Capítulo extraído del libro "**Análisis funcional de sistemas y tecnologías de la información**" de Aníbal Mario Mazza Fraquelli (2025) **ISBN 978-987-26981-3-3**.

Desde las Contraseñas hacia las Frases de Contraseña

Presentación del tema

En el contexto de las Tecnologías de la Información (IT), 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 contraseñas (passwords) y las frases de contraseña (passphrases) representan los métodos más difundidos.

Una password es una cadena de caracteres, generalmente corta, utilizada para autenticar a un usuario. Una passphrase es una secuencia más extensa, usualmente compuesta por varias palabras, diseñada para incrementar la entropía —medida de aleatoriedad o imprevisibilidad— y, por tanto, la seguridad. Desde la perspectiva organizacional y de gestión de sistemas de información, la elección entre ambos mecanismos y el diseño de políticas de autenticación son decisiones de gobernanza de TI que impactan en la confidencialidad, integridad y disponibilidad de la información.

La password: características y limitaciones

Una password típica está compuesta por letras mayúsculas y minúsculas, números y caracteres especiales. Las contraseñas no deben almacenarse en texto plano, sino mediante funciones criptográficas de hash —como SHA-256 o algoritmos específicos bcrypt, scrypt o Argon2— que transforman la contraseña en un resumen irreversible.

El problema principal de las contraseñas tradicionales es que, aunque incluyan complejidad sintáctica, suelen ser cortas —entre ocho y doce caracteres—, lo que reduce su espacio de búsqueda frente a ataques de fuerza bruta o por diccionario. Además, los usuarios tienden a elegir contraseñas predecibles, reutilizarlas en múltiples servicios y escribirlas en lugares físicos para recordarlas, lo que reduce significativamente la seguridad práctica.

La passphrase: características y ventajas

Una passphrase es una frase compuesta por varias palabras, como "CaballoAladoLlamadoPegaso2026" o "mi gato juega con sus juguetes". La seguridad de una passphrase no depende tanto de la complejidad de caracteres especiales como de su longitud y de la entropía generada por la combinación de palabras.

La entropía aumenta exponencialmente con la longitud. Una passphrase de veinticinco caracteres puede ser significativamente más resistente que una password de diez caracteres con símbolos especiales, especialmente frente a ataques de fuerza bruta. Además, resulta más fácil de recordar para el usuario, lo que reduce la tendencia a escribirla en papel o reutilizarla entre servicios.

Comparación estratégica

Aspecto	Password	Passphrase
Longitud	Corta	Larga
Entropía	Limitada por longitud	Alta por extensión
Usabilidad	Difícil de recordar si es compleja	Más fácil de memorizar
Resistencia a fuerza bruta	Menor	Mayor
Resistencia a diccionario	Media	Alta si las palabras son aleatorias

Políticas de gestión de credenciales

Desde la gobernanza de TI, el diseño de políticas de autenticación debe contemplar la longitud mínima —con preferencia por passphrases sobre passwords complejas cortas—, la prohibición de reutilización entre servicios, la rotación periódica solo cuando existe evidencia de compromiso (la rotación forzada frecuente tiende a generar contraseñas más

débiles), el uso de gestores de contraseñas corporativos para reducir la carga cognitiva del usuario, y la implementación de MFA como complemento indispensable.

La autenticación multifactor (MFA) reduce el riesgo incluso si las credenciales son comprometidas: un atacante que obtiene una passphrase válida no puede acceder sin el segundo factor. Esta combinación —passphrase robusta más MFA— constituye el estándar de seguridad recomendado en entornos corporativos.

Conceptos clave

- Password: cadena corta de caracteres con mayor vulnerabilidad ante ataques.
- Passphrase: secuencia de palabras con mayor entropía y mejor usabilidad.
- Entropía como medida de la resistencia de una credencial.
- Hash criptográfico para el almacenamiento seguro de contraseñas.
- MFA como complemento indispensable de cualquier política de credenciales.
- La usabilidad como factor de seguridad real en el comportamiento del usuario.

Preguntas de repaso del tema

1. ¿Cuál es la diferencia conceptual entre password y passphrase?
2. ¿Por qué la longitud es más determinante que la complejidad en la seguridad de una credencial?
3. ¿Qué es la entropía y por qué es relevante en el diseño de credenciales?
4. ¿Por qué las contraseñas no deben almacenarse en texto plano?
5. ¿Qué ventajas ofrece la passphrase desde la perspectiva de la usabilidad?
6. ¿Por qué la rotación forzada frecuente puede generar credenciales más débiles?
7. ¿Qué función cumple el MFA en una política de autenticación robusta?

8. ¿Por qué los gestores de contraseñas corporativos son recomendables?
9. ¿Cómo impacta el comportamiento del usuario en la seguridad práctica de las credenciales?
10. ¿Cómo debe diseñarse una política de autenticación desde la gobernanza de TI?