Universidad de Buenos Aires
Facultad de Ciencias Económicas

# Autenticación y Autorización

## 🛠 Material de Estudio


## 1. Autenticación

**Pregunta clave:** *¿Quién eres?*

La **autenticación** es el proceso mediante el cual un sistema **verifica la identidad** de un usuario, aplicación o dispositivo antes de permitir el acceso. Su objetivo es confirmar que quien intenta ingresar es realmente quien dice ser.

### Mecanismos habituales de autenticación

- **Algo que sabes**: usuario y contraseña, PIN.
- **Algo que tienes**: token, tarjeta inteligente, teléfono móvil.
- **Algo que eres**: huella digital, reconocimiento facial, biometría.
- **Autenticación multifactor (MFA – Multi-Factor Authentication)**: combinación de dos o más factores para mayor seguridad.

### Qué valida la autenticación

- Identidad del usuario.
- Legitimidad del acceso inicial al sistema.
- Existencia de credenciales válidas.

### En términos simples

> La autenticación abre la puerta al sistema, pero no define qué se puede hacer dentro.

---

## 2. Autorización

**Pregunta clave:** *¿Qué puedes hacer?*

La **autorización** determina **qué acciones están permitidas** una vez que el usuario ya fue autenticado. Se basa en reglas, permisos, perfiles y roles definidos previamente por la organización.

### Elementos típicos de autorización

- **Permisos**: leer, crear, modificar, eliminar información.
- **Roles**: administrador, gerente, analista, operador, auditor.
- **Restricciones**: acceso por área, horario, ubicación, tipo de dispositivo.

- **Principio de mínimo privilegio**: cada usuario accede solo a lo estrictamente necesario.

### Qué controla la autorización

- Acceso a datos sensibles.
- Operaciones críticas del negocio.
- Separación de funciones (segregación de tareas).

### En términos simples

> La autorización define hasta dónde puedes avanzar dentro del sistema.

---

## 3. Diferencia clave entre autenticación y autorización

| Aspecto | Autenticación | Autorización |
|---|---|---|
| Pregunta central | ¿Quién eres? | ¿Qué puedes hacer? |
| Momento | Antes de entrar al sistema | Después de ingresar |
| Foco | Identidad | Permisos y privilegios |
| Riesgo si falla | Acceso no autorizado | Uso indebido de la información |

Ambos procesos son **complementarios** y necesarios. Autenticar sin autorizar correctamente expone datos; autorizar sin autenticar es directamente inviable.

---

## 4. Qué debe considerar la administración de empresas

Desde la perspectiva de la **administración y gestión organizacional**, estos conceptos no son solo técnicos, sino **estratégicos**.

### a) Gobierno y control interno

- Definir políticas claras de acceso a los sistemas.
- Alinear roles del sistema con la estructura organizacional.

- Asegurar la segregación de funciones (por ejemplo: quien carga datos no debe aprobarlos).

### b) Gestión del riesgo

- Reducir fraudes internos y externos.
- Proteger información financiera, contable y de clientes.
- Minimizar impactos por errores humanos o accesos indebidos.

### c) Cumplimiento normativo y auditoría

- Facilitar auditorías internas y externas.
- Registrar quién accede, cuándo y qué acciones realiza.
- Cumplir con regulaciones de protección de datos y control corporativo.

### d) Eficiencia operativa

- Evitar accesos innecesarios que generan confusión o errores.
- Automatizar la asignación de roles según el puesto.
- Simplificar altas, bajas y modificaciones de usuarios.

### e) Continuidad del negocio

- Controlar accesos en situaciones críticas.
- Revocar permisos rápidamente ante desvinculaciones.
- Garantizar que los sistemas sigan siendo confiables.

---

## 5. En síntesis para estudiantes de administración

- **Autenticación** asegura *quién accede*.
- **Autorización** controla *qué puede hacer*.
- Ambas son pilares del **control interno**, la **seguridad de la información** y la **buena gestión empresarial**.
- No son decisiones puramente técnicas: **impactan directamente en la gobernanza, el riesgo y la toma de decisiones**.

Entender estos conceptos permite a los futuros administradores **dialogar correctamente con el área de sistemas**, tomar mejores decisiones y evaluar los riesgos tecnológicos dentro de la organización.

## 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.**