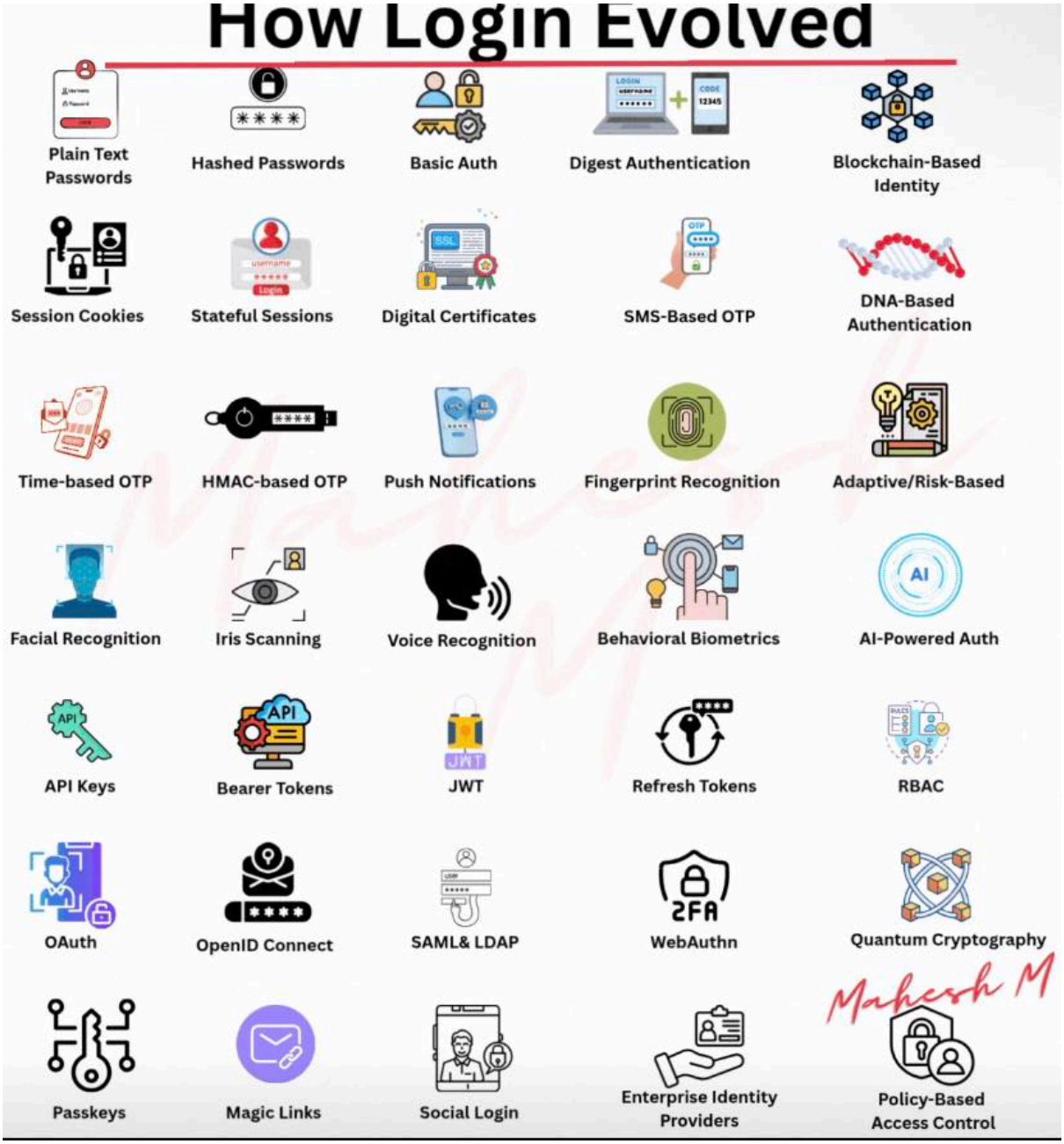
Universidad de Buenos Aires
Facultad de Ciencias Económicas

La Evolución del Log In

Material de Estudio



Traducción y Comentarios

Evolución de los mecanismos de inicio de sesión (Login)

A continuación se presenta la traducción y reorganización de los mecanismos de autenticación que aparecen en la imagen, ordenados de manera didáctica y progresiva para estudiantes de Licenciatura en Administración, con foco en los elementos que deben considerar desde la gestión de Tecnologías de la Información.

---

1. Métodos Básicos de Autenticación (Primera Generación)

Estos mecanismos representan los primeros modelos de identificación digital. Son simples, pero presentan debilidades significativas si no se complementan con controles adicionales.

- **Contraseñas en texto plano (Plain Text Passwords)**

  Las contraseñas se almacenan sin cifrado. Son altamente inseguras.

- **Contraseñas con hash (Hashed Passwords)**

  La contraseña se transforma mediante una función hash criptográfica antes de almacenarse. Mejora la seguridad.

- **Autenticación Básica (Basic Authentication – Basic Auth)**

  Método simple que envía usuario y contraseña codificados, generalmente en encabezados HTTP.

- **Autenticación Digest (Digest Authentication)**

  Mejora de Basic Auth que utiliza hash para evitar enviar la contraseña directamente.

