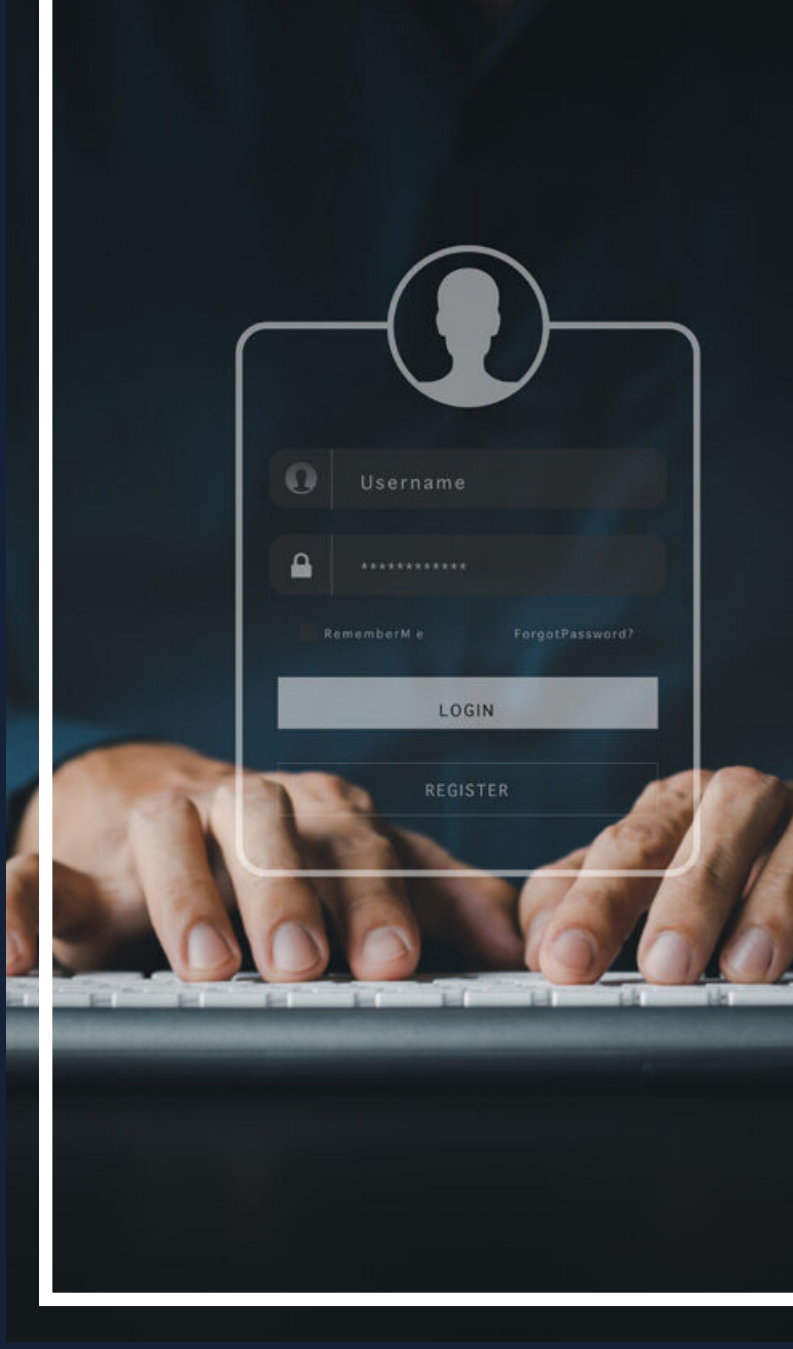
CCN-CERT

BP/35



Uso y gestión de contraseñas

INFORME DE BUENAS PRÁCTICAS

MAYO 2026

ccn-cert
centro criptológico nacional

Edita:

Fecha de edición: mayo de 2026

Índice

1. Sobre CCN-CERT, CERT Gubernamental Nacional

El CCN-CERT es la Capacidad de Respuesta a incidentes de Seguridad de la Información del Centro Criptológico Nacional, CCN, adscrito al Centro Nacional de Inteligencia, CNI. Este servicio se creó en el año 2006 como **CERT Gubernamental Nacional español** y sus funciones quedan recogidas en la Ley 11/2002 reguladora del CNI, el RD 421/2004 de regulación del CCN y en el RD 311/2022, de 3 de mayo, regulador del Esquema Nacional de Seguridad (ENS), modificado por el RD 951/2015 de 23 de octubre.

Su misión, por tanto, es contribuir a la mejora de la ciberseguridad española, siendo el centro de alerta y respuesta nacional que coopere y ayude a responder de forma rápida y eficiente a los ciberataques y a afrontar de forma activa las ciberamenazas, incluyendo la coordinación a nivel público estatal de las distintas Capacidades de Respuesta a Incidentes o Centros de Operaciones de Ciberseguridad existentes.

Todo ello, con el fin último de conseguir un ciberespacio más seguro y confiable, preservando la información clasificada (tal y como recoge el art. 4. F de la Ley 11/2002) y la información sensible, defendiendo el Patrimonio Tecnológico español, formando al personal experto, aplicando políticas y procedimientos de seguridad y empleando y desarrollando las tecnologías más adecuadas a este fin.

De acuerdo con esta normativa y la Ley 40/2015 de Régimen Jurídico del Sector Público es competencia del CCN-CERT la gestión de ciberincidentes que afecten a cualquier organismo o empresa pública. En el caso de operadores críticos del sector público la gestión de ciberincidentes se realizará por el CCN-CERT en coordinación con el CNPIC.

2. Introducción

Las contraseñas constituyen la primera línea de defensa frente a posibles accesos no autorizados en cualquier sistema, aplicación o bien, servicio digital. Se consideran el mecanismo más extendido de autenticación y, pese a los avances tecnológicos en biometría o la posibilidad de autenticarse sin contraseña, continúan siendo un elemento crítico en la protección de la información personal y corporativa.

Sin embargo, la gestión deficiente de las contraseñas o repetidas en distintos servicios sigue siendo una de las principales causas de brechas de seguridad. El uso de claves simples, como combinaciones previsibles de nombres, fechas o patrones de teclado, junto con la reutilización de contraseñas en multitud de plataformas, incrementa de manera exponencial el riesgo de exposición ante filtraciones o ataques de tipo *credential stuffing* (uso automatizado de credenciales filtradas para acceder a otros servicios).

Actualmente, los atacantes disponen de herramientas automatizadas de *cracking* y diccionarios con la capacidad de comprobar millones de combinaciones por segundo, lo que convierte las contraseñas cortas o poco complejas, en un blanco fácil. A todo ello, se suman los ataques de ingeniería social o suplantación de identidad que explotan la falta de cultura de seguridad en los usuarios para obtener sus credenciales.

Time it takes a hacker to brute force your password in 2025

Hardware: 12 x RTX 5090 | Password hash: bcrypt (10)

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	57 minutes	2 hours	4 hours
6	Instantly	46 minutes	2 days	6 days	2 weeks
7	Instantly	20 hours	4 months	1 year	2 years
8	Instantly	3 weeks	15 years	62 years	164 years
9	2 hours	2 years	791 years	3k years	11k years
10	1 day	40 years	41k years	238k years	803k years
11	1 weeks	1k years	2m years	14m years	56m years
12	3 months	27k years	111m years	917m years	3bn years
13	3 years	705k years	5bn years	56bn years	275bn years
14	28 years	18m years	300bn years	3tn years	19tn years
15	284 years	477m years	15tn years	218tn years	1qd years
16	2k years	12bn years	812tn years	13qd years	94qd years
17	28k years	322bn years	42qd years	840qd years	6qn years
18	284k years	8tn years	2qn years	52qn years	463qn years

Hive Systems

Read more and download at hivesystems.com/password

Ilustración 1: dificultad en la rotura de contraseñas **(1)**

Una contraseña débil de solo ocho caracteres con letras minúsculas puede ser vulnerada en cuestión de segundos con el *hardware* disponible. En cambio, una *passphrase* larga y compleja, que combine distintos tipos de caracteres, puede resistir durante mucho más tiempo, incluso frente a los equipos más potentes. Esta información pone de relieve la importancia de la longitud y la complejidad como factores determinantes en la seguridad de las credenciales, y sirve de referencia práctica para evaluar la eficacia de nuestras propias políticas de contraseñas.

