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**.

Los Controles de Acceso a los Componentes de los Sistemas de Información

Presentación del tema

Los controles de acceso a los componentes de un sistema de información 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 representa un activo que debe protegerse frente a accesos no autorizados, modificaciones indebidas o usos inapropiados. Los controles de acceso se articulan en torno a los principios de confidencialidad, integridad y disponibilidad —modelo CIA— y constituyen una herramienta de gobernanza que define políticas, asigna privilegios y gestiona riesgos tecnológicos.

El modelo AAA: autenticación, autorización y auditoría

El control de acceso se compone de cuatro procesos fundamentales que forman el modelo AAA: identificación (el usuario declara quién es), autenticación (se verifica que la identidad declarada sea legítima), autorización (se determina qué acciones puede realizar el usuario autenticado) y auditoría (se registran todas las acciones para trazabilidad).

La autenticación puede basarse en algo que el usuario sabe (contraseña), algo que tiene (token físico) o algo que es (biometría). La Autenticación Multifactor (MFA) combina al menos dos factores, reduciendo significativamente la probabilidad de acceso no autorizado.

Modelos de autorización y principio de mínimo privilegio

Una vez autenticado el usuario, el sistema determina sus permisos mediante distintos modelos de autorización. El modelo discrecional (DAC) otorga al propietario del recurso la facultad de definir quién accede. El modelo obligatorio (MAC) define los permisos mediante políticas centrales de seguridad. El modelo basado en roles (RBAC) asigna permisos según el rol organizacional: el rol "Contador" accede al módulo financiero; el rol "Gerente Comercial", a reportes de ventas. RBAC es ampliamente utilizado por su eficiencia administrativa y escalabilidad.

El principio de mínimo privilegio (Least Privilege) establece que cada usuario debe poseer únicamente los permisos estrictamente necesarios para desempeñar su función. Su implementación requiere revisión periódica de accesos y eliminación de privilegios obsoletos.

Control de acceso físico, lógico y en la nube

Los sistemas de información requieren controles tanto físicos —tarjetas de proximidad, biometría, control perimetral— como lógicos —usuarios y contraseñas, firewalls, listas de control de acceso (ACL), segmentación de red—. Ambos niveles deben integrarse para lograr seguridad integral.

En redes, el control de acceso se implementa mediante firewalls, sistemas NAC (Network Access Control), VLAN y autenticación centralizada LDAP. En entornos de nube, las herramientas IAM y el modelo ABAC permiten controlar accesos en contextos distribuidos y dinámicos.

Gestión del ciclo de vida del acceso e impacto organizacional

El acceso debe gestionarse durante todo el ciclo laboral del empleado: alta con asignación inicial de permisos, modificación ante cambios de rol y baja con revocación inmediata de accesos. La permanencia de cuentas activas de ex empleados representa una vulnerabilidad crítica frecuentemente subestimada.

La ausencia o debilidad en controles de acceso puede generar robo de información, fraude interno, incumplimiento normativo e interrupción operativa, con consecuencias financieras, legales y reputacionales significativas. El control de acceso es, en definitiva, una condición estructural para la sostenibilidad en entornos digitales contemporáneos.

Conceptos clave

- Modelo AAA: identificación, autenticación, autorización y auditoría.
- Tres modelos de autorización: DAC, MAC y RBAC.
- Mínimo privilegio para reducir superficie de ataque y abuso interno.
- MFA como mecanismo de reducción del riesgo de acceso no autorizado.
- Gestión del ciclo de vida del acceso: alta, modificación y baja.
- Integración de controles físicos y lógicos para seguridad integral.

Preguntas de repaso del tema

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?
6. ¿Por qué la permanencia de cuentas de ex empleados es una vulnerabilidad crítica?
7. ¿Qué diferencia existe entre el modelo DAC y el modelo MAC?

8. ¿Cómo impacta la autenticación multifactor en la reducción del riesgo de acceso no autorizado?
9. ¿Por qué el control de acceso en la nube requiere herramientas específicas como IAM y ABAC?
10. ¿Cómo contribuye el control de acceso a la gobernanza de TI?