Universidad de Buenos Aires
Facultad de Ciencias Económicas

Desde las Passwords y Hacia las PassPhrases

AR Tema extractado del libro "**Análisis Funcional de Sistemas y Tecnologías de la Información**" de Aníbal M. Mazza Fraquelli - ISBN 978-987-26981-3-3

---

1. Presentación del Tema

En el contexto de las Tecnologías de la Información (TI), la autenticación constituye uno de los pilares fundamentales de la seguridad informática. El control de acceso a sistemas, aplicaciones, redes y bases de datos depende, en gran medida, de mecanismos que permitan verificar la identidad de los usuarios. Dentro de estos mecanismos, las **passwords** (contraseñas) y las **passphrases** (frases de contraseña) representan los métodos más difundidos y tradicionales.

Una **password** es una cadena de caracteres —generalmente corta— utilizada para autenticar a un usuario frente a un sistema. Por su parte, una **passphrase** es una secuencia más extensa, usualmente compuesta por varias palabras, diseñada para incrementar la entropía (entropy: medida de aleatoriedad o imprevisibilidad) y, por tanto, la seguridad.

Desde la perspectiva organizacional y de gestión de sistemas de información, comprender las diferencias técnicas, operativas y estratégicas entre passwords y passphrases resulta esencial. No se trata únicamente de una cuestión técnica, sino de una decisión de gobierno de TI (IT Governance) que impacta

directamente en la confidencialidad, integridad y disponibilidad de la información (modelo CIA: Confidentiality, Integrity, Availability).

Para los estudiantes de licenciatura en administración, el análisis de este tema debe orientarse a la toma de decisiones: ¿qué políticas de autenticación implementar?, ¿cómo equilibrar seguridad y usabilidad?, ¿qué riesgos implica una mala gestión de credenciales?, ¿cómo se integran estos mecanismos dentro de un Sistema de Gestión de Seguridad de la Información (SGSI, en inglés ISMS: Information Security Management System)?

---

2. Desarrollo

2.1. Definición técnica de Password

Una **password** es un secreto compartido entre el usuario y el sistema. Generalmente está compuesta por:

- Letras mayúsculas y minúsculas
- Números
- Caracteres especiales

Ejemplo clásico: **P@sssW0rd!**

Desde el punto de vista técnico, las passwords no deberían almacenarse en texto plano (plain text), sino mediante funciones criptográficas de hash (hash functions), tales como SHA-256 (Secure Hash Algorithm 256 bits) o algoritmos específicos para contraseñas como bcrypt, scrypt o Argon2.

El problema principal de las passwords tradicionales es que, aunque incluyan complejidad sintáctica, suelen ser cortas (8–12 caracteres), lo que reduce su espacio de búsqueda frente a ataques de fuerza bruta (brute force attack) o ataques por diccionario (dictionary attack).

2.2. Definición técnica de Passphrase

Una **passphrase** es una frase larga compuesta por varias palabras, por ejemplo: **CaballoAladoLlamadoPegaso2026 o Mi gato juega con sus juguetes**

La seguridad de una passphrase no depende tanto de la complejidad de caracteres especiales, sino de su **longitud** y de la **entropía total generada por**

la combinación de palabras.

Desde la teoría de la seguridad informática, la entropía aumenta exponencialmente con la longitud. Una passphrase de 25 caracteres puede ser significativamente más segura que una password de 10 caracteres con símbolos especiales.

2.3. Diferencias fundamentales

Desde el enfoque de TI y administración de sistemas, las principales diferencias son:

Aspecto	Password	Passphrase
Longitud	Corta	Larga
Estructura	Combinación de caracteres	Combinación de palabras
Entropía	Limitada por longitud	Alta por extensión
Usabilidad	Difícil de recordar si es compleja	Más fácil de memorizar
Seguridad frente a fuerza bruta	Menor	Mayor

2.3.1. Seguridad

La seguridad de una credencial se mide por su resistencia a:

- Ataques de fuerza bruta
- Ataques por diccionario
- Ataques híbridos
- Ingeniería social (social engineering)

Una passphrase bien construida incrementa drásticamente el tiempo necesario para romperla mediante ataque automatizado.

Por ejemplo:

- Password de 10 caracteres → puede romperse en horas/días dependiendo del hardware.

- Passphrase de 30 caracteres → puede requerir millones de años con los mismos recursos computacionales.

Desde el punto de vista organizacional, esto reduce el riesgo residual (residual risk) en la matriz de riesgos de TI.

2.4. Usabilidad y experiencia de usuario (UX)

Un error frecuente en las políticas de seguridad corporativa es imponer passwords altamente complejas y cortas, que generan:

- Reutilización de contraseñas.
- Anotaciones en papel.
- Uso de patrones predecibles.
- Fatiga del usuario.

La passphrase ofrece una ventaja clave: es más fácil de recordar una frase coherente que una cadena aleatoria de símbolos.

Ejemplo comparativo:

- Password: `Xf7!kP2@z`
- Passphrase: `Mi gato azul viaja en tren 2026`

Desde el enfoque de administración, una política que promueva passphrases puede mejorar el cumplimiento normativo y reducir incidentes derivados del factor humano.

2.5. Integración en políticas de Seguridad de la Información

En un Sistema de Gestión de Seguridad de la Información (SGSI / ISMS), la política de contraseñas forma parte de los controles de acceso (Access Control).

Normativas como:

- ISO/IEC 27001 (Information Security Management Systems)
- NIST SP 800-63 (Digital Identity Guidelines)

recomiendan cada vez más:

- Mayor longitud.