La preocupación por la seguridad no es nueva. En la década de 1960, *John Shepherd-Barron* diseñó el primer cajero automático para *Barclays* y propuso que los usuarios introdujeran un código para identificarse. Inicialmente pensó en un PIN de 6 dígitos, pero tras consultar con su esposa, redujo la longitud a 4 dígitos

(1) Con autorización de *Hive Systems*, www.hivesystems.com

2. Introducción

para equilibrar seguridad y facilidad de uso. Este método se convirtió en un estándar global, y aunque la norma ISO 9564 permite PINs de hasta 12 dígitos, la mayoría de los cajeros siguen usando 4 por compatibilidad y simplicidad. A pesar de ofrecer solo 10.000 combinaciones posibles, el contexto lo hace seguro gracias a factores como el uso conjunto con tarjeta, limitación de intentos y vigilancia física.

Con el auge de Internet en los años 90, se popularizó el uso de contraseñas alfanuméricas y comenzaron a exigirse reglas de complejidad (mayúsculas, minúsculas, números y símbolos) ya que los sistemas no admitían claves de una longitud superior a 8 o 12 dígitos. En 1995, AT&T patentó la autenticación de doble factor (2FA), marcando el inicio de medidas más robustas. Sin embargo, a partir de 2010, las filtraciones masivas evidenciaron que muchas contraseñas eran débiles o reutilizadas, lo que llevó a cuestionar la utilidad de cambiarlas frecuentemente y a promover el uso de frases largas y únicas.

En este contexto, el uso de *passphrases* (frases de paso) se presenta como una estrategia eficaz para fortalecer la autenticación tradicional. A diferencia de las contraseñas convencionales, las *passphrases* son más largas, naturales y fáciles de recordar, lo que permite aumentar la entropía (nivel de aleatoriedad y complejidad) sin sacrificar la usabilidad.

Además, se recomienda acompañar esta práctica con el uso de gestores de contraseñas. Estas herramientas permiten almacenar, cifrar y sincronizar credenciales de forma segura, evitando la exposición accidental o el uso de contraseñas repetidas.

Por lo tanto, el empleo combinado de *passphrases* robustas, gestores de contraseñas y autenticación multifactor (MFA) representa, hoy por hoy, una de las mejores defensas frente al robo de identidades digitales y accesos no autorizados.

3. Buenas prácticas de uso y gestión de contraseñas basadas en *passphrases*

En el ámbito de la ciberseguridad, la protección de las credenciales constituye un pilar esencial en la defensa de la identidad digital. Las contraseñas o, más concretamente las *passphrases*, representan la llave de acceso a sistemas, servicios y datos sensibles, por lo que su gestión debe abordarse con criterios de seguridad, coherencia y responsabilidad.

A continuación, se detallan las buenas prácticas más relevantes, con una visión técnica y de concienciación adaptada al contexto actual de amenazas:

a **Evitar reutilizar contraseñas en diferentes plataformas o servicios.**

Reutilizar contraseñas es una de las principales causas de compromiso de cuentas en cadena. Cuando una credencial se ve expuesta en una brecha de datos, los ciberatacantes la prueban automáticamente en otros servicios

mediante técnicas como, por ejemplo, *credential stuffing*.

Usar una *passphrase* única por servicio garantiza que una posible filtración no afecte a múltiples cuentas. Además, el uso de gestores de contraseñas facilita esta práctica, evitando así, que el usuario tenga que recordar múltiples claves distintas.

b **Uso de *passphrases* en lugar de contraseñas cortas o complejas difíciles de recordar.**

Las *passphrases* o frases de paso son una alternativa segura, actual y práctica frente a las contraseñas convencionales. Mientras que una contraseña de 8 caracteres puede ser descifrada por fuerza bruta en cuestión de horas o días, una *passphrase* de 18 o más caracteres puede resistir ataques durante miles de años, según cálculos basados en la entropía o nivel de aleatoriedad.

Ejemplos con el tiempo necesario para romper la clave por ataque por fuerza bruta:

- Contraseña tradicional: *M4dr1d!25* (3 horas)
- Contraseña robusta: *vLogDT%bSnAc25* (68.519.838.080 siglos)
- *Passphrase* robusta: *EnunlugardelaMancha!25* (9.434.088.127.396 siglos)

El uso de *passphrase* tiene como ventajas principales:

- Mayor longitud significa mayor seguridad ante ataques automatizados.
- Uso de palabras o frases ayuda a recordarlo de manera más fácil.
- Posibilidad de incluir minúsculas, mayúsculas, espacios, números o símbolos para elevar la entropía.
- Es compatible con gestores de contraseñas y autenticadores modernos.

Se ha de tener en cuenta que una buena práctica es que la *passphrase* tenga sentido personal, pero no sea predecible ni se pueda relacionar con información pública del usuario, por ejemplo, fechas de nacimiento, nombres de familiares, lugares comunes, etc.

c **Activar el doble factor de autenticación (2FA) proporciona una segunda capa de seguridad independiente de la contraseña.**

Incluso si una *passphrase* se viera comprometida, el atacante tendría la necesidad de tener un segundo elemento de verificación (*token*, app autenticadora o huella digital).

Su activación reduce drásticamente el riesgo de acceso no autorizado.

Recomendación: priorizar aplicaciones autenticadoras o llaves de seguridad físicas frente al uso de SMS.

3. Buenas prácticas de uso y gestión de contraseñas basadas en *passphrase*

d **No compartir las credenciales por correo electrónico, mensajería o redes sociales.**

Se trata de información sensible y como tal, deben considerarse del mismo nivel de confidencialidad que los datos financieros o personales.

Compartir este tipo de información por medios no cifrados podría provocar su interceptación mediante *phishing*, *malware* o ingeniería social.

En contextos corporativos o de organización, se recomienda utilizar plataformas seguras de intercambio de cifrado o funciones de compartición segura en gestores de contraseñas. Si no se dispone de un medio seguro por el que enviar las credenciales, no es aconsejable enviar el usuario y contraseña por el mismo medio. En ese caso, se recomienda remitir la contraseña por un medio diferente al que se haya enviado el usuario, por ejemplo, el correo electrónico.

e **Actualizar las contraseñas tras incidentes de seguridad o filtraciones.**

Aunque las *passphrases* de mayor longitud no requieren una rotación frecuente, deben renovarse inmediatamente si hay sospechas de acceso no autorizado o exposición pública.

En entornos profesionales, las políticas internas de ciberseguridad deben definir plazos de renovación adaptados al nivel de criticidad del sistema.

f **Comprobar filtraciones mediante servicios especializados.**

Herramientas o bases de datos de *data breaches* verificadas permiten identificar si alguna credencial ha sido comprometida.

Esta práctica ayudaría a detectar incidentes de forma temprana y evitar, en la medida de los posible, la explotación de credenciales filtradas en otros sistemas.

g **Desconfiar de formularios o enlaces sospechosos.**

El *phishing* es una de las técnicas más eficaces para el robo de credenciales. Los atacantes imitan páginas legítimas para engañar al usuario y obtener sus datos de acceso.