---

2. Gestión de Sesiones

Estos mecanismos permiten mantener al usuario autenticado durante una interacción continua con el sistema.

- **Cookies de sesión (Session Cookies)**

  Archivos pequeños almacenados en el navegador para mantener la sesión activa.

- **Sesiones con estado (Stateful Sessions)**

El servidor almacena información de la sesión del usuario.

- **Tokens de actualización (Refresh Tokens)**

  Permiten renovar sesiones sin solicitar credenciales nuevamente.

---

3. Autenticación Basada en Tokens y API

Muy utilizada en arquitecturas modernas y sistemas distribuidos.

- **Claves API (API Keys – Application Programming Interface Keys / Claves de Interfaz de Programación de Aplicaciones)**

  Identificadores utilizados para permitir acceso a servicios.

- **Tokens Bearer (Bearer Tokens)**

  Tokens que otorgan acceso a recursos si son presentados correctamente.

- **JWT (JSON Web Token – Token Web en formato JSON)**

  Token firmado digitalmente que contiene información verificable del usuario.

---

4. Autenticación Multifactor (MFA – Multi-Factor Authentication / Autenticación Multifactor)

Agrega capas adicionales de seguridad.

- **OTP basado en SMS (SMS-Based One-Time Password – Contraseña de un solo uso enviada por SMS)**
- **OTP basado en tiempo (Time-Based OTP – TOTP / Time-Based One-Time Password)**
- **OTP basado en HMAC (HMAC-Based One-Time Password – HMAC: Hash-based Message Authentication Code / Código de Autenticación basado en Hash)**
- **Notificaciones Push (Push Notifications)**
- **2FA (Two-Factor Authentication – Autenticación de Dos Factores)**

Desde la administración, estos mecanismos reducen riesgos de fraude y accesos indebidos.

5. Autenticación Biométrica

Utiliza características físicas o conductuales.

- **Reconocimiento de huella digital (Fingerprint Recognition)**
- **Reconocimiento facial (Facial Recognition)**
- **Escaneo de iris (Iris Scanning)**
- **Reconocimiento de voz (Voice Recognition)**
- **Biometría conductual (Behavioral Biometrics)**

  Analiza patrones de comportamiento como velocidad de tipeo.
- **Autenticación basada en ADN (DNA-Based Authentication)**

  Tecnología experimental.

---

6. Autenticación Basada en Certificados y Criptografía

- **Certificados digitales (Digital Certificates)**

  Utilizan infraestructura de clave pública (PKI – Public Key Infrastructure / Infraestructura de Clave Pública).
- **WebAuthn (Web Authentication – Autenticación Web)**

  Estándar moderno sin contraseña.
- **Passkeys (Claves de acceso sin contraseña)**

  Basadas en criptografía de clave pública.
- **Criptografía cuántica (Quantum Cryptography)**

  Modelo emergente basado en principios de mecánica cuántica.

---

7. Sistemas de Identidad Federada

Permiten autenticarse a través de terceros.

- **OAuth (Open Authorization – Autorización Abierta)**

Protocolo que permite acceso delegado.

- **OpenID Connect**

  Capa de identidad construida sobre OAuth.

- **SAML (Security Assertion Markup Language – Lenguaje de Marcado para Aserciones de Seguridad)**
- **LDAP (Lightweight Directory Access Protocol – Protocolo Ligero de Acceso a Directorios)**
- **Proveedores de Identidad Empresarial (Enterprise Identity Providers)**
- **Inicio de sesión social (Social Login)**
- **Magic Links (Enlaces mágicos de autenticación por correo)**

---

8. Modelos Avanzados y Adaptativos

- **Autenticación basada en riesgo (Adaptive/Risk-Based Authentication)**

  Ajusta el nivel de verificación según el riesgo detectado.

- **Autenticación impulsada por IA (AI-Powered Authentication – Artificial Intelligence / Inteligencia Artificial)**

  Utiliza aprendizaje automático para detectar anomalías.

- **Identidad basada en Blockchain (Blockchain-Based Identity)**

  Gestión descentralizada de identidad digital.

- **RBAC (Role-Based Access Control – Control de Acceso Basado en Roles)**

  Asigna permisos según funciones organizacionales.

- **Control de acceso basado en políticas (Policy-Based Access Control)**

  Define reglas dinámicas según contexto.

Enfoque para estudiantes de Administración

Desde la gestión de Tecnologías de la Información, los estudiantes deben comprender que:

1. No todos los mecanismos ofrecen el mismo nivel de seguridad.

2. La autenticación impacta en riesgo operacional, cumplimiento normativo y protección de datos.
3. La elección del modelo depende del nivel de criticidad del sistema.
4. En entornos empresariales, la combinación de métodos es la práctica recomendada.
5. La gestión de identidad es un componente clave de la gobernanza digital.

En sistemas financieros, logísticos o de recursos humanos, una autenticación débil puede generar:

- Fraude interno.
- Pérdida de información sensible.
- Incumplimientos regulatorios.
- Daño reputacional.

La evolución del login refleja la creciente complejidad de los riesgos digitales y la necesidad de integrar seguridad, gobernanza y estrategia tecnológica dentro de la administración moderna.

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.