Universidad de Buenos Aires
Facultad de Ciencias Económicas

Controles Administrativos de los Sistemas de Información

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 administrativos de los Sistemas de Información (SI – *Information Systems*)** constituyen el conjunto de políticas, normas, procedimientos, estructuras organizativas y mecanismos de supervisión que orientan y regulan el uso, protección y gestión de los recursos tecnológicos en una organización. A diferencia de los controles técnicos (firewalls, cifrado, sistemas de detección de intrusiones) o físicos (cerraduras, biometría, control perimetral), los controles administrativos operan en el plano normativo y de gobernanza, estableciendo el marco que define cómo deben diseñarse, implementarse y supervisarse los demás controles.

Desde la perspectiva de las Tecnologías de la Información (TI), los controles administrativos representan el nivel estratégico de la seguridad y del gobierno de TI. Sin un marco normativo claro, incluso las mejores soluciones tecnológicas pueden resultar ineficaces, inconsistentes o mal aplicadas. Estos controles determinan responsabilidades, delimitan funciones, establecen procesos de aprobación y definen criterios de evaluación del riesgo.

Para estudiantes de licenciatura en administración, el estudio de los controles administrativos es fundamental porque conecta la dimensión tecnológica con la

estructura organizacional, la cultura corporativa, el cumplimiento normativo y la gestión del riesgo. La seguridad de la información no se sostiene únicamente con herramientas técnicas, sino con decisiones estratégicas, liderazgo y procesos formales.

Desarrollo

1. Concepto y Alcance de los Controles Administrativos

Los controles administrativos pueden definirse como el conjunto de disposiciones formales que regulan el comportamiento organizacional en relación con el uso y protección de los sistemas de información. Incluyen:

- Políticas de seguridad.
- Normas internas.
- Procedimientos operativos.
- Manuales de usuario.
- Planes de contingencia.
- Esquemas de segregación de funciones.
- Programas de capacitación.
- Auditorías y revisiones periódicas.

Su objetivo principal es reducir la probabilidad de incidentes derivados de errores humanos, negligencia, ambigüedad organizacional o ausencia de responsabilidad definida.

En términos de gestión de riesgos, los controles administrativos disminuyen la vulnerabilidad organizacional al establecer reglas claras y mecanismos de supervisión.

---

2. Políticas de Seguridad de la Información

La política de seguridad constituye el documento rector que establece:

- Objetivos de protección.
- Alcance de aplicación.

- Responsabilidades.
- Consecuencias por incumplimiento.

Debe alinearse con estándares como:

- ISO/IEC 27001 (Sistema de Gestión de Seguridad de la Información).
- COBIT (*Control Objectives for Information and Related Technologies* / Objetivos de Control para Información y Tecnologías Relacionadas).
- NIST (National Institute of Standards and Technology / Instituto Nacional de Estándares y Tecnología).

Una política eficaz no es meramente declarativa; debe ser comprensible, aplicable y auditada periódicamente.

---

3. Gestión de Riesgos Tecnológicos

Uno de los pilares de los controles administrativos es la **gestión del riesgo (Risk Management / Gestión del Riesgo)**.

El proceso incluye:

1. Identificación de activos.
2. Identificación de amenazas.
3. Identificación de vulnerabilidades.
4. Evaluación de impacto.
5. Definición de tratamiento.

La ecuación del riesgo (Amenaza × Vulnerabilidad × Impacto) guía la priorización de controles.

Desde la administración, este proceso permite asignar recursos de manera racional y proporcional al nivel de exposición.

---

4. Segregación de Funciones

La **Segregación de Funciones (SoD – *Segregation of Duties* / Separación de Funciones)** es un control administrativo que impide que una misma persona controle todas las etapas de un proceso crítico.

Ejemplo en TI:

- Un administrador configura sistemas.
- Otro audita configuraciones.
- Un tercero aprueba cambios.

Este mecanismo reduce la probabilidad de fraude interno o abuso de privilegios.

---

5. Gestión del Ciclo de Vida del Acceso

Los controles administrativos establecen procedimientos para:

- Alta de usuarios.
- Modificación de roles.
- Baja y revocación de accesos.

La ausencia de procedimientos formales puede generar cuentas activas innecesarias, aumentando la superficie de ataque.

---

6. Planes de Continuidad y Recuperación

Los controles administrativos incluyen:

- BCP (Business Continuity Plan / Plan de Continuidad del Negocio).
- DRP (Disaster Recovery Plan / Plan de Recuperación ante Desastres).