Antes de introducir una *passphrase*:

- Verificar siempre la dirección del sitio (URL).
- Asegurar el uso de una conexión HTTPS válida.
- No acceder desde correos o enlaces no solicitados.
- Utilizar navegadores y sistemas actualizados con filtros *antiphishing* activos.

h **Utilizar otro idioma como medida adicional de seguridad en *passphrases*.**

Considerada como una práctica avanzada y actualmente poco extendida, el uso

de más de un idioma incrementa la entropía lingüística y reduce, por tanto, la eficacia de los ataques de diccionario, que suelen basarse en listas de palabras en inglés o en el idioma del usuario objetivo.

Ejemplos de uso de otro idioma:

- Combinación de español e inglés: *MilibrofavoritoTheGreatGatsby"!*
- Combinación de español y francés: *LoslunesJeBoisDuCafeEnLaTerrasse**
- Combinación de español y alemán: *MeineKatzeLiebtElsofaporlamañana/*

Algunas de las principales ventajas:

- Mejora la resistencia a ataques de diccionario dirigidos.
- Mantiene la memoria si el usuario domina o asocia el idioma con una frase significativa.
- Dificulta la predicción de estructuras gramaticales o palabras comunes.
- Dificulta la previsión de los ataques automatizados basados en patrones lingüísticos.

El uso de otro idioma conocido por el usuario y evitar combinaciones difíciles de recordar, es clave en esta práctica. Del mismo modo que lograr una frase natural, coherente y única, no simplemente mezclar palabras al azar.

No se debe verificar la robustez de una contraseña en las webs que existen al efecto ya que, a parte del desconocimiento de las "relaciones" de dichas webs, a partir de ese momento nuestra *passphrase* pasará a formar parte de diccionarios que, en caso de filtración, se incorporarán al *software* correspondiente. En caso de querer verificar la fortaleza de una contraseña, se podrá probar con una similar.

Recomendación: los gestores de contraseñas actuales permiten almacenar estas *passphrases* largas y multilingües sin limitaciones, lo que facilita su adopción incluso en entornos colaborativos.

4. Características clave de una *passphrase*

El uso de *passphrases* (frases de paso) representa una evolución en la gestión segura de contraseñas. Frente a las contraseñas tradicionales, cortas y difíciles de recordar, *passphrases* brindan un equilibrio óptimo entre seguridad, facilidad de uso y resistencia ante ataques.

A continuación, se detallan sus principales características y el motivo por el cual su adopción se considera una buena práctica.

a **Mayor longitud: entre 16 y 100 caracteres.**

Una de las principales diferencias y más relevante entre una contraseña convencional y una *passphrase* es la longitud de esta.

Las *passphrases* se componen de una secuencia de palabras o grupo de palabras que puede llegar a alcanzar longitudes de entre 16 y 100 caracteres, lo que incrementa exponencialmente su complejidad frente a un intento de descifrado.

Cuanto mayor sea la longitud de la clave, más combinaciones posibles deberá probar un atacante para descifrarla. Por ejemplo:

- Una contraseña de 8 caracteres (mezclando letras, números y símbolos) puede ser vulnerada por fuerza bruta en minutos u horas con sistemas actuales.
- En cambio, una *passphrase* de 25 caracteres, incluso compuesta únicamente por letras, podría tardar miles de años en ser descifrada mediante los mismos métodos que la anterior.

La segunda opción no es solo de mayor longitud y resistente, sino también mucho más fácil de recordar para el usuario.

4. Características clave de una *passphrase*

Por tanto, la longitud es el principal factor de seguridad, incluso más importante que el uso excesivo de símbolos o la rotación constante de contraseñas.

b **Más seguras: por su extensión y longitud, son más difíciles de descifrar.**

Las *passphrases* ofrecen una mayor seguridad frente a ataques de fuerza bruta, diccionario o combinaciones automatizadas gracias a su extensión y estructura imprevisible.

A diferencia de las contraseñas tradicionales o cortas, las frases extensas amplían el espacio de búsqueda de forma exponencial: cada palabra adicional multiplica las combinaciones posibles, haciendo el ataque computacionalmente inviable.

Además, las ***passphrases*** permiten incorporar diversidad de caracteres y patrones lingüísticos que no suelen estar presentes en los diccionarios empleados por los atacantes.

Por ejemplo, incluir espacios, acentos, mayúsculas, signos de puntuación, números o símbolos intercalados en el texto añade una capa extra de complejidad sin comprometer el proceso de memorizarla.

Ejemplos de ***passphrases*** seguras:

- *ElQueLeeMuchoYAnda7MuchoVeMuchoYSabeMucho**
- *¡HoyEs29SiempreTodavía2025!*
- **Tancortoelamor%Tanlargoelolvido33**

Cada una de ellas combina longitud, variación de mayúsculas y símbolos y, un significado personal que facilita su retención sin comprometer la seguridad.

Recomendación: una buena medida es que los símbolos y los números estén intercalados en el texto. De esa forma se incrementa la complejidad.

Asimismo, las *passphrases* son más resistentes frente a ataques basados en patrones culturales o sociales, ya que su estructura no se limita a palabras aisladas sino a secuencias lógicas y únicas para cada usuario.

c **Fáciles de recordar: uso de palabras comunes o frases mnemotécnicas.**

Uno de los principales inconvenientes de las contraseñas complejas tradicionales es su difícil memorización. Esto lleva a los usuarios a anotarlas, reutilizarlas o simplificarlas, comprometiendo la seguridad.

Sin embargo, las *passphrases* aprovechan el funcionamiento natural de la memoria humana: recordamos mejor las frases con significado que cadenas aleatorias de caracteres.

El uso de frases mnemotécnicas o con sentido personal permite crear claves de mayor longitud y robustas sin necesidad de almacenarlas físicamente ni depender exclusivamente de gestores.

La clave es que la frase tenga coherencia y relación con la experiencia o rutinas del usuario, pero que no sea fácilmente deducible por terceros.

Ejemplos de frases mnemotécnicas:

- *MiprimercochefueunRenaultnegro2009!!*
- *LamúsicadeSabinaesmiBSO1999**
- *ElinfiltradoEsMiPeliFavorita25!*

Todos estos ejemplos son frases extensas, lógicas y memorizables, pero extremadamente difíciles de adivinar o descifrar mediante herramientas automáticas. Su carácter "natural" reduce la probabilidad de que el usuario las olvide o las comparta de forma inadvertida.

Recomendación: combinar idiomas o expresiones personales añade un nivel extra a la seguridad sin perder la capacidad de memorizarlo. Por ejemplo:

- *ElRetratodeDorianGray**
- *ReadyParaElViajeDeMiVida27!*

d **Personalizables: inclusión de espacios, mayúsculas, símbolos y números.**

Otra de las grandes ventajas de las *passphrases* frente a las contraseñas tradicionales es su flexibilidad de construcción.

Pueden incluir espacios entre palabras, así como mayúsculas, signos de puntuación, tildes, símbolos o números. Esta personalización amplía la complejidad sintáctica y tipográfica de la clave, lo que incrementa su resistencia frente a ataques automatizados.

A diferencia de las políticas antiguas que obligaban a cumplir normas rígidas (como incluir al menos una mayúscula, un número y un símbolo especial en una contraseña corta), las recomendaciones en la actualidad priorizan la longitud y la naturalidad.

Una *passphrase* bien construida puede ser tanto o más segura que una contraseña llena de caracteres especiales difíciles de recordar.

Ejemplos de personalización efectiva:

- *MiLibroFavoritoEs"Hamlet"!*
- *¿QuiénDijoQueLaSeguridadNoEsDivertida?*
- *24HorasLeyendo_24HorasViajando**

Estos ejemplos muestran cómo los usuarios pueden combinar diferentes tipos de caracteres sin perder coherencia ni legibilidad, logrando una *passphrase* fuerte, fácil de memorizar y adaptada al estilo personal del usuario.

