Universidad de Buenos Aires
Facultad de Ciencias Económicas

Controles de Acceso

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

Presentación del Tema

Los **controles de acceso a los componentes de un Sistema de Información (SI – *Information Systems*)** constituyen uno de los pilares fundamentales de la seguridad en entornos digitales organizacionales. Su finalidad es garantizar que únicamente las personas, procesos o sistemas debidamente autorizados puedan acceder a recursos tecnológicos específicos, en el nivel y momento adecuados.

Un sistema de información está compuesto por múltiples elementos interrelacionados: hardware, software, bases de datos, redes, aplicaciones, dispositivos móviles, infraestructuras en la nube y servicios externos. Cada uno de estos componentes representa un activo que debe ser protegido frente a accesos no autorizados, modificaciones indebidas o usos inapropiados.

Desde el punto de vista conceptual, los controles de acceso se articulan en torno a los principios de:

- **Confidencialidad (Confidentiality)**
- **Integridad (Integrity)**
- **Disponibilidad (Availability)**

conocidos como el modelo **CIA (Confidentiality, Integrity, Availability / Confidencialidad, Integridad y Disponibilidad)**.

Para estudiantes de licenciatura en administración, comprender los controles de acceso implica analizar cómo la organización define políticas, asigna privilegios, supervisa el uso de recursos y gestiona riesgos tecnológicos, asegurando que la arquitectura de seguridad se encuentre alineada con la estrategia corporativa.

Desarrollo

1. Concepto General de Control de Acceso

El **control de acceso (Access Control)** es el conjunto de mecanismos técnicos y administrativos que regulan quién puede acceder a qué recursos, bajo qué condiciones y con qué nivel de privilegio.

En términos estructurales, el control de acceso se compone de cuatro procesos fundamentales:

1. Identificación (Identification)
2. Autenticación (Authentication)
3. Autorización (Authorization)
4. Auditoría (Accounting / Logging)

Este modelo suele denominarse **AAA (Authentication, Authorization, Accounting / Autenticación, Autorización y Registro)**.

---

2. Identificación y Autenticación

2.1 Identificación

La identificación consiste en declarar la identidad del usuario (por ejemplo, mediante un nombre de usuario).

2.2 Autenticación

La autenticación verifica que la identidad declarada sea legítima. Puede basarse en:

🏛️

- Algo que el usuario sabe (contraseña).
- Algo que el usuario tiene (token físico).
- Algo que el usuario es (biometría).

La **Autenticación Multifactor (MFA – Multi-Factor Authentication / Autenticación Multifactor)** combina al menos dos factores, reduciendo significativamente la probabilidad de acceso no autorizado.

Ejemplo:

En una plataforma ERP (Enterprise Resource Planning / Planificación de Recursos Empresariales), el acceso financiero puede requerir contraseña más código temporal generado por aplicación móvil.

---

3. Autorización y Gestión de Privilegios

Una vez autenticado, el sistema determina qué acciones puede realizar el usuario. Este proceso se denomina autorización.

3.1 Modelo Discrecional (DAC – Discretionary Access Control / Control de Acceso Discrecional)

El propietario del recurso define quién accede.

3.2 Modelo Obligatorio (MAC – Mandatory Access Control / Control de Acceso Obligatorio)

Los permisos son definidos por políticas centrales de seguridad.

3.3 Modelo Basado en Roles (RBAC – Role-Based Access Control / Control de Acceso Basado en Roles)

Los permisos se asignan según el rol organizacional.

El RBAC es ampliamente utilizado en organizaciones modernas debido a su eficiencia administrativa y escalabilidad.

Ejemplo:

- Rol “Contador”: acceso a módulo financiero.
- Rol “Gerente Comercial”: acceso a reportes de ventas.
- Rol “Administrador TI”: acceso a configuraciones técnicas.

---

4. Principio de Mínimo Privilegio

El **Principio de Mínimo Privilegio (Least Privilege Principle)** establece que cada usuario debe poseer únicamente los permisos estrictamente necesarios para desempeñar su función.

Este principio reduce:

- Riesgo de abuso interno.
- Impacto de errores humanos.
- Superficie de ataque ante compromisos de credenciales.

Desde la perspectiva administrativa, su implementación requiere revisión periódica de accesos y eliminación de privilegios obsoletos.

---

5. Control de Acceso Físico vs. Lógico

Los componentes de un sistema de información pueden requerir controles físicos y lógicos.

5.1 Acceso Físico

Incluye:

- Tarjetas de proximidad.
- Cerraduras electrónicas.
- Biometría.
- Control perimetral.

5.2 Acceso Lógico

Incluye:

- Usuarios y contraseñas.

- Firewalls.
- Listas de control de acceso (ACL – Access Control Lists / Listas de Control de Acceso).
- Segmentación de red.

Ambos niveles deben integrarse para lograr seguridad integral.

