Guía rápida para crear contraseñas robustas (y no olvidarlas)

El primer paso indispensable en la ciberseguridad de las empresas

cosmomedia.
digitalización para tu negocio

INTRODUCCIÓN

¿Por qué una contraseña sencilla es un problema importante para tu pyme?

Seamos directos: **tu contraseña es el muro de contención más importante** que tienes. Cuando gestionas una **pyme**, la seguridad no es un extra, es una necesidad vital. Y, nos guste o no, la mayoría de los problemas de seguridad empiezan justo aquí: con una clave débil o predecible. Esto convierte un simple acceso en una invitación abierta para cualquier hacker.

El peligro de las contraseñas débiles

Los atacantes no necesitan ser genios; solo necesitan software.

A través de programas pueden ejecutar millones de combinaciones posibles por segundo en lo que se conoce como "**Ataques de fuerza bruta"**.

Si usas el nombre de tu hijo o "123456", estás dando las llaves en la mano. Y lo peor: si usas la misma clave simple para tu Wi-Fi, tu correo y el CRM, un solo fallo puede comprometer a tu empresa entera.

Una contraseña débil expone tu negocio a:

Ataques automáticos: Programas que prueban claves hasta dar con la tuya.
Claves de diccionario: Uso de listas con las contraseñas más comunes.
Contagio total: Si usas la misma clave en todos lados, te expones por completo.

La regla de oro: longitud y complejidad

Regla #1: No bajes de los 12 caracteres

- Olvídate de las claves de 8 caracteres. El tiempo que tarda un hacker en romper tu clave crece de forma exponencial con cada letra extra que añades.
- Una clave de 8 caracteres se rompe en horas; **una contraseña de 12 a 15 caracteres puede tardar años en hackearse** o requiere de una tecnología mucho más avanzada.

Regla #2: Una receta llena de ingredientes (diversidad)

Una clave fuerte no solo es larga, también es variada. No puede ser una palabra que encuentres en un libro. Debe ser una **mezcla caótica** que confunda a los algoritmos de ataque y evite cualquier patrón reconocible.

Una clave que funciona incluye:

Mayúsculas y minúsculas (A, b, C, d)

Números (1, 2, 3, 4)

Símbolos (!, $, %, &)

Sin sentido aparente: Que no sean palabras o datos personales

¡Para tener en cuenta!

Clave Floja: MiEmpresa2025 (Fácil de adivinar)

Clave Fuerte: !M1b13t0d0E$t4L1br3* (Larga y revuelta)

El método definitivo (Passphrase)

La técnica infalible: Usar una frase contraseña (Passphrase)

No tienes que ser un genio para **recordar una clave indescifrable**. El secreto está en las Passphrases (frases contraseña). Se trata de **crear una clave larga** (cumpliendo el requisito de longitud) que, a la vez, sea **fácil de recordar**, porque se basa en una frase personal que solo tú conoces.

3 pasos para crear tu Passphrase inolvidable

Paso 1: Piensa en una frase que te guste

Elige una oración personal, una letra de canción que no sea famosa, o un refrán. Debe ser algo largo y fácil de recordar para ti.

Ejemplo de Frase Base: "Mi bicicleta es azul y tiene tres marchas"

Paso 2: Transfórmala y hazla rara (Sustitución)

Aquí es donde aplicamos la complejidad. **Sustituye algunas letras por números o símbolos** que se parezcan visual o fonéticamente (la "e" por "3", la "o" por "0", la "a" por "4", etc.)

Sustituciones: M por M, i por 1, e por 3, s por $, t por 7...

Resultado: "M1B1C1cL3t4E4zuLy71Ene7r3M4rch4$"
(¡Una clave de 37 caracteres!)

Paso 3: Sella con símbolos al inicio y al final

Añade un par de símbolos al principio y al final como refuerzo final

Resultado Final: #M1B1C1cL3t4E$4zuL y 71Ene7r3$M4rch4$!

Tienes una clave que detiene a las máquinas, pero que tu cerebro recuerda con una simple frase.

Gestión y uso práctico

Gestión inteligente: No te repitas jamás

Para protegerte de amenazas, debes crear una clave única para cada servicio. Usar la misma clave en el Wi-Fi, el correo y la banca es un riesgo inaceptable.
Ahora, sabemos lo que estás pensando... ¿Cómo recordarlas todas?

Tu herramienta esencial: Un gestor de contraseñas

Los gestores de contraseñas son la **herramienta de ciberseguridad más eficaz que existe**. Funcionan como una **caja fuerte digital** que almacena todas tus claves, protegidas por una única clave maestra (donde usarás tu Passphrase)

¿Por qué es indispensable? El gestor de contraseñas:

1. **Crea por ti**: Genera claves aleatorias y complejas para cada cuenta
2. **Guarda seguro:** Las almacena cifradas, lejos de miradas indiscretas
3. **Rellena**: Las introduce automáticamente cuando las necesitas
4. **Neutraliza**: Detiene la reutilización de claves en tu empresa

Gestores de contraseñas más populares

Bitwarden, 1Password, LastPass

Olvídate del papel y de las notas sin cifrar

La nota adhesiva junto a la pantalla NO es más segura. De hecho, es la forma más rudimentaria de comprometer tu ciberseguridad.

Si necesitas guardar información sensible fuera del gestor, asegúrate de que esté en un **archivo cifrado con una contraseña muy fuerte**. No uses archivos de texto sin proteger ni hojas de cálculo en la nube.

La capa extra de seguridad

El doble factor de autenticación (2FA): La doble cerradura

Si un atacante consigue tu contraseña, el Doble Factor de Autenticación (2FA) actúa como una segunda cerradura, impidiéndole la entrada. Es el paso de seguridad más importante después de tener una clave robusta.

¿Qué es y dónde ponerlo en marcha?

El 2FA exige dos pruebas de identidad: Algo que sabes (tu clave) y Algo que tienes (un código temporal enviado a tu móvil). Si el hacker no tiene tu teléfono, no entra.

Puedes activarlo en:

- **Correo electrónico: especialmente en Webmail**
- **Banca y finanzas online**
- **Plataformas de gestión de la pyme: CRM, ERP, etc**
- **Tu Gestor de Contraseñas (para proteger la clave maestra)**

Recomendación: Es mucho más seguro usar **Apps de Autenticación** (como Google Authenticator o Authy) para generar códigos temporales que depender de los códigos enviados por SMS.

Resumen rápido. Cierra la puerta

La seguridad de tu pyme arranca aquí. Audita tus accesos y aplica estas reglas:

ACCIÓN CLAVE	REQUISITO BÁSICO	BENEFICIO INMEDIATO
Longitud	Mínimo **12-15 caracteres**	Inmunidad contra ataques automáticos
Creación	Usar el método **Passphrase**	Claves complejas fáciles de recordar
Gestión	Implementar un **Gestor de contraseñas**	Elimina la reutilización y aumenta la unicidad
Verificación	Activar el **2FA** en cuentas críticas	Protección total ante el robo de credenciales

Y cierra la puerta de tu seguridad digital.

¿Necesitas un plan de ciberseguridad completo?

En Cosmomedia, somos expertos en digitalización y queremos que tu negocio crezca sobre cimientos sólidos.

Si buscas ir más allá de las contraseñas y necesitas una asesoría experta para seguir blindando tu infraestructura digital, somos tu aliado de confianza.

Te ayudamos a identificar los siguientes pasos necesarios para mantener tu negocio seguro y competitivo.

Te ayudamos a gestionar la ciberseguridad de tu empresa

hola@cosmomedia.es