Recomendaciones:

- Evita sustituir todas las letras por números o símbolos de forma predecible (por ejemplo, "3" por "E" o, "@" por "a"), ya que estos patrones son ampliamente conocidos por los atacantes. Por ejemplo,

en “amazonas”, tendrían que probar 8 combinaciones diferentes sin contar las “a” mayúsculas. Es decir, si se sustituye, que no sea por todas.

- Aprovechar la libertad de formato para generar frases originales y largas, con sentido y estructura natural.

En resumen, su longitud y estructura las hacen mucho más resistentes a ataques de fuerza brutal o diccionario; su carácter mnemotécnico facilita el proceso de memorizarla y su capacidad de personalización permite adaptarlas al estilo y necesidades del usuario sin comprometer la protección.

Adoptar el uso de *passphrases* dentro de una política de gestión de contraseñas no solo mejora la seguridad individual, sino que refuerza la seguridad de la organización.

5. Clasificación de *passphrases*

La utilización de *passphrases* se ha consolidado como una alternativa actual, segura y eficaz frente a las contraseñas tradicionales. Su principal fortaleza radica en combinar longitud, complejidad y facilidad en el proceso de memorizar. Tres factores que refuerzan la protección frente a accesos no autorizados o ataques automatizados.

Según las recomendaciones de organismos especializados en la seguridad de la información y ciberseguridad, el uso de *passphrases* permite incrementar la complejidad de la clave y, con ello, su resistencia ante ataques de fuerza bruta, de diccionario o de ingeniería social.

Existen principalmente dos tipos de *passphrases*, cuya elección dependerá del entorno, el nivel de riesgo y las necesidades del usuario: aleatorias y mnemotécnicas.

5.1. *Passphrases* aleatorias

Las *passphrases* aleatorias se generan a partir de palabras seleccionadas al azar, sin un sentido lógico o gramatical entre ellas. En este tipo de *passphrase* se basa en la complejidad pura, es decir, en el grado de aleatoriedad de la combinación de palabras que la forman.

Cada palabra añadida a la frase aumenta exponencialmente las posibles combinaciones, dificultando enormemente los intentos de descifrado mediante ataques de diccionario o fuerza bruta. Por ello, las *passphrases* aleatorias se consideran ideales en entornos que requieren máxima seguridad, como accesos administrativos, cifrado de dispositivos, monederos digitales o sistemas críticos.

5.1.1. Generación y métodos

La eficacia de una *passphrase* aleatoria depende directamente de la calidad del proceso de generación.

Una frase de paso será verdaderamente segura solo si se obtiene mediante métodos que garanticen aleatoriedad, la ausencia de patrones predecibles y la suficiente longitud.

Uno de los principales riesgos en la creación de contraseñas o *passphrases* proviene de los hábitos humanos previsibles: los usuarios tienden a elegir palabras familiares, temáticas recurrentes o combinaciones que, aunque parezcan únicas, pueden ser fácilmente deducidas mediante ataques de diccionario o análisis estadístico.

Por ello, se recomienda que las *passphrases* aleatorias se generen empleando fuentes de complejidad verificables y procedimientos controlados, ya sea de forma automatizada o manual, pero siempre con criterios de seguridad comprobables.

A continuación, se describen los métodos más fiables y recomendados:

a **Listas de palabras estandarizadas.**

Una de las estrategias más extendidas consiste en generar *passphrases* a partir de listas de palabras normalizadas y auditadas, cuya finalidad es proporcionar un conjunto predefinido de términos comunes, no redundantes y seleccionados de forma neutral para maximizar la complejidad.

Entre las más conocidas destacan:

- **BIP39 Wordlist:** desarrollada inicialmente en el ámbito de la tecnología *blockchain* y las criptomonedas, incluye 2048 palabras cuidadosamente seleccionadas para evitar ambigüedades ortográficas o fonéticas. Esta lista permite generar secuencias con una complejidad verificable, lo que hace muy útil para crear *passphrases* seguras y resistentes a ataques de diccionario.
- **EFF Wordlists:** elaboradas por la *Electronic Frontier Foundation*, estas listas están diseñadas específicamente para generar *passphrases* de alta seguridad mediante el mediante el método *diceware*. La EFF publicó diferentes versiones, optimizadas para diversos idiomas y tamaños de conjunto, siempre con el objetivo de ofrecer palabras comunes, pronunciables y aleatorias.

El uso de este tipo de listas tiene dos ventajas fundamentales:

- **Transparencia y fiabilidad:** las listas son públicas, revisadas y validadas, lo que garantiza su neutralidad y entropía matemática.
- **Compatibilidad:** pueden integrarse en *scripts*, gestores de contraseñas o aplicaciones de seguridad sin necesidad de conexión a Internet, reduciendo riesgos de exposición.

b **Gestores de contraseñas y herramientas de generación segura.**

Otra opción práctica y segura es el uso de gestores de contraseñas que incorporan sistemas de generación de *passphrases* basados en algoritmos criptográficamente seguros.

Existen herramientas que permiten crear *passphrases* aleatorias mediante el uso de generadores internos que emplean números aleatorios pseudoaleatorios seguros garantizando así que las palabras elegidas no sigan patrones predecibles.

Estos gestores permiten definir parámetros personalizables, tales como:

- Número de palabras a incluir.
- Separadores (espacio, guiones o símbolos).
- Inclusión opcional de mayúsculas, cifras o signos de puntuación.
- Idioma o conjunto léxico utilizado (por ejemplo, español inglés o combinaciones multilingües).

Además de generar las *passphrases*, los gestores de contraseñas las almacenan mediante algoritmos robustos, evitando así, la exposición de las credenciales y reduciendo, por tanto, el riesgo de pérdida o reutilización.

5.1.2. Recomendaciones generales

Una vez definidos los distintos métodos de generación de *passphrases* aleatorias y su relevancia dentro de las estrategias de protección de credenciales, resulta imprescindible establecer una serie de buenas prácticas orientadas a garantizar su eficacia y seguridad a largo plazo.

El proceso de creación no debe entenderse como una acción aislada, sino como parte de una política integral de ciberseguridad en la que intervienen la robustez técnica, la gestión responsable por parte del usuario y el cumplimiento de estándares reconocidos.

Una *passphrase* solo será realmente segura si se genera, almacena y gestiona bajo criterios verificables de aleatoriedad y confidencialidad. Por este motivo, antes de adoptar un método concreto, conviene tener en cuenta una serie de recomendaciones que refuerzan la complejidad, la integridad y la trazabilidad del proceso de creación, tanto en entornos personales como corporativos.

A continuación, se plantean recomendaciones generales:

- Usar al menos 5 o 6 palabras para alcanzar una complejidad superior a 70 bits de entropía **(2)**, considerada segura incluso frente a ataques de fuerza bruta prolongados.

(2) La entropía de una contraseña o *passphrase* se mide en bits de entropía, que representan la impredecibilidad y aleatoriedad de la contraseña. Cuanto mayor sea la entropía, más segura será la contraseña. La fórmula para calcularlo es: $E = \log_2 (R_2)$, donde R es el rango de caracteres disponibles y L es la longitud de la contraseña.

- Preferir el uso de herramientas cuyas funcionalidades de seguridad hayan sido evaluadas por un tercero y dispongan de una certificación de seguridad.
- Evitar generadores en línea no verificados, ya que podrían registrar las palabras producidas.
- No utilizar *passphrases* generales, aunque sean aleatorias; cada credencial debe ser única.
- En entornos corporativos, integrar los procesos de generación dentro de políticas centralizadas de gestión de identidad (IAM) o gestores corporativos de contraseñas.