---

6. Control de Acceso en Redes

En infraestructura de red, el control de acceso se implementa mediante:

- Firewalls.
- Sistemas NAC (Network Access Control / Control de Acceso a la Red).
- VLAN (Virtual Local Area Network / Red de Área Local Virtual).
- Sistemas de autenticación centralizada como LDAP (Lightweight Directory Access Protocol / Protocolo Ligero de Acceso a Directorios).

El objetivo es impedir que dispositivos no autorizados se conecten a la red corporativa.

---

7. Control de Acceso en Entornos en la Nube

En servicios de **Cloud Computing (Computación en la Nube)**, el control de acceso adquiere mayor complejidad debido a la distribución geográfica y virtualización.

Se utilizan herramientas como:

- IAM (Identity and Access Management / Gestión de Identidad y Acceso).
- Políticas basadas en atributos (ABAC – Attribute-Based Access Control / Control Basado en Atributos).

El error en configuraciones de acceso en la nube constituye una de las principales causas de brechas de seguridad.

---

8. Auditoría y Registro de Accesos

El control de acceso no se limita a permitir o denegar ingreso; requiere monitoreo constante.

Se implementan:

- Logs de actividad.
- SIEM (Security Information and Event Management / Gestión de Eventos de Seguridad).
- Alertas de acceso sospechoso.

La auditoría permite detectar accesos indebidos y constituye evidencia ante investigaciones internas o regulatorias.

---

9. Gestión del Ciclo de Vida del Acceso

El acceso debe gestionarse a lo largo de todo el ciclo laboral del empleado:

1. Alta: asignación inicial de permisos.
2. Modificación: actualización según cambios de rol.
3. Baja: revocación inmediata de accesos.

La permanencia de cuentas activas de ex empleados representa una vulnerabilidad crítica.

---

10. Riesgos Asociados a Controles Deficientes

La ausencia o debilidad en controles de acceso puede generar:

- Robo de información.
- Fraude interno.
- Acceso no autorizado a datos personales.
- Incumplimiento normativo.
- Interrupción operativa.

Desde el punto de vista financiero, una brecha de seguridad puede generar costos legales, sanciones regulatorias y pérdida de confianza del mercado.

---

11. Integración con Gestión de Riesgos

El diseño de controles de acceso debe basarse en análisis de riesgo:

Riesgo = Amenaza × Vulnerabilidad × Impacto

Si el impacto de una brecha en el módulo financiero es alto, los controles deben ser más estrictos.

La inversión en controles debe justificarse mediante análisis costo-beneficio y retorno sobre la inversión en seguridad (ROSI – Return on Security Investment / Retorno sobre la Inversión en Seguridad).

---

12. Ejemplo Aplicado

Supongamos una empresa donde:

- Todos los empleados tienen acceso completo al sistema contable.
- No existen restricciones por rol.
- No se auditan accesos.

Amenaza: fraude interno.

Vulnerabilidad: ausencia de segregación.

Impacto: pérdidas financieras significativas.

Implementando RBAC, MFA y auditoría periódica, el riesgo se reduce sustancialmente.

---

13. Dimensión Estratégica para la Administración

Desde la perspectiva administrativa, los controles de acceso son instrumentos de gobernanza tecnológica. Permiten:

- Proteger activos críticos.
- Cumplir regulaciones.
- Preservar reputación corporativa.
- Garantizar continuidad del negocio.

El administrador debe comprender que el control de acceso no es un obstáculo operativo, sino un mecanismo de preservación del valor organizacional.

Conclusión

Los controles de acceso a los componentes de un sistema de información constituyen una pieza central de la arquitectura de seguridad organizacional. A través de procesos estructurados de identificación, autenticación, autorización y auditoría, la organización regula la interacción entre personas y recursos tecnológicos.

La implementación adecuada de modelos como RBAC, MFA y el principio de mínimo privilegio reduce vulnerabilidades, limita impactos potenciales y fortalece la resiliencia institucional. Desde la perspectiva de la administración, el control de acceso debe integrarse en la estrategia de gestión de riesgos y gobierno corporativo, asegurando que la tecnología opere como habilitador del negocio y no como fuente de exposición innecesaria.

La correcta gestión del acceso es, en definitiva, una condición estructural para la sostenibilidad y competitividad en entornos digitales contemporáneos.

Preguntas de autoevaluación

1. ¿Cuáles son las diferencias entre identificación, autenticación y autorización?
2. ¿Qué ventajas ofrece el modelo RBAC frente a otros modelos de control de acceso?
3. ¿Por qué el principio de mínimo privilegio reduce la exposición al riesgo?
4. ¿Qué riesgos emergen cuando no se auditan los accesos a sistemas críticos?
5. ¿Cómo se integran los controles de acceso en la gestión estratégica del riesgo tecnológico?

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.