- Menor énfasis en complejidad forzada.
- Eliminación de cambios periódicos innecesarios si no hay compromiso.

La tendencia moderna es privilegiar **longitud sobre complejidad artificial**.

2.6. Relación con Autenticación Multifactor (MFA)

La password o passphrase pertenece al factor:

Algo que el usuario sabe (Something you know)

Pero hoy los sistemas corporativos integran:

- Algo que el usuario tiene (token, smartphone).
- Algo que el usuario es (biometría).

La Autenticación Multifactor (MFA: Multi-Factor Authentication) reduce el riesgo incluso si la password es comprometida.

No obstante, incluso con MFA, la robustez de la passphrase sigue siendo relevante, especialmente en accesos privilegiados (privileged accounts) como:

- Administradores de bases de datos.
- Root en servidores Linux.
- Administradores de dominio en Active Directory.

2.7. Gestión organizacional de credenciales

Desde la mirada administrativa, no basta con definir passwords fuertes. Se requiere:

1. Política formal de contraseñas.
2. Capacitación al usuario.
3. Uso de gestores de contraseñas (password managers).
4. Registro y monitoreo de accesos (logging & monitoring).
5. Evaluación periódica de riesgos.

Un gestor de contraseñas corporativo permite generar passphrases únicas y evitar reutilización entre sistemas críticos como:

- ERP (Enterprise Resource Planning)
- CRM (Customer Relationship Management)
- Sistemas financieros
- Plataformas cloud

2.8. Impacto en la Gestión de Riesgos de TI

En una matriz de riesgos (Risk Matrix), la debilidad de passwords incrementa:

- Probabilidad de incidente.
- Impacto financiero.
- Impacto reputacional.
- Riesgo legal.

Un ataque exitoso por password débil puede derivar en:

- Violación de datos personales.
- Sanciones regulatorias.
- Interrupción operativa.
- Pérdida de confianza del cliente.

Por lo tanto, la decisión entre password y passphrase no es trivial; es una decisión estratégica en la gestión de activos digitales.

2.9. Ejemplo organizacional

Caso hipotético:

Una empresa implementa passwords obligatorias de 8 caracteres con cambio cada 30 días. Resultado:

- Usuarios reutilizan patrones.
- Se detectan múltiples accesos no autorizados.
- Se incrementan tickets de soporte.

La empresa migra a:

- Passphrases mínimas de 16 caracteres.
- Eliminación de cambios periódicos obligatorios.
- Implementación de MFA.

Resultado:

- Disminución de incidentes.
- Reducción de costos de soporte.
- Mejora en cumplimiento de seguridad.

Este ejemplo demuestra que la política de credenciales impacta directamente en la eficiencia administrativa.

---

3. Conclusión

La diferencia entre passwords y passphrases trasciende la mera extensión de caracteres. Se trata de un cambio conceptual en la gestión de la autenticación dentro de las organizaciones.

Mientras la password tradicional prioriza la complejidad sintáctica en espacios reducidos, la passphrase privilegia la longitud y la entropía total, ofreciendo mayor seguridad y mejor usabilidad.

Desde la perspectiva de las Tecnologías de la Información y la administración de sistemas, la adopción de passphrases:

- Reduce riesgos de ciberseguridad.
- Mejora la experiencia del usuario.
- Disminuye costos operativos.
- Fortalece el gobierno de TI.
- Se alinea con estándares internacionales.

En un entorno donde los activos digitales constituyen el núcleo del valor organizacional, la correcta gestión de credenciales es un elemento crítico del control interno y de la estrategia de seguridad.

Preguntas de autoevaluación

1. Explique la diferencia técnica entre password y passphrase desde el concepto de entropía.
2. ¿Por qué la longitud es más relevante que la complejidad sintáctica en la seguridad de autenticación?
3. ¿Cómo se integra la política de contraseñas dentro de un Sistema de Gestión de Seguridad de la Información?
4. Analice el impacto organizacional de una política inadecuada de passwords en términos de gestión de riesgos.
5. Explique la relación entre passphrases y autenticación multifactor en entornos corporativos.

Material de Clases

Compilado por **Aníbal M. Mazza Fraquelli** Doctor de la Universidad de Buenos Aires para el uso de sus clases en la Facultad de Ciencias Económicas de la Universidad de Buenos Aires.

Contenidos de esta página

Los contenidos **aquí incluidos integran desarrollos y escritos propios del autor, así como materiales de terceros (documentos, textos, fragmentos, conceptos, imágenes, esquemas, definiciones u otros recursos),** los cuales son utilizados a título ilustrativo, explicativo o formativo, respetando la normativa vigente en materia de derechos de autor y citando las fuentes cuando corresponde.
La selección, organización, adaptación pedagógica y contextualización de los contenidos constituye un trabajo original del autor, orientado a facilitar los procesos de enseñanza y aprendizaje.
Este material no persigue fines comerciales y su reproducción, total o parcial, queda limitada al ámbito educativo, debiendo preservarse siempre la mención de la autoría y las fuentes originales.

Autorización de uso

Se permite la reproducción, comunicación pública, distribución y utilización total o parcial de los contenidos de su material, en formato físico o digital, con fines exclusivamente educativos, académicos o de divulgación, siempre que se respete la integridad del contenido y se incluya la correspondiente referencia a la fuente y a la autoría.
Las ideas, opiniones e interpretaciones contenidas en este material corresponden exclusivamente al autor.
Queda expresamente excluido cualquier uso con fines comerciales.