En síntesis, la generación de *passphrases* debe basarse en aleatoriedad, verificable, longitud adecuada y almacenamiento cifrado.

5.2. *Passphrases* mnemotécnicas

Las frases mnemotécnicas es una técnica de memoria que consiste en crear una palabra, frase, verso o asociación fácil de recordar que ayuda a recordar información mediante la relación con algo más simple, familiar o divertido.

En este sentido, las *passphrases* mnemotécnicas se construyen a partir de frases con sentido lógico o personal, lo que las hace más fáciles de recordar sin perder robustez. Esto se debe al principio de la memoria asociativa: el cerebro humano recuerda mejor las ideas o frases con significado que las secuencias aleatorias de caracteres.

Este tipo de *passphrase* resulta especialmente útil para usuarios individuales, entornos de teletrabajo o accesos personales donde la usabilidad y la seguridad son igualmente importantes.

5.2.1. Generación y método

Para la construcción de una *passphrase* mnemotécnica eficaz y segura, se deben cumplir tres condiciones fundamentales que garanticen un equilibrio adecuado entre

facilidad de memorización, longitud suficiente y robustez criptográfica frente a intentos de descifrado o suplantación de identidad:

1) **Tener sentido personal o lógico, sin ser fácilmente predecible.**

2) **Superar los 16 caracteres de longitud.**

a Incorporar variaciones naturales, como mayúsculas, acentos, signos de puntuación o números significativos no obvios. Es recomendable incluir faltas de ortografía en las palabras y caracteres locales (por ejemplo, la "ñ").

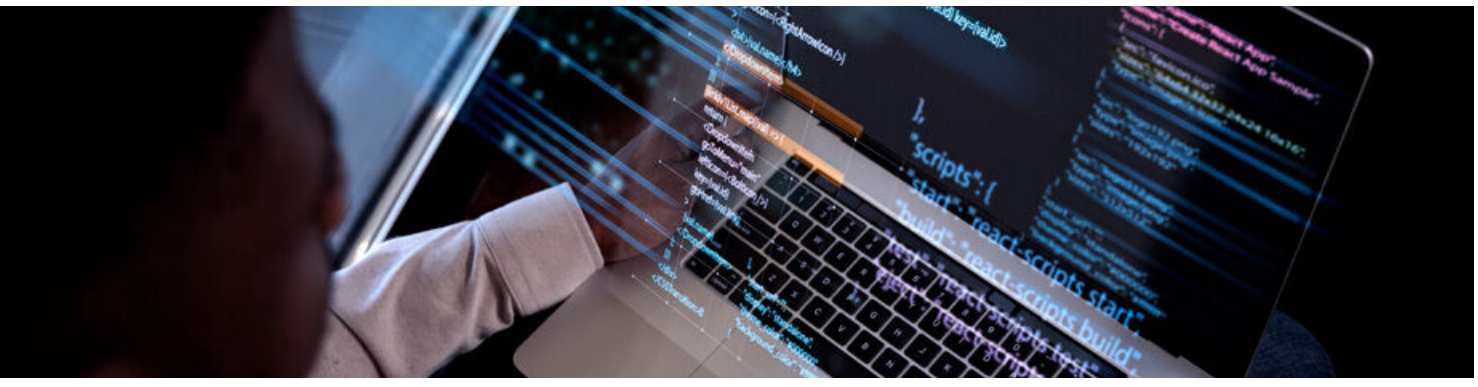
A continuación, algunos ejemplos de posibles contraseñas creadas mediante la práctica mnemotécnica:

- *SiempreTomoCafé@ntesDeLeerElPeri0dico#7*
- *@MalTiemp0BuenaWifi!*
- *ElCaféDeLas#7#MeDespiertaSiempre!*

Estas frases son fáciles de recordar, personales y lo suficientemente extensas para ofrecer una alta resistencia ante ataques. No obstante, es importante tener en cuenta los ataques de ingeniería social.

Estos ataques buscan obtener información personal mediante engaños o manipulación, por lo que no se recomienda usar frases que identifiquen al usuario fácilmente, como expresiones que suela decir, datos personales, gustos evidentes o referencias públicas. Si una *passphrase* refleja demasiado la forma de hablar o detalles sobre el usuario, un atacante podría deducirla.

Para evitar este tipo de ataques, se recomienda combinar palabras o ideas que resulten fáciles de recordar para el usuario, pero que no estén relacionadas directamente con él, ni sean predecibles. Además, evitar todo lo posible anotar las contraseñas en libretas o *post-its*.



5.2.2. Ventajas

Las ventajas que presentan este tipo de *passphrase* son diversas y se relacionan tanto con su facilidad de uso y recordatorio como con su eficiencia en términos de seguridad y resistencia frente a ataques:

- **Alta memorización:** pueden recordarse sin necesidad de anotarlas ni recurrir a gestores.
- **Fácil adopción:** son compatibles con políticas de concienciación y formación en ciberseguridad.
- **Personalización natural:** cada usuario puede crear su propio sistema o patrón de frases.

5.2.3. Inconvenientes

Sin embargo, es importante tener en cuenta los siguientes inconvenientes o limitaciones, ya que, a pesar de las ventajas que ofrecen las *passphrases* mnemotécnicas, su eficacia puede verse reducida si no se construyen, gestionan o actualizan adecuadamente. A continuación, se enumeran algunos aspectos a considerar para evitar vulnerabilidades asociadas a su uso:

- Riesgo de previsibilidad si la frase se basa en información pública o compartida (nombre de mascotas, fechas personales, etc.).
- Utilizar una *passphrase* que no tenga la longitud mínima recomendada para garantizar un nivel adecuado de seguridad.
- Las frases o expresiones utilizadas habitualmente y que pudieran ser obtenidas por ingeniería social.

6. Gestores de contraseñas

Un gestor de contraseñas es una herramienta diseñada para almacenar y gestionar de forma segura las credenciales de acceso a diversas cuentas. Permite crear contraseñas únicas y seguras, facilitando su recuperación automática para iniciar sesión en las cuentas. Además, algunas de estas herramientas pueden realizar otras funciones complementarias como:

- La sincronización de contraseñas en varios dispositivos y sistemas operativos.
- La detección de fallos de seguridad y vulnerabilidades como, por ejemplo; si la contraseña se emplea en diferentes páginas *webs* y sugieren cambiarla.
- Advertencia de si un sitio web es fraudulento para proteger al usuario de posibles estafas.

Un gestor de contraseña funciona guardando los datos de inicio de sesión, como nombres de usuario y contraseñas, en una base de datos cifrada a la que solo se puede acceder mediante una contraseña maestra (*master password*). Esta contraseña maestra es la única que el usuario necesita recordar, ya que la herramienta se encarga de proporcionar los accesos.

Existen tres tipos de gestores de contraseñas:

- **Con instalación local**, es decir; se instalan en el ordenador o móvil.
- **En línea:** guardan las contraseñas cifradas en servidores seguros. Se puede acceder desde cualquier dispositivo conectado a Internet.
- **Basado en *tokens*:** las contraseñas se almacenan en un dispositivo aparte.

TIPO	LUGAR DE ALMACENAMIENTO	CONEXIÓN A INTERNET	VENTAJAS	DESVENTAJAS
Local	En tu dispositivo (PC, móvil, USB).	No	Control total sobre tus datos. No depende de servidores externos.	Si pierdes el archivo o el equipo, puedes perder las contraseñas. Sin sincronización automática.
En línea (basado en nube)	En servidores cifrados del proveedor.	Sí	Acceso desde cualquier dispositivo. Sincronización automática. Copias de seguridad incluidas.	Depende de Internet. Riesgo si el servicio sufre una brecha de seguridad.
Basado en *tokens* o dispositivos físicos	En un dispositivo externo (*token* o llave USB).	Solo al usar el dispositivo.	Seguridad física muy alta. Difícil de *hackear* a distancia.	Si pierdes el *token* pierdes acceso (sin copia de seguridad). Menos práctico para uso diario.