Estos planes establecen protocolos ante eventos críticos como fallas técnicas, desastres naturales o ciberataques.

Su eficacia depende de:

- Pruebas periódicas.
- Actualización constante.
- Asignación clara de responsabilidades.

---

7. Gestión de Cambios

El **Change Management (Gestión de Cambios)** es un control administrativo que regula modificaciones en sistemas, aplicaciones o infraestructura.

Un procedimiento formal debe contemplar:

- Solicitud documentada.
- Evaluación de impacto.
- Aprobación formal.
- Implementación controlada.
- Validación posterior.

La ausencia de este control puede generar inestabilidad operativa.

---

8. Capacitación y Concientización

Los programas de **Security Awareness (Concientización en Seguridad)** son controles administrativos clave para reducir errores humanos.

Incluyen:

- Formación en detección de phishing.
- Buenas prácticas de contraseñas.
- Protocolos de reporte de incidentes.

La inversión en capacitación reduce vulnerabilidades asociadas al factor humano.

---

9. Auditorías y Monitoreo

Los controles administrativos requieren mecanismos de verificación:

- Auditorías internas.
- Auditorías externas.
- Revisiones periódicas de cumplimiento.
- Indicadores clave de desempeño (KPI – *Key Performance Indicators* / Indicadores Clave de Desempeño).

La auditoría no solo detecta incumplimientos, sino que fortalece la cultura de responsabilidad.

---

10. Gestión de Proveedores

Los terceros representan un riesgo relevante.

Los controles administrativos deben incluir:

- Evaluación de riesgos de proveedores.
- Acuerdos de nivel de servicio (SLA – *Service Level Agreement* / Acuerdos de Nivel de Servicio).
- Cláusulas de confidencialidad.
- Evaluaciones periódicas.

La externalización sin control adecuado puede comprometer datos sensibles.

---

11. Cumplimiento Normativo

Las organizaciones deben cumplir con marcos regulatorios que exigen controles administrativos formales.

El incumplimiento puede generar:

- Multas.
- Pérdida de licencias.
- Daño reputacional.

La formalización documental es indispensable para demostrar cumplimiento.

---

12. Integración con Controles Técnicos y Físicos

Los controles administrativos actúan como marco rector de:

- Controles técnicos (cifrado, firewalls).
- Controles físicos (acceso a centros de datos).

Sin políticas claras, la implementación técnica puede carecer de coherencia estratégica.

---

13. Ejemplo Aplicado

Una empresa implementa tecnología avanzada de seguridad, pero carece de políticas formales de acceso y revisión periódica.

Resultado:

- Permisos acumulados.
- Desactualización de cuentas.
- Confusión en responsabilidades.

La implementación de un manual formal de acceso y auditoría periódica reduce el riesgo significativamente.

---

14. Dimensión Estratégica

Desde la perspectiva de la administración, los controles administrativos:

- Definen la gobernanza de TI.
- Orientan inversiones en seguridad.
- Facilitan auditorías.
- Refuerzan la cultura organizacional.
- Reducen incertidumbre.

Son, en esencia, la arquitectura normativa que sostiene la seguridad tecnológica.

Conclusión

Los controles administrativos de los sistemas de información constituyen el marco estratégico que regula la protección y gestión de los activos digitales en una organización. A través de políticas formales, gestión de riesgos, segregación de funciones, planes de continuidad y auditorías, la organización establece límites claros y responsabilidades definidas que reducen vulnerabilidades y fortalecen la resiliencia institucional.

Desde la perspectiva administrativa, estos controles no son meramente formales o burocráticos, sino herramientas esenciales de gobernanza tecnológica. Sin ellos, los controles técnicos y físicos carecen de coherencia estructural. La

seguridad de la información se construye sobre liderazgo, normas claras y supervisión constante, elementos que configuran la base organizacional de toda arquitectura tecnológica sostenible.

Preguntas de autoevaluación

1. ¿Cuál es la diferencia entre controles administrativos, técnicos y físicos?
2. ¿Por qué la gestión de riesgos es un componente central de los controles administrativos?
3. ¿Cómo contribuye la segregación de funciones a la reducción del fraude interno?
4. ¿Qué rol cumplen los planes BCP y DRP dentro de la gobernanza de TI?
5. ¿Por qué los controles administrativos deben integrarse con controles técnicos y físicos?

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.