7. Escenarios posibles: móviles y ordenadores

El uso seguro de contraseñas y *passphrases* debe adaptarse a los distintos entornos y dispositivos en los que los usuarios gestionan su identidad digital. Tanto los ordenadores personales como los teléfonos móviles, independientemente del sistema operativo, representan a día de hoy puntos de acceso fundamentales a información sensible y servicios críticos.

Por ello, resulta esencial comprender las particularidades de cada entorno, así como aplicar medidas específicas que refuercen la protección frente a amenazas, accesos no autorizados o pérdida de dispositivos.

7.1. Seguridad en dispositivos móviles

Los teléfonos móviles son actualmente una de las principales superficies de ataque. Al concentrar comunicaciones, banca, redes sociales y documentos de trabajo, su compromiso puede tener consecuencias graves tanto a nivel personal como profesional.

7.1.1. Autenticación y contraseñas

En los distintos sistemas operativos, *iOS* o *Android*, el sistema de autenticación debe configurarse de forma que combine comodidad y seguridad. Aunque ambos sistemas operativos promueven el uso de la biometría (huella dactilar, reconocimiento facial), esta tecnología no sustituye completamente a una contraseña o *passphrase*, sino que actúa como método de desbloqueo rápido.

Es importante destacar que la biometría, aunque práctica, aún presenta limitaciones técnicas y de fiabilidad:

- No puede modificarse en caso de compromiso (una huella o un rostro no son "renovables" como una contraseña).
- Algunos sensores pueden fallar o ser eludidos bajo ciertas condiciones de luz, humedad o manipulación.
- En entornos de alta seguridad, se desaconseja confiar exclusivamente en métodos biométricos, recomendando combinarlos con una *passphrase* o PIN complejo.

7.1.2. Recomendaciones prácticas para móviles

Resulta fundamental aplicar una serie de medidas preventivas y configuraciones adecuadas que refuercen la protección del dispositivo frente a pérdida, robo, acceso no autorizado o explotación de vulnerabilidades.

A continuación, se detallan las recomendaciones prácticas más relevantes para dispositivos móviles, aplicables tanto a sistemas *Android* como *iOS*, orientadas a fortalecer la autenticación, la privacidad y la integridad de la información almacenada:

a Utilizar códigos de bloqueo de al menos seis dígitos, preferiblemente alfanuméricos si el sistema operativo lo permite.

b Ocultar la breve visualización del carácter de la tecla que se está pulsando.

c Evitar los patrones de desbloqueo visual, fácilmente observables o reproducibles (ataques *smudge* – reproducen el patrón basándose en las marcas que se dejan en la pantalla).

d Activar la autenticación de doble factor (2FA) en todas las aplicaciones críticas (correo, banca, almacenamiento en la nube, redes sociales): preferiblemente

mediante aplicaciones autenticadoras en lugar de SMS, ya que los mensajes pueden ser interceptados o suplantados.

e | Mantener actualizado el sistema operativo y las aplicaciones, ya que muchas brechas de seguridad se explotan a través de vulnerabilidades conocidas.

f | Evitar el uso de redes WiFi-públicas o no cifradas; si es necesario conectarse, hacerlo mediante una VPN confiable.

g | Cifrar el almacenamiento del dispositivo, una opción disponible en la mayoría de los terminales modernos.

h | Configurar la eliminación automática de datos tras varios intentos fallidos de desbloqueo, como medida de contingencia ante pérdida o robo.

7.1.3. Gestores de contraseñas móviles

El uso de gestores de contraseñas seguros en dispositivos móviles resulta fundamental, ya que estas herramientas permiten generar, almacenar y gestionar de forma cifrada contraseñas y *passphrases* robustas, minimizando el riesgo asociado a la reutilización, pérdida o exposición accidental de credenciales.

Los gestores actuales integran funcionalidades avanzadas como autocompletado seguro, sincronización cifrada entre dispositivos y generadores automáticos de contraseñas de alta complejidad, lo que facilita mantener una higiene digital adecuada sin comprometer la seguridad.

No obstante, su uso requiere una configuración responsable y consciente, ya que el gestor actúa como repositorio principal de todas las credenciales del usuario. Configurarlo de forma errónea o la utilización de servicios no confiables puede comprometer la totalidad de los accesos almacenados.

Por ello, se recomienda seguir las siguientes prácticas esenciales para garantizar una gestión segura y eficaz de las contraseñas en dispositivos móviles:

a | Activar la biometría como método de desbloqueo complementario, pero nunca como único factor de autenticación.

b | Proteger el acceso al gestor mediante una *passphrase* maestra larga, única y compleja.

c Sincronizar únicamente con servicios cifrados, controlados y verificados, evitando el uso de almacenamiento en la nube públicos o desconocidos que puedan suponer un riesgo para la confidencialidad de los datos.

d Uso de herramientas incluidas en el Catálogo de Productos STIC (CPSTIC **(3)**) y configuradas mediante su Procedimiento de Empleo Seguro.

7.2. Seguridad en ordenadores

Los ordenadores continúan siendo los puntos principales de acceso a entornos corporativos y de trabajo remoto, por lo que requieren un enfoque de seguridad más estructurado y administrado.

7.2.1. Autenticación principal

La creación de una *passphrase* o contraseña de inicio de sesión sólida sigue siendo el primer nivel de defensa frente a ataques.

- En ***Windows***, se recomienda combinar la contraseña de usuario con *Windows Hello* (PIN local o reconocimiento facial), activando además la autenticación multifactor cuando se empleen cuentas *Microsoft* o corporativas.
- En ***macOS***, el cifrado completo del disco junto con una *passphrase* larga y compleja es esencial para proteger la información.
- En ***Linux***, se recomienda el cifrado de disco, y el uso de *passphrases* en lugar de contraseñas simples para la autenticación local y sudo.

7.2.2. Doble factor y gestión de credenciales

En todos los sistemas operativos, el uso de autenticación multifactor (MFA) se considera una medida esencial de ciberseguridad. Este mecanismo añade una capa adicional de protección que complementa la contraseña o *passphrase*, dificultando que un atacante puede acceder a un sistema o servicio incluso si ha conseguido comprometer las credenciales principales.

(3) https://cpstic.ccn.cni.es

7. Escenarios posibles: móviles y ordenadores

El principio fundamental del MFA consiste en combinar dos o más factores de verificación independientes, normalmente basados en:

- **Algo que el usuario sabe** (una contraseña o *passphrase*).
- **Algo que el usuario tiene** (un dispositivo físico, *token* o aplicación autenticadora).
- **Algo que el usuario es** (un rasgo biométrico, como huella o reconocimiento facial).

De esta manera, se evita que el robo o filtración de una contraseña se traduzca automáticamente en un acceso exitoso, reforzando la integridad y la confidencialidad de las cuentas.

8. Recuperación de contraseña: “olvidé mi contraseña”

“Olvidé mi contraseña” es una función de recuperación de acceso que ofrecen la mayoría de las plataformas digitales, como correos electrónicos, redes sociales, bancos o gestores de contraseñas.

Su objetivo es permitir que el usuario recupere el acceso a su cuenta de forma segura y verificada, en caso de haber olvidado o perdido su contraseña, sin llegar a perder la cuenta.

A continuación, se muestran los casos más comunes en los que se debe emplear esta función:

- **El usuario no recuerda su contraseña actual:** este es el caso más habitual. Puede suceder por diferentes motivos, lo más común es porque hace mucho que el usuario no accede a la cuenta, que el usuario cambia varias veces de contraseña o usa muchas cuentas distintas.
- **Intento de acceso:** existe la posibilidad de que alguien intente acceder con nuestras credenciales, dejando bloqueada la cuenta por superar el número de intentos fallidos.
- **Cambio de dispositivo y las contraseñas no están guardadas:** a veces, al cambiar de móvil o computadora, se pierden los datos almacenados automáticamente en el navegador o gestor de contraseñas del sistema. Si el usuario no ha hecho una copia de seguridad o no ha sincronizado las contraseñas, la opción “Olvidé mi contraseña” permite restablecer el acceso rápidamente sin depender del dispositivo anterior.

8.1. Procedimiento para la recuperación de contraseñas

Esta función se aplica a la mayoría de los servicios en línea como el correo, redes sociales, banca digital, etc. El proceso tiene dos objetivos: verificar que el usuario es realmente el dueño de la cuenta y restablecer su acceso de forma segura. A continuación, se indica un procedimiento general que puede ayudar a ejecutar un cambio de contraseña:

a **Accede a la página de inicio de sesión del servicio.**

b **Haz clic en la opción “¿Olvidaste tu contraseña?” u “Olvidé mi contraseña”**

Generalmente aparece debajo del campo donde se ingresa la contraseña.

c **Selecciona un método de verificación.**

El sistema pedirá comprobar su identidad, normalmente mediante:

- Enlace enviado a tu correo alternativo.
- Código enviado por SMS o app autenticadora.
- Pregunta o método de recuperación configurado previamente.
    - **Recomendación**: evitar usar respuestas evidentes o fáciles de adivinar. En su lugar, utilizar respuestas aleatorias o no predecibles que solo el usuario conozca o que no estén relacionadas con información personal real.
- Abre el enlace o ingresa el código recibido.

Esto confirma que es el propietario de la cuenta.

d **Crea una nueva contraseña segura.**

Recomendaciones: aplicar los consejos de esta guía.

- Utilizar una *passphrase* mnemotécnica (5 o 6 palabras)
- Combinar mayúsculas, minúsculas, números y símbolos.
- Evitar nombres, fechas o palabras comunes.

e **Confirma el cambio e inicia sesión con tu nueva contraseña.**

Verifica que todo funcione correctamente y actualiza la clave en el gestor de contraseñas, en caso de utilizarlo.

9. Cambio de contraseña maestra en gestores de contraseña

Si se desea cambiar la contraseña maestra, del gestor de contraseña, por razones, como: olvido, posibilidad de que alguien pudiera verla, mucho tiempo sin actualizarla, o deseo de fortalecer su seguridad general, el proceso varía respecto al procedimiento de recuperación de contraseña general para un determinado acceso.

Antes de trazar los pasos generales para el cambio de contraseña maestra, se significa que el proceso puede variar según el gestor que se utilice. No obstante, la lógica es la misma:

a **Inicia sesión en tu gestor de contraseñas.**

b **Ve al menú de configuración o cuenta.**

Busca una opción como **"Seguridad"**, **"Cuenta"** o **"Cambiar contraseña maestra"**.

c **Introduce tu contraseña actual.**

Esto es necesario para verificar tu identidad antes de permitir el cambio.

9. Cambio de contraseña maestra en gestores de contraseña

d **Crea una nueva contraseña maestra segura.**

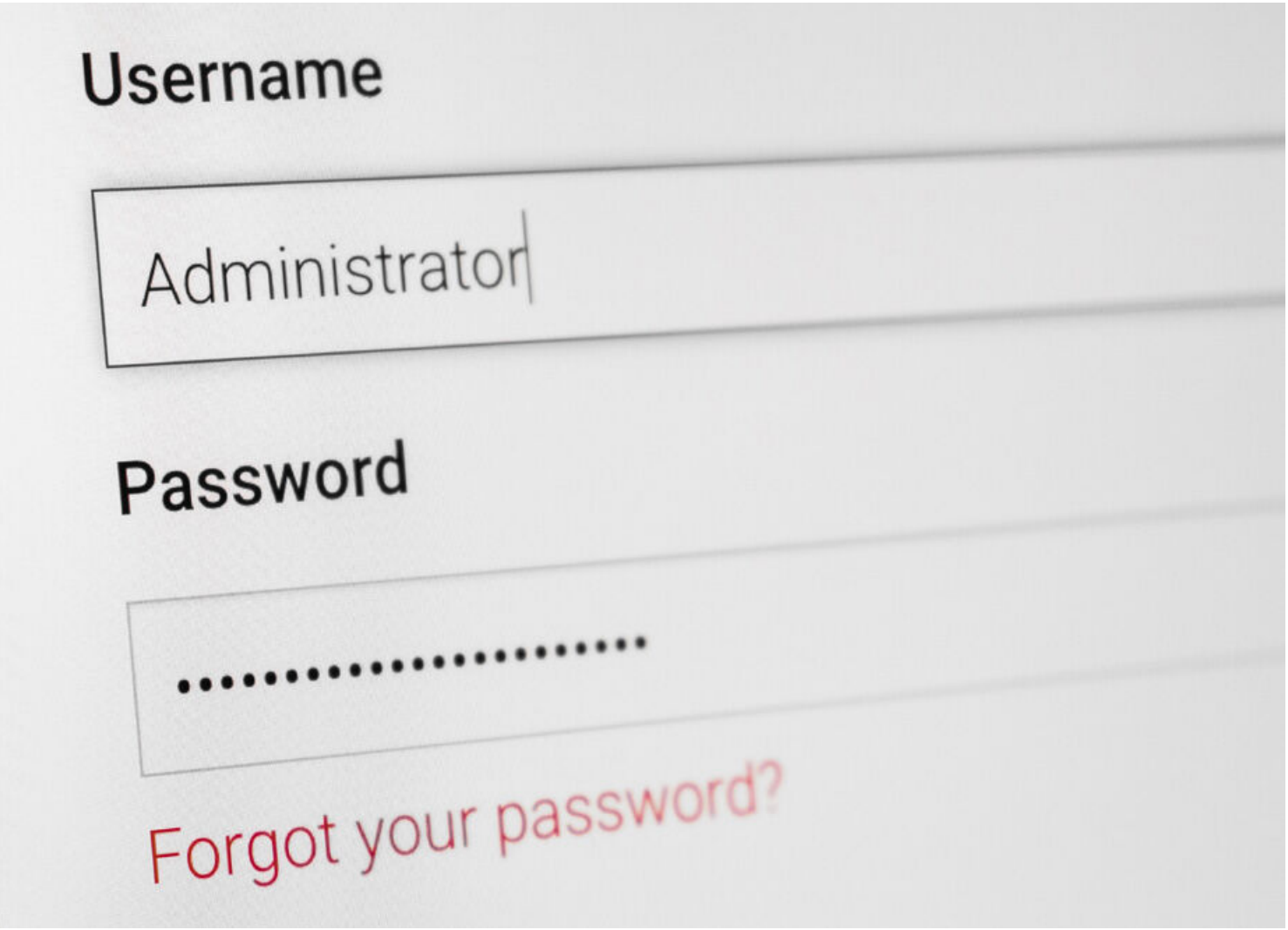
Usa una *passphrase* mnemotécnica, fácil de recordar, pero difícil de adivinar. Aplica los consejos aprendidos en esta guía.

e **Confirma la nueva contraseña.**

El gestor cifrará todas sus contraseñas con la nueva clave maestra.

f **Guarda o sincroniza los cambios.**

Si el gestor usa almacenamiento en la nube, habrá que esperar a que se sincronice correctamente.



10. Doble factor de autenticación

Las contraseñas continúan siendo el principal mecanismo de protección contra accesos no autorizados. Sin embargo, su eficacia depende de cómo se creen, gestionen y protejan.

El uso combinado de contraseñas fuertes (o *passphrases*), un gestor de contraseñas y el doble factor de autenticación (2FA) ofrece una protección integral frente a la mayoría de los ataques digitales actuales.

El doble factor de autenticación (2FA) es un método de seguridad que añade una segunda capa de verificación al iniciar sesión en una cuenta. En lugar de depender solo de una contraseña (algo que sabes), se añade otro elemento (algo que tienes o algo que eres). Esto reduce el riesgo de accesos no autorizados, incluso si el atacante logra obtener la contraseña.

Existen tres tipos de elementos que pueden usarse para verificar la identidad:

- **Algo que sabes.**
- **Algo que tienes.**
- **Algo que eres.**

TIPO DE FACTOR	DESCRIPCIÓN	EJEMPLOS
Algo que sabes	Información que se conoce.	*Contraseña, PIN, respuesta de seguridad.*
Algo que tienes	Un dispositivo o *token* físico.	*Código SMS, app autenticadora, llave USB.*
Algo que eres	Rasgos biométricos únicos.	*Huella digital, rostro, voz, iris.*

El 2FA combina al menos dos factores diferentes para reforzar la seguridad de nuestras cuentas. La mayoría de los casos, el 2FA combina el primer y segundo tipo.

10.1. Buenas prácticas para usar 2FA

Activar el doble factor de autenticación (2FA) es esencial para fortalecer la seguridad de las cuentas, pero su eficacia depende de cómo se utilice y gestione. No solo basta con activarlo, sino que es necesario aplicar una serie de buenas prácticas que garanticen que esta medida realmente proteja frente a ataques y suplantaciones de identidad.

A continuación, se presentan las principales recomendaciones para configurar, mantener y aprovechar correctamente el 2FA en servicios digitales:

a Actívalo siempre que esté disponible, especialmente en:

- Cuentas de correo electrónico.
- Gestores de contraseñas.
- Banca en línea y servicios financieros.
- Redes sociales y plataformas de trabajo.

b No es recomendable usar los mensajes de texto (SMS) como método de doble factor de autenticación, ya que son vulnerables a ataques de *SIM swapping* (robo del número telefónico). En su lugar, las *apps* autenticadoras o *tokens* físicos son más seguros.

c Guarda los códigos de respaldo (*recovery codes*) en un lugar seguro y *offline*.

- No los guarde en el correo ni en capturas de pantalla.
- Puede almacenarlos en un gestor de contraseñas o en una copia cifrada.

d Evita confiar en un solo dispositivo.

Si usa una *app* autenticadora, haz una copia de seguridad o sincronización segura.

e Desactiva el 2FA antes de cambiar de teléfono, o transfiere tu *app* autenticadora correctamente, para no perder el acceso.

f Desconfía de mensajes o correos que pidan los códigos de 2FA.

Ningún servicio legítimo pedirá esos datos por correo, SMS o llamada.

g Combina 2FA con una contraseña fuerte o *passphrase*.

El doble factor no sustituye una contraseña segura: ambos se complementan.

10.2. Funcionamiento práctico de 2FA

Inicio de sesión

Primero se accede a la página o aplicación del servicio que se desea usar, como, por ejemplo: el correo electrónico, una red social o la plataforma de trabajo, y se introduce el nombre y contraseña de usuario. Es así como se completa el primer factor de autenticación (algo que sabes).

Si el servicio no tuviera 2FA, una vez introducida las credenciales, el usuario tendría acceso al servicio. Sin embargo, con el 2FA activado, quedaría realizar otra prueba adicional para verificar que realmente quien se está identificando es el usuario y no es ningún atacante que haya obtenido la contraseña.

Segunda verificación

Tras validar la contraseña, el sistema solicita una segunda prueba de identidad, que suele ser "algo que tienes" o "algo que eres".

Esta segunda capa puede funcionar de distintas maneras:

Código temporal (TOTP)

La opción más común: se utiliza una *app* autenticadora que muestra un código de 6 dígitos que cambia cada 30 segundos. Este código se genera localmente en el dispositivo móvil, por lo que nadie más podría verlo ni interceptarlo. Por ejemplo:

1. *Inicio de sesión en una cuenta de Dropbox.*

2. *Introducción tu contraseña.*

3. *Abre Authy, observa el código: "938214".*

4. *Escríbelo antes de que pasen los 30 segundos.*

5. *Acceso autorizado.*

Llave física de seguridad (*hardware token*)

En lugar de un código, utiliza una pequeña llave USB o NFC. Cuando el sistema lo solicita, el usuario debe conectar la llave o acercarla al dispositivo, y esta firma criptográficamente la solicitud de inicio de sesión.

Es el método más seguro, ya que la llave guarda una clave privada imposible de copiar y solo responde si el usuario la porta.

Verificación biométrica

Algunos dispositivos o servicios usan la huella digital, rostro o iris como segundo factor. Por ejemplo, un dispositivo móvil puede pedir la huella tras ingresar la contraseña antes de abrir el gestor de contraseñas o una app bancaria.

Códigos temporales de un solo uso

Una característica clave de los códigos temporales es el tiempo de vida. Normalmente duran 30 segundos. Esto significa que, aunque un atacante consiguiera el código por algún medio, en pocos segundos dejaría de ser válido. De esta forma, el riesgo de reutilizarlo en otro intento de acceso es prácticamente nulo.

Este sistema se basa en un estándar llamado *Time-based One-Time Password* (TOTP), que sincroniza el reloj interno del servidor y del dispositivo autenticador para generar códigos que coincidan solo durante ese pequeño intervalo.

Acceso confirmado

Una vez introducido el código correcto, activada una llave física o validado el rasgo biométrico, el sistema verifica ambas pruebas y concede el acceso. En ese momento, el servidor sabe que:

- Quien intenta entrar conoce la contraseña legítima (*algo que sabes*).
- Además, tiene en su poder el dispositivo o llave registrada (algo que tienes) o posee el rasgo biométrico válido (*algo que eres*).

En suma, el uso del doble factor de autenticación, junto con contraseñas robustas o *passphrases* seguras y una gestión adecuada de credenciales, reduce de forma significativa el riesgo de incidentes y filtraciones. Esa combinación hace que casi ningún atacante pueda suplantarte, incluso si hubiera robado su contraseña en una filtración o un intento de *phishing*.

11. Decálogo de recomendaciones

La gestión adecuada de las contraseñas es un pilar fundamental para garantizar la seguridad de la información y prevenir accesos no autorizados. A continuación, se presenta un decálogo de recomendaciones que recoge las mejores prácticas para la creación, uso y protección de contraseñas y *passphrases*:

Decálogo de recomendaciones para *uso y gestión de contraseñas*

1. Utilizar preferiblemente *passphrases* antes que contraseñas.
2. No reutilizar contraseñas.
3. Usar *passphrases* de, al menos, 20 caracteres.
4. Utilizar *passphrases* fáciles de recordar.
5. Evitar construir *passphrases* con palabras predecibles.
6. Construir *passphrases* con caracteres del idioma local.
7. Activar el 2FA siempre que sea posible.
8. Usar un gestor de contraseñas cuando el número de contraseñas a recordar sea elevado.
9. En respuestas de "olvidé mi contraseña" poner cosas aleatorias no predecibles ni que se correspondan con la respuesta real o la vida personal.
10. No anotar las contraseñas en libretas o *post-its*.

ccn-cert
centro criptológico nacional

Uso y gestión de contraseñas

INFORME DE BUENAS PRÁCTICAS

www.ccn.cni.es

www.ccn-cert.cni.es

oc.ccn.cni.es